http://www.lanmag.ru ОКТЯБРЬ 2017

ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

App Store

Google play

Сетевые технологии

Что следует знать про SD-WAN?
Однопарный Ethernet: первые шаги
Какой стандарт Wi-Fi выбрать?

ISSN 1027086-8
17010
771027 086001

http://www.lanmag.ru
ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

ОКТЯБРЬ 2017

Читайте нас на Facebook

Читайте нас в Twitter

Программно определяемое все

С появлением концепции программируемых сетей (Software-Defined Network, SDN) термин «программно определяемый» быстро приобрел популярность: в последние годы его стали добавлять практически ко всему, что имеет хоть какое-то отношение к ИТ. Описывая свое видение будущего, IBM даже ввела понятие «программно определяемое все» (Software-Defined Everything, SDE). Однако, несмотря на всеобъемлющие притязания, оно используется в достаточно узком смысле — применительно к центрам обработки данных (Software-Defined Data Center, SDDC). Между тем идея абстрагирования сервисов от нижележащей инфраструктуры находит применение и за их пределами.

Собственно говоря, концепция SDN разрабатывалась в числе прочего и для территориально распределенных сетей. Не случайно фонд Open Network Foundation, целью создания которого было продвижение программируемой сетевой инфраструктуры, был образован крупнейшими операторами ЦОДов и телекоммуникационными компаниями: Deutsche Telecom, Facebook, Google, Microsoft, Verizon и Yahoo.

В последние год-два рынок решений Software-Defined WAN (SD-WAN) бурно развивается. Все больше компаний выдвигают соответствующие предложения; в частности, недавно свои решения представили Citrix и Riverbed (см. подробнее раздел «Канал новостей»). По оценке IDC, если два года назад, в 2015 году, объем этого рынка составлял всего 225 млн долларов, то в 2017-м он достигнет 1,19 млрд! Откуда такая популярность? Реализация SD-WAN позволяет упростить подключение офисов, сократить затраты на каналы, повысить надежность связи и т. д. Если вы не знакомы с этим подходом, самое время познакомиться: краткий ликбез в статье Александра Комарова «Что вы знаете про SD-WAN?».

Программно определяемые вычисления (также известные как серверная виртуализация) появились раньше, но именно благодаря виртуализации сетей стало возможно распространять эти принципы на многие другие области. (Вопрос прояснения терминологии — чем принципиально виртуализация отличается от программной определяемости — способен завести в дебри казуистики, в контексте же данного материала важно лишь их относительное положение на кривой цикла зрелости технологий Gartner: многие технологии из первой группы близки к плато продуктивности, тогда как многие из второй далеки от зрелости.)

Однако шумиха вокруг традиционных областей применения программно определяемого подхода, если верить Gartner, начинает спадать, на вершине оказываются новые темы, и одна из них — программно определяемая безопасность. Так, Cloud Security Alliance предложил модель защиты Software-Defined Perimeter (SDP). Сетевой периметр настолько размыт, что традиционные средства не способны его защитить. По сути, SDP предполагает динамическое создание индивидуального периметра для каждого пользователя, что позволяет, в частности, скрыть сетевые ресурсы от тех, кто не прошел авторизацию и идентификацию.

Сегодня на любую букву алфавита можно найти нечто программно определяемое, а на некоторые даже несколько: например, на «б» — от программно определяемых батарей до программно определяемого бизнеса. В таком мире для достижения большей продуктивности и люди должны стать программно определяемыми. И все развивается в этом направлении: микрочипы уже имплантируются в человеческое тело, заменяя пропуска и карты. LAN

Дмитрий Ганьжа

http://www.lanmag.ru
ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN 12+
№ 10, октябрь 2017

РУКОВОДИТЕЛЬ ПРОЕКТА
Чекалина Е. В. *lena@osp.ru*
ГЛАВНЫЙ РЕДАКТОР
Ганьжа Д. Х. *diga@lanmag.ru*
ВЕДУЩИЙ РЕДАКТОР
Барсков А.
ЛИТЕРАТУРНЫЙ РЕДАКТОР
Качинская Т.
КОМПЬЮТЕРНАЯ ВЕРСТКА
Рыжкова М.
МАРКЕТИНГ И КОММУНИКАЦИИ
Данильченкова Е.
ПРОИЗВОДСТВЕННЫЙ ОТДЕЛ
Блохина Г.

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ
ООО «Издательство «Открытые системы»
Адрес издателя и редакции:
Россия, 127254, г. Москва,
проезд Добролюбова, дом 3, строение 3, каб. 13

Адрес для корреспонденции:
123056, г. Москва, а/я 82, lan@lanmag.ru,
Тел.: +7 495 725-4780/83, +7 499 703-1854
Факс: +7 495 725-4783

В номере использованы иллюстрации
и фотографии издательства
«Открытые системы», 123rf.com.

Журнал зарегистрирован в Роскомнадзоре.
Свидетельство о регистрации СМИ
ПИ №ФС77-63550 от 30 октября 2015 г.

Отпечатано в ООО
«Богородский полиграфический комбинат»,
142400, Московская обл., г. Ногинск,
ул. Индустриальная, д. 40б

Журнал выходит 10 раз в год.
Общий тираж 13000 экз.
(включая 3000 экз. PDF-версии)

Цена свободная.

Дата выхода в свет:
24.10.2017 г.

ОТКРЫТЫЕ СИСТЕМЫ
Open Systems Publications

ПРЕЗИДЕНТ
Михаил Борисов
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
Галина Герасина
ДИРЕКТОР ИТ-НАПРАВЛЕНИЯ
Павел Христов
КОММЕРЧЕСКИЙ ДИРЕКТОР
Татьяна Филина

Wi-Fi «под зонтиком» SD-WAN

На прошедшей в Москве конференции Riverbed представила продукты Wi-Fi приобретенной недавно компании Xirrus, решения для мониторинга пользовательского опыта и новые подходы к построению WAN-сетей.


Фото: Riverbed

Александр Стулов, глава представительства Riverbed Technology в России и СНГ: «Переход к гибридным ИТ-средам стимулирует внедрение программно определяемых решений SD-WAN, в которых сетевое взаимодействие определяется требованиями со стороны приложений»

По прогнозу IDC, к 2020 году объем рынка решений SD-WAN вырастет до 6 млрд долларов. Для сравнения: эта цифра сопоставима с объемом рынка традиционных маршрутизаторов. Ставки высоки, поэтому многие сетевые вендоры сконцентрировались на продвижении именно решений SD-WAN, и Riverbed не исключение.

На состоявшейся 26 сентября конференции Александр Стулов, глава представительства Riverbed Technology в России и СНГ, выделил несколько тенденций, определяющих новые требования к организации территориально распределенных сетей (WAN). Одна из них — переход к гибридным ИТ-средам, когда необходимые для работы приложений ресурсы могут находиться на удаленных площадках, включая собственные ЦОДы заказчика, частные облака в коммерческих ЦОДах и публичные облака. При этом необходимо обеспечить оперативное подключение новых сетевых сервисов и новых узлов (филиалов), что крайне сложно сделать на основе традиционных технологий WAN. Поэтому все чаще заказчики обращаются к программно определяемым решениям SD-WAN, в которых сетевое взаимодействие подчиняется требованиям со стороны приложений.

По словам Сергея Козлова, руководителя группы системных инженеров Riverbed Technology в России и СНГ, у предлагаемого компанией SD-WAN-решения SteelConnect есть ряд уникальных особенностей. В частности, это наличие конвергентного устройства SteelHead SD, сочетающего функции шлюза SD-WAN и WAN-оптимизатора. Шлюзы SD-WAN имеют встроенную функциональность межсетевого экрана и защиты от угроз. Еще одна интересная особенность решения SteelConnect — возможность объединения в программно определяемой сети как WAN-, так и LAN-составляющих, к последним относятся коммутаторы локальной сети и точки доступа Wi-Fi.

Существенное усиление своего предложения в части построения локальных сетей Riverbed получила благодаря покупке компании Xirrus — разработчика решений Wi-Fi. Эта компания известна в первую очередь своими уникальными массивами, содержащими несколько точек доступа с секторными антеннами и встроенным контроллером. Такой массив может обслуживать тысячи пользователей и очень эффективен там, где необходимы решения высокой плотности. Продукты Xirrus, помимо отличной масштабируемости, отличаются еще гибким выбором моделей внедрения: так, система управления может быть размещена в частном или публичном облаке.

По мнению Сергея Козлова, продукты Xirrus отлично вписываются в общую концепцию решений Riverbed, чему способствует, в частности, реализация функций МСЭ и глубокого анализа пакетов (DPI) на каждой точке доступа. В планах компании — ввести эти продукты «под зонтик» общей системы управления SteelConnect.

Еще одним инновационным решением, представленным на конференции в Москве, стала система мониторинга опыта конечных пользователей (End User Experience, EUE) Riverbed Aternity. Как отмечают в Riverbed, в условиях, когда цифровизация бизнеса становится ключевым направлением его развития, управление цифровым опытом пользователей становится критически важной задачей. Системы управления инфраструктурой могут показывать, что все ее компоненты (LAN, WAN, ЦОД…) работают отлично, но при этом конечный пользователь будет испытывать проблемы. Оперативно выяснить их причину поможет система, собирающая комплексные данные, в том числе с агентов, установленных на устройствах самих пользователей.

Эта система сопоставляет три основные группы данных. Первая — о производительности приложений, включая облачные, SaaS, мобильные, VDI и др. Вторая — о производительности устройств (скорость ввода-вывода, работа процессора, неожиданные отключения и пр.). Наконец, третья группа — данные о поведении самого пользователя. Именно мониторинг поведения пользователя позволяет выявить ситуации, когда в плохой работе приложения виноват он сам, а не инфраструктура.

Александр Барсков

Сетевая видеокамера AXIS Q1659

Видеонаблюдение или фотография?

Вы когда-нибудь задумывались, что будет, если объединить профессиональную фотографию и видеонаблюдение? Теперь эта идея воплотилась в жизнь. Видеокамера AXIS Q1659 имеет сверхвысокое разрешение, живые цвета и высокую контрастность изображения в сочетании с прекрасной проработкой деталей на уровне цифровой зеркальной фотокамеры (DSLR). Для данной видеокамеры представлен богатый ассортимент объективов Canon EF. Следует отметить, что данная модель является топовой в линейке сетевых видеокамер Axis. Иными словами, эта видеокамера сочетает в себе лучшее от видеонаблюдения и фотографии, поэтому теперь не нужно выбирать что-то одно.

Подробнее на www.axis.com/products/axis-q1659

AXIS COMMUNICATIONS

Citrix обустраивает цифровое рабочее место

На прошедшей в Москве конференции Synergy Unplugged компания Citrix представила свои новые решения для организации рабочего места будущего.

К ключевым особенностям цифровых рабочих мест в Citrix относят объединенные функциональные возможности, систему защиты следующего поколения и контекстный анализ. Все это реализуется в обновленной среде Citrix Workspace, которая унифицирует управление различными приложениями (мобильными, SaaS, Web, Windows) и данными, а также консолидирует доступ, контроль и рабочие процессы. Однако за единым интерфейсом обновленного портала доступа StoreFront скрывается множество используемых технологий и решений. Среди многочисленных анонсов и обновлений продуктов Citrix Сергей Халяпин, главный инженер представительства Citrix в России и странах СНГ, выделил три: NetScaler Management and Analytics System (MAS), NetScaler Software-Defined WAN (SD-WAN), обновления XenApp и XenDesktop.

NetScaler MAS позволяет автоматизировать развертывание устройств NetScaler, их управление и мониторинг на одной или нескольких площадках, а также в облаке. Во втором квартале Citrix выпустила облачный вариант своего решения NetScaler MA Service. Этот сервис помогает контролировать всю инфраструктуру доставки приложений, управлять ею, выполнять диагностику, а также предоставляет различные аналитические модули для определения производительности и обеспечения безопасности.

Фото: Дмитрий Ганьжа

Ральф Шмидт, директор Citrix по подготовке продаж в СНГ и Восточной Европе: «Подход Citrix позволяет осуществить постепенный переход в облако с учетом имеющейся у компании инфраструктуры и актуальных бизнес-задач»

Так, в модуле Security Analytics используются алгоритмы машинного обучения, позволяющие выявлять аномальные действия пользователей. С помощью данных, получаемых от XenApp, Xen Mobile ShareFile и NetScaler, отслеживаются различные аспекты поведения пользователей: способы доступа, используемые приложения, сетевой трафик, запрашиваемые данные и т. д. При обнаружении нетипичных, потенциально опасных действий могут применяться различные меры: от записи выполняемых операций до полного блокирования пользователя — в зависимости от оценки степени риска.

Citrix NetScale CloudBridge был в очередной раз переименован (ранее этот продукт был известен как WANScaler и Branch Repeater) и теперь называется NetScaler SD-WAN. Прежний инструмент, применявшийся для оптимизации работы территориально распределенной сети, теперь преобразован в масштабируемое решение для поддержки корпоративной программно определяемой сети WAN, которое реализует наложенную сеть поверх уже существующей. Его главное предназначение — обеспечение быстрой и надежной доставки приложений в филиалы. NetScaler SD-WAN позволяет отслеживать более 4000 различных приложений в каждом сетевом сегменте. Как отмечает Сергей Халяпин, в отличие от других решений данный продукт способен, например, определить, какое именно приложение Microsoft Office используется.

NetScaler SD-WAN доступен в виде как физического, так и виртуального устройства, где собраны все необходимые для работы филиала сетевые функции. Так, в версию 9.1 добавлена поддержка пограничного маршрутизатора и VPN, а в версию 9.2, которая появилась в марте, — МСЭ/NAT. Кроме того, благодаря поддержке сервиса Zero Touch Deployment установленные устройства NetScaler SD-WAN могут быть удаленно сконфигурированы централизованным образом, при этом привлекать технического специалиста не понадобится: после идентификации устройства правильные настройки будут применены автоматически, причем именно те, какие требуются данному филиалу.

Во все редакции Xen Desktop добавлена поддержка технологии App Layering, которую Citrix приобрела вместе с компанией Unidesk. Каждое приложение помещается в отдельный слой и монтируется вместе с виртуальной машиной по запросу. Образ операционной системы и образ приложения могут обслуживаться отдельно. Любые вносимые изменения не будут затрагивать другие компоненты. «При обычном подходе ОС и приложения представляют собой единое целое. Один образ может содержать 20–30 продуктов. Если нужно что-либо поменять в одном из них, приходится изымать весь образ из эксплуатации, — поясняет Сергей Халяпин. — В случае же Layering каждый продукт доступен как отдельный виртуальный слой. Чтобы внести изменения, достаточно изъять его, не трогая весь остальной стек. Более того, можно обновить ОС и продолжить использовать те же слои».

И это только некоторые из многочисленных анонсов и обновлений, представленных в течение года. Кроме того, помимо таких традиционных для Citrix направлений, как виртуализация рабочих мест, доставка приложений и мобильные решения, компания активно работает в области дополненной/виртуальной реальности и Интернета вещей.

Дмитрий Ганьжа

Panasonic
BUSINESS

ДАЙТЕ МНЕ UC-ПЛАТФОРМУ, И Я ПЕРЕВЕРНУ МИР

UC-платформа KX-NSX2000/1000
SIP-видеотелефон KX-HDV430

Унифицированные коммуникации. Передовые технологии. Оптимизация расходов.

UC-платформа KX-NSX – это переворот в представлении о традиционных офисных коммуникациях от Panasonic. Современные IP-технологии и все необходимые сервисы позволят сотруднику работать из любой точки мира.

- Высокая надежность системы за счет «горячего» резервирования
- Возможность подключения до 2000 IP-абонентов
- Поддержка всех существующих коммуникационных сервисов

Мы создаем платформу для вашего бизнеса, чтобы вы перевернули этот мир!

www.panasonic.com b2b.panasonic.ru

ПЯТЬ ЛЕТ ГАРАНТИИ 5 ПОДРОБНЕЕ НА САЙТЕ WWW.PANASONIC.COM

Информационный Центр Panasonic: для Москвы 8-495-725-05-65, для регионов РФ 8-800-200-21-00 (звонок бесплатный)
На правах рекламы ООО «Панасоник Рус» – уполномоченного представителя компании Panasonic Corporation Ltd. на территории России

Fluke Networks готовит предложения для российского рынка

Новые решения Fluke Networks позволяют не только протестировать кабельную проводку, но и упростить управление проектом по ее сертификации.

Спад, наблюдавшийся в 2014–2015 годах на рынке СКС, оказал негативное воздействие и на бизнес Fluke Networks в России. Однако, как только наметилось оживление, компания вновь активизировала свою деятельность и сейчас рассчитывает на рост этого рынка (особенно в сегменте решений для ЦОДов), который, по прогнозу британского аналитического агентства BSRIA, составит 5–10% в 2018 году. «Если в прошлом в России у нас был лишь локальный представитель, то теперь мы являемся частью структуры Fluke CIS и имеем собственный склад», — отметил Роберт Лайтен, директор по глобальному маркетингу и взаимодействию с заказчиками. (Fluke Networks, как и Fluke Corporation, а также Tektronix, входит в состав холдинга Fortive.) Теперь оборудование может поставляться со склада, что значительно сокращает сроки поставки. Кроме того, цены выставляются в рублях и меняются не чаще раза в квартал.

Российский рынок СКС — это преимущественно рынок неэкранированных решений. Однако, по данным BSRIA, на долю экранированной проводки, прежде всего за счет ее использования в центрах обработки данных, приходится 18% продаж медных решений, которые, в свою очередь, составляют три четверти рынка.

Фото: Дмитрий Ганьжа

Анализаторы Fluke DSX-5000 позволяют выявить не только некорректность экранирования, но и место, где цельность экрана нарушена

На протяжении долгих лет в кабельной отрасли велся спор о сравнительных преимуществах неэкранированной и экранированной проводок и о влиянии неправильного экранирования на параметры передачи. Эта дискуссия обострилась с появлением 10-гигабитных приложений 10GBase-T, в частности, относительно соблюдения требований к характеристикам, когда экран не замкнут. Эксперименты подтверждали, казалось бы, обе точки зрения: и параметры выдерживаются, и электромагнитные помехи заметно увеличиваются.

На практике ситуация усугублялась тем, что существующие тестеры не могли точно определять правильность экранирования, так как прямые измерения не позволяли это сделать. Если экран между кабелем и разъемом не соединен с одной стороны, то электромагнитная защищенность ухудшается на 10 дБ, если с двух — еще на 10 дБ. По словам Кристиана Шиллаба, инженера-консультанта в отделе маркетинга EMEA, с неправильным экранированием приходится довольно часто сталкиваться на рынках, особенно на российском, где отсутствует многолетний опыт установки соответствующих систем. В результате заказчик, заплативший за экранированную систему, получает решение, которое по своим характеристикам ненамного лучше неэкранированного.

На основании данных о множестве соединений (неэкранированных, правильно и неправильно экранированных) Fluke Networks удалось выявить повторяющиеся шаблоны для ряда параметров, в частности различных видов импеданса. С помощью этих шаблонов оказалось возможным точно определить, подсоединен ли экран к разъему коммутационной панели (при наличии общего заземления у коммутационных панелей существующие тестеры показывают наличие экрана). Более того, кабельный анализатор Fluke Networks DSX-5000 позволяет выявить не только некорректность экранирования, но и место, где цельность экрана нарушена.

Настройка тестера часто осуществляется вручную, поэтому такое конфигурирование чревато ошибками. Чтобы автоматизировать эту процедуру, Fluke Networks предложила в свое время программное обеспечение LinkWare для ПК, а недавно появилась его облачная версия LinkWare Live. Это позволяет избежать ситуаций, когда ошибка обнаруживается только в конце тестирования: например, выясняется, что сертификация проводилась на соответствие другой категории кабеля и классу канала, из-за чего всю процедуру приходится повторять заново.

Как показал опрос Fluke Networks, проведенный среди специалистов по монтажу, тестирование на соответствие неправильно выбранным нормам — весьма распространенная проблема. Более того, именно по этой причине происходят наибольшие потери времени при тестировании и сертификации кабельных систем. Благодаря LinkWare Live менеджер проекта может определить необходимые тесты удаленно, что исключает возможность совершения исполнителем этой типовой ошибки. После завершения тестирования анализатор не надо привозить в офис, чтобы загрузить результаты тестов — они в любой момент скачиваются по Wi-Fi нажатием одной кнопки.

Сервис LinkWare Live предоставляется бесплатно. Как отмечает Алексей Гончаренко, менеджер по работе с партнерами в России и СНГ, это решение весьма актуально для России с ее обширной территорией, так как руководитель проекта получает возможность управлять проектом по сертификации СКС удаленно. Кроме того, с такой работой могут справиться технические специалисты с минимальной квалификацией.

Дмитрий Ганьжа

РЕШЕНИЯ ДЛЯ СОВРЕМЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ ОТ РИТ СНГ
ПРОИЗВЕДЕНО В РОССИИ

ШКАФЫ И СТОЙКИ РИТ СНГ

ШИРОКИЙ ВЫБОР:

- Шкафы и стойки (настенные и напольные, антивандальные, климатические, аккумуляторные)
- Системы изолированных коридоров для ЦОД
- Системы напольных покрытий для ЦОД
- Системы распределения питания

Интерактивный каталог http://cabinets.rit.ru – выбор конструктива и конфигуратор решений под ваши требования

ПРЕИМУЩЕСТВА:

- Лучшее соотношение цена-качество
- Доступность со склада в Москве
- Широкий ассортимент аксессуаров
- Специальные условия для партнеров

РИТ СНГ – ведущий поставщик комплексных систем в области СКС, сетевой инфраструктуры, телекоммуникационных шкафов и промышленных решений.

Тел.: +7 (495) 363-95-28
www.rit.ru

Extreme обещает бережно отнестись к приобретенным активам Avaya

Что будет делать Extreme Networks с продуктами купленного подразделения Avaya Networking?


Фото: «Открытые системы»

Сергей Гусаков, региональный менеджер Extreme Networks: «Продуктовые линейки Extreme Networks и Avaya Networking во многом пересекаются, но мы всегда очень бережно относимся к разработкам приобретаемых компаний»

Вопрос дальнейшей судьбы продуктов Avaya Networking объяснимо волнует российских партнеров и заказчиков Avaya. Ситуацию прояснили представители московского офиса Extreme Networks на семинаре, организованном компанией CompTek — одним из основных партнеров Avaya в России.

Напомним, что в рамках процесса реструктуризации задолженности Avaya была вынуждена расстаться с частью активов. Оставив себе основные продуктовые группы (системы унифицированных коммуникаций, ВКС и контакт-центры), она продала Extreme Networks свое сетевое подразделение Avaya Networking. Кстати, недавно (13 сентября) Avaya согласовала план погашения задолженности с ключевыми кредиторами «первой линии». Поэтому есть все шансы, что уже осенью компания, которая по факту чувствует себя вполне неплохо (она прибыльна, активно ведет разработки, выпускает новые продукты), выйдет из неприятной процедуры банкротства.

Максим Ковалев, руководитель направления Avaya в CompTek, заверил партнеров в доступности сетевых продуктов Avaya и гарантировал непрерывность бизнеса в рамках соглашения с Extreme. В свою очередь, Сергей Гусаков, региональный менеджер Extreme Networks, рассказал, что до конца текущего финансового года (то есть до 1 июля 2018 года) продукты Avaya будут продаваться через отлаженные логистические процедуры этой компании. Сервис по техническому обслуживанию формально также пока предоставляется от Avaya, хотя фактически сервисные инженеры этой компании уже переехали в офисы Extreme Networks.

Сергей Гусаков признал, что продуктовые линейки Extreme Networks и Avaya Networking во многом пересекаются. При этом, по его словам, Extreme Networks всегда очень бережно относится к разработкам приобретаемых ею компаний. В качестве примера он привел ситуацию с Enterasys. Эта компания была приобретена в 2013 году, и до сих пор сохраняются почти все основные линейки ее продуктов — закрыта лишь линия коммутаторов доступа, да и то только в этом году.

Extreme Networks работает на рынке, на котором многие годы доминирует один вендор, и большинство проектов, где используются ее продукты, — гетерогенные. Поэтому компанией накоплена большая экспертиза по интеграции продуктов различных производителей. Основой для такой интеграции часто выступает ее ПО управления, которое изначально разрабатывалось с учетом поддержки оборудования других вендоров. Компания вполне обоснованно гордится этим ПО с мощными средствами по анализу трафика и автоматизации процедур обслуживания и модернизации сети.

Первым шагом по интеграции продуктов любой компании (и Avaya Networking не будет исключением) в портфель решений Extreme станет перевод этих продуктов под «зонтик» единой системы управления. При этом эксперты Extreme с восторгом отзываются о решении Avaya Fabric Connect, называя его уникальной сетевой фабрикой, разработанной для кампусных сетей. Эта технология основана на протоколе маршрутизации IS-IS для обмена информацией о сервисах и построении кратчайших маршрутов между коммутаторами и позволяет существенно упростить процедуры администрирования сетей. В числе ее преимуществ: автоматизация подключения новых сетевых устройств и внедрения новых сервисов, обеспечение высокой доступности сетей, эффективные средства безопасности.

