# СЕТЕВАЯ ФАБРИКА: НОВЫЙ ПОДХОД К ПОСТРОЕНИЮ КОРПОРАТИВНЫХ ЛВС

**СЕРГЕЙ ПОЛИЩУК**
*sepolisc@cisco.com*

В статье описаны трудности, стоящие сегодня перед корпоративной службой IT, и предложен современный подход к их устранению на основе сетевой фабрики Cisco Software-Defined Access (SD-Access). Рассмотрены ключевые компоненты и технологии, лежащие в основе Cisco SD-Access, а также принципы их работы. Подробно проанализированы преимущества, предлагаемые фабрикой SD-Access бизнесу.

## ПОСТАНОВКА ЗАДАЧИ

Сегодня корпоративная сеть превратилась в важнейший инструмент ведения бизнеса. Поверх сети действует множество бизнес-процессов, связанных с передачей информации. Поэтому обеспечение непрерывности их работы, а значит, и высокой доступности сети становится приоритетным требованием бизнеса.

Быстрое развитие технологий и цифровизация приводят к тому, что количество использующих сеть бизнес-процессов продолжает расти. В результате необходима поддержка новых сервисов, устройств, пользователей и т. д.

Но подобные требования — обеспечение высокой доступности и внедрение новых сервисов — противоречат друг другу. С одной стороны, для выполнения первого требования сети нужна стабильность. С другой — второе требование по определению связано с изменениями, то есть с нестабильностью.

Это представляет собой фундаментальную проблему для типовой, классической корпоративной сети, поскольку противоречивые требования предъявляются к одной и той же IP-сети.

Существует хорошо зарекомендовавший себя подход к решению сложных задач — декомпозиция, которая предусматривает разбиение одной задачи на несколько более простых. Примеры подобного подхода — семиуровневая модель OSI или четырехуровневая модель DoD в решении задачи сетевого взаимодействия.

Декомпозицию можно применить и в данном случае, воспользовавшись концепцией сетевой фабрики, или оверлея (overlay) (рис. 1).

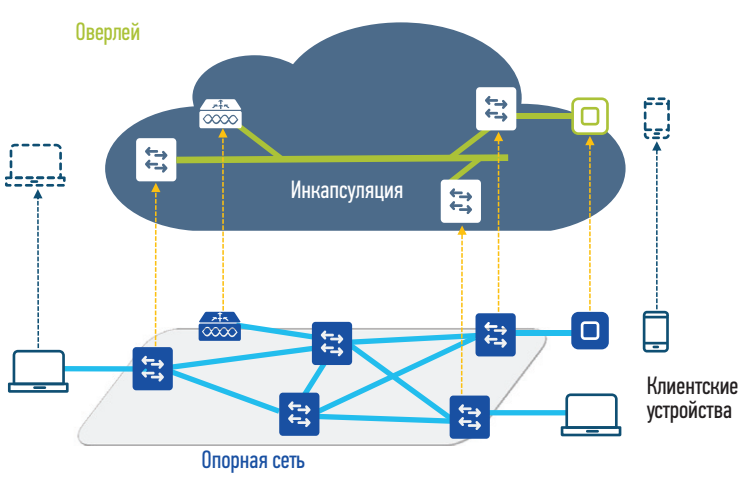



**РИС. 1.** ▶ Концепция сетевой фабрики (оверлея)

Оверлей — это логическая топология, построенная поверх некоторой низлежащей топологии (underlay), опорной сети. Оверлей всегда использует какой-либо вид инкапсуляции трафика для передачи поверх опорной сети, например GRE, CAPWAP, VXLAN и т. д.

Таким образом, в сетевой фабрике присутствуют две топологии. Первая, нижележащая топология, обеспечивает надежный транспорт на основе маршрутизируемой сети. Она не реализует сервисы и политики. Эту задачу выполняет вторая, оверлейная сетевая топология. Она отделена от низлежащей топологии, как, например отделены друг от друга протоколы разных уровней модели OSI.

Появление двух сетевых топологий дает развязку противоречащих друг другу требований. В этом и заключается принципиальная разница между классической сетью и сетевой фабрикой, что и позволяет сетевой фабрике преодолеть трудности, с которыми не может справиться классическая сеть.

