Վիրտուալացումն այսօր տարածվում է ոչ միայն սերվերների, այլև ցանցերի և պահեստավորման համակարգերի վրա. Դա պահանջում է այն բիզնեսը, որը պատրաստ չէ վճարել չօգտագործվող ՏՏ ռեսուրսների համար, և նույնիսկ դրա տեղադրման համար պահանջվում է շատ ժամանակ: Ընկերությունների ամբողջ ռազմավարությունն այժմ կառուցվելու է SDN- ի և SDDC- ի (ծրագրային ապահովմամբ սահմանված տվյալների կենտրոն) շուրջ, որոնցով կարող եք ավտոմատացնել ընդհանուր գործառույթները, ինչպիսիք են վիրտուալ մեքենաների ստեղծումը և պահեստավորման ռեսուրսների բաշխումը: SDN գործիքներն ավելի հեշտ և արդյունավետ են դարձնում քլոուդի կոնֆիգուրացիաների կառավարումը: Կորպորատիվ հատվածի համար սա բարդ ենթակառուցվածքների կառավարման և օպտիմալացման հնարավորություն է, իսկ միջին և փոքր բիզնեսի համար` հանրային քլոուդների հետ արդյունավետ աշխատանքի գործիք:

Ժամանակակից միտումները, ինչպիսիք են ինտերնետին միացված սարքերի թվի աճը, տեղեկատվության ծավալների էքսպոնենցիալ աճը, ամպային տեխնոլոգիաների զարգացումը, BYOD-ը, մեծ տվյալները, փոխում են կորպորատիվ հեռահաղորդակցությունը մեր աչքի առաջ: Քանի որ ցանցի տրաֆիկի ծավալը շարունակում է աճել, բիզնեսը գնալով ավելի մեծ կարիք ունի լայնածավալ ցանցերի կազմաձևման:

Այս առաջադրանքը կարող է պարզեցվել SDN (Software-Defined Networking) ծրագրակողմնորոշված ցանցերի և NFV (Network Function Virtualization) ցանցերի ֆունկցիոնալ վիրտուալացման միջոցով, որոնք թույլ են տալիս փոխանցել ցանցի տարրերը կարգավորելի ծրագրակազմի վերահսկողության ներքո՝ դրանք դարձնելով ավելի խելացի և հեշտացնելով դրանց կառավարումը:

Ավանդական ցանցի կառավարումը սովորաբար պահանջում է ցանցին միացված յուրաքանչյուր սարքի առանձին կազմաձևում: Օրինակ, մի քանի Cisco անջատիչների վրա VLAN-ի կազմաձևումն անխուսափելիորեն ենթադրում է յուրաքանչյուրի մուտք և անհրաժեշտ պարամետրերի կատարում: Այս մոտեցումը հաջողությամբ աշխատել է նախկինում, բայց կարող է ժամանակատար լինել, քանի որ կազմակերպություններն իրենց ցանցերին ավելացնում են աշխատողների բերած սարքեր և բազմաթիվ ամպային ծառայություններ:

SDN-ը կարող է օգնել, քանի որ ցանցի կառավարման նպատակն է թույլ տալ, որ տարբեր սարքեր (ընկերությանը, աշխատակիցներին կամ տարբեր արտադրողներին պատկանող) միանան ցանցերին և օգտագործեն դրա ռեսուրսները « ո՞վ-ի՞նչ-որտե՞ղ-ինչպե՞ս-ինչու՞» սկզբունքով ամեն անգամ ցանցին միանալուց: Սա պահանջում է քաղաքականության հետևողական կիրառում բոլոր սարքերում: Հետագայում, քաղաքականությունը փոխող ադմինիստրատորը ստիպված չի լինի ժամեր ծախսել յուրաքանչյուր սարքի վրա առանձին փոփոխություններ կատարելու համար, և այդ փոփոխությունները պետք է հետևողական լինեն ձեռնարկության համար: Սա SDN- ի դերն է: Նրանք ապահովում են հետևողական, համեմատաբար արագ ցանցի կառավարում՝ թույլ տալով փոփոխություններ ամբողջ ցանցում մեկ կառավարման վահանակից:

Կարևոր է նաև, որ ցանցի վիրտուալացման մեխանիզմը կառուցվի անվճար ծրագրակազմի հիման վրա, ինչը թույլ է տալիս ցանցի ադմինիստրատորներին ավելի արագ և արդյունավետ կառավարել տվյալների մեծ հոսքը մեկ կոնսոլից:

Վիրտուալիզացիան ոչնչացնում է սերվեր արտադրողների բիզնեսը։ Արտադրողները պետք է փնտրեն եկամտի նոր աղբյուրներ, օրինակ՝ ավելի լավ իրենց արտադրանքը հարմարեցնեն վիրտուալացմանը, և այսօր շատ ընկերությունների արտադրանքն ի սկզբանե օպտիմիզացված են հիպերվիզորների համար: SDN- ի ի հայտ գալով, ցանցային սարքավորումների շուկայում նման իրավիճակ է նկատվելու։ Ցանցի վիրտուալացումը նախատեսված է ամպերի մասշտաբայնության սահմանափակումը վերացնելու համար, որը հիմնարար նշանակություն ունի ամպերի զարգացման համար: Մենք դեռ կարող ենք ձեռքով կառավարել ցանցերը մի քանի կլաստերների ներսում, որոնք տեղակայված են նույն տվյալների կենտրոնում, բայց երբ այդպիսի կլաստերները շատ են և դրանք աշխարհագրականորեն ցրված են, խնդիրը դառնում է շատ ավելի բարդ: Երբ խոսքը վերաբերում է տվյալների կենտրոնների միջև փոխգործակցության կազմակերպմանը, սա հենց Cisco-ի ոլորտն է:

SDN-ը ցանցային սարքավորումների արտադրողներին ներկայացնում է նոր մարտահրավերներ՝ ամպերի հետ աշխատելու նոր սցենարներին աջակցելու համար, օրինակ՝ բազմաթիվ փաթեթների փոխադրման հնարավորություն երկար հեռավորությունների վրա:

Երթուղիչների և անջատիչների սեփական կառավարման վահանակները սև արկղեր են օգտագործողների համար, և SDN-ը պոտենցիալ թույլ է տալիս շրջանցել դրանք՝ երրորդ կողմի ծրագրակազմի կողմից վահանակները բաց դարձնելով բաց արձանագրությունների միջոցով, ինչպիսիք են՝ OpenFlow-ն: Թողունակությունը կարող է տուժել, բայց դա այժմ այդքան էլ կարևոր չէ՝ այսօր շատ ավելի կարևոր է ցանցերն անորոշ ժամանակով մասշտաբայնացնելու, ցանցի մեկուսացումը, թափանցիկ վերահսկումներն ու հուսալիությունը վերացնելու ունակությունը: Ամպերի ստեղծմամբ հետաքրքրված ցանկացած կազմակերպություն պետք է զբաղվի ցանցային վիրտուալացման և SDN տեխնոլոգիաներով: Առաջիկա հինգ տարիների ընթացքում ցանցային սարքավորումների բոլոր արտադրողները իրենց լուծումները կհարմարեցնեն SDN-ին, իսկ յոթից տաս տարի հետո ծրագրային ապահովմամբ սահմանված ցանցերը կդառնան սովորական պրակտիկա:

**Ի՞նչ է NFV-ն**

**NFV(Network Functions Virtualization) -** ցանցային ծառայությունների մատուցման զարգացող մոտեցում է, որը հնարավորություն է տալիս փոխարինել թանկարժեք, մասնագիտացված, անվտանգություն և բեռի հավասարակշռում իրականացնող սարքավորումները ծրագրային լուծումներով, որոնք աշխատում են որպես վիրտուալ մեքենաներ ոլորտի ստանդարտ սերվերների վրա: NFV-ն անջատում է ցանցային գործառույթները մասնագիտացված ապարատային սարքերից և դրանք հասցնում վիրտուալ սերվերներին, որոնք միավորում են տարբեր գործառույթներ մեկ ֆիզիկական սերվերի մեջ: Այս մոտեցումը նվազեցնում է ծախսերը և նվազագույնի հասցնում տեղում և ձեռքով սպասարկման անհրաժեշտությունը, քանի որ վիրտուալ սարքերը փոխարինում են մասնագիտացված ցանցային սարքավորումներին:

Ցանցային ադմինիստրատորները կարգավորում և վերահսկողություն են իրականացնում օպերացիոն համակարգի միջոցով, որը համակարգում է ցանցի բոլոր վիրտուալ սարքերը: Ինչպես վիրտուալ մեքենաները, այնպես էլ վիրտուալ սարքավորումները կարող են ընտրվել և տեղակայվել ըստ անհրաժեշտության:

NFV-ն թույլ է տալիս փոխարինել թանկարժեք ցանցային սարքավորումները պարզ ծրագրային սարքերով:

Եթե ​​հաճախորդին անհրաժեշտ է ավելացնել ցանցային նոր գործառույթներ, ծառայության մատակարարը կարող է դա անել՝ գործարկելով նոր վիրտուալ մեքենա: Նմանապես, ցանցի գործառույթը դադարում է, երբ այն այլևս անհրաժեշտ չէ: Օրինակ, ցանցում նոր ծածկագրման ապարատային սարք տեղադրելու փոխարեն, վաճառողը կարող է գաղտնագրման ծրագրակազմը տեղակայել ստանդարտացված սերվերի կամ անջատիչի վրա, որն արդեն ցանցում է:

Ցանցի գործառույթների վիրտուալիզացումը նվազեցնում է ցանցի օպերատորների կախվածությունը մասնագիտացված ապարատային սարքերից և բարելավում է մասշտաբայնությունը, ինչպես նաև ռեսուրսների օգտագործման արդյունավետությունը (վիրտուալ մեքենան կարող է ազատվել մեկ այլ ծրագիր գործարկելու համար, երբ այդ վիրտուալ մեքենայի վրա աշխատող ծրագրային սարքն այլևս անհրաժեշտ չէ) և կարգավորելիություն ամբողջ ցանցում։ NFV-ն չպետք է շփոթել վիրտուալացված ցանցի հետ, քանի որ NFV-ն որպես տեխնոլոգիական հասկացություն ենթադրում է բեռնաթափում միայն ցանցի գործառույթներից, այլ ոչ թե ամբողջ ցանցից: Կարևոր է նաև նշել, որ NFV-ն տարբերվում է վիրտուալ ցանցի գործառույթներից (VNF): Այս տերմինը սովորաբար վերաբերում է վիրտուալ մեքենայում հավելվածում աշխատող ցանցային գործառույթին։

NFV- ի հիմնական առավելությունները ներառում են հետևյալը՝

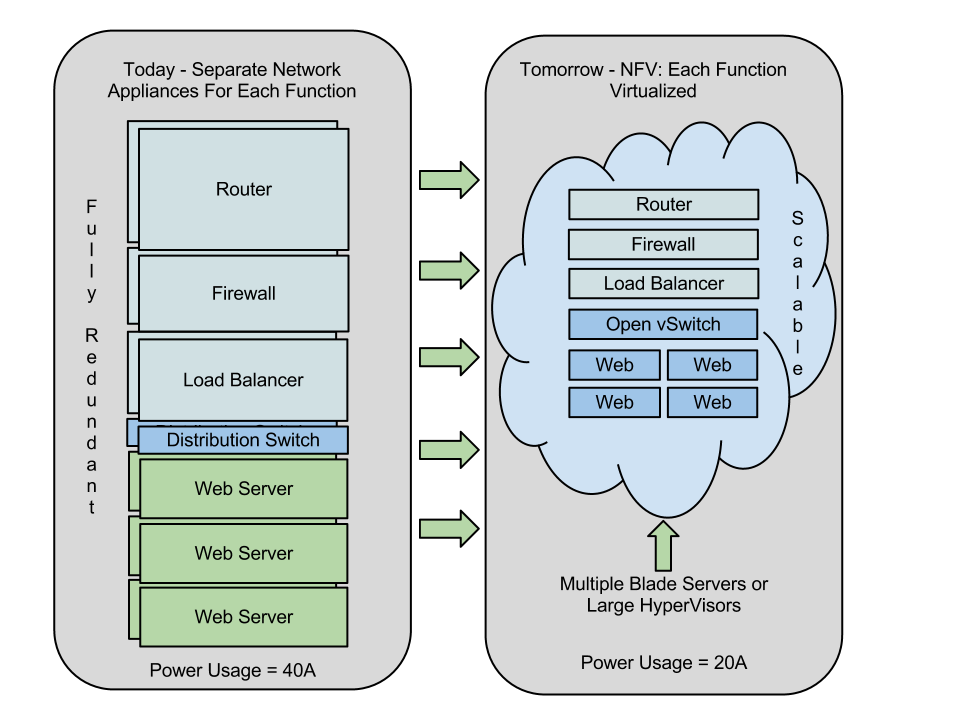
* ավելի քիչ տարածք ցանցային սարքավորումների տեղադրման համար.
* էներգիայի սպառման նվազեցում․
* ցանցի սպասարկման ծախսերի կրճատում․
* ցանցի պարզ և արագ արդիականացում:

ՏՏ ենթակառուցվածքների վիրտուալացումը շարունակվում է տարիներ շարունակ: Աշխատանքը ցանցերում հաջորդ քայլն է այն օպերատորների համար, ովքեր ձգտում են հետևել տեխնոլոգիական առաջընթացին: Ծրագրերը ծանրաբեռնում են ցանցերը՝ թողունակության, ճկունության և արագության առումով, սակայն երթևեկության գագաթնակետին դիմակայելու համար լայնածավալ ցանցերի ստեղծումը շատ օպերատորների համար անհասանելի է, քանի որ այն շատ թանկ է: Միևնույն ժամանակ, մեկ ծրագրի համար ծրագրերի վրա հիմնված սարքավորումներ գնելը, այնուհետև մշակելը և հարմարեցումը` 8-10 տարի անխափան աշխատանք ապահովելու համար (ներդրումների ռացիոնալ վերադարձի երաշխիք), խիստ իրատեսական չէ: NFV- ն, ծրագրային ապահովման հետ մեկտեղ, ապահովում է ավելի մեծ արձագանք և վերահսկում ցանցի և դրա հիմնական գործառույթների նկատմամբ:

Մուրի օրենքի շնորհիվ ցանցային գործառույթները, որոնք նախկինում հնարավոր էին միայն բարձր մասնագիտացված ծրագրակազմով և սարքերով, այժմ կարող են ամբողջությամբ տեղակայվել ծրագրային ապահովման մեջ՝ կտրուկ փոխելով օպերատորների և ծառայություններ մատուցողների ցանցի շուկան:

Պատկերացրեք մի բանկ, որն ունի բազմաթիվ մասնաճյուղեր: NFV- ն ակնթարթորեն նվազեցնում է կապիտալ ծախսերը, քանի որ բանկին անհրաժեշտ սարքավորումները գնվում են ավելի քիչ, ավելի փոքր ծավալով և ավելի ցածր գներով: NFV-ն նաև կրճատում է գործառնական ծախսերը, քանի որ սարքավորումների համար բանկը պահանջում է ավելի քիչ ֆիզիկական տարածք և էներգիայի ծախսեր:

Սարքավորումների վրա կապիտալ ծախսերի փոխարեն բանկը պարզապես վճարում է մասնաճյուղի վիրտուալ սարքերի լիցենզիաների համար: Քանի որ բիզնեսի մարտահրավերները փոխվում են՝ հաճախորդների վարքագծի փոփոխման, մասնաճյուղերի գտնվելու վայրի կամ նոր բանկային ծառայությունների ավելացման արդյունքում, բանկը կարող է հեշտությամբ մեծացնել կամ նվազեցնել ռեսուրսների օգտագործումը` ճիշտ ժամանակին տեղադրելով հատուկ ցանցային ծառայություններ: NFV- ն այն փոփոխությունների մի մասն է, որոնք տեղի են ունենում ցանցի ծրագրային և ապարատային ապահովումների աշխատանքի փոխազդեցության մեջ: SDN-ի հետ համատեղ, NFV տեխնոլոգիան ստեղծում է միջավայր՝ ավտոմատացման և ծրագրավորման տարբեր հնարավորություններով: Բացի այդ, NFV-ն օպերատորներին և ծառայություններ մատուցողներին հնարավորություն է տալիս տեղակայել ավելի շատ հաճախորդների վրա հիմնված ցանցային ենթակառուցվածքներ, որոնք դինամիկորեն հարմարվում են հաճախորդների կարիքներին և պահանջներին: Խոշոր ցանցի օպերատորները դիմում են NFV տեխնոլոգիային` ծրագրավորելիության և բաց ստանդարտների համար: Բացի այդ, դա նրանց ազատում է սեփական ցանցային հարթակների սահմանած սահմանափակումներից:



<https://networkguru.ru/network-function-virtualization-nfv/>

<https://shalaginov.com/2015/12/27/sdn-%D0%B8-nfv-%D0%BA%D0%B0%D0%BA-%D1%8D%D1%82%D0%BE-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%B5%D1%82-%D0%BD%D0%B0-%D1%81%D0%B5%D1%82%D0%B8-%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0/>