Технологию Fabric Connect уже используют более 1000 заказчиков по всему миру, включая Россию. Причем есть проекты, где в одну фабрику объединено порядка 500 коммутаторов. По словам представителей Extreme, нет никаких сомнений, что эта технология, равно как и поддерживающие ее коммутаторы (Virtual Services Platform, VSP), будет и дальше развиваться. Причем уже осенью 2017 года, как пообещали в Extreme, поддержка Fabric Connect будет реализована в коммутаторах Extreme Networks, использующих операционную систему EXOS, а также в продуктах Wi-Fi Extreme Wireless, что позволит применять эти продукты для подключения пользователей к сетевой фабрике.

У Extreme имеется своя сетевая фабрика, но компания позиционирует ее в качестве решения для ЦОДов. Скорее всего, в ближайшее время, если сделка по покупке у Broadcom подразделения Brocade успешно завершится, у Extreme Networks появится еще несколько ЦОДовских фабрик. Таким образом, компания будет располагать самым широким ассортиментом подобных сетевых решений на рынке. Как будет осуществляться интеграция продуктов Brocade? Будем информировать вас по мере появления информации.

Александр Барсков

Fortinet укрепляет фабрику безопасности

На Fortinet Security Day компания представила свое видение актуальных задач ИБ и решения для их реализации.

Fortinet успешно развивает свой бизнес как во всем мире, так и в России. По итогам прошлого года оборот компании увеличился больше чем на четверть и достиг 1,275 млрд долларов при том, что, по данным Gartner, рынок сетевой безопасности вырос всего на 7%. Почти 15% своего дохода — 183 млн долларов — компания потратила на исследования и разработки. Это позволяет ей удерживать лидирующие позиции на этом рынке. Так, в 2016 году было продано 700 тыс. устройств, что в два с лишним раза больше, чем у ближайшего конкурента. Средства активно инвестируются не только в разработку технологий и покупку перспективных компаний, но и в людей: в прошлом году к работе приступили еще 644 новых сотрудника.

Выступая на прошедшем в Москве Fortinet Security Day, Джо Сарно, вице-президент по международным продажам, выделил три сегмента рынка безопасности: защиту критической инфраструктуры и гибридных облаков, а также интеллектуальное обнаружение угроз. Согласно недавнему исследованию Forrester Research, свыше половины опрошенных компаний сталкивались в течение года с нарушениями безопасности систем SCADA/ICS. «Мы считаем, что операционные технологии/IoT станут следующим полем битвы, — заявил Джо Сарно. — Текущее положение дел напоминает мне ситуацию начала 90-х, когда были обнаружены первые вирусы». Для борьбы с этими угрозами Fortinet делает акцент на сегментации с целью разделения все более тесно интегрируемых производственной и ИТ-сети.

Чтобы обеспечить безопасную работу с различными облачными сервисами, в начале этого года компания выпустила брокер доступа к облакам FortiCASB. Атаки становятся гораздо более изощренными, соответственно, средства защиты должны становиться все более интеллектуальными. Новое решение FortiGuard Threat Intelligence Service (TIS), где для обнаружения угроз используется аналитика Больших Данных, позволяет оперативно их выявлять. Сервис FortiGuard доступен на рынке 15 лет, и ежедневно 2,5 млн подключенных к нему датчиков и устройств фиксируют 50 млрд различных угроз. Применение средств искусственного интеллекта в FortiGuard TIS должно обеспечить проактивную защиту от самых актуальных. Кроме того, Fortinet планирует добавить 2000 различных отчетов о соответствии требованиям регулирующих органов. Пока TIS находится на стадии бета-тестирования.

Анонсированную в прошлом году инфраструктуру Security Fabric в компании считают третьим поколением архитектуры сетевой безопасности после брандмауэров с контекстной проверкой и межсетевых экранов следующего поколения. Между тем Fortinet приобрела компанию AccelOps — ведущего производителя SIEM. Одноименный продукт стал частью Security Fabric под названием FortiSIEM. А благодаря партнерской программе Fabric Ready Partner Program, через открытые API в фабрику безопасности могут быть интегрированы решения других поставщиков. К программе присоединились уже 60 вендоров, в том числе Cisco, Brocade, HPE и др.


Фото: Дмитрий Ганьжа

Джо Сарно, вице-президент Fortinet: «Fortinet, вероятно, единственный вендор, кто может предоставить решения практически для всех сегментов рынка информационной безопасности»

Fortinet Security Fabric охватывает целый комплекс решений для обеспечения безопасности — от контроля доступа и межсетевых экранов (МСЭ) до средств предотвращения целевых атак. «Мы считаем, что фабрика безопасности, в которую входят решения для защиты от различных зловредов не только на границе сети, но и внутри сети, позволяет сделать то, что раньше было невозможно, — защитить всю сеть целиком», — заявил в своем выступлении Михаил Родионов, глава представительства Fortinet в России и Казахстане. Фабрика Fortinet реализует концепцию непрерывной сегментации, что позволяет обеспечить безопасность в условиях размытого периметра.

Основу Fortinet Security Fabric составляют межсетевые экраны FortiGuard. В этом году Fortinet была включена Gartner в квадрат лидеров МСЭ следующего поколения. Широкая линейка межсетевых экранов — от оборудования начального уровня и виртуальных устройств до мощных шасси — позволяет реализовать сегментацию на всех уровнях сети. МСЭ могут взаимодействовать в рамках фабрики, что позволяет видеть полную картину того, что происходит в сети, и предпринимать согласованные действия для ее защиты. По словам Михаила Родионова, межсетевые экраны Fortinet должны стоять в ядре сети. Так, мощные МСЭ серии 7000 способны обеспечивать инспекцию приложений на скорости 100 Гбит/с.

Дмитрий Ганьжа

Под знаком SD

КРОК предлагает полный набор решений для программно-определяемых сетей и различные модели их реализации. Среди них — «SD-WAN как сервис».

Максим Казаков, эксперт направления сети передачи данных КРОК MKazakov@croc.ru

Цифровые технологии становятся основой бизнес-процессов все большего числа компаний и организаций, а это значит, что требования к сетевой инфраструктуре неизменно растут. Она должна обеспечивать максимально оперативную поддержку быстро меняющихся бизнес-задач, гарантируя при этом высокий уровень надежности и прозрачности. Традиционные процедуры конфигурирования и изменения настроек, когда сетевой администратор вручную работает с каждым отдельным сетевым устройством, не позволяют уложиться в жестко определяемые временные рамки — чтобы компания смогла быстро вывести на рынок новые услуги. Да и с ростом числа сетевых узлов ручные методы управления становятся неприемлемыми.

На помощь приходят технологии программно-определяемых сетей (Software-Defined Networking, SDN). Суть SDN заключается в отделении функций передачи трафика от задач его управления. В традиционных коммутаторах и маршрутизаторах эти процессы неотделимы друг от друга и реализованы в одной «коробке». **Согласно концепции SDN, вся логика управления трафиком выносится в так называемые контроллеры, которые отслеживают работу сети и отвечают за ее конфигурацию.**

SDN-подход позволяет управлять сетью в целом на программном уровне. А это означает, что, определив один раз правила обслуживания трафика или логику работы сети для того или иного приложения, можно одним кликом мышки активировать соответствующие настройки на всех узлах сети. И неважно, сколько таких узлов (десять или тысяча), — все необходимые изменения будут применены автоматически. В результате сетевым администраторам больше не надо тратить массу времени на перенастройку, переходя от «коробки» к «коробке». В итоге существенно снижается вероятность ошибки, связанной с человеческим фактором, повышаются надежность и скорость адаптации сети к запуску новых сервисов и приложений. И это только некоторые преимущества использования SDN.

На сегодняшний день SDN выступает в трех **«ипостасях». Исторически внедрение технологии SDN началось с центров обработки данных (ЦОДов), где она и по сей день активно применяется для виртуализации сетей и ИТ-инфраструктуры в целом.** Пример такого решения — Cisco ACI (Application Centric Infrastructure), где функцию контроллера выполняет Cisco APIC. В продуктовой линейке этого производителя представлен и APIC-EM — первый коммерчески доступный SDN-контроллер Cisco для корпоративной кампусной сети. Стоит отметить, что «SDN для ЦОДов» является частью глобальной концепции Cisco DNA (Digital Network Architecture), основанной на открытых программных интерфейсах API.

Второе направление — это использование принципов «программной определяемости» в транспортных сетях. Здесь основные интересанты внедрения SDN — операторы связи, которые пока только присматриваются к новой технологии или находятся на этапе пилотных внедрений.

Наконец, третье направление — решения SD-WAN (Software Defined WAN), в первую очередь предназначенные для корпоративных заказчиков с распределенными филиальными сетями. Чем больше сеть филиалов, тем большую выгоду получает заказчик от применения программно-определяемой технологии.

Технология SD-WAN предполагает автоматическое формирование частной (корпоративной) сети с шифрованием информации и передачей трафика по всем типам подключенных каналов связи. При этом соблюдаются требования, предъявляемые бизнес-приложениями к каналам связи по полосе пропускания, задержкам, приоритизации и т. д. В основе SD-WAN лежит «умный» контроллер, благодаря которому осуществляется автоматическое управление всеми устройствами доступа, расположенными в узлах WAN-сети (в филиалах, удаленных офисах или других точках присутствия компании). Он позволяет централизованно изменять настройки сетевого оборудования в филиалах, отслеживать состояние сети, загрузку и качество работы каналов в онлайн-режиме, а также оперативно обнаруживать возникающие в каналах связи неполадки.

Несмотря на централизацию управления, технология SD-WAN в первую очередь предназначена для работы с децентрализованными сетевыми элементами. В качестве сетевых элементов могут использоваться как специализированные устройства, так и недорогое оборудование, построенное на базе референсной x86-архитектуры. Современные многоядерные процессоры и модули ускорения шифрования могут «прокачивать» гигабиты трафика в секунду с поддержкой полного функционала, включая разбор пакетов для распознавания приложений и решения дополнительных задач, таких как межсетевое экранирование, антивирусная защита, оптимизация трафика и т. д.

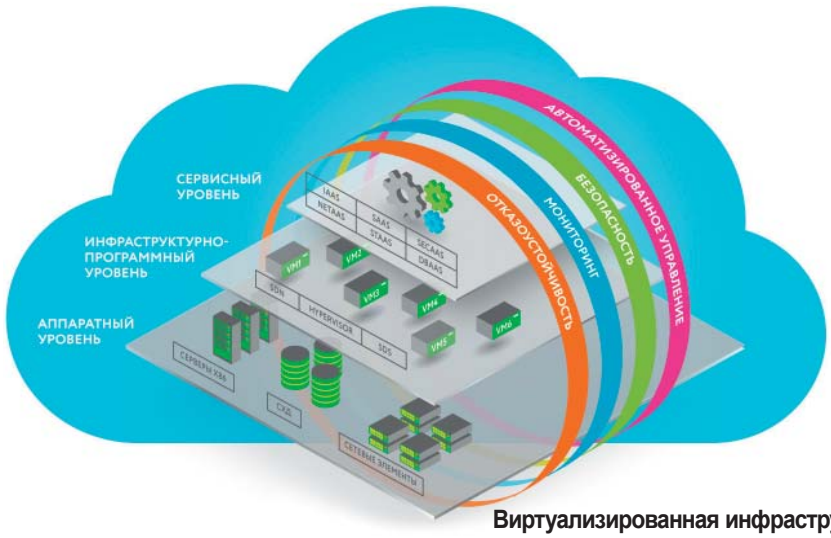
SD-WAN позволяет быстро подготовить сеть к подключению новых сервисов или развертыванию новых приложений. По сути, это общее преимущество всех категорий SD-решений,

но для WAN-сети, узлы которой могут быть разбросаны по огромной территории, оно может оказаться решающим для принятия решения о внедрении. Благодаря SD-WAN на адаптацию распределенной многофилиальной сети к запуску новых сервисов и активацию политик требуются не недели и месяцы (как в традиционной сети), а часы или даже минуты.

Важны не только централизация и автоматизация управления, но и то, что это управление в сети SD-WAN осуществляется на уровне приложений. Другими словами, именно приложение, его особенности и приоритет для бизнеса компании определяют то, как соответствующий трафик будет направляться и обрабатываться в сети. Это еще одно принципиальное отличие SD-WAN от традиционных систем управления.

Другое важное преимущество — оптимизация использования каналов связи, ведущая к сокращению затрат на их аренду. Например, если ранее для передачи голоса или видео без сбоев применялся только дорогой выделенный MPLS-канал, то теперь за счет реализованных в SD-WAN алгоритмов интеллектуального распределения трафика можно активно использовать несколько обычных интернет-каналов, а в качестве резерва — беспроводной канал, например LTE. Система сама анализирует качество связи по всем доступным интерфейсам и в случае деградации одного интернет-канала может перенаправить трафик в другой доступный, отвечающий заданным критериям. Выбор канала опять-таки реализуется на уровне приложений. Скажем, некритичный Skype-трафик будет направляться через Интернет, а трафик сеанса видео-конференц-связи руководства — через выделенный MPLS-канал.

Еще один плюс — оптимизация общих затрат на сеть. Переход от проприетарных «коробок» к устройствам на базе стандартной архитектуры x86 — это возможность существенно снизить как CAPEX, так и OPEX. Установив в филиале такое недорогое устройство, можно, помимо классических сетевых функций, «поднять на нем» функции оптимизации трафика, сервисы безопасности и т. д. — и все это будет централизованно управляться с единой консоли.



Виртуализированная инфраструктура

Изначально концепция SD-WAN была разработана несколькими американскими стартапами, которыми впоследствии заинтересовались крупные мировые игроки, включая Cisco. Сегодня эта компания предлагает в области SD-WAN решение Meraki, ориентированное на построение сетей Wi-Fi на удаленных площадках, а также активно продвигает подход iWAN на базе классических маршрутизаторов и APIC-EM в роли контроллера. Кроме того, в сентябре 2017 года Cisco завершила процесс покупки компании Viptela (одного из первых стартапов, представивших SD-WAN как законченный продукт) с дальнейшим намерением объединить ее технологии SD-WAN с линейками маршрутизаторов ISR и ASR.

Несмотря на молодость технологии SD-WAN, на нее уже обратили внимание многие российские заказчики. **КРОК в своей лаборатории в рамках «СПОРТа» (Созвездия Программно-Определяемых Решений) протестировал большинство представленных на рынке систем SD-WAN.** Три варианта контроллеров развернуты в лаборатории на постоянной основе, кроме того, имеется большой парк тестового оборудования для практического моделирования различных задач заказчиков.

Используя SDN-технологии и в своем облаке, КРОК предлагает управление корпоративной сетью на основе SD-WAN в формате управляемого сервиса (Managed Services) с ежемесячной оплатой. В облаке интегратора развернуто полнофункциональное многопользовательское решение SD-WAN. Оно позволяет заказчику управлять своим оконечным оборудованием из облака, начиная от процесса его инициализации и заканчивая применением специфичных политик и правил. Причем, в случае недоступности контроллеров в облаке, сами оконечные устройства продолжают работать в автономном режиме, обеспечивая связь между филиалами. В качестве оконечных устройств КРОК предлагает оборудование как на базе x86-платформы, так и с использованием проприетарных «коробок» — в зависимости от особенностей конкретного проекта и предпочтений заказчика. Сильно удешевляет решения на базе x86-платформы то, что КРОК получает их по модели bare metal, непосредственно с заводов. За развитие, управление и техническую поддержку ИКТ-инфраструктуры полностью отвечают высококвалифицированные специалисты КРОК.

Глубокая экспертиза в области сетевых технологий и развитая сервисная служба позволяют КРОК предлагать любое сетевое решение как сервис. Есть немало примеров, когда интегратор сам строит клиенту сеть и сам же отвечает за ее обслуживание с выполнением всех необходимых показателей SLA. В случае перехода на программно-определяемые сетевые решения эта модель становится еще более эффективной. Контроллер в надежном облаке КРОК обеспечит управление сетью, при этом заказчик сможет использовать менее дорогое оборудование в узлах сети, что обеспечивает независимость от вендора и снижает затраты на техподдержку. А функциональность, адаптивность и надежность сетевой инфраструктуры на базе SD-технологий — выше.

Генеральный директор, Brain4Net

Олег Щапов: будущее за открытыми сетевыми архитектурами

Зародившись в начале текущего десятилетия в университетской среде, технология SDN сегодня уже активно используется при модернизации всех типов сетей: операторских, корпоративных, ЦОДов. Вместе с появившейся немного позже концепцией виртуализации сетевых функций (NFV) она кардинально меняет подход к построению, эксплуатации и развитию сетевых инфраструктур. О текущем состоянии, проблемах и перспективах внедрений решений SDN и NFV, в преддверии форума RusNet 2017, мы поговорили с Олегом Щаповым, основателем и генеральным директором компании Brain4Net — известного разработчика систем управления сетями передачи данных, обработки сетевого трафика и виртуализации сервисных приложений на базе архитектур SDN и NFV.

Александр Барсков

Журнал сетевых решений/LAN: *Каковы, на ваш взгляд, главные драйверы внедрения технологий SDN и NFV?*
Олег Щапов: Главные драйверы — это потребность в быстром увеличении производительности сетевых соединений и оперативном запуске новых сервисов. Взять, например, операторов связи. Они сталкиваются, с одной стороны, со стремительным ростом трафика, с другой — с острой конкуренцией со стороны интернет-компаний, отбирающих у них доходы. Вклад коммуникационной составляющей в добавочную стоимость конечных сервисов сокращается — связь превращается в коммунальную услугу, такую же, как свет и вода. Телекоммуникационные компании стремятся увеличивать другие составляющие, но без кардинальной перестройки инфраструктуры, без сокращения издержек на ее содержание и развитие сделать это крайне сложно. Традиционные сети связи создавались в расчете на продажу минут и байтов и не очень подходят для предоставления новых сервисов. SDN и NFV — это те технологии, которые позволяют операторам оптимизировать инфраструктуру для работы в новых условиях.

Схожие потребности и у корпоративного сектора. Для развития бизнеса необходимо обеспечить быстрое получение сетевых сервисов. Скажем, раньше для подключения нового филиала к корпоративной сети могли потребоваться недели и месяцы. Сейчас можно отправить устройство в филиал, просто подключить его к сети — и всё: автоматически будут применены все необходимые настройки и подключены все необходимые сетевые сервисы. Более того, современные решения SD-WAN позволяют автоматически определить, через какой тип подключения нужно маршрутизировать трафик данного приложения — частный канал связи, Интернет или сеть сотовой связи. Это позволит снизить нагрузку на дорогие частные каналы связи и использовать сеть Интернет для передачи некритичного трафика (например, потокового видео YouTube).

В целом переход на системы на базе концепций SDN и NFV во многом обусловлен общим развитием технологий виртуализации. Для эффективного использования виртуализированных серверных ресурсов необходима виртуализация сети, которая может быть обеспечена системами SDN, а также виртуализация сетевых сервисов, то есть NFV. Именно виртуализация обеспечивает необходимую оперативность и гибкость получения сервисов. Движение к всеобщей виртуализации необратимо, вопрос только в скорости перехода к новым технологиям.

LAN: *И что же замедляет эту скорость?*
Щапов: Одно из главных препятствий — доступность зрелых решений и квалифицированных специалистов, которые могут их внедрять и обслуживать. Вспомните, внедрение SDN начиналось с ЦОДов. На этих объектах очень небольшие расстояния от управляющего контроллера до коммутаторов, между сетевыми устройствами множество высокоскоростных соединений, сетевая фабрика. За пределами ЦОДов ситуация иная, из-за чего возникает масса сложностей. Коммутатор может находиться от SDN-контроллера на расстоянии в десятки километров, между ними вряд ли будет много скоростных каналов. А в случае аварии на линии связи сеть должна продолжать работать, требования «пяти девяток» не отменяются, все хотят получать надежные сервисы.

Это все создает большие технологические сложности. Мы, например, потратили 2,5 года, чтобы справиться с ними, и считаем, что нам это удалось. Разработанное SDN-решение позволяет строить унифицированную транспортную фабрику не только в ЦОДе, но и за

его пределами. Уникальность нашей фабрики в том, что она работает на втором уровне модели OSI при тесной интеграции с L3-сервисами, использует открытые сетевые платформы, а уровень управления тесно интегрирован с оборудованием. Между тем большинство конкурентов предлагают решения на базе технологий «наложенных сетей» (overlay). К тому же наша фабрика отлично масштабируется: мы планируем до конца года обеспечить поддержку 16 тыс. MAC-адресов на одном кластере контроллеров. С помощью оркестратора можно объединить несколько кластеров. Соответственно, емкость решения еще повышается.

Но разработать управляющую сервисную платформу — это только часть решения проблемы, надо еще найти подходящие сетевые устройства. Здесь тоже не все так просто. Традиционные коммутаторы создавались с другими целями, сейчас возникают новые требования, необходимы новые устройства. Причем задачи меняются не только для производителей коммутаторов, но и для разработчиков чипсетов. Мы стараемся активно работать с основными производителями чипсетов, включая Broadcom и Mellanox, как разработчик сетевой ОС доносим до них свои пожелания, которые учитываются при разработке новых коммутирующих матриц.

> NFV — это не про централизацию, а про организацию микросервисов и их оркестрацию, про формирование цепочек сервисов для решения конкретных задач.

LAN: *Как поставщик независимой сетевой ОС вы ориентируетесь на использование оборудования bare-metal?*

Щапов: Да, стратегия развития продуктов Brain4Net направлена на построение сервисно ориентированных сетей на базе устройств bare-metal. Мы сотрудничаем со всеми основными производителями коммутаторов bare metal, среди которых есть и российские компании — например, новосибирская «Элтекс». Она готовит к выпуску такой коммутатор с портами 10G и 40G, его можно будет использовать совместно с нашей платформой как в ЦОДах, так и за их пределами, в том числе в сетях операторов.

Хочу обратить особое внимание на возможность использования в качестве полноценных коммутаторов устройств, построенных на базе стандартной архитектуры x86, которая предоставляет очень гибкие возможности. Наш виртуальный коммутатор B4N SwitchOS первым (среди сетевых ОС для платформы x86) прошел сертификацию ONF по программе OpenFlow Conformance Testing. Коммутаторы с портами 10G и 40G на базе архитектуры x86 — это уже реальность. У нас есть пилотные проекты

с операторами, которые используют построенные на базе серверов x86 коммутаторы с 48 портами 10G.

В контексте сетевых решений на базе x86 хочу упомянуть наше сотрудничество с еще одной российской компанией — «ДЕПО Компьютерс». Эта компания, известная своими серверами, разработала гибридное решение сервер-коммутатор, которое успешно используется в наших проектах. Оно представляет собой коммутатор на базе платформы x86, который обладает мощными вычислительными возможностями и позволяет запускать различные приложения.

Коммутаторы на базе архитектуры x86 с портами 10G и 40G — это реальность. В пилотных проектах уже используются построенные на базе серверов x86 коммутаторы с 48 портами 10G.

LAN: *Выше мы говорили о построении транспортной фабрики, а какие тенденции определяют развитие сервисных фабрик, основанных на концепции NFV?*
Щапов: Цифровизация экономики и развитие систем Интернета вещей требуют приближения сетевых сервисов к клиентам и конечным устройствам для выполнения необходимых условий SLA, а также минимизации задержки получения сервиса, которая для многих приложений должна составлять микросекунды. Соответственно, вычислительные мощности, на которых собственно и реализуются сервисы, должны располагаться ближе к клиентам. Все развивается по спирали, и от централизации вычислительных средств мы идем к их децентрализации.

LAN: *Но ведь NFV предполагает централизацию, разве нет?*
Щапов: Действительно, на начальном этапе было представление, что все сервисы будет раздавать централизованная монструозная платформа, состоящая из большого числа серверов. Сейчас концепция поменялась. По крайней мере в случае использования решений B4N, вся сервисная логика может быть упакована в один сервер, который можно вынести ближе к конечным устройствам — например, поставить рядом с базовой станцией 5G или в абонентский шкаф. Более того, вычислительные ресурсы, необходимые для предоставления сервисов и первичного анализа собираемой информации, может предоставить коммутатор, построенный на платформе x86. В этом нет никакой сложности.

В каждом конкретном случае оборудование для предоставления сетевых сервисов следует размещать там, где это оптимально для обслуживания конкретных объектов. Этот сервер должен быть частью распределенного облака, чтобы, скажем, для снятия пиковых нагрузок можно было задействовать другие серверы, в том числе установленные в центральном ЦОДе. Реализация такого распределенного облака — задача непростая.

Обобщая, можно сказать: NFV — это не про централизацию, а про организацию микросервисов и их оркестрацию, про формирование цепочек сервисов для решения конкретных задач. Мы в Brain4Net создаем магазин сетевых сервисов — некий аналог App Store для приложений, реализующих различные сетевые функции. Зайдя на нашу платформу, заказчик выбирает нужный ему сервис, загружает и запускает его. Активация нового приложения обычно занимает считанные секунды, максимум несколько минут. Это и есть «сеть по требованию».

LAN: *Можете привести примеры типовых проектов, в которых применяются ваши решения SDN и NFV? На какой стадии они находятся?*
Щапов: Наши решения применяются операторами связи, в том числе российскими, для модернизации metro-сетей, сетей агрегации мобильной связи (backhaul) и т. д. Немало проектов и с корпоративными заказчиками, в том числе государственными, для которых дополнительным стимулом использования наших решений является стремление перейти на отечественные технологии. Среди заказчиков Brain4Net имеются и облачные провайдеры из разных стран. Как я уже говорил, серьезным катализатором для перехода на технологии SDN и NFV служит все более активное использование систем виртуализации серверов.