## ЧТО ТАКОЕ CISCO SD-ACCESS?

Реализацию концепции сетевой фабрики уже можно наблюдать во многих корпоративных сетях. Так, идея фабрики на основе туннелей CAPWAP давно используется в централизованной архитектуре корпоративных беспроводных ЛВС. Другой пример — сети ЦОД на базе решения

Cisco Application Centric Infrastructure (ACI). Фабрики получают распространение и в территориально-распределенных сетях в виде технологий SD-WAN, в частности Cisco IWAN.

Наступает время для появления сетевой фабрики и в кампусных сетях (рис. 2).

Cisco Software-Defined Access (SD-Access) — это реализация концепции сетевой фабрики Cisco для кампусной сети с централизованными средствами управления, автоматизации и оркестрации, а также мониторинга и аналитики.

Данные средства предоставляет контроллер Cisco DNA Center — ключевой элемент решения. Также DNA Center обеспечивает веб-интерфейс администратора и интерфейсы API.

DNA Center работает совместно с сервером контроля доступа Cisco Identity Service Engine (ISE), который предоставляет фабрике сервисы аутентификации, авторизации и контроля доступа (AAA), обеспечивает динамическое помещение пользователей фабрики в группы и средства управления политиками взаимодействия между группами. ISE необходим для реализации в фабрике политики безопасности организации.

С точки зрения сетевой инфраструктуры фабрика состоит из устройств, выполняющих следующие ключевые роли:

- Control Plane Nodes ведут учет текущего местоположения клиентских устройств в пределах фабрики. Это необходимо для свободного перемещения пользователей в пределах фабрики с сохранением назначенных политик и обеспечения мобильности.
- Fabric Border Nodes нужны для подключения фабрики к «внешнему миру» — например, к другим частям корпоративной сети, построенным не на основе фабрики, к Интернету и т. д.
- Fabric Edge Nodes обеспечивают подключение к фабрике клиентских устройств и точек радиодоступа.
- Fabric Wireless Controller представляет собой контроллер беспроводных ЛВС, действующий в составе фабрики.
- Intermediate Nodes поддерживают связь между перечисленными выше устройствами. Они не выполняют никаких функций оверлея, а лишь реализуют опорную, нижележащую сетевую топологию.

