ПОДХОДИ И ПРИЛОЖЕНИЯ ЗА СОФТУЕРНО ДЕФИНИРАНИ МРЕЖИ

Мирослав Славов, Делян Генков*

Технически университет - Габрово, ул. Хаджи Димитър 4, Габрово, България
**кореспондиращ автор: dgenkov@tugab.bg*

SOFTWARE DEFINED NETWORKING APPLICATIONS AND APPROACHES

Miroslav Slavov, Delyan Genkov*

Technical University - Gabrovo, 4, Hadji Dimitar Str., Gabrovo, Bulgaria;
**Corresponding author: dgenkov@tugab.bg*

Abstract

Software defined networking is a modern way to configure and monitor today's networks. Instead of configuring every device separately, this approach allows centralized configuration and monitoring of the networking devices through a software applications. There are still no clear definitions for what exactly is a software defined network. Different vendors have their own appoaches in creating such hardware and applications.

Present paper describes some solutions and applications of software defined networks..

Keywords: Software Defined Network; SDN; Applications; Approaches.

ВЪВЕДЕНИЕ

Софтуерно дефинираните мрежи (Software Defined Network – SDN) е обещаваща технология, която все повече набира популярност и все повече производители на мрежово оборудване се ориентират към нея. Въпреки това съществуват множество проблеми и неясноти по отношение на начина на реализиране и начина на работа на устройствата в тези мрежи. Поради тази причина много от водещите компании в областта на мрежовото оборудване разработват свои собствени решения, които понякога се различават значително по отношение на реализацията и начина на фунциониране.

ИЗЛОЖЕНИЕ

SDN е подход за изграждане на мрежи, които използва софтуерно базирани контролери и приложно програмни интерфейси (API) за комуникация с по-ниско разположената хардуерна инфраструктура и за насочване на трафика в мрежата. [1]

В традиционните мрежи се разполага със специфични мрежови устройства, като напр. маршрутизатори, комутатори и защитни стени, които изпълняват определени задачи. [2]

Мрежовото устройство има различни функции, които трябва да изпълнява. Например, някои от нещата, които рутерът трябва да направи, за да препрати IP пакет са:

- трябва да провери IP адреса на местоназначението в маршрутизиращата таблица, за да разбере къде да препрати пакета;
- необходими са маршрутизиращи протоколи като OSPF, EIGRP или BGP за научаване на мрежите, добавени в таблицата;
- трябва да се използва ARP, за да

разбере MAC адреса на следващото устройство (хоп) или крайния получател и да промени MAC адреса на получателя в Ethernet рамката;

- времето на живот (Time to Live - TTL) в IP пакета трябва да се намали с 1 и контролната сума в заглавната част на IP пакета трябва да се изчисли наново;
- контролната сума на Ethernet рамката трябва да се преизчисли.

Всички тези задачи се изпълняват в някоя от следните три равнини:

- *Контролна равнина (control plane)*
- *Равнина за данни (data plane)*
- *Равнина за управление (management plane)*

Контролна равнина

Контролната равнина е отговорна за обмен на маршрутизираща информация, изграждане на ARP таблицата и т.н. Някои от задачите, които се изпълняват от контролната равнина са:

- научаване на MAC адреси за изграждане на таблица;
- изпълнение на STP за създаване на топология без цикли;
- изграждане на ARP таблици;
- изпълнение на маршрутизиращи протоколи и изграждане на маршрутизираща таблицата;

Равнина за данни

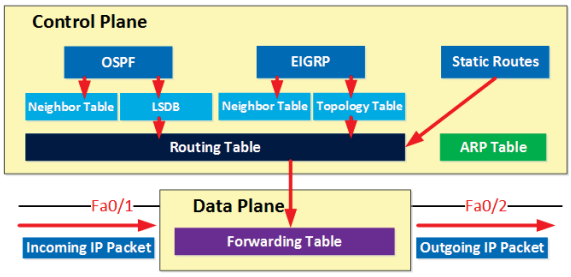
Равнината за данни е отговорна за препращането на трафика. Тя разчита на информацията, която контролната равнина предоставя. Задачи, за които се грижи са:

- опаковане и разопаковане на пакети;
- добавяне или премахване на заглавия като 802.1Q;
- съпоставяне на MAC адреси за пренасочване;
- съпоставяне на IP адреса в полето за получател с маршрутизиращата таблицата;
- променя адресите на източника и получателя, когато се използва NAT;
- изхвърляне на трафик в съответствие със списъците за достъп.