Использование открытых решений на базе OpenFlow и продуктов bare metal предоставляет заказчикам свободу выбора оборудования и позволяет избежать зависимости от одного производителя.

Если говорить о статусе проектов, то большинство находятся пока в стадии пилота. Но это не опытные участки, а внедрение на «живых» сетях с постоянным расширением реализованных на базе новых технологий сегментов.

LAN: *Но многие традиционные производители сетевого оборудования бодро рапортуют о сотнях инсталляций SDN, причем далеко не пилотных…*
Щапов: Тут надо разбираться в том, что понимается под SDN. В принципе, концепцию SDN можно реализовать и на базе закрытых архитектур и проприетарных протоколов. Таких проектов немало. Мы же предлагаем полностью открытые решения с использованием протокола OpenFlow и оборудования bare metal. Уверен, что такой подход дает новый импульс развитию сетевых технологий, предоставляя заказчикам свободу выбора оборудования из широкого списка совместимого аппаратного обеспечения и позволяя избежать проблемы зависимости от одного производителя. Это принципиально иной подход, за которым будущее.

Мы не заставляем наших клиентов менять все сразу — наши решения взаимодействуют с традиционными сетевыми решениями и интегрируются в существующие сети. Какое-то время различные технологии, традиционные и SDN/NFV, будут сосуществовать вместе. Но каждый заказчик стремится как можно быстрее перейти на одну базовую технологию. Одновременно эксплуатировать сети, построенные в соответствии с разными архитектурами, — дороже: надо поддерживать интеграционный стык, это требует времени и денег. Я уверен: как только клиенты убедятся в том, что новые технологии эффективнее решают их бизнес-задачи, полный переход на них будет осуществлен очень быстро. **LAN**

Генеральный директор, ProtoSecurity

Денис Безкоровайный: как обеспечить безопасность приложений при ускоренной разработке

Популярность Web-приложений как основного инструмента онлайн-бизнеса растет из года в год, одновременно с этим все больше привлекая злоумышленников. Между тем, согласно исследованиям Contrast Security, порядка 80% Web-приложений в среднем содержат до 45 уязвимостей, из которых по крайней мере одна имеет высокий уровень критичности. Такая ситуация свидетельствует о недостаточном внимании к вопросам безопасности в процессе разработки. Применение таких средств защиты, как Web Application Firewall, позволяет противостоять эксплуатации уязвимостей, но при этом не устраняет корень проблемы — ошибки в коде. С внедрением методологий ускоренной разработки DevOps положение еще более усугубляется. О том, как выйти из данной ситуации и обеспечить информационную безопасность в условиях быстрой разработки, мы поговорили с Денисом Безкоровайным, генеральным директором ProtoSecurity.

Дмитрий Ганьжа

Журнал сетевых решений/LAN: *В условиях ускоряющейся разработки приложений отставание в реализации мер безопасности становится все более критическим. Как обеспечить должную безопасность приложений в таких условиях?*

Денис Безкоровайный: Да, действительно, скорость разработки увеличивается из года в год. Раньше новый релиз появлялся один раз в квартал или один раз в год, сейчас же, в условиях возрастающей конкуренции, все заказчики стремятся как можно быстрее реализовывать новый функционал. В связи с этим приходится сокращать циклы разработки: релизы выпускаются несколько раз в неделю или даже в день, так что стандартный подход, когда о безопасности задумывались лишь в самом конце, при такой модели работает очень плохо.

LAN: *Как выйти из создавшейся ситуации?*

Безкоровайный: Прежде всего если не владельцы бизнеса, то владельцы приложений должны уделять приоритетное внимание безопасности и осознавать, как последствия взломов, компрометаций и утечки данных скажутся на прибыли компании. Кроме того, необходимо пересмотреть роль специалиста по ИБ: из охранника/надзирателя, который мешает всем процессам и вставляет палки в колеса, как его часто воспринимают, он должен превратиться в партнера и ИБ-коуча.

По статистике, на одного специалиста по информационной безопасности приходится в среднем 100–200 разработчиков. В таких условиях обеспечить должный контроль крайне сложно, а значит, необходимо делиться компетенциями и делать их частью общего процесса. То есть безопасностью должны заниматься не только специалисты по ИБ, но и разработчики, тестировщики, менеджеры продукта. Правильная организация этих процессов и вовлечение в них всех команд, внедрение и насаждение культуры информационной безопасности и есть новая задача ИБ-специалистов.

С одной стороны, это означает трансформацию роли и значимости ИБ в компании, с другой — смену используемых инструментов. Современные приложения собираются из модулей и компонентов, часто модулей на базе открытого кода, а сами готовые приложения распределены между различными микросервисами. В такой среде применение традиционных средств анализа защищенности не всегда эффективно, и не все статические анализаторы исходного кода могут производить быстрые инкрементальные сканирования кода при коротких циклах разработки. Поэтому для реализации безопасности на любом этапе разработки нужны новые инструменты, доступные не только ИБ-специалистам.

Обоснованием замены инструментов может служить тот факт, что на устранение критической уязвимости в конце цикла разработки обычно тратится огромное количество ресурсов. Иными словами, чем позже в процесс создания приложения внедряется безопасность, тем дороже оно обходится. Мы уже подошли к тому моменту, когда количество критичных для бизнеса приложений растет из в года в год экспоненциально, ужесточается и конкуренция, поэтому любая остановка деятельности, вызванная инцидентом безопасности, мгновенно сказывается на конкурентоспособности компании и ее бизнесе в целом.

Приступив уже сегодня к пересмотру роли и функций информационной безопасности в процессе разработки при-

ложений: во-первых, сделав ИБ общей ответственностью различных команд, во-вторых, внедрив методологии DevSecOps в процесс разработки, — компания получит конкурентное преимущество в самое ближайшее время.

LAN: *Методология интеграции принципов безопасности в ускоренный цикл разработки известна под различными названиями: DevSecOps, SecDevOps и DevOpsSec. Чем они отличаются?*
Безкоровайный: По сути DevSecOps, SecDevOps и DevOpsSec — это один подход, применяемый с одной и той же целью, но с разными акцентами на безопасности. Иначе говоря, кто-то ставит ИБ на первое место, кто-то — на последнее. Отсюда и возникли термины DevSecOps, SecDevOps и DevOpsSec.

Чтобы разобраться в самом подходе, необходимо иметь представление о том, что такое DevOps. Раньше в разработке выделялись различные зоны ответственности — каждый отвечал исключительно за свой участок. Разработчики не имели представления о том, где в реальной инфраструктуре будет использоваться приложение, как его станут масштабировать и т. д. А системные администраторы и служба эксплуатации занимались вопросами инфраструктуры и были склонны возлагать ответственность на программистов, если ОС и серверы функционировали без сбоев, но при этом фиксировались какие-то неполадки в работе приложения. Такое перекладывание ответственности тормозило процесс выпуска релизов, снижая тем самым общую эффективность разработки.

Именно в связи с реальной надобностью в переломе ситуации и сформировалась парадигма объединения практик разработки, администрирования и тестирования в рамках общего процесса создания приложения, именуемая DevOps. Важно отметить, что сейчас все еще не существует единого стандарта DevOps — это скорее некий общий подход, когда ответственность за приложение разделена между всеми, кто участвует в его создании и обслуживании.

Точно так же, как и в ситуации с возникновением естественной необходимости в создании DevOps, появилась потребность во встраивании безопасности в этот подход. Ведь нет такой точки на временной шкале разработки приложения, когда наступает момент для обеспечения безопасности, — ранее защиты не было, а теперь ее пора внедрить. Так не бывает. Этим нужно заниматься все время, на каждом этапе жизненного цикла приложения. В результате и возникла идея объединения DevOps и ИБ.

Например, на этапе тестирования качества кода безопасность должна быть интегрирована в этот процесс. Тесты на безопасность следует проводить параллельно с тестами на функциональность, а не по завершении последних. Безопасность должна быть частью меры качества программного продукта. Недостаточно просто учитывать количество ошибок и обнаруженных проблем — при выявлении уязвимостей на этапе тестирования, продукт нельзя переводить на следующую стадию. В идеале появление брешей в коде нужно минимизировать еще до этапа тестирования. Для этого специалистам по ИБ необходимо взаимодействовать с разработчиками, заниматься их обучением.

Совершенно ясно, что невозможно сделать каждого разработчика специалистом по ИБ, поскольку это разные области деятельности и требуют разного уровня подготовки. Однако, согласно концепции DevOps, администраторам необходимо иметь представление об особенностях функционирования программного продукта, а разработчикам — о «поведении» их кода в реальной среде. Точно так же в соответствии с DevSecOps специалисты по ИБ должны внедрять базовые концепции информационной безопасности на уровнях разработки и администрирования.

Таким образом, в рамках DevSecOps роль специалистов по безопасности состоит в улучшении процесса разработки современных приложений с точки зрения их защищенности и, естественно, в защите той среды, в которой это приложение будет работать. В результате ответственность за безопасность распределяется, хотя и неравномерно, между всеми участниками процесса, а не возлагается исключительно на специалиста по ИБ.

Разработчики должны все время помнить о задаче обеспечения ИБ и следовать принципам безопасной разработки приложений хотя бы в той мере, чтобы не допускать базовых ошибок. А руководители должны ввести соответствующие KPI. Например, каждую неделю выпускается очередной релиз. Метрикой качества кода с точки зрения безопасности может служить количество повторяющихся уязвимостей в коде, то есть тех, что ранее уже были выявлены и некорректно устранены. Или количество новых уязвимостей и т. д.

Тогда служба ИБ получит рычаги влияния на разработчиков и возможность мотивировать их на выполнение установленных требований.

Другая задача ИБ — защитить среду, в которой приложение работает: контейнеры, системы распределенных вычислений, виртуальные машины, серверы. Ведь чем сложнее приложение, тем больше точек отказа — мест возможного проникновения злоумышленников.

LAN: *Насколько включение мер безопасности в DevOps замедляет процесс разработки?*
Безкоровайный: Процесс разработки замедляет как раз традиционный подход ИБ — например, применение сканеров для анализа кода на завершающем этапе создания приложения.

Конечно же, внедрение методологии DevSecOps, ее притирка и отладка требуют определенных усилий и чреваты задержками на первых порах: необходимо найти и внедрить нужные инструменты, обучить людей. Однако, когда процесс отлажен, разработка будет идти с прежней скоростью и при этом будет безопасной.

Если же пытаться делать по старинке (быстрая разработка, а потом проверка на безопасность), то, помимо замедления сроков релизов продукта, это приведет к постоянному торгу относительно выбора изменений, которые необходимо внести в код для его защиты.

Как показала практика, компании готовы внедрять процессы безопасной разработки, инвестировать в обучение специалистов и приобретение необходимых инструментов безопасности для поддержки ускоренных циклов разработки. К настоящему моменту уже сложилось понимание того, что создание изначально безопасного продукта позволяет, особенно в таких критичных сферах, как финансы, обогнать конкурентов и при этом избежать ситуации, когда один инцидент ставит под угрозу весь бизнес.

В России, насколько мне известно, масштабных инцидентов наподобие кражи у компании Equifax персональных данных о 143 млн американских граждан пока не происходило, но озабоченность состоянием безопасности приложений на высококонкурентных рынках возрастает, и компании готовы вкладывать средства в безопасную разработку.

LAN: *Внедрение методологии DevSecOps и ей подобных не гарантирует 100-процентной защиты приложений. Все равно необходимо использовать средства и системы защиты. Не проще ли сделать акцент именно на них?*
Безкоровайный: Дополнительные средства защиты, конечно же, нужны как средство лечения симптомов. Однако внешняя защита наименее надежна, ведь ни один поставщик соответствующих решений не дает никакой гарантии. Как ни один разработчик антивирусов не несет ответственности в случае вирусной эпидемии, так и ни один производитель средств защиты Web- и мобильных приложений не заявляет о защите на 100%. Это в принципе невозможно.

Наложенные средства безопасности скорее служат для выявления атак на раннем этапе, чтобы заблокировать доступ злоумышленникам к внутренним системам, для предотвращения их дальнейшего проникновения в них. В случае Web-приложений они позволяют обнаружить и остановить успешную атаку, которая стала возможна из-за наличия уязвимостей, не замеченных разработчиками. Но все подобные средства, например Web Application Firewall, можно потенциально обойти, ведь атака может быть видоизменена таким образом, что не будет замечена системой защиты, или появится абсолютно новый вид атаки, ранее неизвестный.

Использование внешних средств безопасности — это некая дополнительная, компенсационная мера. Основная — выявление уязвимостей в коде приложения.

Ведь успешное отражение атаки — это не итог борьбы со злоумышленником, это всего лишь передышка, которую нужно использовать для поиска уязвимостей в коде и их устранения. И это первое, что необходимо сделать, так как средство безопасности может сегодня работать, а завтра окажется неэффективным, например, из-за ошибки в конфигурации, запуска виртуальной машины в другом ЦОДе и т. п.

Нужно лечить причину болезни, а не ее симптомы, поэтому приоритет необходимо отдавать совершенствованию самого продукта.

LAN: *Между тем на рынке начали появляться решения, поставщики которых обещают обеспечить автоматизированную защиту приложений. Насколько на них можно полагаться?*
Безкоровайный: Применение алгоритмов машинного обучения в автоматизированных системах защиты, конечно, перспективно, к тому же количество атак и инцидентов постоянно возрастает и проанализировать их все вручную, чтобы обновить сигнатуры, уже невозможно. Однако пока нет никаких гарантий точности работы и полноты этих алгоритмов.

Да, действительно, на рынке Web Application Firewall и систем защиты Web-приложений вместо сигнатурного метода (или в дополнение к нему) набирает популярность применение эвристических методов, с помощью которых система учится понимать, что является нормальным поведением, а что — аномальным. Однако после внедрения таких систем возникает немало проблем: их обучение занимает достаточно много времени, а после обновления программного продукта алгоритмы приходится перестраивать, поскольку изменение логики работы пользователя воспринимается как аномальное поведение. Это приводит к ложным срабатываниям, требует дополнительных усилий по администрированию такой системы и т. д.

Невозможно полностью исключить работу аналитиков, заменив их алгоритмами. Наиболее перспективна, на мой взгляд, комбинация ручных методов и машинного обучения, когда специалисты занимаются анализом состоявшихся атак, потенциальных угроз и их источников. Да и у клиентов наибольшее доверие вызывают продукты тех компаний, у которых, помимо алгоритмов для анализа угроз, имеется большой штат квалифицированных исследователей. **LAN**

Генеральный директор, Cabero Wärmetauscher Osteuropa

Глеб Хрущенко: «Конкурентов по уровню надежности у нас нет»

На заре ЦОДостроения вопросу энергоэффективности уделялось мало внимания во всем мире, что уж говорить про Россию. При этом инженерные системы потребляли порой больше, чем обслуживаемые ими ИТ-решения, — только на охлаждение последних тратилось до половины всей потребляемой энергии. В современных ЦОДах этот показатель составляет 20% и менее, что достигается за счет использования энергоэффективных решений. Немецкая компания Cabero предлагает теплообменное оборудование, где реализован ряд интересных технологий, в частности бесчиллерные системы. А компания profITcool адаптирует готовые изделия Cabero с учетом особенностей российского климата. Об энергоэффективных решениях для охлаждения Cabero и спросе на них на отечественном рынке нам рассказал Глеб Хрущенко, генеральный директор Cabero Wärmetauscher Osteuropa.

Дмитрий Ганьжа

Журнал сетевых решений/LAN: *Какие тенденции в области охлаждения ЦОДов вы бы выделили?*
Глеб Хрущенко: Прежде всего я отметил бы интерес к энергоэффективным решениям. По данным Borderstep Institute, энергопотребление ЦОДов составляет более 10% общемирового и продолжает расти. Естественно, разработчики новых ЦОДов стремятся сократить затраты, и российский рынок не исключение. Способов много, и они хорошо известны. Хочется добавить лишь, что Cabero активно работает в этом направлении с момента основания компании в 1980 году.

Заметной тенденцией является рост популярности бесчиллерных систем. Вариаций много, все они чрезвычайно интересны с инженерной точки зрения. В России уже реализовано довольно много подобных систем, среди наиболее известных — охлаждение ЦОДов компании «Яндекс» и суперкомпьютера МГУ. И коммерческие ЦОДы начинают устанавливать такого рода системы. Особенно хочется отметить ЦОД «ДатаПро», где внедрено одно из наших решений с использованием бесчиллерных систем.

Модульные решения (например, контейнерные ЦОДы), на мой взгляд, уже прочно закрепились на российском рынке. Прежде всего они отличаются удобством, надежностью, простотой модернизации ЦОДа и возможностью расширять его по мере необходимости. Хотя Cabero пока не выпускает полностью готовых решений, мы активно сотрудничаем с разработчиками, поставляя компоненты таких систем.

К сожалению, в кризис стало появляться больше систем, в которых качество, надежность и соответствие заявленных параметров предъявляемым требованиям оставляют желать лучшего. Подрядчики заинтересованы прежде всего в низкой стоимости, действуя по старому студенческому принципу «сдал и забыл». Такие решения всегда были и будут, но могу с уверенностью сказать, что эта тенденция носит временный характер. Участники рынка общаются между собой, и негативный опыт эксплуатации подобных систем быстро становится известным, после чего, несмотря на дешевизну, их популярность падает.

LAN: *Предложение и спрос на комплексные решения для построения инженерной инфраструктуры расширяются. Каковы рыночные перспективы у поставщика решений для охлаждения?*
Хрущенко: Мы рады здоровой конкуренции, она не дает почивать на лаврах, заставляя постоянно совершенствоваться и двигаться вперед. Просто представьте себе мир, в котором нет конкурентов. Незачем развиваться, работать над собой, что-либо менять — скучно. Так что перспективы — самые наилучшие.

LAN: *И все же, зачем покупать отдельное решение для охлаждения, если можно приобрести комплексное?*
Хрущенко: Не бывает специалистов во всех областях. Заказчик же в кризис стремится сэкономить, покупая готовые решения напрямую у производителя. Многие интеграторы предпочитают также передать разработку подобных решений производителю на аутсорсинг, сокращая таким образом численность инженерных команд и затраты на содержание персонала.

LAN: *Чем интересен российский рынок для Cabero?*
Хрущенко: Как и любой другой — объемами продаж. Даже в кризис спрос остается довольно большим. Кроме того, в России, помимо прибыли, мы получаем удовольствие от работы с интересными людьми и от реализации интересных инженерных решений.

LAN: *Чем в технологическом плане теплообменное оборудование Cabero отличается от продукции других производителей?*

Хрущенко: В зависимости от того, с чем сравнивать. Если с другим теплообменным оборудованием, то марка Cabero держится на трех китах: качество, надежность, технологии.

Мы используем только высококачественные материалы западноевропейского производства, в основном немецкие. То же самое касается исполнения. На наших заводах действует строгая система контроля качества каждого узла, а специалисты регулярно проходят курсы повышения квалификации. Оборудование разрабатывается с вниманием к каждой детали, а потому максимально надежно. И естественно — технологии. Мы не экономим на научных разработках: любые нововведения проверяем сначала на стендах, а затем на практике — в рамках реализации пилотных проектов.

Поэтому, приобретая оборудование Cabero, заказчик гарантированно получает лучшее из представленного на рынке.

LAN: *Третий кит — это технологии. Какие вы могли бы выделить?*
Хрущенко: Технологий много: от испарительных систем, которые у нас, в отличие от многих, действительно испарительные, а не адиабатические, до систем для Крайнего Севера; от самосливных, предназначенных для охлаждения воды круглый год, до взрывозащищенных. Для описания каждой из них потребовалась бы отдельная статья.

LAN: *В чем преимущества бесчиллерных систем охлаждения и насколько российские заказчики заинтересованы в их внедрении?*
Хрущенко: Энергоэффективность таких систем сложно превзойти. Однако пока в самом операционном зале необходимо использовать и альтернативные системы, в том числе для охлаждения. Нельзя охладить без компрессора стандартную стойку. Интерес к таким системам растет, но массового спроса еще нет. Возможно, именно из-за необходимости подключения альтернативной системы охлаждения внутри самого ЦОДа.

LAN: *Что собой представляет производство в России и что оно дает Cabero?*
Хрущенко: Производство в России позволяет быть ближе к клиенту, обеспечивая возможности быстрого реагирования, упрощенного сервиса, адаптации к условиям рынка и климата. Александре Эрлих, генеральному директору proflTcool, которая является сеньор-консультантом Cabero, удалось собрать молодую целеустремленную команду. Ребята с увлечением работают над совершенствованием вспомогательных узлов к теплообменному оборудованию и создают из нашего оборудования готовые кластеры, благодаря чему наши решения легко внедряются в любую систему. В своем роде это тоже модульные системы.

LAN: *В каких случаях заказчики выбирают оборудование локальной сборки? Дороже ли оно и насколько пользуется спросом?*
Хрущенко: В основном системы российской сборки приобретают госорганизации, финансируемые из госбюджета. В этом вопросе пока больше политики, чем сознательного желания использовать отечественную продукцию. К сожалению, сугубо российские производители пока не смогли впечатлить потребителя. Мне часто приходится слышать от них: «Мы можем выпускать хорошее оборудование, у нас есть конструкторские бюро». При этом вопросы о теплообмене, гидрогазодинамике и аэродинамике ставят их в тупик. Странно для страны с такой сильной инженерной школой.

Нам удается удерживать цены на адаптированные теплообменные аппараты. На российском рынке, к сожалению, сложно производить дешево и качественно. Большим спросом пользуются комплектующие узлы, созданные нашими специалистами на базе западных компонентов, — например, гидромодули. Эти продукты — бесспорные лидеры. Они универсальны, обеспечивают максимальное удобство обслуживания и надежность. Сервисная служба будет очень благодарна, если вы их приобретете.

LAN: *В текущих экономических условиях заказчики хотят дешево и сердито. В какой мере удается обеспечить и приемлемую цену, и высокое качество?*
Хрущенко: При сравнении с аналогичной продукцией аппараты Cabero, безусловно, дешевле. Конечно, если при оценке не лукавить с коэффициентами теплопередачи и материалами.

LAN: *Насколько важным фактором для российских заказчиков при выборе оборудования является его энергоэффективность и стоимость владения? Что предлагает Cabero?*
Хрущенко: Для конечного потребителя низкая стоимость владения является важным доводом. Дальше остается только убеждать и аргументировать. В большинстве случаев это удается, поскольку любой из аппаратов и узлов оборудования Cabero, включая российское, соответствует этим критериям.

LAN: *Как вы оцениваете энергоэффективность российских ЦОДов по реализованным проектам?*
Хрущенко: Если сравнивать показатели PUE, то российские ЦОДы невероятно энергоэффективны, намного больше, чем немецкие. Поскольку мы работаем и в Германии, я могу с уверенностью сказать, что там больше внимания обращают на потребление ресурсов и меньше на такие показатели, как PUE, которыми легко манипулировать. Кроме того, экономия воды и электроэнергии стимулируется экономическими мерами. Например, при подготовке к зимнему периоду вода из системы не сливается в канализацию, поскольку придется платить дважды: первый раз при ее заборе и второй раз при сливе, причем последний зачастую обходится дороже.

LAN: *Какова гарантийная политика Cabero? Как часто происходят обращения по гарантийным случаям?*
Хрущенко: Стандартная гарантия составляет два года. Продленную мы даем без проблем, при этом небольшое увеличение стоимости связано исключительно с необходимостью плановой замены частей, находящихся в постоянном движении, например вентиляторов. Остальные компоненты оборудования Cabero гарантированно проработают без изменения характеристик 15 лет и больше. С уверенностью могу утверждать: сегодня конкурентов по уровню надежности у нас нет. Наши заказчики знают, что это не пустые слова и не бравада.

Недавно одному из инвесторов показывали ЦОД, где установлен суперкомпьютер МГУ, находящийся в эксплуатации с 2012 года (объект закрытый, попасть туда не так просто). Он был в восторге от того, что спустя столько лет оборудование Cabero выглядит «как новое», причем не ухудшились и его технические характеристики. К слову, до сих пор ни одна из частей системы не была заменена, хотя с момента ввода в эксплуатацию прошло уже пять лет. **LAN**

Что вы знаете про SD-WAN?

Если по каким-то причинам вы до сих пор ничего не слышали об SD-WAN, то в течение ближайших двух лет не только много услышите, но и увидите. А скорее всего, будете использовать SD-WAN сами, особенно если деятельность вашей компании связана с эксплуатацией или развитием сетей крупных государственных организаций, банков или розничной торговли.