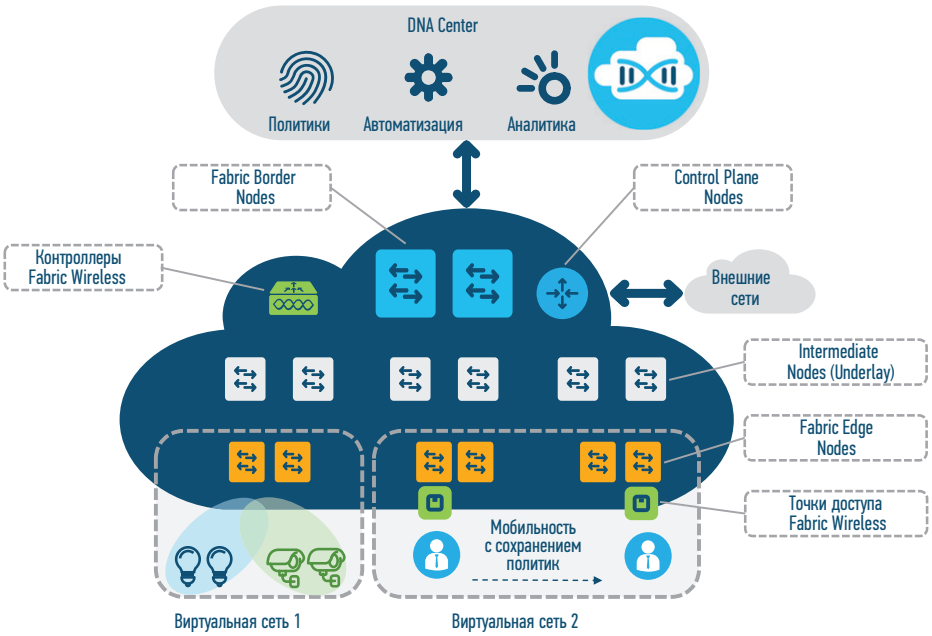



**РИС. 2. ▲** Архитектура сетевой фабрики Cisco SD-Access

С точки зрения технологий data plane фабрики Cisco SD-Access построен на базе инкапсуляции Virtual Extensible LAN (VXLAN). Control plane оверлея использует протокол Locator/ID Separation Protocol (LISP). Политики реализуются с помощью тегов Scalable Group Tag (SGT) технологии Cisco TrustSec. Рассмотрим эти технологии подробнее.

## Data plane оверлея: VXLAN

Data plane фабрики Cisco SD-Access построен на основе инкапсуляции VXLAN с Group Policy Option (VXLAN-GPO). Важное преимущество VXLAN заключается в сохранении первоначального Ethernet-заголовка фрейма. В результате обеспечивается мобильность хостов фабрики не только на Уровне 3, но и на Уровне 2. Это дает гибкий и универсальный транспорт (рис. 3).

Трафик data plane фабрики (фреймы Уровня 2) инкапсулируется в пакеты VXLAN и отправляется по сети. С точки зрения промежуточных устройств фабрики это стандартные пакеты IP со вложенными сегментами UDP, адресованными на порт 4789.

В решении Cisco SD-Access инкапсуляцию трафика в пакеты VXLAN и обратно выполняют пограничные

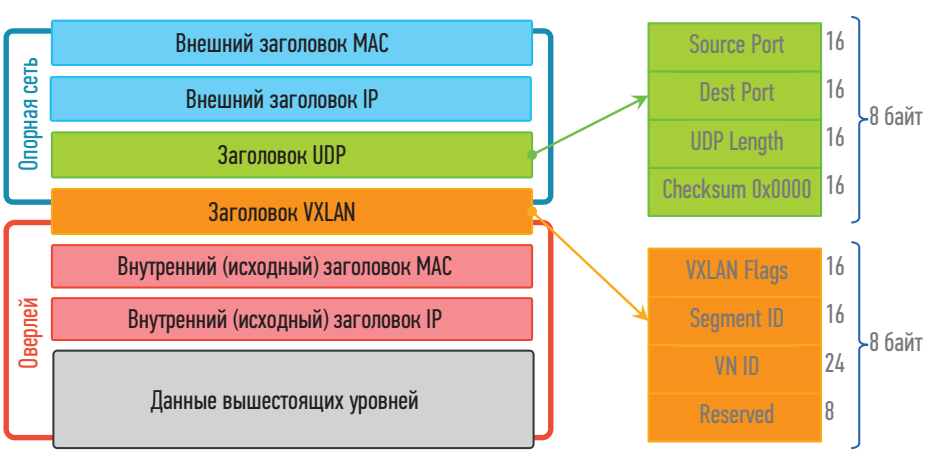



**РИС. 3. ▼** Инкапсуляция в сетевой фабрике

устройства фабрики: Border Nodes и Edge Nodes.