Задачите на равнината за данни трябва да се изпълняват възможно най-бързо, поради което пренасочването на трафика се извършва от специализиран за задачите хардуер (Application-Specific Integrated Circuit – ASIC) и TCAM (Ternary Content Addressable Memory) таблици.

Равнина за управление

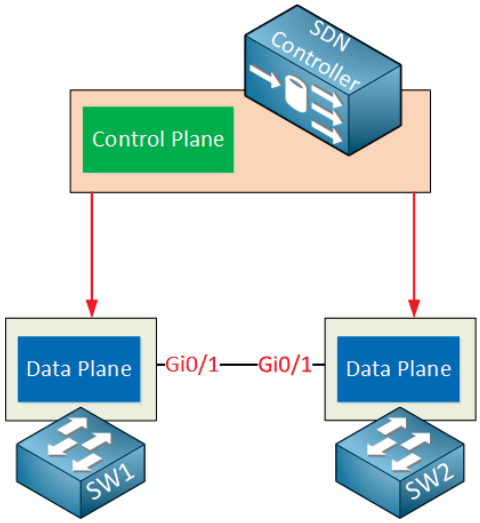
Равнината за управление се използва за достъп и управление мрежовите устройства. Например достъп устройството чрез telnet, SSH или конзолен порт.



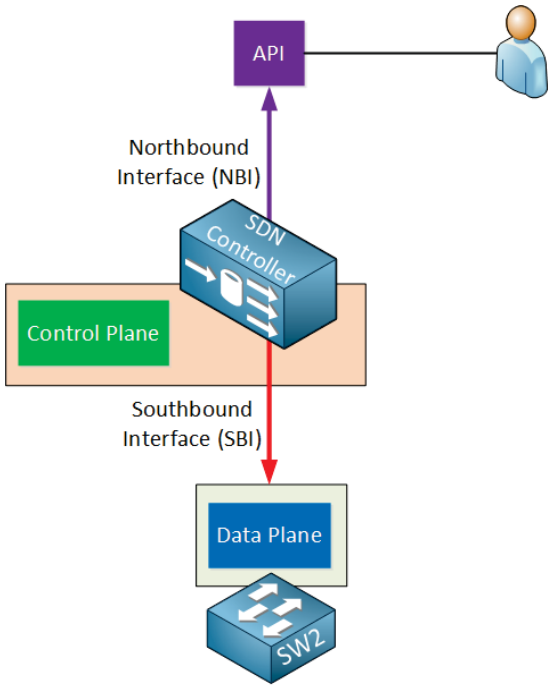
***Фиг. 1**. Контролна, равнина за данни и равнина за управление при традиционните мрежи [2]*

При традиционните мрежи трите равнини са разположение във всяко едно устройство (фиг. 1) и всяко устройство може да изпълнява функции от която и да е равнина или от няколко равнини, което води до разпределение на контролната равнина.

При SDN се реализира разпределение на контролната и равнината за данни, като контролната равнина се централизира, а равнината за данни се разпределя между няколко устройства (фиг. 2). За реализирането на контролната равнина се използват специализирани устройства, наречени SDN контролери. Тези контролери реализират два интерфейса, осъществяващи връзка към останлите две равнини – тази за данни и за управление.