Александр Комаров,
ведущий инженер департамента сетевой интеграции «АМТ-ГРУП»

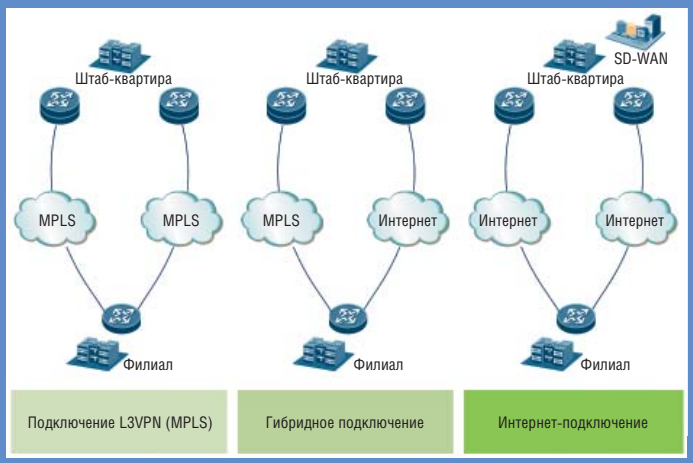


Рис. 1. С появлением SD-WAN стали возможны отказ от аренды дорогих каналов L3VPN и использование каналов Интернета от разных провайдеров с сохранением необходимого качества обслуживания

Рис. 2. Все необходимые настройки сетевое устройство автоматически получает от контроллера

Сети SD-WAN приходят на смену устаревающим традиционным территориально распределенным сетям, как когда-то смартфоны потеснили обычные мобильники. Согласно исследованиям Gartner, более 36% крупных компаний планируют начать пользоваться SD-WAN до конца 2018 года. И каждый год количество сетей SD-WAN будет расти в среднем на 65%.

Решение SD-WAN — это первый большой шаг в реализации концепции программно определяемых сетей SDN применительно к территориально распределенным сетям. Идея программируемых сетей (Software-Defined Network, SDN) состоит в том, что функции контроля и управления выполняются не множеством сетевых устройств, а контроллером SD-WAN.

SD-WAN позволяет отказаться от сложного управления каждым сетевым устройством с помощью командной строки (Command Line Interface, CLI) в пользу централизованного: контроллер SD-WAN рассылает настройки всем устройствам с помощью специального протокола (SNMP, NETCONF и т. п.) и отслеживает состояние маршрутизаторов и каналов связи.

ЧЕМ ЭТО УДОБНО?

Современные маршрутизаторы обладают богатой функциональностью (которая, кстати, во многом определяет их немалую стоимость). Вот только использовать большинство функций, как правило, не удается: чем масштабнее сеть, чем больше различных узлов, тем сложнее конфигурация сетевого оборудования и обеспечение ее согласованности. Отсюда естественным образом следуют два эмпирических факта: чем больше узлов, тем проще настройки; чем сложнее настройки, тем реже они меняются.

В то же время гибкая адаптация сети, необходимая для поддержки разнообразных сервисов, требует как сложных настроек, так и быстрого их изменения.

Представьте, что крупной организации надо провести важное совещание руководителей всех филиалов по видео-конференц-связи. На несколько часов нужно предоставить максимальный приоритет и гарантировать пропускную способность в каналах, достаточную для трафика реального времени.

Или представьте: у той же организации наступает сезон отчетов, когда ответственные подразделения из филиалов загружают на центральные серверы огромные файлы данных. В этом случае нужно выделить необходимую полосу и обеспечить минимум потерь для трафика соответствующих приложений.

Но многие ли сетевые администраторы решатся внести временные изменения в конфигурацию, если речь идет о десятках или даже сотнях устройств? Контроллер SD-WAN позволяет легко создавать настройки маршрутизаторов любой сложности вне зависимости от масштабов сети, а менять их можно очень просто и быстро в соответствии с текущими потребностями.

Чтобы выполнить задачи, описанные выше, администратору сети SD-WAN достаточно заранее создать соответствующие профили качества обслуживания с использованием удобного графического интерфейса. При необходимости он может применить их ко всем нужным устройствам нажатием одной кнопки. Контроллер SD-WAN переведет данные из шаблонов на язык понятных сетевым устройствам команд, отправит эти настройки на маршрутизаторы, обеспечит их непротиворечивость и совместимость с другими настройками — как данного маршрутизатора, так и остальных устройств в сети.

СТРАХОВКА ОТ ОШИБОК

От сетевых инженеров, впервые услышавших про SD-WAN, часто приходится слышать именно этот вопрос: что произойдет, если при настройке маршрутизатора через контроллер SD-WAN будет допущена ошибка?

При настройке сетевых устройств через интерфейс командной строки вероятность ошибки была весьма велика. Так, конфигурационный файл граничного маршрутизатора может содержать более 1000 команд, поэтому при изменении его «вручную» есть по меньшей мере 1000 шансов ошибиться.

Конечно, не все опечатки приведут к потере связи, но ошибки в настройках QoS, маршрутизации и политик информационной безопасности могут дорого обойтись.

Использование в контроллере SD-WAN удобного графического интерфейса и шаблонов позволяет свести вероятность погрешностей к минимуму. Например, для описанных выше сценариев с выделением требуемой полосы определенному типу трафика вводить десятки строк команд уже не понадобится — достаточно выбрать из списка нужное приложение и указать желаемую пропускную способность. Применение команд и контроль за их согласованностью на всех сетевых устройствах возьмет на себя интеллектуальная функция контроллера.

С КАКИМИ ТИПАМИ КАНАЛОВ МОЖЕТ РАБОТАТЬ SD-WAN?

В концепцию SD-WAN изначально была заложена поддержка любых каналов: L3VPN, Интернет, LTE и др. Во-первых, это удобно с точки зрения мониторинга: администратор сети видит на панели управления контроллера актуальное состояние всех каналов вне зависимости от их типа. Но это не самое большое преимущество.

Стоимость каналов Интернета постоянно снижается, а доступная полоса пропускания увеличивается. Сейчас за ту же цену можно арендовать канал с пропускной способностью в 10 раз больше, чем 10 лет назад, и зачастую по качеству он не будет уступать выделенному L3VPN, для которого оператор предоставляет гарантированный уровень обслуживания. Поэтому с появлением SD-WAN стали возможны отказ от аренды дорогих каналов L3VPN и использование каналов Интернета от разных провайдеров с сохранением необходимого качества обслуживания (см. рис. 1).

Сеть SD-WAN постоянно отслеживает состояние всех каналов по различным параметрам и переключает трафик критичных приложений с канала на канал, если качество связи оказывается ниже заданного порога.

ZTP: ВКЛЮЧИЛ И РАБОТАЙ

Несмотря на бурное развитие средств удаленного администрирования, до недавнего времени начальной настройкой маршрутизаторов в большинстве случаев

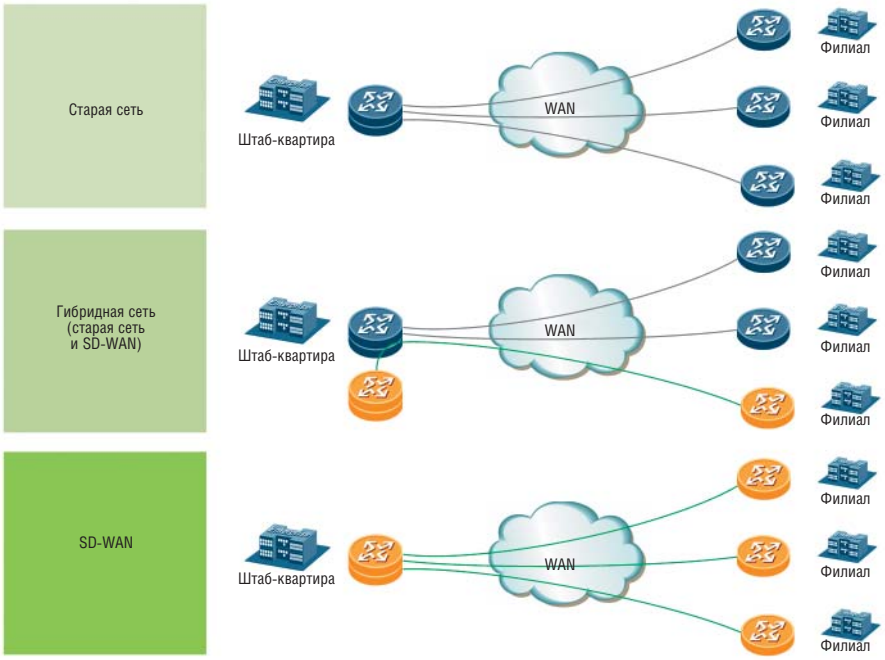


Рис. 3. Наиболее рациональный сценарий — переход на SD-WAN по мере добавления в сеть новых узлов или по ходу плановой замены оборудования на существующих

занимался квалифицированный сетевой инженер. Он должен был находиться рядом с устройством на расстоянии не более 3 м (стандартная длина кабеля для подключения к служебному COM-порту), то есть иметь локальный доступ к оборудованию.

Представьте, что маршрутизаторы доставлены морем во Владивосток для установки по всему Дальнему Востоку или Сибири, а специалисты находятся в Москве или Санкт-Петербурге. Что в этом случае делать? Отправлять оборудование к инженерам или наоборот? Возможны, конечно, и другие варианты, но удобнее всего использовать Zero Touch Provisioning.

При использовании ZTP сетевые устройства любых размеров и функциональности вводятся в строй так же просто, как домашние интернет-центры plug-and-play. Производители по-разному реализуют функцию ZTP, но все стремятся сделать так, чтобы для запуска маршрутизатора надо было всего лишь подключить кабель и подать питание. Контроллер SD-WAN автоматически настроит маршрутизатор в соответствии с параметрами, которые определил администратор для данного узла (группы узлов), но сначала маршрутизатор должен получить информацию для связи с контроллером.

Каждый вендор решает эту задачу по-своему. Например, маршрутизаторам SD-WAN Riverbed начальные настройки передаются через сервер DHCP или с помощью флешки, которая отправляется на объект монтажа вместе с маршрутизатором. А Huawei предлагает следующий способ: с помощью электронной почты или SMS монтажник отправляет контроллеру идентификатор устройства (серийный номер) и в ответ получает письмо с гиперссылкой. Затем достаточно подключиться к маршрутизатору через интерфейс управления и щелкнуть по этой ссылке. Сетевое устройство автоматически получит от контроллера все необходимые настройки (см. рис. 2).

Есть и другие реализации, но все они призваны максимально упростить ввод в строй нового оборудования.

ПЕРЕХОД НА SD-WAN

Стратегия перехода на SD-WAN определяется текущим состоянием сети (архитектурой, используемым оборудованием) и желаемой реализацией SD-WAN. Интуитивно кажется, что проще внедрять решение SD-WAN того производителя, чья техника уже используется в сети. Однако старые модели чаще всего не будут поддерживать управление через новый, пусть и того же производителя, контроллер SD-WAN. Кроме того, переход на SD-WAN может оказаться хорошим поводом приобрести оборудование другой марки, если к существующему накопилось много претензий.

Сегодня любой контроллер SD-WAN может управлять устройствами только того же производителя. К такому развитию событий нужно быть готовым, но это не повод отказываться от тех удобств, которые приносит внедрение SD-WAN. Как показывает история внедрения сетей SDN в центрах обработки данных, между появлением рабочих проприетарных решений и выработкой единого стандарта по управлению устройствами могут пройти годы.

Наиболее рациональный сценарий — переход на SD-WAN по мере добавления в сеть новых узлов (маршрутизаторов) или по ходу плановой замены оборудования на существующих узлах (см. рис. 3). На промежуточной стадии часть устройств будет оставаться под «ручным» управлением, а новые — под управлением контроллера SD-WAN. При этом обмен трафиком и маршрутной информацией между маршрутизаторами будет происходить как обычно. Чем больше устройств окажется под управлением контроллера SD-WAN, тем быстрее и удобнее станет управление сетью. **LAN**

Промышленный интернет. Сети на производстве

Удешевление производства сенсоров и развитие аналитических приложений создали предпосылки для зарождения Промышленного интернета. Однако его появление было бы принципиально невозможным без организации информационного обмена между функциональными доменами и другими компонентами систем Промышленного интернета, включая пользователей и промышленные установки. Именно обеспечению этого информационного обмена и должны способствовать современные промышленные сети.

Андрей Гречин,
системный архитектор, Cisco

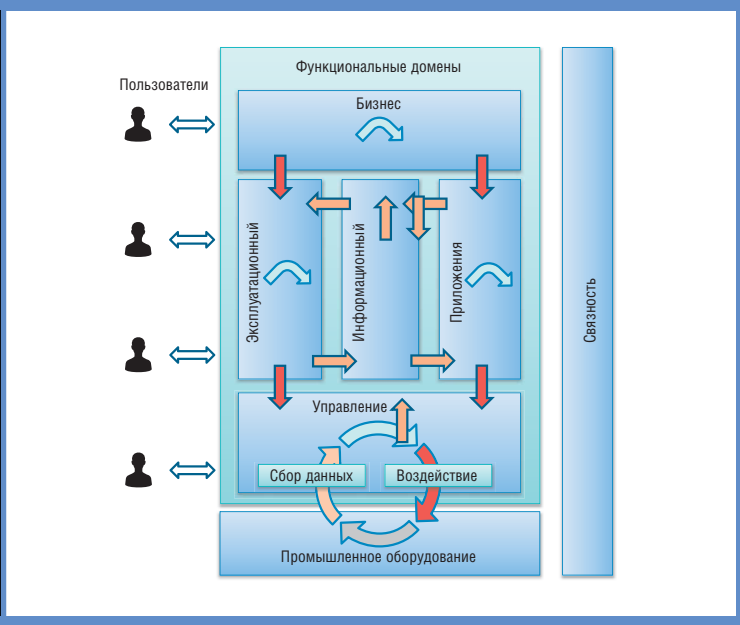


Рис. 1. Функциональные домены

АРХИТЕКТУРА ПРОМЫШЛЕННОГО ИНТЕРНЕТА

В соответствии с архитектурой Industrial Internet Reference Architecture, разработанной Industrial Internet Consortium, система Промышленного интернета подвергается декомпозиции на функциональные домены (см. рис. 1). Они образуют важные типовые строительные блоки (частично уже существующие на предприятиях), которые могут применяться в различных отраслях. Каждая система Промышленного интернета будет содержать по крайней мере следующие функциональные домены:

- **Управление** — набор функций уровня АСУ ТП (взаимодействие с промышленным оборудованием, чтение данных, создание управляющих команд в соответствии с логикой контуров управления и т. п.).
- **Эксплуатационный** — набор функций для управления конфигурацией, мониторинга и оптимизации одной или нескольких подсистем доменов управления.
- **Информационный** — набор функций для сбора данных из разных доменов (прежде всего из доменов управления), а также для преобразования, сохранения и анализа этих данных с целью получения информации более высокого уровня о системе Промышленного интернета (технологии Data Lake и т. п.).
- **Приложения** — реализация логики приложений, выполняющих определенные бизнес-функции. Укрупненный уровень управления всей системой Промышленного интернета в долгосрочной перспективе и глобальном масштабе. Этот домен может включать в себя логику приложения, правила, модели и т. д. Его можно представить и как домен аналитики.
- **Бизнес** — обеспечение сквозных операций системы Промышленного интернета путем их интеграции с традиционными или новыми типами подсистем управления бизнес-процессами, планирования и т. п. Примерами таких систем могут быть ERP, CRM, PLM, MES, HRM, управление материальными ценностями, управление проектами и многие другие.

Функциональные домены могут подвергаться дальнейшей декомпозиции в зависимости от конкретных требований к системе Промышленного интернета. В результате какие-то отдельные функции могут быть добавлены, исключены, объединены друг с другом или выделены из уже имеющихся.

Использование различных сетевых технологий позволяет обеспечить связность, то есть возможность обмена данными между участниками как в пределах самого функционального домена, так и между функциональными доменами в одной или разных системах Промышленного интернета. Обмен данными в рамках одного домена может состоять из опроса датчиков, сообщений о событиях и изменениях состояния, аварийных сигналов, команд, обновлений конфигурации и т. п. Обмен между доменами может содержать команды по результатам аналитической обработки информации из нескольких доменов, автоматически создаваемых планов обслуживания оборудования и т. п.

Фактически целью Промышленного интернета является обеспечение бесшовного обмена информацией между различными доменами и отраслями. Однако за долгие годы предшествующего развития для каждого домена были разработаны отдельные наборы сетевых технологий и протоколов, предназначенные для решения узкого круга задач. Кроме того, чтобы сохранить сделанные инвестиции и ускорить инновации, при внедрении систем Промышленного интернета практически всегда предусматривается интеграция существующих систем с новыми технологиями, из-за чего предложить универсальное решение невозможно.

В таких условиях вопросы совместимости будут актуальны для всех уровней стека Промышленного интернета, даже в рамках одного домена. Например, на канальном уровне могут возникнуть проблемы объединения нескольких сегментов Ethernet, если при их построении использовались фирменные расширения протоколов, поддерживаемых в оборудовании разных производителей. На уровне фреймворка потребуется не только преобразовать промышленные протоколы, но и изменить формат данных (см. таблицу).

Если все домены и отрасли, использующие разные сетевые технологии, попытаться интегрировать друг с другом напрямую, то это приведет к образованию полносвязной схемы с количеством связей $N \times (N-1)/2$ и, как следствие, к существенному усложнению архитектуры.

Для обеспечения полной связности в рамках одного функционального домена нужно выбрать основной

Модель стека Промышленного интернета	Модель OSI (ISO/IEC 7498)	Концептуальная совместимость уровней
Фреймворк	7. Прикладной	Синтаксическая совместимость: структурированные типы данных, передаваемые между конечными узлами. На этом уровне используется общий протокол для обмена данными; структура данных однозначно определена.
	6. Представительский	
	5. Сеансовый	
Транспортный	4. Транспортный	Техническая совместимость: биты и байты, передаваемые между конечными узлами, с использованием однозначно определенного протокола.
Сетевой	3. Сетевой	Сетевая совместимость: IP-пакеты, передаваемые между конечными узлами, которые могут находиться в разных сегментах.
Канальный	2. Канальный	Цифровые кадры между конечными узлами в одном сегменте.
Физический	1. Физический	Модуляция аналоговых сигналов между конечными узлами.

Соответствие уровней взаимодействия систем Промышленного интернета и модели OSI

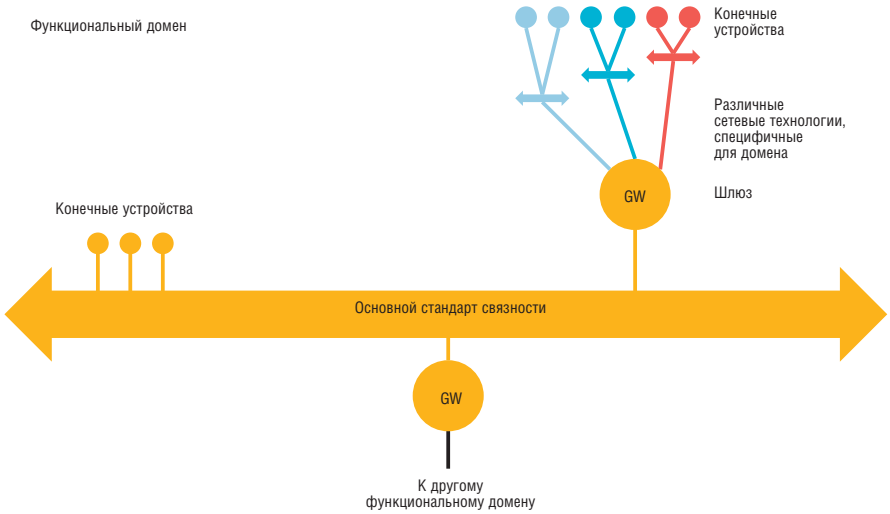


Рис. 2. Подключение различных сетевых технологий в рамках одного домена

стандарт, который должен удовлетворять всем существенным требованиям для данного домена (см. рис. 2). Подключение разнообразных технологий связи (различные варианты Ethernet, беспроводные технологии Wi-Fi, LoRaWAN, LTE и пр.) будет выполнять шлюз. Шлюзы могут обеспечивать дополнительные сервисные функции по преобразованию протоколов прикладного уровня, изменяя структуру данных, и выполнять первичную локальную обработку данных с использованием технологии туманных вычислений, рассмотренную далее. Шлюзы будут также применяться для связи между теми доменами, где используются разные основные стандарты (см. рис. 3).

Подобный подход позволяет существенно улучшить совместимость и масштабируемость по сравнению с полносвязной моделью.

ВЗАИМОДЕЙСТВИЕ ПОДРАЗДЕЛЕНИЙ

Для успешного внедрения систем Промышленного интернета очень важны налаженные коммуникации между различными подразделениями предприятия, отвечающими за поддержку разных доменов.

У производственных и ИТ-подразделений представления о связности и бесшовной интеграции могут существенно различаться. У ИТ-подразделений зона интереса обычно ограничивается сетевым уровнем модели OSI и ниже. Производственные подразделения, отвечающие за поддержку и развитие АСУ ТП в целом, большее внимание уделяют информационному обмену на верхних уровнях, где неизбежно будут возникать проблемы совместимости с унаследованными системами и другими доменами Промышленного интернета.

Оба типа подразделений могли бы сотрудничать в совместных проектах — например, таких как внедрение принтеров или обслуживание промышленных компьютеров. Но, к сожалению, эти и без того достаточно редкие возможности зачастую игнорируются. Обычно поводом для обращения к коллегам служит какая-либо проблема, требующая незамедлительного решения, — например, инцидент информационной безопасности, сбой системы или незапланированный простой. Недостаток взаимодействия и взаимопонимания между двумя командами зачастую приводит к невозможности разработки инновационных решений.

В условиях высокой конкуренции и низких цен на энергоносители владельцы предприятий вынуждены искать новые решения, которые в большинстве случаев находятся на стыке промышленных и ИТ-технологий. Чтобы их внедрить,

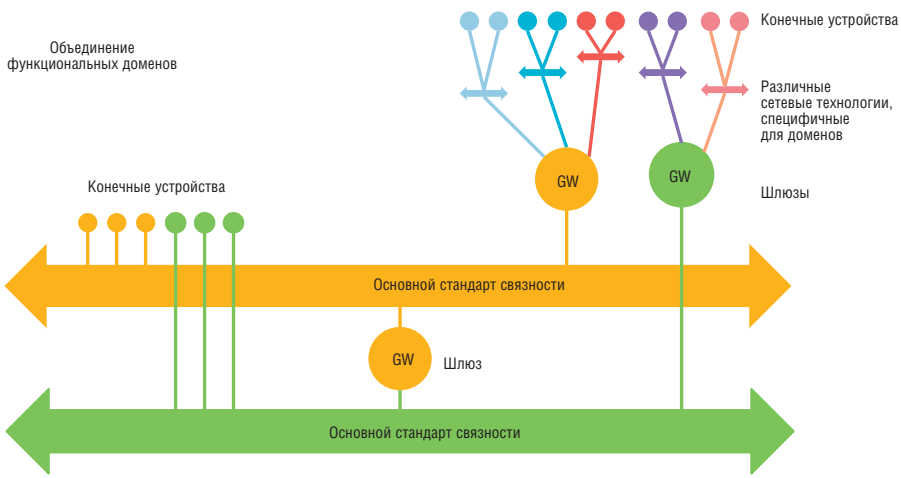


Рис. 3. Интеграция нескольких функциональных доменов

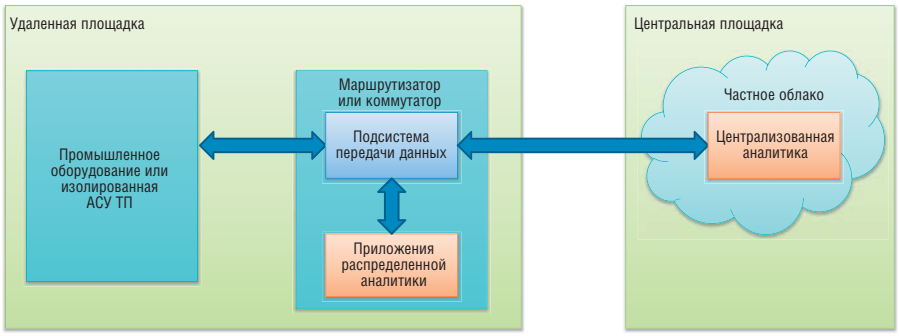


Рис. 4. Организация туманных вычислений (распределенная аналитика)

необходимо кардинальное изменение подхода к организации взаимодействия подразделений.

Производственные предприятия уже начинают заниматься адаптацией своих процессов, технологий и бизнес-моделей. Самые передовые компании и во время кризиса упорно работают над тем, чтобы получить конкурентное преимущество и максимизировать прибыль, повышая эффективность работы. Именно они и будут возглавлять цифровую трансформацию.

Очевидно, что специалистам промышленных и ИТ-подразделений, работающим в отрасли, совсем скоро придется реализовывать новые, куда более сложные проекты. Работа над ними потребует более тесного взаимодействия и поддержки со стороны руководства.

Дальновидные руководители производственных подразделений признают, что из большого объема данных, которые они уже сейчас собирают и используют, можно извлечь дополнительную ценность для предприятия. Но для этого их коллеги из ИТ-подразделений должны сделать данные значимыми и доступными для использования во всей организации, а кроме того, помочь интегрировать их в бизнес-системы, прежде всего в инструменты планирования ресурсов предприятия (ERP) и управления производственными процессами (MES).

В то же время ИТ-подразделения хотят максимально полно реализовать потенциал цифрового предприятия — от улучшения цепочки поставок до внедрения инноваций и минимизации простоев. Однако для этого им нужны специальные знания и поддержка профессионалов, которые понимают и контролируют производственные процессы и оборудование.