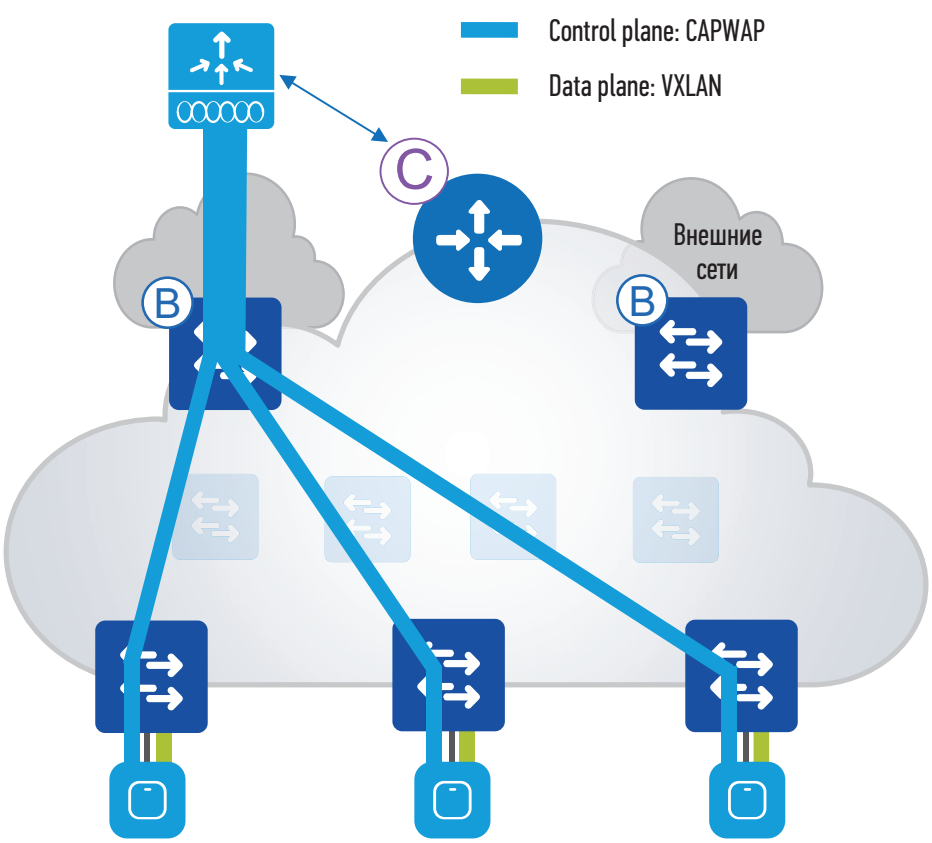
SD-Access также обеспечивает интеграцию беспроводных сетей в фабрику (рис. 4). Данный режим работы называется Fabric Enabled Wireless (FEW). В отличие от централизованной архитектуры БЛВС в режиме FEW трафик пользователей БЛВС туннелируется на коммутатор доступа, а не на контроллер. Таким образом, трафик и проводных, и беспроводных клиентов поступает непосредственно на коммутаторы Edge Node.

В результате обеспечивается одинаковая обработка трафика проводных и беспроводных пользователей, оптимизация путей передачи трафика БЛВС, устранение потенциальных узких мест, характерных для стыка контроллера БЛВС и проводной сети.

Control plane и management plane беспроводной ЛВС в режиме FEW остаются централизованными на контроллере Fabric Wireless.

Таким образом, архитектура беспроводной сети при интеграции в фабрику получает «лучшее из двух миров».

**РИС. 4. ▼**
Интеграция беспроводной ЛВС в фабрику Cisco SD-Access: B — Border Node; C — Control Plane Node




### Control plane оверлея: LISP

Мобильность хостов на уровнях 2 и 3 — неотъемлемое свойство фабрики. С точки зрения data plane мобильность обеспечивается технологией VXLAN, а в качестве control plane применяется протокол LISP.

LISP — это очень эффективный протокол, оптимизированный для мобильности хостов. Фабрика содержит централизованную базу данных пользователей Host Tracking Database (HTDB), работающую на устройствах роли Control Plane Nodes. HTDB хранит информацию о соответствии клиентского хоста Endpoint ID текущему местоположению в пределах фабрики, а также ряд дополнительных атрибутов.

Пограничные устройства фабрики, используя протокол LISP, запрашивают базу HTDB, когда им нужно передать пакет на клиентский хост с неизвестным местоположением, и сохраняют данную информацию в локальном кэше.

Информация поступает в базу от пограничных устройств фабрики по мере подключения и перемещения клиентских хостов.

Таким образом, Cisco SD-Access позволяет хостам свободно перемещаться в пределах фабрики без смены адресов и обеспечивает их мобильность.

### Политики контроля доступа и сегментация: TrustSec

Фабрика предлагает гибкие и масштабируемые средства для реализации политик контроля доступа к ресурсам, а также сегментации и микросегментации пользователей.

Сегментация пользователей долгое время выполнялась с помощью виртуальных топологий, собираемых из VLAN, VRF, MPLS VPN, туннелей и других подобных средств. Такой подход весьма ресурсоемкий и работает тем хуже, чем больше динамики в среде сегментации и чем гранулярнее такая сегментация нужна.