***Фиг. 2**. Контролна и равнина за данни при софтуерно-дефинираните мрежи (SDN) [2]*



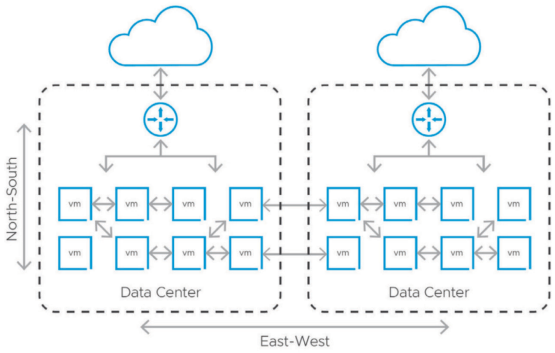
***Фиг. 3**. Северен (northbound) и южен (southbound) интерфейс на SDN контролера [2]*

Двата интерфейса се наричат северен (Northbound Interface – NBI), осъществяващ връзката към равнината за управление, позволяващ управление на контролера и южен интерфейс (Southbound Interface – NBI), осъществяващ връзката към равнината за данни (фиг. 3)

Подходи

Различните компании, занимаващи се с разработка и доставка на мрежово оборудване имат свои собствени реализации на SDN, като някои от тях се базират на софтуерни, други и на хардуерни решения. Някои компании реализират своите решения и на базата на това как се реализират мрежите и каква е преобладаващата посока на трафика.

Някои от SDN мрежите се реализират за да осъществят връзка между отделни виртуални мрежи в един или отделни центрове за данни. Тъй като в тази ситуация трафикът е между виртуалните машини е възможно той да не премине през точка на обединяване (aggregation point), поради което този трафик се нарича и неагрегиран трафик, но е познат като трафик Изток- Запад (East-West traffic). Той е показан на фиг. 4.



***Фиг. 4**. Трафик Изток-Запад (East-West) и трафик Север-Юг (North-South)[3]*

Cisco Systems

Като една от водещите компании в областта на мрежовото оборудване Cisco Systems предлага решение и в областта на SDN. По отношение на управление на трафика в центъра за данни или трафикът Изток-Запад, компанията предлага решение, наречено Cisco ACI (Application Centric Infrastructure).

Cisco ACI опростява управлението на мрежата в центъра за данни и подобрява сигурността чрез предоставяне на централизиран подход, ориентиран към приложението. [4]

С автоматизация и контрол, базиран на политики, той позволява на постигане на гъвкави ИТ операции и ускорява цифровата трансформация в центъра за данни.

Друга важна особеност Cisco ACI е способността му да поддържа мултиоблачни среди.

Някои от предимствата на Cisco ACI включват:

1. опростени мрежови операции;
2. последователно поведение на приложението;
3. повишена гъвкавост и мащабируемост;
4. подобрена сигурност;
5. Поддръжка на много-облачна среда.

Основните блокове на Cisco ACI включват контролерът Application Policy Infrastructure Controller (APIC) и комутаторите Nexus 9000 серии. (фиг. 5)

***Фиг. 5**. Cisco ACI инфраструктура [4]*

Други SDN се реализират за да осъществят връзка между устройства, разположени в кампус мрежи или мрежи в различни клонове на компания и Интернет. Обикновено този трафик е филтриран и преминава през точка, в която той се обединява. Този трафик се нарича трафик Север-Юг (North-South traffic – фиг. 4)

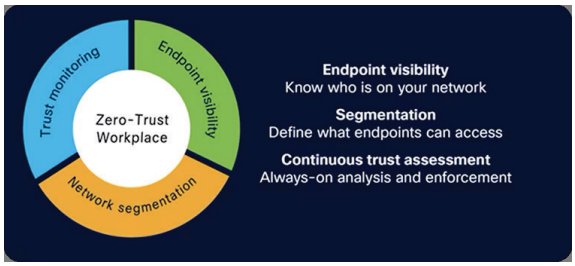
Cisco Systems

По отношение на този тип трафик от компанията Cisco Systems предлагат решение наречено Cisco Application Policy Infrastructure Controller – Enterprise Module – APIC-EM, базирано на контролера на Cisco API – APIC. В последствие компанията заменя това решение с Cisco Software-Defined Access (Cisco SD-Access), което е и актуалното и препоръчвано решение на компанията по отношение на трафик Север-Юг.