Вот почему старый формат взаимодействия подразделений, который часто ограничивался инфраструктурными проектами, должен уступить место более мощным и продуктивным альянсам. Прошло время, когда производственные и ИТ-команды всего лишь реагировали на инциденты. Они должны взять на себя ключевую роль в осуществлении преобразований на своих предприятиях и помогать бизнесу использовать новые возможности, делая его более конкурентоспособным, эффективным и безопасным.

УСКОРЕННОЕ ПРИНЯТИЕ РЕШЕНИЯ БЛАГОДАРЯ ТУМАННЫМ ВЫЧИСЛЕНИЯМ

Сегодня технологии автоматизации и недорогие сенсоры позволяют производственным предприятиям собирать данных больше, чем когда-либо. Однако ценность представляют не сами данные, а уточненные на их основании управленческие или производственные решения. Справедливость данного утверждения особенно очевидна при эксплуатации распределенных производственных систем, когда централизация АСУ ТП может привести к увеличению задержки принятия решения или другим потенциальным проблемам.

Нередко системы АСУ ТП не способны предоставить собираемые данные другим системам предприятия в реальном масштабе времени, в том числе потому, что это делается централизованно, в зависимости от доступности каналов связи. Кроме того, используемые протоколы и форматы данных могут не поддерживаться в других подсистемах в рамках одного домена или разных доменов.

Именно поэтому производственные подразделения рассматривают возможность использования туманных вычислений, благодаря которым все заинтересованные системы или подразделения могут получить доступ к критически важным данным на уровне промышленной площадки в реальном времени (см. рис. 4). В результате ускоряется принятие решений, повышается уровень безопасности, предотвращаются дорогостоящие простои, а также исключаются проблемы совместимости различных сетевых технологий, протоколов и форматов передаваемых данных.

ИТ-подразделения тоже получают существенные преимущества от использования технологий туманных вычислений.

- Повышается масштабируемость системы:
  - данные, чувствительные к задержкам, могут анализироваться максимально близко к их источнику;
  - менее критичные данные могут передаваться на промежуточный хост и использоваться для операционной статистики;
  - наименее критичные данные можно отправить в частное облако для ретроспективного анализа и хранения.
- Функции хоста для туманных вычислений могут быть реализованы на сетевом оборудовании промышленной площадки (например, маршрутизаторе или коммутаторе Ethernet), что устраняет необходимость поддержки нескольких устройств.
- При необходимости реализуется гарантированная доставка данных, в ходе которой передача осуществляется по резервному каналу, или они сохраняются и передаются после восстановления канала связи.
- Требования к пропускной способности и качеству канала связи снижаются.

Фактически туманные вычисления представляют собой одну из сервисных

функций шлюзов подключения к другим доменам или сетевым сегментам, описанным выше в архитектуре Промышленного интернета.

Преимущества такого подхода можно продемонстрировать на примере японской компании Mazak, которая одной из первых внедрила туманные вычисления для поддержки своей операционной деятельности. Этот производитель и оператор многофункциональных роботизированных обрабатывающих станков, распределенных по всему миру, совместно с другими компаниями разработал решение SmartBox. При его использовании на Ethernet-коммутатор, который располагается рядом со станком, загружается специальное программное обеспечение для туманных вычислений. В созданном решении поддерживается протокол MTConnect для сбора большого объема данных о производительности станка (вибрация, температуры, уровни эксплуатационных жидкостей и др.) и для анализа информации в реальном времени. Его внедрение позволило перейти к модели обслуживания оборудования по фактическому состоянию и повысить его загрузку более чем на 10%.

БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

Сейчас уже трудно представить, как может быть реализована концепция Промышленного интернета без беспроводной связи. Промышленные установки, датчики и ПЛК, а также платформы аналитики и вспомогательные технологии подключаются с помощью беспроводных технологий и становятся более эффективными за счет появившейся мобильности. Но до недавнего времени проекты по развертыванию беспроводных сетей на предприятиях не всегда заканчивались успехом.

Условия эксплуатации оборудования на разных предприятиях сильно различаются: при большом количестве металлоконструкций затруднено распространение радиоволн, а при неблагоприятных условиях окружающей среды установленное оборудование подвергается воздействию таких внешних факторов, как пыль, влажность, температура, вибрация. Кроме того, руководители производственных подразделений скептически оценивали возможность поддержки промышленной беспроводной сетью достаточного количества устройств, требуемой пропускной способности, контролируемых сетевых задержек и безопасности, необходимых для критически важных приложений. Поэтому предприятия десятилетиями развертывали повсюду десятки километров кабеля, расходуя немало времени на проектные работы, согласования, строительство сопутствующей инфраструктуры. В конечном счете такие проекты оказывались чрезвычайно затратными.

Однако за последние несколько лет в развитии беспроводных технологий были достигнуты большие успехи. Повышенная отказоустойчивость делает беспроводную связь в промышленных условиях более доступной и практичной, чем когда-либо прежде, вместе с тем ускоряется процесс развертывания.

Новая промышленная беспроводная сеть может изменить к лучшему существующие процессы. Она обеспечивает большую гибкость и адаптируемость при удаленном мониторинге и изменении конфигурации производственных линий. В то же время беспроводная сеть может привести к значительной экономии затрат. Согласно оценке Control Engineering, «беспроводная сеть (на промышленном предприятии) может быть в 10 раз дешевле кабельной инфраструктуры, обеспечивая при этом большую гибкость, мобильность сотрудников, инструментов и оборудования, а также меньшее время обслуживания и устранения неполадок».

Для успешного внедрения беспроводных сетей производственные и ИТ-подразделения должны тесно сотрудничать. Только при таком условии можно рассчитывать на появление новых возможностей. Для ИТ это снижение затрат, ускорение поиска неисправностей, увеличение пропускной способности канала для поддержки голосовых и видеоприложений. А для производственных подразделений — быстрая адаптация ИТ-решений к производственным потребностям, повышение качества выпускаемой продукции и снижение продолжительности запланированных и незапланированных простоев.

Выбор конкретных технологий по-прежнему зависит от решаемых задач. Например, для подключения датчиков на большом удалении (более 10 км) с использованием нелицензируемых частот может использоваться технология LoRaWAN. Она позволяет реализовывать двухсторонний обмен данными, передавать информацию об изменении состояния датчика (контролируемых параметров), а также определять его местоположение без использования GPS. Благодаря адаптивной скорости передачи информации датчики могут длительное время работать от встроенных миниатюрных батарей. А большой выбор готовых датчиков и компонентов для создания новых облегчает адаптацию этой технологии к нуждам заказчика.

Решения на базе традиционных технологий Wi-Fi привлекательны широкой поддержкой Wi-Fi на различных устройствах и инструментах. Однако внедрение сети Wi-Fi на предприятии требует более осторожного подхода, чем любой другой беспроводной технологии. Прежде всего это связано с тем, что для многих будет велик соблазн использовать стандартную Wi-Fi-инфраструктуру и подходы к ее построению для передачи трафика промышленных приложений, не обеспечив необходимой приоритизации, поиска и выявления источников интерференции, а также автоматической перенастройки сети. Большим подспорьем для заказчиков являются руководства по внедрению, разработанные совместно с компаниями — производителями компонентов АСУ ТП, где детально описывается протестированное и поддерживаемое всеми заинтересованными вендорами решение.

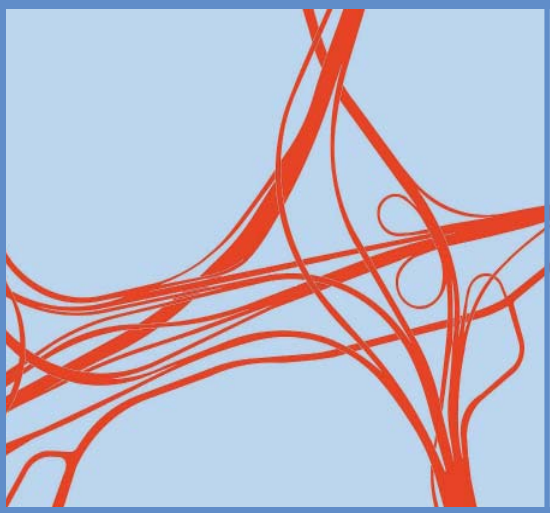
В сфере Wi-Fi-оборудования постоянно предпринимаются усилия по созданию специальных расширений для промышленного применения. Одним из примеров такой работы является реализация протокола Parallel Redundancy Protocol (PRP) на Wi-Fi оборудовании, в соответствии с которым трафик пересылается через два параллельных беспроводных соединения для повышения отказоустойчивости, снижения вариации задержки и облегчения роуминга.

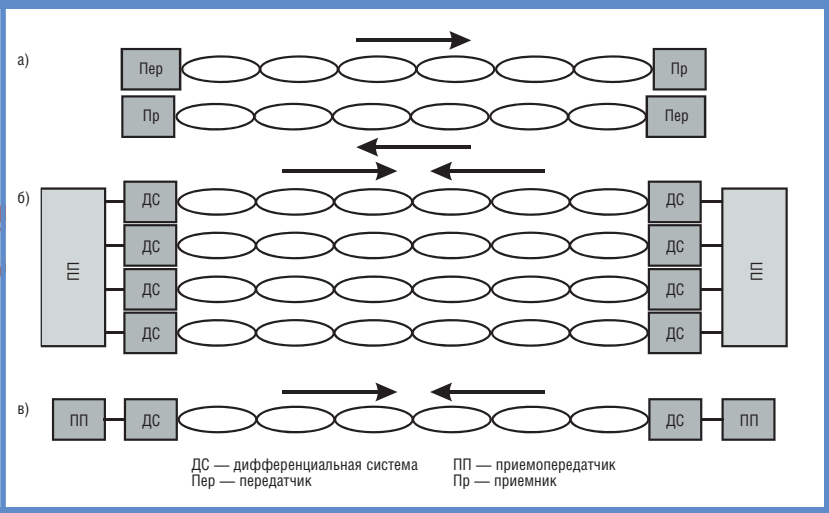
Внедрение беспроводной сети на предприятии создает большой запас для последующего развертывания таких приложений, как отслеживание местоположения мобильного оборудования и сотрудников, создание мобильных рабочих мест, в том числе подключение носимой электроники (камеры и т. п.). LAN

Однопарный Ethernet: первые шаги и перспективы

В современном легковом автомобиле среднего класса насчитывается около 50 оконечных сетевых устройств в виде оснащенных микроконтроллерами датчиков различных физических величин и исполнительных элементов, а в тяжелых грузовиках их и того больше — в среднем около 140. Перевод всех подключений на единый стандарт весьма перспективен с коммерческой точки зрения ввиду высокой емкости рынка. Разработанные IEEE спецификации на однопарный Ethernet призваны заменить популярные в настоящее время шины CAN, FlexRay, MOS и LVDS.

Андрей Семенов,
директор по развитию СУПР, профессор МТУСИ





Варианты организации связи на интерфейсах Ethernet различных разновидностей:
а — Fast Ethernet; *б* — 1G Ethernet; *в* — 100Base-T1 и 1000Base-T1

Современные информационно-коммуникационные системы (ИКС) развиваются достаточно быстро по ряду магистральных направлений. Наиболее значимы среди них следующие:
- Интернет вещей (Internet of Things, IoT);
- системы промышленного назначения;
- облачные вычисления.

Если первые два можно рассматривать как результат эволюционного распространения на новую область уже отработанной ранее техники и подходов к ее использованию, то переход на модель облачных вычислений обеспечивает выход на качественно новый уровень информационной поддержки пользователя. Это происходит потому, что применение подобной схемы значительно улучшает:
- надежность хранения данных за счет выполнения ряда специальных требований, касающихся организации их записи, обеспечения конфиденциальности доступа и защиты от физического уничтожения при возникновении стихийных бедствий, техногенных катастроф, актов терроризма и т. д.;
- качество отклика на поступающий пользовательский запрос, что выражается не только в его быстром формировании, но и в наращивании глубины переработки доступного первичного материала благодаря подключению большего количества ресурсов и организации процедур параллельной обработки.

ФИЗИЧЕСКИЙ УРОВЕНЬ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Нижний физический уровень ИКС реализуется с использованием двух главных подходов, в основу которых положены кабельные и беспроводные решения. В ряде случаев разработчик системы комбинирует их.

Беспроводная техника представлена системами радиосвязи Wi-Fi и беспроводной оптикой. Другие известные и доведенные до практической реализации решения наподобие Li-Fi и Beamcaster в силу различных причин внедряются в единичных случаях. Беспроводная передача используется преимущественно на нижних уровнях структуры ИКС, что обусловлено специфическими ограничениями, в большей или меньшей степени проявляющимися у любого из этих решений: сложность достижения высоких скоростей обмена данными, слабая помехоустойчивость, низкая стойкость к перехвату передаваемой информации, возможность передачи только в условиях прямой видимости и сильная зависимость от погодных условий (системы беспроводной оптики). В результате беспроводная техника получила распространение только в нишевых областях, где значимо проявляются два главных ее достоинства:
- высокая скорость развертывания;
- возможность обеспечения связи с подвижными объектами.

Во всех прочих ситуациях кабельные решения оказываются безальтернативными.

ОСОБЕННОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ КАБЕЛЬНЫХ СИСТЕМ

В качестве среды передачи при организации информационного обмена между точками A и B может быть использовано около десятка основных разновидностей кабелей. Однако с учетом технико-экономической эффективности массовое применение получили преимущественно волоконно-оптическая и симметричная витопарная техника. Другие возможные варианты, и в первую очередь довольно популярные еще в начале 90-х годов прошлого столетия коаксиальные кабели, а также силовая проводка встречаются заметно реже, в основном это узкие нишевые области.

Для кабельных решений, предназначенных для реализации проектов ИКС, справедливы несколько основных постулатов:
- четкое разделение «зон ответственности» основных разновидностей кабелей: волоконная оптика является основным средством передачи данных на большие расстояния, а для малых используются кабели из витых пар;
- симметричные кабели содержат четыре пары проводов с парной скруткой (четверочная скрутка встречается только в полевых шинах систем промышленной автоматизации, а объемы установки многопарных изделий заметно уступают расходу четырехпарных);
- основным типом соединителя служит 8-контактный разъем модульного типа (стандартизованные GG45 и Tera применяются крайне редко).

Указанная техника позволяет достаточно эффективно с экономической точки зрения решить основную массу задач, в том числе по обеспечению информационного обмена с заданной скоростью в реальном масштабе времени.

Важное значение для реализации проектов ИКС имеет тот факт, что кабельная техника и используемое при работе с ней коммутационное оборудование выпускаются многими производителями и обладают свойством модульности и взаимозаменяемости, чему способствует достигнутый уровень стандартизации. Кроме того, глубоко проработана технология установки и доступны различные инструменты, которые ускоряют процесс инсталляции и делают его менее трудоемким. Качество монтажа можно достаточно точно проконтролировать прямо на объекте с помощью удобных в работе полевых кабельных сканеров.

Все это обеспечивает высокую скорость реализации новых проектов и расширение ИКС на уже существующих объектах при сравнительно низкой стоимости элементной базы и монтажа.

КАБЕЛЬНЫЙ ETHERNET НА ТРАНСПОРТЕ

В основе современных ИКС — пакетная передача информации и использование единого формата кадров Ethernet, что позволяет добиться высокой результирующей технико-экономической эффективности. Достоинство такого подхода состоит в возможности создания прозрачной информационной структуры на всех уровнях системы.

Все эти преимущества можно использовать в новых областях, что позволит расширить сферу применения имеющихся технических средств. Одной из перспективных областей внедрения становятся бортовые ИТС различных транспортных средств: поездов, судов, самолетов, автобусов, трамваев и автомобилей. Частично данный потенциал уже реализован в процессе создания информационных систем и сервисов доступа в Интернет для пассажиров. Для этого использовалась традиционная техника, адаптированная к более жестким условиям эксплуатации. Так, в частности, для обеспечения гигабитных скоростей были созданы 8-контактные соединители M12, ранее доступные только в двухпарном варианте.

Однако для видеонаблюдения, диагностики и управления отдельными агрега-

тами современных автомобилей пока применяются преимущественно частные фирменные решения. Переход на единую технологическую платформу весьма перспективен с коммерческой точки зрения, так как емкость рынка достаточно велика. Согласно оценкам IEEE, в современном легковом автомобиле среднего класса имеется около 50 оконечных сетевых устройств в виде оснащенных микроконтроллерами различных датчиков исполнительных элементов, а в тяжелых грузовиках их еще больше — до 140. Всего в транспортных средствах функционируют около 270 млн подключаемых к сети устройств, причем их количество будет ежегодно удваиваться.

С учетом этих обстоятельств именно автомобильная отрасль стала инициатором проведения работ по созданию и стандартизации однопарного Ethernet, который для привлечения внимания и лучшего запоминания получил название «усеченный Ethernet» (Reduced Twisted Pair Ethernet).

Данная технология рассматривается в качестве замены довольно популярных в настоящее время шин CAN, FlexRay, MOST, LVDS.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ «АВТОМОБИЛЬНОГО» ETHERNET

Существующие решения Ethernet могут быть доведены до требуемого уровня эффективности путем глубокой модернизации созданного ранее оборудования и его целенаправленной адаптации на новую область. Два ключевых недостатка существующей 4-парной техники — высокая стоимость (по объемам затрат проводка в современном автомобиле является третьей статьей расходов после двигателя и шасси) и неудовлетворительные массогабаритные показатели — преодолеваются переходом на однопарное исполнение линейной части бортовой ИКС.

Определенное значение имеет и то, что за счет некоторого уменьшения массы сокращаются расходы топлива и снижается экологическая нагрузка на окружающую среду.

Платой за это становится ограничение гарантированной дальности действия. В неэкранированном тракте типа А она составляет 15 м, однако переход на экранированную технику дает возможность организовать тракты типа В, максимальная протяженность которых составляет уже 40 м. Для автомобильных бортовых систем этого вполне достаточно.

Работы по стандартизации проводились в рамках двух проектов. Результаты одного, IEEE 802.3bp, утверждены 30 июня 2016 года. Его главной целью была разработка гигабитного варианта сетевого интерфейса, который в соответствии с правилами формирования кода, принятого IEEE, описывается аббревиатурой 1000Base-T1. Другой, менее скоростной 100-мегабитный вариант 802.3bw, введенный в действие годом ранее, обозначается как 100Base-T1.

От многопарных вариантов Ethernet их однопарные функциональные аналоги отличаются схемой организации связи, что показано на рисунке.

Для новой области применения как никогда актуально дистанционное питание оконечных устройств по централизованной схеме. С учетом этой особенности было разработано оборудование для дистанционного питания по одной паре IEEE 802.3bu. Данная технология известна как Power over Data Lines (PoDL). Мощность потребления приемника при этом ограничивается 50 Вт.

Результатом усилий промышленности стало появление наборов микросхем, интерфейсов на их основе, а также кабелей и соединителей. Они выпускаются несколькими производителями и рассчитаны на эксплуатацию в автомобилях, в том числе при жестких внешних условиях от –40 до +85°С, и в подкапотном пространстве, где температура может достигать +150°С.

Активные микроэлектронные изделия бортовой ИКС по своим характеристикам гармонизированы с остальной автомобильной электроникой. В частности, в них предусмотрен переход в «спящий» режим с током потребления не более 100 мкА, а время возврата в рабочее состояние, с учетом типовых параметров оборудования бортовой диагностики, составляет не более 500 мс.

Характеристики линейной части системы обеспечивают нормальное качество функционирования полнодуплексного канала связи.

ОБОРУДОВАНИЕ 1000BASE-T1

С технической точки зрения в бортовой автомобильной ИКС одинаково важны как скорость передачи, так и гарантированное время доставки сообщения, что достигается обычными для промышленного Ethernet способами путем задания приоритетов и выделения полосы пропускания. Гигабитная пропускная способность востребована только:

- при передаче сигналов телевидения высокой четкости, в том числе видеоассистента при осуществлении движения задним ходом (чтобы минимизировать время задержки, поток данных, генерируемый его камерой, не сжимается и имеет скорость до 800 Мбит/с);
- работе с навигационными системами;
- поддержке функционирования систем настройки спутниковых антенн и иных потребителей, генерирующих несжатые цифровые потоки.

Поскольку потребителей этой группы много, для их подключения к ИКС целесообразно использовать одинаковую технику, а согласование скоростей выполнять с помощью автоматической настройки.

С учетом верхней граничной частоты тракта, составляющей 600 МГц, для формирования линейного сигнала требуется применение многоуровневого кодирования.

В оборудование 1000Base-T1, к созданию которого разработчики приступили в 2012 году, изначально заложен достаточно развитый дополнительный сервис. В частности, предусмотрены следующие возможности:

- использование энергоэффективного Ethernet и переход в режим ожидания, что позволяет минимизировать разряд аккумулятора на стоянке;
- поддержка процедуры блокировки поступления искаженных данных, когда напряжение дистанционного питания отсутствует более 100 мс;
- автоматическое определение скорости передачи в формируемом канале связи.

ОБОРУДОВАНИЕ 100BASE-T1

Разработка 100-мегабитных однопарных сетевых интерфейсов велась с 2012 года на основе предварительных требований, сформулированных Open Alliance в процессе выполнения поисковых НИР. Окончательные спецификации были утверждены в октябре 2015 года. Как

и их более скоростной аналог, интерфейсы 100Base-T1 создавались для автомобильных бортовых ИКС, однако они ориентированы на использование в тех цепях, где гигабитный темп передачи является заведомо избыточным.

Техника данной разновидности называется «Ethernet для автомобилей». От гигабитного варианта она отличается, кроме меньшей скорости передачи, простотой схемы и более экономным энергопотреблением. Максимальная протяженность тракта — 15 м.

С учетом схожести 100Base-T1 и Fast Ethernet, было несложно обеспечить совместимость этого оборудования на уровне электрических сигналов. При этом, однако, функционирование возможно только в режиме полного дуплекса, а вероятность битовой ошибки не превышает 10^{-10}. Для обеспечения заданного качества передачи используется скремблирование исходного сообщения и модуляция вида PAM-3 с кодированием 3B2T, а на приемном конце поступающий сигнал обрабатывается в цифровом сигнальном процессоре DSP перед подачей на решающее устройство. Передача осуществляется в базовой полосе, для развязки направлений передачи и приема используется дифференциальная система.

Для передачи требуется кабель с параметрами Категории 5e или лучше.

ОСОБЕННОСТИ ПРОВОДКИ

Кабели и соединители для построения бортовой ИКС предлагаются в экранированном и неэкранированном вариантах. По мнению ряда аналитиков, чтобы обеспечить функционирование мощных оконечных потребителей, потребуется техника, соответствующая по меньшей мере Категории 6A.

Считается, что фокусная область применения неэкранированного оборудования с его заметно лучшими массогабаритными показателями — это легковые автомобили, где 15-метровой дальности действия вполне достаточно. Экранированные же изделия, гарантированная дальность действия которых достигает 40 м, предназначены для более габаритных автобусов, троллейбусов и грузовых автомобилей, где ограничения для суммарной массы проводов и разъемов не столь жесткие. В немалой степени они оказываются востребованы благодаря более высокой степени защиты от внешних электромагнитных помех различной природы.

Проводкой для однопарного Ethernet занимаются по обе стороны Атлантики. Американские разработчики традиционно тяготеют к неэкранированным решениям, а их европейские коллеги много внимания уделяют экранированной технике.

Для обеспечения необходимой эксплуатационной гибкости в тракте передачи предусмотрена поддержка четырех соединителей. В случае применения экранированной техники на стационарную линию приходится 36 м, остальные 4 м отведены на шнуры. Соответствующий документ разрабатывается ISO/IEC, публикация финальной версии намечена на 2018 год.

Кабель имеет традиционное 100-омное волновое сопротивление. Вне зависимости от варианта его исполнения верхняя граница рабочего частотного диапазона составляет 600 МГц. Из остальных характеристик нормируются затухание, обратные отражения SRL и межкабельное переходное затухание. С учетом рабочего частотного диапазона и принятой схемы организации связи в качестве прототипа целесообразно использовать технику Категории 6A или лучше.

Соединитель должен иметь минимальные размеры. Поэтому в разработанном компанией Harting и выпускаемом серийно соединителе HARTING T1 Industrial применен контактный блок, размеры поперечного сечения которого составляют 6,4 × 3,3 мм. Вилка подключается к розетке линейным движением. В зависимости от варианта исполнения для различных областей эксплуатации обеспечивается степень защиты IP20 или IP67.

ПРОЧИЕ ОБЛАСТИ ПРИМЕНЕНИЯ ОДНОПАРНОЙ ТЕХНИКИ

Гарантируемые сетевыми интерфейсами 100Base-T1 и 1000Base-T1 параметры дальности действия, скорости передачи, времени доставки и стоимостных показателей позволяют использовать эти устройства не только в автомобиле.

Так, для систем промышленной автоматизации и робототехники важное значение имеет возможность работы в широком температурном диапазоне. В оборудовании, применяемом для автоматизации объектов общественной и особенно жилой недвижимости, ценятся такие свойства, как небольшие габариты и гибкость кабеля, а также низкая стоимость кабельных изделий и самого контроллера.

О высоких технических и рыночных перспективах направления однопарных решений Ethernet свидетельствует запуск проекта 802.3cg по созданию интерфейса 10Base-T1 с предельной дальностью действия 1200 м. Завершение разработки соответствующих спецификаций намечено на 2018 год. Как и в случае 100- и 1000-мегабитных систем, для создания столь протяженных линий планируется использовать новые разновидности кабелей. Фокусная область применения новой техники — системы промышленной автоматизации.