Для решения этой проблемы компания Cisco разработала технологию TrustSec, использующую метки Scalable Group Tag (SGT) вместо IP-адресов в качестве критерия принадлежности пакета той или иной группе пользователей и специализированные списки SGACL для контроля доступа.

Такой подход позволяет отделить функции адресации от контроля доступа, дает сети гибкость и автоматизацию применения политик контроля доступа.

В фабрике Cisco SD-Access значение метки передается в составе заголовков VXLAN оверлея. Заголовок VXLAN содержит поля VN ID и Segment ID (24- и 16-разрядные соответственно), как показано на рис. 3. Эти поля предназначены для передачи информации о принадлежности пакета определенной виртуальной сети VN (адресуется свыше 16 млн VRF) и группе SGT технологии TrustSec (адресуется свыше 64 тыс. меток). Таким образом, TrustSec изначально является неотъемлемым функционалом фабрики. Кроме того, инкапсуляция метки SGT в заголовок VXLAN облегчает внедрение TrustSec — ведь от промежуточных устройств опорной сети не требуется работа с метками.

Контроль доступа, настройка и внедрение политик доступа производятся на сервере Cisco ISE. В результате Cisco SD-Access предлагает готовые автоматизированные

средства реализации политики контроля доступа организации, а также сегментации и микросегментации пользователей.

## ЗАЧЕМ SD-ACCESS БИЗНЕСУ

Технические особенности и преимущества новых технологий, как правило, интересны IT-специалистам. Но ведь корпоративная сеть строится прежде всего для решения задач бизнеса. А задачи, интересующие бизнес, в конечном счете относятся к трем ключевым направлениям:

1. Повышение выручки.
2. Сокращение издержек.
3. Снижение рисков.

Рассмотрим подробнее, каким образом сетевая фабрика может оказать помощь бизнесу в каждом из этих направлений. Сравним две условные сети: классическую и на основе архитектуры Cisco SD-Access (далее — сеть SD-Access).

Под классической сетью будем понимать кампусную сеть с коммутируемым уровнем доступа и маршрутизируемым ядром. Предположим, что контроль доступа в сети реализуется путем задания списков контроля доступа, а большинство операций по настройке, поиску и устранению неисправностей проводится вручную. Сеть использует RADIUS-сервер для аутентификации, авторизации и контроля доступа пользователей.

Под сетью SD-Access будем подразумевать сеть, построенную на основе сетевой фабрики Cisco SD-Access, включающей инфраструктуру, контроллер DNA Center, а также сервер контроля доступа Cisco ISE.

### Повышение выручки

Корпоративные сети, в отличие от сетей операторов связи, по своей природе связаны с выручкой компании не напрямую, а косвенно, за счет обслуживания бизнес-процессов.

Разница между классической корпоративной сетью и сетью SD-Access заключается в том, что сеть SD-Access позволяет более оперативно запускать бизнес-процессы, опирающиеся на сеть, быстрее получать нужный бизнес-результат.

Бизнес-результатом может быть не только запуск новых бизнес-процессов, приносящих прибыль, но и оптимизация имеющихся процессов, приводящая к повышению продуктивности пользователей, — например, внедрение новых мультимедийных систем совместной работы.

Время — деньги, и в условиях цифровизации влияние IT на скорость выполнения бизнес-инициатив становится все заметнее. Увеличение скорости может приводить к существенным финансовым результатам. А в некоторых случаях скорость настолько критична, что он нее полностью зависит успех всей бизнес-инициативы. В конечном счете выигрыш в скорости способствует получению конкурентного преимущества и расширению занимаемой доли рынка.

Сеть SD-Access помогает этого добиться за счет уровня оркестрации и автоматизации функций, недоступного в классической сети. Весь рабочий процесс DNA Center ориентирован в первую очередь на бизнес-намерения, по принципу «сверху вниз». Администратор задает высокоуровневые детали сети и политики, а DNA Center транслирует их в конкретные настройки сетевого оборудования. Такой подход позволяет бизнесу быстро получить действующую сеть с нужными политиками.