Cisco SD-Access позволява реализирането на т.нар. работна среда с нулева довереност (Zero-Trust Workplace), като позволява създаване на правила за сигурност по отношение на устройствата, разположени в мрежата, постоянно наблюдение на тези устройства и изолирането им при откриване на заразени или устройства, представляващи заплаха за мрежата.

Възможности на работната среда с нулево доверие

Cisco SD-Access помага за рационализиране на процеса на предоставяне на достъп до потребители и устройства, като същевременно намалява повишения риск от неизвестни IoT устройства. (фиг. 6) Чрез използване на мрежова инфраструктура и телеметрия за информиране и налагане на сигурността, SD-Access може да предостави възможности на работното място с нулево доверие за IoT крайни точки и управлявани потребителски устройства, като същевременно помага да се осигури непрекъснат доверен достъп.



***Фиг. 6**. SD-Access Zero-Trust Workplace [5]*

Реализирането на Zero-Trust Workplace чрез Cisco SD-Access позволява:

- идентифициране и проверка на всички крайни точки и потребители, включително IoT крайни точки, които се свързват към мрежата
- създаване на политика и сегментиране, за осигуряване на достъп с най-малко привилегии въз основа на крайна точка и потребителски тип
- непрекъснато наблюдаване на поведението на крайната точка, включително криптиран трафик, за да се осигури съответствие
- спиране разпространението на заплахи, включително ransomware, като се постави под карантина всяка крайна точка, която проявява злонамерено или несъответстващо поведение. [5]

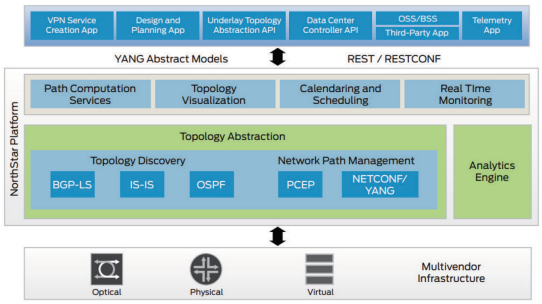
Juniper Networks

Компанията Juniper Networks предлага решение за софтуерно дефинирани глобални мрежи (SD-WAN), което се състои от хардуерни маршрутизатори серия NXF, собствен контролер - NorthStar Controller и централизирано приложение за управление на мрежата - Contrail Networking control and management system [6].

В устройствата е вграден Open vSwitch – програмна рамка с отворен код за комутатор и мрежова автоматизация, която ефективно оптимизира потоците данни, осигурява цялостни маршрутизиращи функции и подобрява производителността.

Контролерът NorthStar Controller е мощно и гъвкаво решение за инженеринг на трафик, което позволява детайлна видимост и контрол на IP/MPLS потоците в големи доставчици на услуги и корпоративни мрежи. Той позволява на мрежовите оператори да оптимизират своята мрежова инфраструктура чрез проактивен мониторинг, планиране и изрично маршрутизиране на големи натоварвания от трафик динамично въз основа на посочените ограничения. Контролерът е базиран на архитектурата Path Computation Element (PCE), описана в документа RFC 5440 [7].

Концепцията, вложена в контролера за маршрутизация се нарича Source Packet Routing in Networks (SPRING). Тя представлява SDN-базиран метод за маршрутизация, в който контролерът управлява мрежовите ресурси и насочва трафика според нуждите на приложението. Архитектурата на контролера е показана на фигура 7.