Кроме того, в рамках поисковых НИР изучается возможность создания однопарных систем 2,5, 5 и 10G Ethernet. Если учесть опыт разработки 40-гигабитных систем, для однопарного 10-гигабитного варианта вполне может быть обеспечена как минимум 30-метровая дальность действия.

ЗАКЛЮЧЕНИЕ

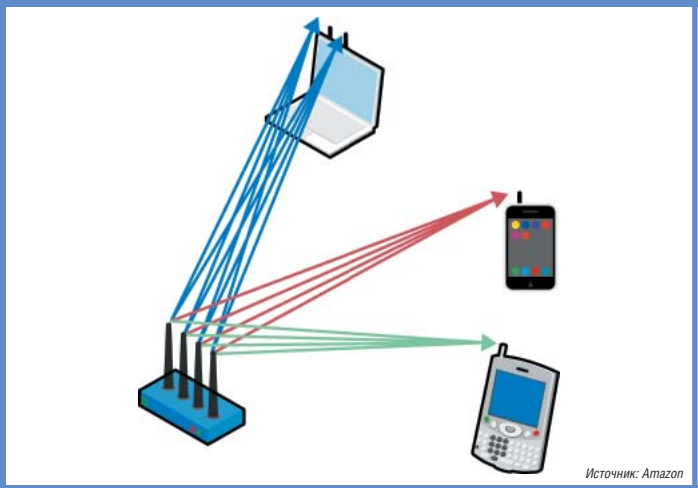
Создание однопарного Ethernet открывает возможность применения единой технологии для организации обмена данными в такой емкой области, как бортовые информационные системы современных автомобилей и иных транспортных средств. Дальность действия и исполнение аппаратной части однопарного Ethernet открывают перспективы для его внедрения в других областях, в частности в системах автоматизации зданий.

В стандартах на сетевые интерфейсы изначально предусмотрен ряд сервисов, благодаря которым заметно увеличивается практическая эффективность решения в целом. Однопарная схема имеет запас для дальнейшего совершенствования, особенно это касается увеличения дальности действия и скоростей передачи. Сохранение 100-омного волнового сопротивления не только ускоряет и упрощает разработку, но и облегчает тестирование готовых стационарных линий и трактов. LAN

Wi-Fi всякий-разный

До недавнего времени каждая очередная версия стандарта Wi-Fi была призвана заменить предшествующую. Однако задачи, решаемые с его помощью, настолько разные, что подход «один стандарт на все случаи жизни» не отвечает предъявляемым требованиям. Это отражается в разработке специфических стандартов для различных применений. И хотя скорость по-прежнему имеет значение, на первое место выходят другие факторы: емкость, стоимость, управляемость, поддержка различных приложений — от низкоскоростных подключений IoT до высокоскоростного потокового видео 4K.

Дмитрий Ганьжа,
главный редактор «Журнал сетевых решений/LAN»



Источник: Amazon

Рис. 1. В случае MU-MIMO точка доступа может осуществлять передачу сразу нескольким клиентам, благодаря чему повышается эффективность использования спектра

Источник: TP-Link

Рис. 2. При использовании всех трех диапазонов (800 Мбит/с на 2,4 ГГц, 1,733 Гбит/с на 5 ГГц и 4,6 Мбит/с на 60 ГГц) максимальная пропускная способность первого WiGig-маршрутизатора TP-Link AD7200, оснащенного четырьмя гигабитными Ethernet-портами, составляет 7,2 Гбит/с

Двадцать лет назад, в 1997 году, появился первый стандарт на Wi-Fi, обеспечивавший скромные по нынешним временам 1–2 Мбит/с. С тех пор поддерживаемая скорость возросла на три порядка и теперь составляет несколько гигабитов в секунду. А в разрабатываемых стандартах пропускную способность Wi-Fi планируется увеличить до нескольких десятков гигабит (см. таблицу). Так, стандарт 802.11ay обещает более 20 Гбит/с и, возможно, даже свыше 100 Гбит/с в диапазоне 60 ГГц.

На протяжении всего своего пути развития Wi-Fi проигрывал проводному Ethernet в скорости: все-таки радиоволны — не лучшая среда для передачи. Однако этот относительный недостаток оказался гораздо менее важным по сравнению с таким достоинством, как мобильность: Wi-Fi стал предпочтительным способом доступа в Сеть. Как сообщает Эдгар Фигуера, глава Wi-Fi Alliance, еще в 2015 году через Wi-Fi было передано более 50% интернет-трафика, а по данным Cisco, пользователи Wi-Fi и абоненты сотовой связи генерируют свыше двух третей всего сетевого трафика.

Без Wi-Fi как без рук. Этот способ передачи данных стал культурным явлением: наличие качественного беспроводного доступа теперь столь же насущная необходимость, как вода в кране или свет в розетке. Так, при выборе отеля большинство постояльцев обращают внимание на доступность Wi-Fi, и, согласно недавнему исследованию 2Europe Ltd, проведенному по заказу компании ZyXEL, его низкое качество является второй после внешнего шума причиной жалоб. Впрочем, это неудивительно, ведь 38% европейских отелей не могут обеспечить стабильный доступ в Интернет из-за того, что сеть не справляется с большим количеством подключенных устройств.

И хотя скорость по-прежнему имеет значение, при увеличивающейся плотности использования Wi-Fi, особенно в общественных местах, и растущем разнообразии применений на первое место в разработке стандартов выходят другие факторы: емкость, стоимость, управляемость, поддержка различных приложений — от низкоскоростных подключений IoT до высокоскоростного потокового видео 4K. Потребность удовлетворить разнообразные запросы находит отражение в новых стандартах. И конечно, поддержка более высоких скоростей никогда не будет лишней.

ГИГАБИТНЫЙ РУБЕЖ

Текущий уровень достижений в области беспроводных локальных сетей характеризуется стандартом 802.11ac Wave 2 — соответствующее оборудование Wi-Fi Alliance начал сертифицировать в прошлом году. По сравнению с Wave 1 скорость передачи данных на физическом уровне возросла с 1,3 до 2,3 Гбит/с в диапазоне 5 ГГц (хотя это все еще ниже специфицированного предела в 6,9 Гбит/с в стандарте IEEE на 802.11ac).

Помимо повышения скорости, была увеличена максимальная возможная ширина канала — с 80 до 160 ГГц. Теоретически это поможет облегчить передачу больших файлов. Кроме того, добавлена поддержка четвертого пространственного канала, что тоже должно способствовать повышению производительности. Расширен спектр рабочих частот в диапазоне 5 ГГц, поэтому доступных каналов стало больше. Таким образом, устройства будут меньше создавать помех друг другу.

Пожалуй, главным отличием второй волны от первой является поддержка многопользовательского множественного ввода-вывода (Multi-User Multi-In Multi-Out, MU-MIMO): на каждое устройство может направляться отдельный пространственный поток. Иначе говоря, точка доступа теперь способна осуществлять передачу данных на несколько устройств одновременно (до четырех клиентских устройств 1×1:1 MIMO в случае точки доступа 4×4:4 MIMO), что повышает эффективность использования спектра (см. рис. 1). Однако MU-MIMO в 802.11ac поддерживает трафик только от точки доступа к клиентам, возможность передачи в обратном направлении будет реализована в стандарте 802.11ax (см. следующий раздел).

В конце прошлого года появились первые устройства стандарта 802.11ad, более известного как WiGig. В данном случае теоретический максимум пропускной способности составляет 8 Гбит/с (первые выпущенные устройства поддерживают только около 4,6 Гбит/с). Однако с точки зрения функциональности новый стандарт во многом похож на своих предшественников. Его главной отличительной чертой является работа в диапазоне 60 ГГц — точнее, в интервале от 57 до 66 ГГц в зависимости от страны (в России ГКРЧ разрешила использовать весь диапазон для устройств стандарта 802.11ad).

Как известно, чем выше частота, тем сильнее затухание. Соответственно, связь возможна только в условиях прямой видимости на расстоянии до 10 м, поскольку даже одна стена становится непреодолимым препятствием для сигнала WiGig. В случае соединений точка-точка при использовании специальных антенн дальность может быть увеличена, что позволит подключать станции сотовой связи.

Благодаря доступности широкого диапазона частот 9 ГГц WiGig позволяет передавать большие объемы данных (см. рис. 2). Изначально этот стандарт разрабатывался как замена кабельного подключения, по крайней мере в пределах комнаты. В качестве перспективных приложений рассматриваются обмен файлами (соединение компьютеров с принтерами и другой периферией), потоковая передача видео с высоким разрешением, дополненная реальность и т. п.

Как и в случае с диапазоном 5 ГГц, вряд ли переход на 60 ГГц будет быстрым. Для ускорения этого процесса предусмотрена поддержка динамического переключения сеансов, то есть устройства Wi-Fi смогут динамически переключаться между стандартными диапазонами 2,4 и 5 ГГц и новым 60 ГГц. ABI Research прогнозирует, что до 2021 года будет продано 4,7 млрд устройств WiGig.

БОЛЬШИЕ НАДЕЖДЫ НА 802.11AX

Многие из выдвигаемых требований и запросов призваны удовлетворить разрабатываемый стандарт 802.11ax. Он должен будет обеспечить скорость до 10 Гбит/с в диапазоне не только 5 ГГц, но и 2,4 ГГц, что не предусмотрено в 802.11ac. Однако главным достоинством этого стандарта станут не повышение скорости и расширение диапазона, а увеличение плотности подключений. Он разрабатывается в расчете на поддержку таких ресурсоемких приложений, как потоковое видео, виртуальные частные сети и видеоконференции в гетерогенных сетях с множеством активных пользователей.

В случае проводных подключений соединений 100 Мбит/с вполне достаточно для большинства имеющихся приложений.

Между тем Wi-Fi уверенно преодолел планку 1 Гбит/с. Однако проводные сети являются коммутируемыми, тогда как беспроводные — разделяемыми. Иначе говоря, доступная полоса пропускания делится между несколькими абонентами, и каждый получает свою долю. Соответственно, проблема не столько в пропускной способности беспроводной системы, сколько в устранении возможных перегрузок и конфликтов.

Предшествующие стандарты Wi-Fi были рассчитаны на более-менее нерегулярное использование, при этом предполагалось, что трафик асимметричный: объем загрузки больше объема выгрузки. 802.11ax решает проблему высокой плотности путем пересмотра механизмов работы Wi-Fi, для чего были заимствованы некоторые лучшие практики LTE. Одна из них — использование множественного доступа с ортогональным частотным разделением (Orthogonal Frequency Division Multiple Access, OFDMA).

В случае OFDMA каждый канал делится на множество более мелких подканалов со своей частотой и до 30 клиентов могут совместно использовать канал, вместо того чтобы ждать удобного момента для передачи. В результате повышается эффективность его использования, так как абонентам не приходится конку-

Какое решение Wi-Fi выбрать?

За неполные 20 лет своей истории технология Wi-Fi проникла почти во все электронные устройства. Точки доступа теперь работают на гигабитных скоростях, научились управлять диаграммой направленности и могут обслуживать нескольких абонентов одновременно. У комитета 802.11 давно закончились буквы для обозначения новых технологий (и соответствующих рабочих групп), и он перешел на двухбуквенные наименования.

Ориентироваться в этом многообразии стандартов, подстандартов и дополнений становится все сложнее: помимо имеющихся технологий, необходимо принимать во внимание и те, которые вот-вот появятся, ведь они обещают скорость 5–10–20 Гбит/с. Но мы живем здесь и сейчас, и зачастую нас интересует более практическая задача: как выбрать решение на ближайшие пять лет, чтобы впоследствии не пожалеть об этом. Поэтому позвольте сфокусироваться на этом вопросе, не претендуя на всеобъемлемость.

Выбор стандарта: n, ac Wave 1, ac Wave 2. На данный момент при построении сети Wi-Fi нельзя полностью отказаться от стандарта n, потому что стандарты ac используются в диапазоне 5 ГГц, а значительная часть конечных устройств работает в 2,4 ГГц. Поэтому, скорее всего, новая точка доступа будет двухдиапазонной: n (2,4 ГГц) + ac Wave 1/2 (5 ГГц). В офисе есть смысл использовать ТД 802.11ac Wave 2: возможно, уже совсем скоро многие ваши коллеги будут иметь устройства с поддержкой каналов 160 МГц и режима MU-MIMO. Что касается уличных сетей, в России вряд ли удастся извлечь преимущество от реализации ac Wave 2: если повезет, на одну точку доступа вам выделят канал 20 МГц для 5 ГГц и еще 20 МГц вы займете в 2,4 ГГц, сославшись на положение об устройствах малого радиуса действия. Кроме этого, из-за жуткой помеховой обстановки в городе вы, скорее всего, предпочтете использовать направленные антенны, поэтому про MU-MIMO придется забыть.

Wi-Fi требуется инфраструктура. К каждой точке доступа должен быть проложен кабель от коммутирующей подсистемы (существующей или планируемой). В офисе это обычно витая пара, на улице — витая пара или оптика. На сегодняшний день и на ближайшую перспективу вполне достаточно гигабитных каналов: несмотря на описываемые в стандартах высокие скорости, все они являются предельным случаем и относятся к передаче данных в радиоканале. Реальный трафик через порт Ethernet гораздо меньше.

Отдельные точки доступа можно объединить по радио с помощью технологии Mesh/WDS, поэтому убедитесь в том, что эта функциональность поддерживается. Кроме того, уже на этапе планирования инфраструктуры стоит задуматься о питании. Если используемые коммутаторы не поддерживают PoE, рядом с коммутатором или точкой доступа придется разместить инжектор питания, которому потребуется розетка 220 В.

Контроллеры Wi-Fi. Контроллер Wi-Fi не описывается стандартами 802.11, поэтому на рынке представлено много различных решений. Современный контроллер выполняет две основные задачи: управление сетью Wi-Fi и ее мониторинг. Контроллер может быть реализован программно или аппаратно. Программный контроллер — это либо ПО, запускаемое на одной из точек доступа в сети (как правило, это применимо только в небольших сетях, скажем до 30 точек доступа), либо ПО, устанавливаемое на сервере. Отдельно следует отметить облачные решения: некоторые вендоры предлагают такой сервис, так что пользователям не нужно устанавливать в сети собственный сервер, следить за его обновлением и т. д.

Аппаратный контроллер представляет собой отдельное устройство, как правило, того же производителя, что и точки доступа. По своей сути, это тот же сервер управления, но в маленьком корпусе и с логотипом вендора. Некоторые производители совмещают контроллер с коммутатором. Одно время была даже мода на «тупые» точки доступа, которые передавали всю информацию в сыром виде на контроллер, а последний осуществлял всю обработку, но этот подход не прижился.

Антенны. Большое количество антенн у современных точек доступа — это вынужденная необходимость. Поскольку самое простое решение — использовать отдельную внешнюю антенну на каждый приемопередатчик (chain), то общее количество антенн может достигать шести и даже восьми. В результате такая точка доступа выглядит как паук и своим внешним видом может привлечь, пожалуй, только вандала. Современные технологии позволяют внутри корпуса раз-

рировать за канал, рассылая широковещательные сообщения, когда канал освобождается.

OFDMA делит спектр на так называемые временно-частотные ресурсные блоки (Resource Unit, RU). Точка доступа 802.11ax, которая выполняет функции центрального координатора, распределяет подканалы (RU) между станциями для приема и передачи, поэтому с точки зрения абонента сеть оказывается неперегруженной.

Благодаря возможности одновременного использования диапазонов 2,4 и 5 ГГц число доступных для передачи данных каналов может быть дополнительно увеличено. А использование квадратурной амплитудной модуляции (Quadrature Amplitude Modulation, QAM) позволяет передавать больше данных в одном пакете. Если в 802.11ac многопользовательская передача осуществлялась только при загрузке, то в 802.11ax поддержка MU-MIMO MU стала двунаправленной.

Среди других улучшений 802.11ax — значительное увеличение времени работы от батареи. С помощью функции «Пробуждение по расписанию» (Wake Time Scheduling) точка доступа сможет сообщать клиенту, когда ему можно

местить сложные антенные системы, в том числе направленные антенны с высоким коэффициентом усиления и антенны с поддержкой MU-MIMO. Если в сети, уличной или офисной, планируется большая плотность размещения абонентов, обратите внимание на наличие в портфолио у производителя антенны с узкой диаграммой направленности.

Поддержка старых клиентов a/b/g. Массовый выпуск таких устройств закончился более 10 лет назад, поэтому им можно смело сказать «до свидания» и отключить их поддержку в свойствах точек доступа. Если же вы один из тех «счастливчиков», кто использует в своем хозяйстве старые (как правило, специализированные) устройства a/b/g, то поинтересуйтесь, поддерживает ли приобретаемое оборудование режим Airtime Fairness. Это не панацея, но хотя бы не позволит старым устройствам «съесть» всю пропускную способность точек доступа.

Бесшовный роуминг / хэндовер. Сегодня почти все обладатели смарфонов используют приложения для передачи голоса и видео реального времени (WhatsApp, Viber, Skype, Telegram, FB Messenger и др.). При перемещении абонента между точками доступа, смена точки может занять некоторое время и вызвать задержку переключения (handoff-time). При OPEN-аутентификации или доступе с паролем (Pre-shared Key, PSK) задержка переключения минимальна (при условии использования качественного оборудования от ведущих вендоров) и не влияет на работу таких приложений.

Когда используется сервер RADIUS, смена точки доступа потребует повторной аутентификации клиента на RADIUS, что может занять 500 мс и более, так что перебои в связи гарантированы! Один из механизмов обеспечения бесшовности в этом случае — стандарт 802.11r. Его основная задача — кешировать ключ на точках доступа, чтобы абонента не нужно было повторно аутентифицировать на сервере RADIUS при смене точки доступа. 802.11r поддерживается только современными мобильными устройствами, поэтому разные вендоры предлагают проприетарные методы для «старых» клиентов, например Opportunistic Key Caching (OKC).

Расширенная функциональность. Описание возможностей современных точек доступа может занять несколько листов, поэтому остановимся на основных функциях, которые вам наверняка потребуются:

а) умное управление радиопараметрами (сканирование соседних каналов без сброса абонентских сеансов, возможность переключения канала при ухудшении помеховой обстановки, управление выходной мощностью для снижения внутрисистемной помехи или для управления покрытием территории);

б) поддержка собственного гостевого портала и/или возможность http/https-редиректа на внешние гостевые порталы;

в) поддержка Band Steering для подключения двухдиапазонных клиентов в диапазоне 5 ГГц, который, как правило, менее загружен помехами;

г) балансировка нагрузки, обеспечивающая равномерное распределение клиентов между несколькими точками доступа, что исключает наличие перегруженных точек при пустующих соседних;

д) технология Passpoint (Hotspot 2.0) заинтересует, пожалуй, только мобильных операторов: она позволяет аутентифицировать абонента на основе SIM-карты и направлять мобильный трафик через сеть Wi-Fi, когда абонент оказывается в зоне ее действия;

е) API для разработчиков будет востребован там, где сеть Wi-Fi строится для решения нестандартных задач (например, для получения данных о местоположении абонентов либо для интерактивных приложений с учетом поведения абонентов).

Цена. Последний пункт в этом перечне, но не последний по своему значению для заказчика — это цена решения, которая складывается из стоимости точек доступа, лицензий для разблокирования нужного функционала (например, 802.11r или 802.11s), контроллера, лицензий на подключение точек доступа к контроллеру, услуг техподдержки. Если вы ориентируетесь на решения из высшей лиги, то будьте готовы заплатить по всем перечисленным статьям. Но альтернатива есть — например, платформа cnPilot с контроллером cnMaestro: последний можно использовать бесплатно, так же как и услуги техподдержки.

Сергей Голованов,
региональный технический директор
Cambium Networks,
sergey.golovanov@cambiumnetworks.com

Стандарт	Год	Скорость	Диапазоны	Улучшения по сравнению с предыдущим поколением
802.11	1997	1–2 Мбит/с	2,4	Исходный стандарт; использование 2,4 ГГц вместо 900 МГц
802.11b	1999	11 Мбит/с	2,4	Более чем 5-кратное увеличение пропускной способности
802.11a	1999	54 Мбит/с	5	Начало использования диапазона 5 ГГц
802.11g	2003	54 Мбит/с	2,4	5-кратное улучшение пропускной способности
802.11n	2009	300–600 Мбит/с	2,4, 5	MIMO/OFDM, каналы шириной 40 МГц, 6+-кратное увеличение пропускной способности
802.11ac (Wave 1)	2013	433–1270 Мбит/с	5	Каналы 80 МГц
802.11ac (Wave 2)	2015	2167 Мбит/с	5	Каналы 160 МГц, более 3 потоков MIMO, многопользовательский MIMO
802.11ad	2012	7 Гбит/с	60	Эффективная пропускная способность свыше 3 Гбит/с
802.11ax	2019?	10 Гбит/с	2,4, 5	10 Гбит/с, двунаправленный MU-MIMO
802.11ay	2017?	20+ Гбит/с	45+	Потенциально свыше 100 Гбит/с

Краткая история Wi-Fi в стандартах

заснуть и когда проснуться. Периоды сна непродолжительны, но их достаточно много, что позволяет значительно сэкономить заряд батареи.

Появление первых продуктов 802.ax ожидается уже в следующем году, хотя стандарт вряд ли будет принят ранее 2019 года.

Wi-Fi ДЛЯ РАЗНЫХ ЗАДАЧ

До недавнего времени каждая очередная версия стандарта Wi-Fi была призвана заменить своего предшественника. Так, например, 802.11ac быстрее, менее чувствителен к помехам и поддерживает больше клиентов, чем его предшественник 802.11n. Однако из-за разнообразия задач, для которых используется Wi-Fi, подход «один стандарт на все случаи жизни» перестает соответствовать предъявляемым требованиям. Это проявляется в разработке специфических стандартов для различных применений.

Первым таким стандартом стал 802.11ad (WiGig). Он обеспечивает высокую скорость передачи, но на небольшом расстоянии (см. подробнее раздел «Гигабитный рубеж»). Одним из целевых приложений является трансляция потокового видео с мобильного устройства на телевизор. Так, по оценкам Strategy Analytics, передача видео ультравысокой четкости (UHD) объемом 60 Гбайт займет менее 2,5 мин.

Возможность использовать широкую, если не повсеместную, инфраструктуру удешевляет подключение устройств Интернета вещей и делает Wi-Fi естественным кандидатом для этих целей. Многие из них, вероятно, будут подключаться с помощью разрабатываемого стандарта 802.11ah. Если WiGig предназначен для передачи больших объемов данных на короткие расстояния, то 802.11ah, получивший название HaLow, наоборот, ориентирован на передачу меньших объемов на весьма значительные расстояния, причем, что важно для приложений IoT, стандарт рассчитан на очень малое потребление энергии.

Спецификация HaLow одобрена, чипсеты доступны на рынке, но некоторые аналитики считают, что из-за слишком позднего появления ему будет трудно составить конкуренцию стандартам сотовой связи, предлагающим схожие возможности, например LTE-M. К тому же распространению HaLow будет препятствовать и его работа в нетипичном для Wi-Fi субгигагерцевом диапазоне, причем в разных регионах мира используются разные частоты: 700 МГц в Китае, 850 МГц в Европе и 900 МГц в США. По оценкам ABI Research, к 2020 году ежегодно будет продаваться 11 млн устройств с чипсетами 802.11ah. С учетом прогнозов роста Интернета вещей это совсем немного.

Впрочем, для подключения устройств IoT могут использоваться и другие стандарты Wi-Fi. Так, например, 802.11ax рассматривается в качестве одного из кандидатов для обеспечения работы IoT; в частности, благодаря поддержке MU-MIMO и меньшим интервалам между каналами (78,125 кГц), 18 клиентов могут одновременно отправлять данные в канале 40 МГц. А стандарт 802.11p предусматривает поддержку выделенных коротких соединений (Dedicated Short-Range Communications, DSRC), которые могут применяться, например, в беспилотных автомобилях.

Еще один новый стандарт, 802.11af (так называемый White-Fi или SuperWi-Fi), рассчитан на передачу больших объемов данных на большие расстояния. Он использует свободный частотный спектр между телевизионными каналами (полосы 6–8 МГц). Конкретные частоты в диапазоне от 54 до 790 МГц каждая страна определяет самостоятельно. Благодаря дальности передачи до нескольких километров, основное предназначение этого стандарта — обеспечение связи в сельской местности.

СВЕТЛОЕ БУДУЩЕЕ WI-FI

Wi-Fi осваивает все новые и новые территории, помогая решать все более сложные задачи: масштаб претензий сторонников этой технологии на новые рыночные ниши растет вот уже несколько лет. Так, в прогнозе Wi-Fi Alliance на текущий год указывается, что благодаря новым стандартам Wi-Fi способен справиться с большинством тех сценариев, где требуются высокая емкость и низкая задержка, для реализации которых и создается следующее поколение сотовой связи 5G.

Помимо описанных в статье стандартов, ведутся и другие многочисленные разработки для улучшения характеристик и функциональности Wi-Fi, в которых наряду с IEEE активную роль играет Wi-Fi Alliance. Так, например, в рамках инициатив Multiband Operations и Optimized Connectivity Experience ведется поиск способов автоматического распределения клиентов между точками доступа и частотными диапазонами.