В классической сети внедрение политик, которые в конечном счете и дают нужный бизнесу функционал, обычно затруднено в связи со сложными и неконсистентными конфигурациями, а также отсутствием удобных критериев применения политик (из-за чего в качестве такого критерия обычно используется IP-адрес). В результате схема адресации становится перегруженной возложенными на нее задачами, в настройках функций и политик появляется много взаимозависимостей, конфигурация сети становится весьма негибкой — внесение изменений занимает все больше времени и несет за собой риски. А ведь именно это, как правило, и нужно делать для выполнения повседневных бизнес-задач и запуска новых бизнес-инициатив.

В связи с неоднородностью конфигураций и различиями в функционале оборудования, типичными для классической сети, итоговое решение тоже получается неоднородным относительно применения технологий и политик. Это замедляет и усложняет внедрение.

Может оказаться, что нужная технология требует наличия сквозного функционала во всех промежуточных устройствах сети. Невыполнение этого условия сделает внедрение технологии затруднительным или вообще невозможным.

Сеть SD-Access предлагает решение данной проблемы благодаря разделению функций транспорта и политик между опорной сетью и оверлеем, автоматизированному внедрению консистентных конфигураций и удобным средствам применения политик на основе меток SGT (Scalable Group Tag). В результате нужные политики можно ввести в действие быстро и надежно.

Кроме того, решение однородно и с точки зрения внедрения политик — функционал реализуется на пограничных узлах фабрики, а транспортная сеть для них прозрачна. Такая прозрачность весьма удобна и с позиции требований к функционалу устройств опорной сети — ведь от них нужен только транспорт IP-пакетов. Тем самым заметно упрощается задача сквозного наличия необходимых функций, характерная для классической сети.

Таким образом, сеть SD-Access предлагает бизнесу значительный выигрыш в скорости внедрения соответствующих сервисов и политик.

### Снижение издержек

По данным внутреннего исследования Cisco, в 2016 году в корпоративных сетях более 90% изменений производилось вручную, даже несмотря на широкий выбор систем управления, и значительная часть времени IT-персонала тратилась лишь на поддержание сети в работоспособном состоянии.

Компаниям в любом случае нужны квалифицированные IT-специалисты для эксплуатации как классической сети, так и SD-Access. Но последняя предоставляет возможность значительно сократить затраты времени на работу с низкой добавленной ценностью, например на выполнение рутинных операций.

Компания была бы в выигрыше, если бы сеть позволяла перенаправить время и усилия IT-персонала с рутины на решение более важных, стратегических задач, на оптимизацию поддержки существующих бизнес-процессов и помощь в запуске новых, на получение более высоких результатов.

Сотрудники были бы в выигрыше, если бы использовали рабочее вре-

мя не на рутинные операции, мало помогающие повысить квалификацию и ценность на рынке труда, а на изучение передовых технологий, внедрение новых решений и в конечном счете на помощь работодателю в достижении конкретных бизнес-результатов.

Сеть SD-Access предоставляет такие возможности и компании, и сотрудникам. Оркестрация и автоматизация, ориентация на внедрение политик и бизнес-намерений, возможности быстрого внедрения элементов сетевой инфраструктуры и клиентских устройств по всей компании, функционал аналитики экономят время и силы, позволяют использовать их максимально продуктивно.

### Снижение рисков

Сеть SD-Access помогает существенно снизить риски компании, связанные с недоступностью бизнес-процессов и угрозами информационной безопасности.

По данным Gartner, стоимость часа простоя бизнес-процессов в корпоративной среде может составлять сотни тысяч долларов США.

Кампусная сеть, сеть центрального офиса, для которой в первую очередь и предназначено решение SD-Access, — ключевой компонент типовой корпоративной сети. Обычно на нее опираются практически все бизнес-процессы, связанные с сетью.

Наиболее распространенная причина сбоев в кампусной сети и, как следствие, недоступности бизнес-процессов — человеческий фактор. А по данным Cisco, по этой же причине происходит около 70% нарушений корпоративных политик.