***Фиг.** 7. Архитектура на NorthStar [8]*

Contrail Networking е прост, отворен и гъвкав продукт за автоматизация на облачна мрежа с SDN архитектура. Със своята мащабируема архитектура с микроуслуги, приложението организира виртуални мрежи с производителност на облачни услуги.

Приложения на SDN

Софтуерно дефинираните мрежи намират приложение в много разнообразни сценарии. Тук са показани само някои идеи за възможни приложения:

- Центрове за управление на данни, които ще осигуряват облачни услуги на клиентите си. Там се предвижда да се обслужват много клиенти едновременно и сървърните и мрежови ресурси трябва да се скалират динамично, на базата на нуждите на потребителите. Концепцията SDN в центъра за управление на данни позволява да се изгради една голяма топология на канално ниво, която да избягва много копия на еднакви пакети и по този начин да позволи бърза миграция на виртуалните машини между физическите ресурси [9];
- Паралелни връзки през глобални мрежи – много организации имат основна и резервна връзка между отдалечените си мрежи. Традиционните маршрутизиращи протоколи обикновено избират по-добрия път и използват него, а резервния стои неизползван и се активира само когато основният отпадне. Със софтуерно дефинираните мрежи може да се управлява трафика на потребителите динамично, поотделно за всеки пакет или за всеки поток данни и така да се използва по-ефективно мрежовата топология;
- В домашни мрежи – прилагането на подхода на софтуерно дефинираните мрежи може да потребителите видимост за използването на мрежата и за евентуални проблеми в нея, дори преди те реално да се случат. Освен това този подход може да осигури на потребителите средства за по-добро управление на ресурсите, например тегленето на голямо количество данни или мрежовите компютърни игри, използвани от един член

на семейството да не могат да провалят процеса на отдалечена работа или онлайн конференция за друг член.

ЗАКЛЮЧЕНИЕ

В настоящия доклад са описани някои подходи за изграждане на софтуерно дефинирани мрежи и приложението им в съвременния свят. Тази концепция представлява един нов поглед към компютърните мрежи, който се развива все повече и е предмет на бъдещи изследвания. Бъдещите планове на екипа включват изграждане на опитна постановка за изследвания, тестване на различни контролери и изграждане на приложения с реално приложение в практиката.

Източник на финансиране: Настоящият документ е изготвен с финансовата помощ на договор № 2405E за провеждане на научни изследвания по проект на тема: „Усъвършенстване на обучението чрез информационни и комуникационни технологии“ към Технически университет – Габрово.

ЛИТЕРАТУРА

[1] VMware, What is Software-Defined Networking (SDN), https://www.vmware.com/topics/software-defined-networking (30.10.2024 г.)

[2] NetworkLessons, Introduction to SDN (Software Defined Networking), https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-to-sdn-software-defined-networking (30.10.2024 г.)

[3] Michael Rebmann, A Closer Look at VMware NSX Security, https://www.cloud13.ch/2022/12/21/a-closer-look-at-vmware-nsx-security/ (03.11.2024 г.)

[4] Cisco Systems, Cisco Application Centric Infrastructure (ACI) https://ebooks.cisco.com/story/cisco-application-centric-infrastructure-aci/page/1 (03.11.2024 г.)

[5] Cisco Systems, Cisco Software-Defined Access for Zero-Trust Workplace At-a-Glance https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/at-a-glance-c45-738181.html (03.11.2024 г.)

[6] Juniper Networks, Contrail Service Orchestration, https://www.juniper.net/us/en/products/sdn-and-orchestration/contrail.html (03.11.2024)

[7] JP. Vasseur, JL. Le Roux, Path Computation Element (PCE) Communication Protocol (PCEP), IETF, Request for Comments: 5440

[8] NetworkScreen, Juniper Networks NorthStar Controller, https://www.networkscreen.com/NorthStar-Controller.asp, (01.11.2024 г.)

[9] Nick Feamster, Software Defined Networking Course, The University of Chicago, Coursera, https://www.coursera.org/learn/sdn/home/module/1 (11.01.2023).