Все прогнозы по дальнейшему распространению Wi-Fi весьма оптимистичны. Количество используемых устройств Wi-Fi уже превысило численность населения Земли. По данным Wi-Fi Alliance, только в этом году будет продано около 3 млрд устройств с поддержкой Wi-Fi, а к концу года их общее число составит почти 9 млрд. Так что лучшее для этой технологии, несмотря на ее солидный 20-летний возраст и обилие конкурентов, конечно, впереди. LAN

Полоса препятствий для хакеров

Защититься от атак и вирусов помогут только комплексные меры безопасности, предусматривающие использование новейших средств защиты корпоративной сети.

Андрей Врублевский,
руководитель направления оптимизации и контроля сети компании «КРОК»

Хотим мы того или нет, но с каждым годом хакеры используют все более изощренные способы кибератак, а пострадать от них может любая компания — и международный гигант, и небольшое семейное предприятие. Общемировой ущерб от кибернападений измеряется миллиардами долларов. Вирусы не только бьют по репутации компании, но и нарушают бизнес-процессы. Например, японскому автопроизводителю Honda из-за атаки, случившейся в июне 2017 года, пришлось остановить работу завода на целые сутки.

Как показало расследование инцидентов, вызванных шифровальщиками WannaCry и Petya, вирусы использовали одну и ту же уязвимость в реализации протокола SMB в операционных системах Windows. Petya, атаковавший компании по всему миру через месяц после WannaCry, нанес ничуть не меньший ущерб, чем его предшественник, из чего можно сделать вывод, что к рекомендациям по обновлению ПО и установке заплат мало кто прислушался. Результат, думаю, все видели в заголовках СМИ.

ЧТО ТАИТ СЕТЬ: УГРОЗЫ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

Первые экземпляры вируса чаще всего проникают в сеть через корпоративную почту. Например, отдел кадров получает письмо с резюме во вложении. Сотрудник HR-службы при всем желании не сможет догадаться, заражено оно или нет, так как все письма отправляются соискателями с личных адресов.

Заражение может происходить незаметно: вирус самостоятельно распространяется по сети компании через уязвимые компьютеры. Дело в том, что трафик инспектируется в основном только на участке «Интернет — корпоративная сеть». Если вирус уже внутри, исследование трафика на угрозы чаще всего не осуществляется.

Распространяясь невероятно быстро, вирус может в одночасье парализовать все бизнес-процессы. В основном цель злоумышленников — вымогательство, но у шифровальщика есть и другие неприятные последствия: остановка работы промышленного оборудования, банкоматов, касс в магазинах.

Если на компьютерах пользователей и серверах имеется уязвимость, то через нее, как по приглашению, за периметр могут попасть и другие угрозы — например, шпионское ПО, которое наносит вред компании исподтишка, воруя конфиденциальные данные. Это опять-таки лишь один из возможных сценариев. Уязвимости есть везде, даже в самых проработанных программах или операционных системах, а вариантов воспользоваться ими очень много.

ЗАЩИТА В ЭПОХУ ШИФРОВАЛЬЩИКОВ

Самый элементарный способ снизить риск заражения вирусами — следить за сообщениями о новых угрозах (рассылки партнеров, официальные сообщения компаний и исследовательских групп и т. п.) и своевременно обновлять ПО. Полезные ИТ-инструменты для этих целей предлагают ведущие разработчики в области обеспечения сетевой безопасности: Palo Alto, Fortinet, Check Point и др.

Эффективным средством противодействия угрозам является сервис «песочницы», благодаря которому разработчики получают огромное количество экземпляров вредоносных файлов и могут оперативно предоставлять информацию (сигнатуры) своим подписчикам — компаниям, у которых установлены межсетевые экраны того или иного вендора. Это позволяет максимально быстро в автоматическом режиме блокировать вредоносное ПО после его обнаружения на глобальном уровне. Сервис песочницы может быть реализован как облачная услуга или размещен в инфраструктуре заказчика по модели on-premise.

Наиболее эффективный способ защиты на текущий момент — реализовать в компании комплексный подход к информационной безопасности: установить антивирус (для защиты оконечных устройств) и межсетевой экран следующего поколения, а кроме того, воспользоваться возможностями песочницы. Каждый из этих вариантов по отдельности — не панацея, но вместе они создают серьезную полосу препятствий для хакеров.

Представим себе компанию, на почтовый сервер которой приходит письмо со встроенным вредоносным кодом. В зависимости от квалификации хакеров, он может либо вообще не проникнуть в систему (например, если используется неактуальный метод атаки), либо углубиться «внутрь» ровно настолько, насколько ему позволят имеющиеся средства защиты. Комплексная защита воздвигает сразу несколько препятствий на пути к данным и корпоративным системам: антивирус защищает конечные устройства, а песочница и межсетевой экран — всю сеть, как бы создавая щит, который не пропускает подозрительные объекты.

Инновационные ИТ-инструменты защиты конечных устройств, такие как Traps компании Palo Alto, умеют не просто выполнять анализ сигнатур, но и бороться с неизвестными угрозами нулевого дня. Traps выявляет отклонения в стандартной работе программных продуктов (например, нетипичное обращение к другим участкам памяти) и при необходимости блокирует подозрительные действия.

К сожалению, как показывает опыт прошлого лета, даже не все крупные компании обладают подобной системой. Наиболее ответственный подход к обеспечению безопасности продемонстрировали банки, поскольку подобные инциденты (особенно публичные) для них наиболее критичны. Этот вопрос остро стоит на повестке дня у предприятий из нефтегазового и телекоммуникационного секторов. В зоне повышенной опасности находятся розничные сети, поскольку из-за большого количества подрядчиков, партнеров и множества магазинов, расположенных в самых разных регионах страны, вирус может легко распространиться по цепочке. Следует всегда помнить о том, что игнорирование собственной защиты может иметь самые негативные последствия не только для самой компании, но и для всех, с кем она взаимодействует. LAN

Переключатели KVM: акцент на видео

Несмотря на сокращение серверного рынка, переключатели клавиатуры, видео и мыши продолжают пользоваться стабильным спросом благодаря расширению их области применения за пределы традиционных серверных. С появлением новых форматов видео перед производителями KVM-оборудования встала новая задача — обеспечить эффективную передачу и распределение сигналов с разрешением 4K

Дмитрий Ганьжа,
главный редактор «Журнала сетевых решений/LAN»

Рис. 1. Переключатели KVM находят все более широкое применение за пределами ЦОДов — в авиадиспетчерских, банках, в военных организациях и организациях здравоохранения, на ТВ-студиях. На фото пример использования KVM в диспетчерской

Рис. 2. Использование KVM позволяет вынести шумные и греющиеся компьютеры в отдельное помещение, а на рабочих столах оставить только клавиатуру, мышь и монитор. Пример организации подключения в ситуационном центре

Согласно Reports'n'Reports, в 2016 году объем мирового рынка KVM составил 663 млн долларов и продолжает расти, правда, невысокими темпами — около 2% в год. Близкую оценку (650 млн долларов) и примерно тот же прогноз роста дает Technavio, которая среди множества факторов и тенденций выделяет следующие: увеличение спроса на KVM со стороны малых и средних компаний, все более широкое применение KVM с подключением по оптическому кабелю и использование интеллектуальных KVM в промышленных приложениях.

Одним из наиболее интересных — и крупных — сегментов является рынок IP KVM. По данным GlobalInfoResearch, его объем составил 323 млн долларов в 2015 году, то есть около половины всего рынка переключателей, а растет он заметно быстрее — более чем на 10%. Как и на рынке KVM в целом, перечень производителей ограничен двумя десятками компаний: Aten, Avocent (в составе Emerson), Raritan (Legrand), APC, Black Box, Guntermann & Drunck, Tripp Lite и некоторые другие. При этом на тройку лидеров приходится свыше половины оборота — 57%.

На развитие рынка IP KVM влияет множество противоречивых факторов. С одной стороны, пользователи заменяют аналоговые переключатели KVM на IP KVM, поскольку последние обеспечивают возможность удаленного управления. С другой стороны, большинство современных серверов поставляется со встроенными сервисными процессорами, поэтому потребность в KVM снижается (сервисные процессоры позволяют запускать виртуальные сессии KVM).

Переход от аналоговых к цифровым интерфейсам характерен и для других сегментов рынка KVM, в частности, аналитическая IHS Markit отмечает тенденцию перехода на цифровые модели в сегменте высокопроизводительных переключателей. Однако до сих пор аналоговые устройства пользуются заметным спросом: по данным IHS, на долю стоечных аналоговых переключателей приходится около четверти всего объема рынка. Среди других тенденций аналитики IHS выделяют растущую популярность защищенных решений в сегменте настольных KVM. Если раньше они использовались преимущественно в государственных учреждениях, то теперь все шире применяются на таких вертикальных рынках, как финансы и здравоохранение, где вопросам обеспечения безопасности придается особое значение.

РОССИЙСКИЙ РЫНОК KVM

Для российского рынка KVM характерны те же тенденции, что и для мирового. Спрос на эту категорию устройств остается стабильным, поставщики отмечают небольшой рост продаж. Как указывает Анатолий Маслов, технический эксперт Tripp Lite, в последние пару лет основной объем закупок приходится на крупные компании, которые при оснащении рабочих мест в офисах стремятся гарантировать требуемый уровень безопасности, например, когда одному сотруднику предоставляется доступ к двум серверам или системным блокам. Дополнительный спрос обеспечивают закупки для ЦОДов интеллектуальных многопортовых KVM со встроенными дисплеями или с возможностью управления по IP.

KVM-оборудование можно разделить на три основные группы: KVM-удлинители (передают на большие расстояния сигналы компьютерных интерфейсов); KVM-переключатели (позволяют управлять несколькими компьютерами с одного/нескольких рабочих мест); матричные KVM-переключатели (позволяют большой группе пользователей управлять множеством компьютеров, при этом каждый может работать с любым сервером). Как утверждает Николай Клочков, главный инженер «Ай Эм Эс» (Interactive Multimedia Solutions), лидерами спроса являются KVM-удлинители, на втором месте — KVM-переключатели. В сложных проектах, когда количество специалистов и компьютеров велико, используются матричные KVM-переключатели.

KVM применяются для решения специфических задач, соответственно, KVM-оборудование — это не массовый продукт, оно востребовано в определенных отраслях. По словам Николая Клочкова, интерес к KVM зависит не от масштабов компании, а от сферы ее деятельности и сопряженных с ней задач и условий работы сотрудников. Выбор наиболее подходящих KVM-устройств: удлинителей (KVM или IP KVM), переключателей (KVM, матричных KVM, IP KVM) и прочих устройств — зависит от специфики деятельности, задач и масштабов проектов, количества рабочих мест и компьютеров.

Заказчики, как правило, знают, для решения каких задач им необходимы KVM, что, по словам Игоря Калинина, директора по маркетингу компании «Колан», свидетельствует о зрелости рынка. Он отмечает изменение структуры совокупного спроса: если раньше поступали запросы на одно, два, в крайнем случае три устройства, а крупные партии приобретались редко, то сейчас увеличилась доля закупок для реализуемых проектов, а мелких заказов становится меньше.

Среди тенденций рынка Игорь Калинин выделяет спрос на IP KVM и многопортовые устройства. Так, если ранее в тендерах запросы ограничивались преимущественно оборудованием с 8 портами, то сейчас нужны устройства с 16/32 портами и более. Другая заметная тенденция — переход на цифровые интерфейсы (с VGA на DVI и HDMI); в частности, обновление парка серверов и компьютеров с новыми интерфейсами стимулирует замену KVM-переключателей в крупных госструктурах. Однако устройства с интерфейсом VGA по-прежнему широко применяются в ЦОДах, где рост интереса к DVI невелик. Спрос на оборудование с поддержкой PS/2 минимален, в основном покупаются устройства с USB.

НОВЫЕ НИШИ ДЛЯ KVM

Переключатели KVM находят все более широкое применение за пределами ЦОДов: в авиадиспетчерских, банках, в военных организациях и медицинских учреждениях, на ТВ-студиях, — в том числе благодаря таким новым возможностям, как поддержка видео 4K (см. рис. 1).

Использование KVM позволяет вынести шумные и выделяющие много тепла компьютеры в отдельное помещение, а на рабочих столах оставить только клавиатуру, мышь и монитор. Тем самым улучшается эргономика рабочего пространства, обеспечивается необходимый уровень комфорта, повышается эффективность труда (см. рис. 2). Не случайно, как отмечает эксперт Tripp Lite, KVM наиболее востребованы в решениях для организации рабочего места — например, когда в целях безопасности необходимо обеспечить для одного сотрудника раздельное пользование серверами или системными блоками.

Источник: Tripp Lite

Рис. 3. Настольный двухпортовый переключатель KVM/аудио/USB B004-DP2UA2-K производства Tripp Lite позволяет контролировать два компьютера с поддержкой DisplayPort 1.2 с разрешением до 4K посредством одного комплекта из монитора DisplayPort, клавиатуры и мыши USB

Операционному сотруднику банка зачастую необходим доступ к Интернету и одновременно к внутренней информации, которая хранится на сервере, не подключенном к глобальной сети. В этом случае использование KVM-переключателя позволяет сотруднику работать с двумя независимыми серверами или системными блоками со своего рабочего места. По словам Анатолия Маслова такие KVM отличаются невысокой стоимостью и достаточной защищенностью, чаще всего они двухпортовые и без внешнего питания.

Схожие требования к комфорту и безопасности рабочего места предъявляются и в других отраслях. Так, специалистам диспетчерских служб и центров управления полетами приходится решать серьезные задачи по обеспечению безопасности полета. Такая деятельность требует большой сосредоточенности, поэтому рабочие места должны быть удобными. Однако, как указывает специалист «Ай Эм Эс», используемые в диспетчерских мощные крупногабаритные компьютеры слишком шумят и выделяют много тепла.

В итоге нарушаются строгие производственные нормы, установленные для авиационных предприятий. Кроме того, оборудование, используемое сотрудниками диспетчерских, нуждается в особых условиях эксплуатации: бесперебойное питание и определенный температурный режим. А это достигается только при размещении серверов в специальных комнатах.

С неменьшим риском сопряжена работа военных и полиции. Как правило, они тоже нуждаются в оборудовании для передачи на большие расстояния компьютерных интерфейсов и видео в высоком разрешении и режиме онлайн. Передача сигналов аудио и видео без потери качества — необходимое условие работы и ТВ-студий. Сотрудники служб теле- и радиовещания также не должны отвлекаться на шум, производимый мощными серверами. Для решения всех этих задач идеально подходит профессиональное KVM-оборудование, заключает Николай Клочков.

Переключатели KVM все более широко применяются в аудиовизуальной отрасли. Как указывают в «Колан», KVM-решения стали внедряться в системы видеотрансляций в качестве устройств управления и контроля. В частности, LCD KVM используются для локального контроля и управления источниками системы трансляции, а удлинители IP KVM — для удаленного управления из зоны отображения трансляции контента. Известные производители видеорешений (Kramer, TNTv и др.) стали создавать и предлагать на рынке устройства трансляции видеоконтента по IP с возможностью удаленного управления через RS232 и USB-интерфейс.

Среди других областей применения можно выделить здравоохранение. Как отмечает Анатолий Маслов, с 2018 года вступает в силу федеральный закон о реализации приоритетного внедрения в стране телемедицины, в связи с чем он ожидает повышения спроса на решения KVM, которые могут быть использованы для централизованного удаленного администрирования.

IP KVM И ПОДДЕРЖКА ВИДЕО 4K

IP KVM приобретают все большую популярность, причем все чаще они применяются и для тех задач, где ограничения на расстояние позволяют использовать и традиционные решения. Николай Клочков объясняет популярность передачи данных по IP наличием возможности задействовать существующую инфраструктуру и, таким образом, сэкономить время и деньги на прокладке кабелей. В качестве еще одного преимущества он отмечает лучшую помехозащищенность.

Востребованность технологий IP KVM увеличивается в числе прочего за счет улучшения их качественных характеристик. «Технология передачи данных по IP, в частности интерфейсов периферийных устройств и видео, активно совершенствуется, — говорит Николай Клочков. — Данный вид решений все меньше нагружает используемое сетевое оборудование, при этом качество передаваемых видеосигналов не ухудшается. Кроме того, если раньше наблюдались сильные задержки в трансляции сигналов, то сейчас они сократились до сотых миллисекунды и теперь практически незаметны человеческому глазу».

На видео приходится основной объем трафика, поэтому все основные технологические достижения, отмечает Анатолий Маслов, связаны с увеличением объема соответствующей информации. Если ранее достаточно было передачи сигналов с разрешением VGA, то сейчас все чаще приходится сталкиваться с необходимостью коммутации видеосигнала 4K. Поддержка передачи видео 4K в KVM-решениях очень важна

для ТВ-студий, компаний из широковещательной отрасли и других сфер, где приходится работать с графикой и видео, где не допускаются потери их качества и какие-либо задержки при передаче данных.

Соответствующие решения появились у многих производителей (см. рис. 3). Так, решение KVM over IP Matrix System пополнилось двумя удлинителями KVM поверх IP: KE8950 и KE8952 для подключения одного дисплея 4K HDMI (вторая модель поддерживает PoE). Данные устройства обеспечивают передачу видео Ultra High Definition (UHD) с разрешением 3840 × 2160 и частотой 30 Гц при глубине цвета 36 бит. Для передачи по сети данные шифруются с помощью 128-разрядного алгоритма AES.

Американский производитель Black Box представил модуль 4K60 для своей матричной системы DKM, которая широко используется ТВ-студиями. Благодаря ее модульной реализации не надо полностью заменять систему, чтобы воспользоваться преимуществами новой технологии, — достаточно установить новую карту. Данный модуль позволяет передавать видео от оборудования, оснащенного цифровым интерфейсом DisplayPort 1.2 с разрешением до 4096 × 2160 и частотой 60 Гц, на расстояние до 140 м по витопарному кабелю и до 10 км по оптическому.

ПРОГРАММНО ОПРЕДЕЛЯЕМОЕ ВИДЕО

Дальнейшее развитие KVM-решений будет зависеть от темпов совершенствования технологий в целом, прежде всего средств передачи видеосигналов как наиболее востребованного сегодня формата данных. Например, сформированный в прошлом году консорциум производителей Software-Defined Video over Ethernet (SDVoE) ставит перед собой цель обеспечить доставку сигналов HDMI по обычной сети Ethernet с минимальной задержкой. Разрабатываемая технология предназначается для того же круга задач, что и матричные переключатели, удлинители KVM, контроллеры видеостен и процессоры изображений.

Сетевая архитектура SDVoE предполагает использование готовых коммутаторов Ethernet, так что соответствующее решение обойдется дешевле, чем решение на базе HDBaseT, при этом оно отличается большей гибкостью и масштабируемостью. Обработка сигнала возлагается на конечные точки, сигнальные процессоры которых конвертируют аудио- и видеосигналы между HDMI и Ethernet.

Технология SDVoE стандартизует интерфейс между конечными точками и программным обеспечением, что создает предпосылки для появления нового класса приложений. Позволяя отказаться от использования матричных переключателей, разработка которых требует немалых вложений, эта технология значительно снижает барьер для входа на рынок. Так что в скором времени можно ожидать появления новых приложений и новых игроков, а вслед за этим — изменения привычной расстановки сил на рынке. LAN

Ничего лишнего

Дедупликация нашла широкое применение как способ справиться с ростом издержек на инфраструктуру резервного копирования при увеличении объемов данных.

Сергей Орлов,
независимый эксперт (sorlov1958@yandex.ru)

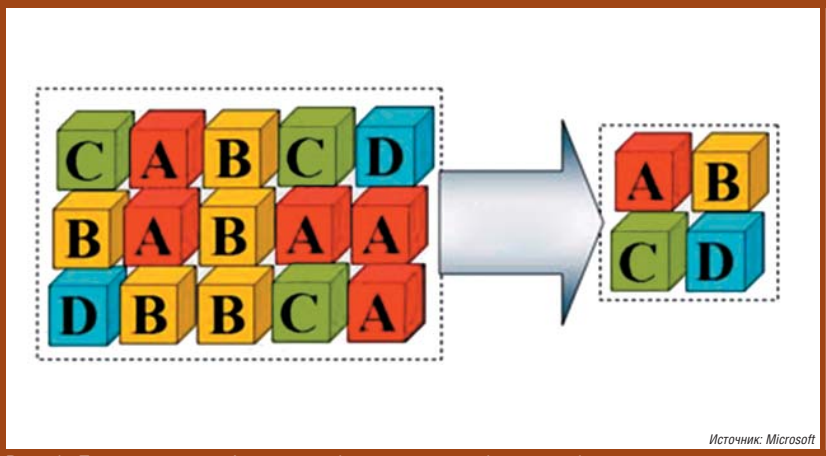


Рис. 1. Дедупликация: файлы разбиваются на небольшие блоки переменного размера (32–128 Кбайт), среди них выявляются повторяющиеся, и для каждого дублируемого блока оставляется только одна копия — другие заменяются ссылкой на нее

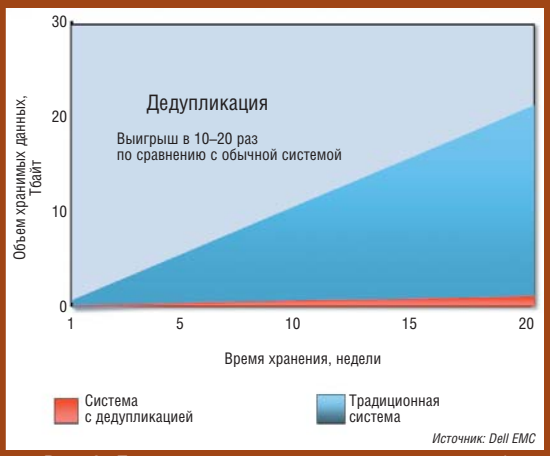


Рис. 2. Дедупликация радикально сокращает объем передаваемых и хранимых данных, позволяя устранить узкие места в ИТ-инфраструктуре и уменьшить затраты на хранение

Доступность и сохранность данных — залог непрерывности бизнес-процессов и эффективности работы. Сегодня данные — один из самых ценных активов, поэтому их резервное копирование и архивное хранение — наиболее типичные задачи, а система резервного копирования — важная часть любой корпоративной информационной системы. При правильной организации она способна надежно защитить критичные данные.

Внедрение систем резервного копирования дает возможность оперативно восстанавливать информацию в самых разных ситуациях, однако и они не лишены недостатков. Традиционные проблемы — неэффективное использование емкости хранения (объем резервных копий за неделю может вдвое превысить объем исходных данных), низкая скорость копирования, непредсказуемое время восстановления (как правило, намного больше планируемого), не очень высокая надежность (по данным Gartner, риск невозможности восстановления превышает 10%).

Решения для резервного копирования и восстановления должны эффективно функционировать в условиях экспоненциального роста данных, ужесточения требований регуляторов и сокращения окон резервного копирования. Крайне желательно также обеспечить снижение затрат, связанных с защитой данных. Преодолеть перечисленные проблемы призвана дедупликация данных. В том или ином виде ее предлагают в своих продуктах все ведущие вендоры систем резервного копирования корпоративного класса.

УСТРАНЕНИЕ ИЗБЫТОЧНОСТИ

Дедупликация, по определению IDC, — это технология создания из дубликатов единой копии данных с возможностью совместного доступа, повышающая эффективность использования емкости систем хранения. Согласно Microsoft, это процедура поиска и удаления дублирующихся данных без ущерба для их качества и целостности с целью уменьшения объема пространства, занимаемого данными (см. рис. 1).

Блоки, общие для нескольких файлов, хранятся в виде одной копии, поэтому требования к емкости хранения всех файлов снижаются. Удаляя повторяющиеся последовательности данных, дедупликация позволяет значительно сократить объем передаваемых и/или хранимых данных. Чтобы еще сильнее его уменьшить, дедупликацию нередко сочетают с компрессией (сжатием), называя все это уплотнением данных.

При запросе файл собирается из соответствующих блоков (для пользователя или приложения этот процесс прозрачен), поэтому, применяя дедупликацию к файлам, можно не беспокоиться о том, что работа приложений осложнится или доступ пользователей к файлам окажется невозможен. Дедупликация снижает издержки, сводя к минимуму накладные расходы на хранение и передачу данных.

ДЕДУПЛИКАЦИЯ В СИСТЕМАХ РЕЗЕРВНОГО КОПИРОВАНИЯ

При использовании в системах резервного копирования дедупликация помогает решить целый ряд проблем и дает весомые преимущества (см. табл. 1).

Основные причины использования дедупликации данных в системе резервного копирования — небольшой размер резервных копий (см. рис. 2), снижение потребности в емкости хранения, сокращение сетевого трафика, уменьшение окна резервного копирования. Ежедневно выполняемое полное резервное копирование позволяет гарантировать быстрое восстановление за один шаг.

В системах резервного копирования с функцией дедупликации возможны различные варианты хранения резервных копий: ленточные накопители и библиотеки, виртуальные ленточные библиотеки, дисковые массивы и системы хранения данных, в том числе со встроенной дедупликацией. Дедупликация выполняется «на лету» (в процессе резервного копирования или архивирования), поэтому на диске, а также в облачных хранилищах (cloud backup) сохраняются уже дедуплицированные данные.