Это неудивительно, поскольку современные сети сложны. Контроллер DNA Center берет на себя значительную часть рутинных операций, скрывает сложность сети, предоставляя человеку возможность сосредоточиться на задании политик и бизнес-намерений. Широкие возможности контроллера в области оркестрации и автоматизации значительно снижают вероятность сбоев из-за человеческого фактора.

Каждая классическая сеть уникальна своей комбинацией настроенных функций, набором оборудования и программного обеспечения, а также топологией. Хотя вендоры и прилагают значительные усилия по тестированию новых продуктов и контролю их качества, существует очень высокая вероятность, что подобная уникальная конфигурация не будет протестирована в точно таком виде, как внедрена. Это повышает риски введения в эксплуатацию.

В случае автоматического внедрения с помощью контроллера наблюдается иная картина. В сеть вводятся конфигурации, созданные в результате совместной деятельности разработчиков элементов сетевой инфраструктуры и контроллера, архитекторов лучших практик внедрения. Вендору гораздо проще протестировать такие конфигурации, поскольку количество комбинаций функций и степень их уникальности значительно ниже, чем в классической сети. Кроме того, подобные «типовые» конфигурации будут не уникальны, как в случае классической сети, а применены во многих сетях по всему миру. Это снижает риски внедрения.

Другая проблема классических сетей заключается в неполном внедрении нужного функционала, не следовании или частичном следовании рекомендациям и лучшим практикам. Другими словами, имеющееся оборудование и ПО могут располагать функционалом безопасности, высокой доступности и т. д., необходимым для снижения рисков. Но вовсе необязательно, что данный функционал действительно введен в эксплуатацию из-за перегруженности сотрудников IT рутинными операциями и опасений, связанных с трудностями внедрения. В результате бизнес не получает пользу от оплаченных, но не внедренных функций, не снижает риски для выполнения бизнес-процессов.

К тому же в условиях нехватки времени IT-персонала консистентность конфигураций устройств классической сети имеет тенденцию к снижению, а реализация временных полумер вместо системных решений — к повышению. Это увеличивает сложность сети, страдают качество и объем выполненных работ. В результате риски сбоев и нарушений политики безопасности опять растут.

Сеть SD-Access предлагает решение этих проблем за счет автоматизации внедрения нужного функционала и внесения дальнейших изменений.

Кроме того, возможности контроллера в области оркестрации и автоматизации дополняются функционалом аналитики. DNA Center обеспечивает IT-персонал полной и детальной информацией об инцидентах, происходящих в сети, выводами об их влиянии на сеть и пользователей. Эти сведения помогают быстро предпринять конкретные действия, направленные на устранение инцидентов. Также DNA Center проводит анализ трендов и помогает на их основе реализовать проактивный подход к эксплуатации сети.

Сеть SD-Access имеет интегрированный функционал сегментации пользователей за счет технологий виртуальных сетей и TrustSec, а также средства поведенческого анализа Stealthwatch и выявления угроз в зашифрованном трафике Encrypted Traffic Analytics (ETA).

В результате сеть SD-Access предлагает бизнесу инструментарий, позволяющий значительно снизить риски сбоев бизнес-процессов, вызванных как человеческим фактором, так и угрозами информационной безопасности.

## ЗАКЛЮЧЕНИЕ

Фабрика Cisco Software-Defined Access (SD-Access) представляет собой новый подход к созданию корпоративных ЛВС и делает большой шаг вперед по сравнению с классическими сетями. По значимости этот шаг можно сравнить с переходом от компьютеров с интерфейсом командной строки к компьютерам с графическим интерфейсом пользователя.

Возможности фабрики в области автоматизации и оркестрации помогают службе IT исполнять требования бизнеса быстро и качественно, минимизировать рутину и сосредоточиться на задачах, имеющих более высокую ценность для работодателя и дающих конкурентные преимущества на рынке труда.

А бизнес получает преимущества в скорости выполнения инициатив и решения задач, опирающихся на сеть, более эффективное использование ресурсов, возможности повышения доступности и безопасности сети.

В конечном счете фабрика помогает бизнесу добиться улучшений по всем трем направлениям — увеличению выручки, сокращению издержек и снижению рисков. ⬢