Требования к емкости сокращаются в среднем 10–30 раз, значительно повышаются скорость и надежность восстановления и извлечения данных. Но ничто не дается даром: дедупликация требует затрат. Нужны вычислительные ресурсы, к тому же происходит снижение производительности систем или увеличивается их стоимость. Поэтому нужно выяснять, какие издержки неизбежны при использовании каждого метода.

ВИДЫ ДЕДУПЛИКАЦИИ

Существуют разные виды, или методы, дедупликации, у каждого свои преимущества и недостатки (см. табл. 2).

Дедупликация может выполняться на источнике данных или непосредственно в хранилище. В зависимости от этого распределяется вычислительная нагрузка. При первом методе данные обрабатываются на стороне клиента и по окончании дедупликации пересылаются на устройства хранения. В результате нагрузка на сеть снижается, но на клиентах приходится устанавливать специализированное ПО и оснащать их значительными вычислительными ресурсами. Второй метод предусматривает применение более мощных и дорогих СХД, но затраты на первоначальную передачу данных фактически не снижаются. В любом случае нужно учитывать, что требования дедупликации к ресурсам системы достаточно высоки.

ЭФФЕКТИВНОСТЬ ДЕДУПЛИКАЦИИ

По данным Dell EMC, дедупликация на источнике позволяет сократить емкость хранения до 50 раз, трафик — до 500 раз, время резервного копирования — до 10 раз. Однако ее эффективность очень сильно зависит от типа данных. Очевидно, что наибольший эффект достигается, когда данные обладают большой избыточностью, а также когда копируются и/или сохраняются после внесения незначительных изменений.

В общем случае для неструктурированных данных (файлы документов, журналов, образов и виртуальных машин, электронной почты и архивов) характерен высокий коэффициент дедупликации — их объем нередко уменьшается в 20–30 раз. Например, хорошо дедуплицируются файлы виртуальных машин (VHD): экономия может составлять до 90% (см. рис. 3). Дедупликация структурированной информации, например баз данных, не настолько эффективна (обычно до 5–8 раз).

Дедупликация мультимедийных файлов тоже не обеспечивает большой экономии. Изображения, видео (JPEG, GIF, TIF, MPEG, и др.), результаты сжатия и шиф-

Преимущество	Что оно дает
Уменьшение окон резервного копирования	При традиционном резервном копировании передаются большие объемы данных, поэтому «вписаться» в окно резервного копирования достаточно сложно, а иногда и невозможно. Дедупликация позволяет выполнить резервное копирование в пределах выделенного окна благодаря уменьшению объема копируемых данных.
Сокращение времени восстановления	Сокращение объема данных позволяет хранить резервные копии на дисках, а не на магнитных лентах, поэтому восстановление работы информационной системы значительно ускоряется и становится более надежным.
Снижение стоимости хранения резервных копий	Объемы данных сокращаются, а значит, снижаются требования к емкости систем хранения.
Защита растущего объема корпоративных данных	Дедупликация позволяет эффективно выполнять резервное копирование возрастающих объемов хранимых данных.
Повышение уровня безопасности в катастрофоустойчивых решениях	При дедупликации в сочетании с репликацией копии данных можно хранить вне площадки. Отпадает необходимость операций с ленточными носителями.
Защита данных в организациях с филиальной структурой	Защиту и восстановление данных, хранящихся в удаленных филиалах, часто желательно централизовать. При создании единого хранения дедупликация упрощает процесс передачи больших объемов данных по сети. Поскольку диски используются только для размещения уникальных данных, их можно с минимальными затратами реплицировать по сети на удаленные площадки для осуществления быстрого аварийного восстановления.

Таблица 1. Основные преимущества дедупликации в системах резервного копирования

Вид дедупликации	Особенности
Онлайновая, потоковая дедупликация, дедупликация «на лету» или дедупликация перед сохранением	Осуществляется по мере поступления данных, избыточность устраняется еще до записи на СХД. То есть дедупликация происходит в реальном времени, временное хранение данных на дисках отсутствует. Данные записываются на диск уже дедуплицированными. Требуемое количество операций ввода-вывода и объем хранения меньше, но скорость обработки данных должна быть достаточно высокой.
Постпроцессная, послеоперационная дедупликация или дедупликация после сохранения данных	Данные временно сохраняются на дисках и позже считываются и обрабатываются механизмом дедупликации. В результате ускоряется процесс их копирования, но требуется дополнительная емкость для временного хранения.
Комбинированный метод	Онлайновая дедупликация на источнике данных сменяется постпроцессной обработкой, когда скорость их поступления достигает определенного предела.

Таблица 2. Основные схемы дедупликации

рования, картографические и сейсмические данные, файлы САПР — все эти форматы проблемные для дедупликации.

Хорошо дедуплицируются редко изменяемые данные, поскольку постоянный доступ к данным и их изменение могут свести к минимуму эффект дедупликации. Microsoft не рекомендует применять дедупликацию к серверам Hyper-V, SQL и Exchange, файлам запущенных виртуальных машин, большим файлам (более терабайта). Она может функционировать на файловом, блочном или битовом уровне (см. табл. 3).

В некоторых схемах, основанных на хешировании, для повышения коэффициента дедупликации применяется предварительная обработка данных. Если данные обрабатываются на стороне клиента, дедупликация блоков переменной длины позволяет значительно уменьшить время резервного копирования, так как сохраняются только уникальные сегменты. Этот метод более эффективен, чем традиционная дедупликация сегментов фиксированной длины, когда даже небольшие изменения в наборе данных приводят к резервному копированию всего файла.

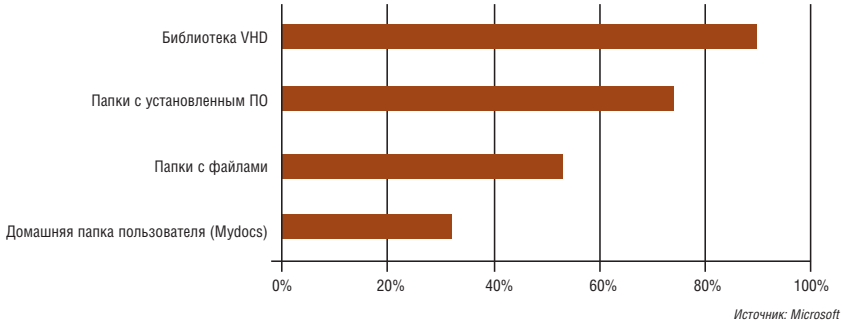
В системах резервного копирования могут использоваться и иные методы дедупликации (см. табл. 4 и рис. 4). К тому же разработчики систем хранения применяют разные алгоритмы дедупликации, в том числе достаточно сложные, для которых нужно больше процессорных ресурсов. Поэтому величина коэффициента дедупликации зависит от реализации этой технологии.

Рассмотрим некоторые системы резервного копирования более детально.

IBM SPECTRUM PROTECT И PROTECTIER

Система IBM Spectrum Protect позволяет уменьшить риск потери данных за счет постоянного инкрементного резервного копирования и дедупликации. Она поддерживает множество разных видов хранилищ, в том числе гибридные облака, и помогает автоматизировать управление информацией.

IBM удерживает позицию одного из ведущих производителей систем резервного копирования, в том числе благодаря запуску технологии облачного многоуровневого хранения для IBM Spectrum



Источник: Microsoft

Рис. 3. Эффективность дедупликации в Windows Server 2012 при ее применении к разным типам файлов: библиотекам VHD, файлам для развертывания ПО, общим и пользовательским файлам

Protect. Это решение позволяет осуществлять безопасное и простое в управлении автоматическое резервное копирование данных в облаке.

IBM TS7650G ProtecTIER Deduplication Gateway обладает одними из лучших в отрасли показателями скорости дедупликации в реальном времени. Емкость хранилища резервных копий может превышать 25 Пбайт. В сочетании с системами хранения данных (от IBM или других вендоров) TS7650G ProtecTIER повышает производительность хранилища и обеспечивает долговременное хранение и доступность данных, находящихся в резервных копиях и архивах.

Производительность резервного копирования при дедупликации виртуальной ленточной библиотеки (VTL), осуществляемой в реальном времени, при передаче данных достигает 9 Тбайт в час. По информации IBM, в системе в компактном корпусе 2U применяется алгоритм поддержания целостности данных без хеширования, поэтому риск потери данных из-за коллизий хеш-функций сводится к нулю (см. рис. 5).

Благодаря патентованному алгоритму дедупликации HyperFactor, не использующему хеш-функции, требуемая емкость системы хранения данных уменьшается в 25 раз и более. По мнению разработчиков, с его помощью можно существенно снизить затраты и обеспечить корпоративный уровень целостности данных. Индекс хранится в оперативной памяти и не затрудняет обработку больших массивов данных (до 10 Тбайт), что не исключено в случае хеширования.

Приложение резервного копирования записывает данные на ProtecTIER как в обычную ленточную библиотеку. При этом сохраняется только уникальная информация, на уже существующую создаются ссылки. Когда данные устаревают, ссылки удаляются и место освобождается.

AVAMAR ОТ DELL EMC

Дедупликация сегментов переменной длины, которая осуществляется на устройстве клиента, реализована в системе резервного копирования Avamar от Dell EMC. Avamar — комплексное программно-аппаратное решение для резервного копирования и восстановления данных, интегрируемое с СХД Data Domain. Оно поддерживает виртуальные и физические среды, корпоративные приложения, сетевые системы хранения данных (NAS) и ПК, защиту данных удаленных офисов.

Глобальная дедупликация на стороне клиента уменьшает объем резервного копирования. Специфика глобальной дедупликации заключается в том, что при любом типе или количестве внешних устройств и сеансов данные копируются и сохраняются в пуле дедупликации один раз. Как отмечают в Dell EMC, сокращение времени на ежедневное резервное копирование достигает 90%, нагрузка на сеть (в терминах необходимой пропуск-

Уровень дедупликации	Описание
Файловая дедупликация	Операции выполняются на уровне файлов. В основном применяется к архивным данным. Эффект минимален по сравнению с другими типами дедупликации.
Блочная дедупликация	Работает на уровне блоков данных. Используется в системах хранения данных и операционных системах (например, в Windows Server). Применяется к архивным данным, виртуализированным средам (например, VDI).
Битовая дедупликация	Обладает самой высокой эффективностью, но наибольшей ресурсоемкостью. Нередко используется в сетевом оборудовании для уменьшения трафика.

Таблица 3. Уровни дедупликации

Продукт	Способ дедупликации
Veritas Backup Exec и NetBackup	При дедупликации используется алгоритм хеширования MD5; размер блока фиксированный — от 32 Кбайт до 1 или 16 Мбайт. Метаданные хранятся в СУБД PostgreSQL. Дедупликация резервных копий осуществляется на уровне блоков и предусматривает отслеживание изменений блоков (Change Block Tracking). Она выполняется и на клиенте, и на сервере, либо используются возможности СХД.
Veeam Backup & Replication	Предлагается 4 способа дедупликации и 5 уровней сжатия данных. Это позволяет выбрать оптимальный баланс расхода ресурсов хранения и нагрузки на прокси-сервер при выполнении заданий резервного копирования и репликации. Один из уровней сжатия разработан специально для систем хранения данных с поддержкой дедупликации. Для минимального влияния на производительность и достижения большего коэффициента сжатия используются достаточно большие блоки данных. При сжатии данных, совместимом с аппаратной дедупликацией, применяется алгоритм Run-Length Encoding (RLE). При этом данные дедуплицируются дважды: сначала средствами Veeam, а потом на устройстве хранения, — что позволяет еще больше снизить объемы данных. Дедупликация и сжатие данных выполняются как на источнике (прокси-сервере), так и перед записью на диск. Благодаря этому уменьшается нагрузка на сеть.
Acronis Backup Advanced	Размер блока автоматически меняется от 1 байт до 256 Кбайт. Алгоритм выбора блока оптимального размера работает для резервных копий как на уровне дисков, так и на уровне файлов. Дедупликация выполняется в два этапа: на источнике данных (с помощью агента резервного копирования) и в хранилище (как фоновый процесс, который запускается после завершения копирования).
Dell EMC Avamar	Это программно-аппаратный комплекс с хеш-дедупликацией и блоками данных переменной длины от 1 до 64 Кбайт. Дедупликация сегментов данных переменной длины позволяет значительно ускорить резервное копирование, так как сохраняются только уникальные изменения, внесенные за день. При этом создаются ежедневные полные резервные копии данных для немедленного восстановления в один этап.
HPE Data Protector	Дедупликация имеет две реализации: Dynamic Deduplication с размером блока 4 Кбайт, где используется алгоритм хеширования SHA-1 с контрольной суммой (CRC), и Accelerated Deduplication с алгоритмом поиска подобных объектов в наборах данных. В СХД HPE 3PAR дедупликация производится «на лету» на специальной микросхеме ASIC, установленной в контроллере массива. Это позволяет разгрузить процессоры массива и включить дедупликацию для всех типов данных без потери производительности.
IBM Spectrum Protect (семейство Tivoli Storage Manager)	Дедупликация, выполняющаяся с использованием алгоритмов хеширования SHA-1 и MD-5, реализована на уровне дискового хранилища с размером блока, равным размеру блока СХД. Метаданные хранятся во внутренней СУБД.

Таблица 4. Некоторые продукты резервного копирования с функцией дедупликации

Источник: IBM

Рис. 4. IBM Spectrum Protect (Tivoli Storage Manager, TSM): дедупликация на сервере и на клиенте

ной способности) уменьшается на 99%, а суммарная емкость дисковых систем хранения данных — на 95%.

Система разделяет данные, подлежащие резервному копированию, на сегменты, сжимает их и применяет для каждого уникальный хеш-идентификатор. Затем она определяет, производилось ли ранее резервное копирование сегмента, и копирует только уникальную информацию. Резервное копирование одних и тех же данных никогда не выполняется.

Быстрое одноэтапное восстановление данных исключает необходимость восстанавливать последние целостные полные и инкрементные резервные копии. Надежность сервера Avamar и возможность восстановления данных резервного копирования проверяются ежедневно. Решение позволяет оперативно восстановить данные конкретного приложения.

Avamar можно развертывать и в виде только программного решения. EMC Avamar Virtual Edition (AVE) представляет собой виртуальное устройство с функцией дедупликации для резервного копирования и восстановления. AVE позволяет развернуть полнофункциональный сервер Avamar в среде виртуализации VMware или Microsoft Hyper-V. Когда в качестве системы хранения используется Data Domain Virtual Edition, AVE можно масштабировать до 16 Тбайт.

Среди технологических особенностей решения можно выделить несколько наиболее полезных: наличие специального кеша уникальных файлов и блоков, что позволяет осуществлять обход файловой системы значительно быстрее, чем в случае традиционного резервного копирования; поддержку большинства известных корпоративных приложений, таких как SAP, Oracle, MS SQL и других; поддержку технологии VMware Changed Block Tracking (CBT) для отслеживания измененных блоков (позволяет ускорить процесс резервного копирования и восстановления), а также наличие специального плагина для vCenter для управления прямо из этой консоли.

Среди новых возможностей продукта — поддержка облаков и многоуровневое хранение. Кроме того, Avamar также может предложить вариант организации долговременного хранения в частном облаке — как с использованием системы Data Domain, так и без нее. Data Domain Cloud Tier поддерживает облака Azure, Amazon, Virtustream и любые устройства, использующие протокол S3. Облачное резервное копирование — одна из тенденций в резервировании данных (см. рис. 6).

РЕЗЕРВНОЕ КОПИРОВАНИЕ В ОБЛАКО

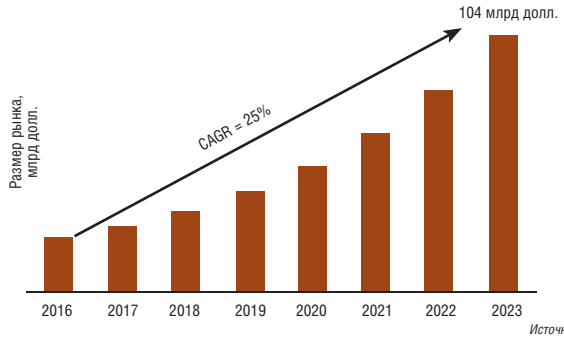
Современные решения дают возможность создавать резервные копии данных в облаке, что позволяет надежно сохранить и восстановить их, высвободив время и ресурсы. Например, система Commvault поддерживает резервное копирование в облако Amazon S3 и другие S3-совместимые хранилища (см. рис. 7).

Исходные данные могут находиться на любой площадке: на стороне клиента, в другом коммерческом ЦОДе или в облаке (см. рис. 8). Таким образом, можно быстро реализовать преимущества резервного копирования данных в облако, используя его как расширение корпоративной ИТ-инфраструктуры. В числе преимуществ такого решения:

- быстрое и надежное резервное копирование, оперативное восстановление данных;
- отсутствие необходимости в дорогостоящих шлюзах и сложных промежуточных решениях;

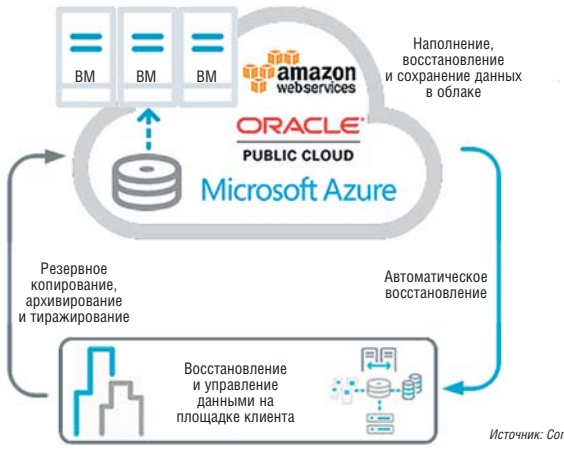
Источник: IBM

Рис. 5. Решение TS7650G ProtecTIER Deduplication Gateway с производительностью до 2500 Мбайт/с использует технологию резервного копирования в реальном времени, позволяющую «вписаться» в окна резервного копирования и избежать нарушения текущей работы



Источник: IDC

Рис. 6. По прогнозу IDC, мировой рынок облачного хранения (Cloud Storage) будет расти в среднем на 25% в год



Источник: Commvault

Рис. 7. Использование объектных облачных хранилищ системой Commvault

По данным Amazon

Рис. 8. Возможные сценарии резервного копирования в облако

- возможность заменить ленточное хранилище облачным;
- использование облака для аварийного восстановления.

Компании все чаще применяют комбинированный подход: дисковые массивы в сочетании с копированием в облако. Такая стратегия хранения резервных копий позволяет ускорить резервное копирование наиболее актуальных данных и снизить стоимость владения соответствующей инфраструктурой резервного копирования. Использование дедупликации дает возможность не только оптимизировать занимаемую резервными копиями емкость хранилищ, но и уменьшить сетевой трафик при резервировании в облако, что делает эту технологию еще более актуальной.

Постоянное развитие и интеграция решений дедупликации данных разработчиками систем резервного копирования и производителями систем хранения будет способствовать большей экономичности предлагаемых решений, снижению стоимости внедрения, более быстрому перемещению резервных копий между территориально удаленными площадками. **LAN**

Сетевые напольные шкафы LINEA N глубиной 1000 мм

Ассортимент шкафов серии LINEA N, выпускаемых ГК IEK, пополнился конструктивами глубиной 1000 мм с различными типами дверей. Двери могут быть обзорными (со стеклом), металлическими, перфорированными (перфорация 80%), располагаться спереди или сзади.

Ширина шкафов составляет 600 мм, высота варьируется: 18, 24, 28, 33, 38, 42 и 47 юнитов. Благодаря двойным боковым стенкам, оснащенным замками и защелками, обслуживание или демонтаж размещенного в шкафу оборудования может выполнять один человек.

Возле кабельных вводов предусмотрены посадочные места для установки щеточных вводов, при использовании которых степень защиты шкафа может быть повышена до IP31. Внутри можно одновременно установить четыре потолочные вентиляторные панели общей мощностью 1000 CFM. Допустимая статическая нагрузка, подтвержденная испытаниями, составляет 1000 кг.

На выбор предлагаются два типа 19-дюймовых профилей: стандартные и L-образные для серверов. Вертикальные монтажные профили имеют двойную маркировку и могут регулироваться по глубине с шагом 20 мм. Максимальная полезная глубина составляет 900 мм.

Шкафы комплектуются трехточечными ригельными замками с тягами. Конструкция может устанавливаться на регулируемые опоры или ролики, а также на регулируемые опоры и ролики одновременно.

Все шкафы поставляются на поддоне в прочной деревянной обрешетке, благодаря чему обеспечивается их целостность и сохранность даже при транспортировке на очень дальние расстояния.

Сетевой радар для обнаружения вторжений Axis D2050-VE

Сетевой радарный датчик Axis D2050-VE способен обеспечить точное и надежное обнаружение движущихся объектов в контролируемых зонах при различных световых и погодных условиях. Устройство отправляет в реальном времени информацию о местоположении, скорости, ракурсе и размере движущегося объекта. Дальность обнаружения у этого устройства больше, чем у пассивных ИК-детекторов, а поле обнаружения шире. Случаи ложного срабатывания на перемещения насекомых и мелких животных, движущиеся тени и световые блики сведены к минимуму.

Датчик Axis можно использовать в качестве автономного устройства, а также в составе системы видеонаблюдения. Благодаря открытому интерфейсу он совместим с камерами Axis, легко интегрируется с программным обеспечением AXIS Camera Station, AXIS Camera Management и другими системами для управления видеонаблюдением, что обеспечивает удобство эксплуатации и обслуживания. Запуск видеозаписи на камере, активация громкоговорителя или включение освещения для отпугивания нарушителей и улучшения условий визуального подтверждения с помощью камер легко настраиваются.

Это недорогое монтируемое на стену устройство предназначено главным образом для использования вне помещений. Угол охвата контролируемой зоны обнаружения составляет 120 градусов, дальность — 50 м. Питание по технологии Power over Ethernet Plus (PoE+) упрощает установку датчика, а благодаря высокой степени защиты классов IP66, IK08 и NEMA 4X он может использоваться в неблагоприятных климатических и прочих условиях. Датчик защищен от вандализма и может эксплуатироваться при температурах от –40 до +60 °C

Четырехканальные усилители аудиосигналов Converge PA

Серия усилителей аудиосигналов ClearOne Converge PA предназначена для профессионального применения. Четырехканальные усилители класса D дополняют коммутаторы и аудиоплатформы, позволяя добиться четкого и чистого звучания. Все каналы являются независимыми, поэтому одно устройство может обслуживать сразу четыре зоны.

Модели PA 460 и PA 4120 оснащаются защитой от короткого замыкания линии громкоговорителей, от перегрузки по входу и выходу, а также от перегрева свыше +55°C. Индикатор наличия сигнала на входе и выходе каждого канала отображается в реальном времени, позволяя оперативно найти и устранить причину неполадок. Кроме того, предоставляется возможность выбора нагрузки путем переключения из низкоомного режима в трансляционный. Иначе говоря, к одним выходам можно подключать нагрузку 8 Ом, а к другим — 70/100 В, применяя усиление и в холлах, и в кабинетах. Модели различаются главным образом уровнем мощности: PA 460 обеспечивают 4×60 Вт, PA 4120 в два раза больше — 4×120 Вт.

Входная и выходная группы реализованы на клеммных блоках Phoenix, максимальный входной уровень составляет +20 dBu. Для точечной подстройки усиления, активации режима ожидания и фильтра High Pass Filter (HPF) можно использовать ручное переключение, для чего на передней панели предусмотрена индикация. Функция HPF наиболее эффективна, когда частота среза должна составлять 80 Гц (рабочий диапазон — от 80 Гц до 20 кГц).

Для экономии электроэнергии предусмотрен режим автоотключения: автоматический переход в режим ожидания выполняется отдельно для каждого канала, когда входной сигнал отсутствует в течение 1 мин. Если такой необходимости нет, режим ожидания можно отключить на каждом канале независимо. Еще одна особенность — возможность подачи энергии от аварийного источника питания 24 В постоянного тока (ИБП или генератора) при сбое или выходе из строя основного.

cnPilot

Wi-Fi премиум-класса
по доступным ценам

cambiumnetworks.com/wifi-ru

Cambium Networks™

ИНТЕРНЕТ
ТЕЛЕФОНИЯ · ТЕЛЕВИДЕНИЕ

В ОФИСЕ, КВАРТИРЕ И КОТТЕДЖЕ

для физ. лиц
до 100 Мбит/с

для юр. лиц
до 400 Мбит/с

Срок подключения - от 3 до 7 дней.

КРЕДО-ТЕЛЕКОМ
нам доверяют с 1995г.

- широкополосный доступ в Интернет со скоростью до 400 Мбит/с;
- каналы связи VPN, L2 VPN, VPLS;
- подключение соединительных линий и телефонных номеров в кодах 495/496/498/499;
- виртуальная АТС;
- организация общественных хот-спот Wi-Fi и закрытых корпоративных Wi-Fi зон;
- виртуальный и физический хостинг;
- облачный сервер.

Оборудование предоставляется клиентам во временное пользование бесплатно.

8-800-100-8281
БЕСПЛАТНЫЙ КРУГЛОСУТОЧНЫЙ ТЕЛЕФОН

НАШ САЙТ: WWW.RMT.RU