**Ի՞նչ է SDN-ը**

**SDN(**software-defined networking**)** ցանցային ճարտարապետություն է, որը թույլ է տալիս խելամտորեն և կենտրոնացված վերահսկել (այսինքն ՝ ծրագրավորել) ցանցը` օգտագործելով ծրագրակազմ: Սա թույլ է տալիս օպերատորներին հետևողականորեն և համակողմանի կառավարել ամբողջ ցանցը՝ անկախ օգտագործվող ցանցի հիմնական տեխնոլոգիայից:

Ընկերությունները, օպերատորները և ծառայություններ մատուցողները շրջապատված են մի շարք մրցակից ուժերով: Մուլտիմեդիա բովանդակության ծավալի էական աճը, ամպային հաշվարկների պայթյունավտանգ զարգացումը, բջջային սարքերի օգտագործման ավելացումը և ծախսերը նվազեցնելու մշտական ​​պահանջները հանգեցնում են ավանդական բիզնես մոդելների ոչնչացման:

Մրցակցության մեջ մնալու համար, շուկայի խաղացողներից շատերը դիմում են SDN տեխնոլոգիային՝ ցանցի կառուցվածքում և գործողություններում հեղափոխություն կատարելու նպատակով։

SDN-ը թույլ է տալիս կենտրոնացված ծրագրավորել ցանցի վարքագիծը` օգտագործելով ծրագրակազմ և բաց API-ներ: Դասական փակ ցանցային հարթակների բացումը և SDN-ի կառավարման մակարդակի ներդնումը օպերատորներին հնարավորություն է տալիս հետևողականորեն կառավարել ամբողջ ցանցը և դրա սարքերը՝ անկախ ցանցում օգտագործվող հիմնական տեխնոլոգիաների բարդությունից:

SDN-ն ապահովում է ցանցի հետևողական կառավարում, որը կարող է բաղկացած լինել բարդ տեխնոլոգիական բաղադրիչներից:

Կան չորս հիմնական ոլորտներ, որոնցում SDN-ն առավելություն է տալիս կազմակերպություններին`

1. Ցանցի ծրագրավորելիություն: SDN-ն թույլ է տալիս վերահսկել ցանցի վարքագիծը` օգտագործելով ծրագրակազմ, որը տեղադրված չէ ֆիզիկական կապ ապահովող ցանցային սարքերում: Արդյունքում, օպերատորները կարող են հարմարեցնել իրենց ցանցերի վարքագիծը` նոր ծառայություններին և նույնիսկ կոնկրետ հաճախորդներին աջակցելու համար: Ապարատային ծրագրակազմից տարանջատումը թույլ է տալիս օպերատորներին արագ տեղակայել նորարար տարբերակված ծառայություններ՝ առանց սեփականության իրավունքով պատկանող հարթակների սահմանափակումների:
2. Տրամաբանորեն կենտրոնացված ինտելեկտուալ վերահսկողություն:

SDN տեխնոլոգիան հիմնված է տրամաբանորեն կենտրոնացված ցանցային տոպոլոգիաների վրա, որոնք ապահովում են ցանցային ռեսուրսների խելացի կառավարում: Բաշխվում են ցանցի կառավարման ավանդական մեթոդները: Սարքերը գործում են ինքնավար և սահմանափակ տեղեկություններ ունեն ցանցի վիճակի մասին: SDN տեխնոլոգիայով տրամադրված կենտրոնացված վերահսկողությունը թողունակության կառավարումը, վերականգնումը, պաշտպանությունը և քաղաքականությունը դարձնում է չափազանց խելացի և պարզեցված՝ կազմակերպությանը տալով ցանցի համապարփակ պատկերացում:

1. Ցանցի աբստրակցիա:

SDN-ի վրա հիմնված ծառայություններն ու ծրագրերը տարանջատված են հիմնական տեխնոլոգիաներից, իսկ ֆիզիկական միացման սարքավորումները դուրս են մղվում ցանցի կառավարումից: Սարքավորմամբ կապված կառավարման ինտերֆեյսների փոխարեն՝ ծրագրերը ցանցի հետ փոխազդում են API-ների միջոցով:

1. Հասանելիություն։

SDN-ի ճարտարապետությունները հնարավորություն են տալիս վաճառողների միջև փոխգործունեություն ապահովել և նպաստել առևտրային չեզոք էկոհամակարգի ստեղծմանը` դրանով իսկ ավետելով հասանելիության նոր դարաշրջան: SDN-ի հիմքում բաց լինելն է: Բաց API- ները աջակցում են մի շարք ծրագրերի, ներառյալ քլոուդի կարգավորիչ լուծումները, OSS / BSS, SaaS և բիզնեսի կարևոր ցանցային ծրագրերը: Բացի այդ, խելացի ծրագրակազմը թույլ է տալիս վերահսկել տարբեր վաճառողների սարքավորումները ` օգտագործելով բաց ծրագրավորվող ինտերֆեյսներ, ինչպիսիք են OpenFlow-ն: Ի վերջո, SDN- ի միջոցով առաջադեմ ցանցային ծառայություններն ու ծրագրերը կարող են գործել ընդհանուր ծրագրային միջավայրում:

SDN տեխնոլոգիայի հիմնական առավելությունն այն ծրագրեր գրելու ունակությունն է, որոնք օգտագործում են SDN API և ծրագրերին վերահսկում են ցանցի վարքագիծը: SDN-ը թույլ է տալիս օգտվողներին զարգացնել ծրագրեր՝ հիմնված ցանցի բնութագրերի վրա, վերահսկել դրա կարգավիճակը և ինքնաբերաբար հարմարեցնել կոնֆիգուրացիան հատուկ պայմանների համար:

Այնուամենայնիվ, ոչ բոլոր տարրերն են կենտրոնացված: Գործառույթները, ինչպիսիք են խափանումների վերականգնումը, մոնիթորինգը, պաշտպանությունը, որոնք արդյունավետ են բաշխվելիս, մնում են ներկառուցված ցանցի տարրերի մեջ:

**SDN- ի և NFV- ի առաջացման նախադրյալները**

Մի շարք փորձագետներ ցանցային արդյունաբերության ներկա իրավիճակը բնութագրում են որպես «կրիտիկական և հեղափոխական»: Շուկայում գերիշխող փակ (գույքային) լուծումները ներկայացնում են ծրագրերի համար «սև արկղեր», իսկ տարբեր վաճառողների լուծումների փոխգործունակությունը լավագույն դեպքում ապահովվում է ինտերֆեյսի մակարդակում: Ցանցերը չափազանց բարդ են, ինչը դժվարացնում է դրանց մասշտաբավորումը, կառավարումը և հուսալիությունը: Ակնհայտ է, որ դա խոչընդոտում է դրանցում գործող ցանցերի և ծրագրերի հետագա զարգացմանը:

«Ծագրային ապահովմամբ սահմանված» ցանցերի ( SDN) և ցանցային գործառույթների վիրտուալացման (NFV) հասկացությունների առաջացման հիմնական նախադրյալներն են՝ տվյալների տրաֆիկի և ցանցին միացված սարքերի արագ աճ:

**SDN-ի և NFV-ի հասկացությունները**

SDN- ն և Network Function Virtualization- ը (NFV) խարխլում են ցանցերի ավանդական շուկան և սպառնում՝ Cisco-ի, Juniper Networks-ի և Hewlett-Packard-ի սարքավորումների շահութաբեր բիզնեսին: SDN-ն և NFV-ն ցանցի կառավարման և գործառույթների առաջադրանքները տեղափոխում են թանկարժեք սարքավորումներից դեպի ծրագրային ապահովում, որոնք կարող են աշխատել ավելի էժան զանգվածային արտադրության համակարգերի վրա: Նպատակն է ստեղծել ավելի ճկուն, ծրագրավորվող և ավտոմատացված ցանցեր:

SDN-ի հիմնական սկզբունքներն են՝ տվյալների ղեկավարման և փոխանցման պրոցեսների բաժանումը, ցանցի կենտրոնացված ղեկավարումը օգտագործելով միասնական ծրագրային գործիքներ, ֆիզիկական ցանցային ռեսուրսների վիրտուալացումը։ OpenFlow արձանագրությունը տվյալների մշակման պրոցեսի ղեկավարման պրոտոկոլ է, որոնք փոխանցվում են ցանցում երթուղիչներով և անջատիչներով, իրականացնելով SDN տեխնոլոգիան։

SDN-ի հիմնական էությունն այն է, որ ցանցի ղեկավարման մակարդակը (network control plane) ֆիզիկապես տարանջատվի տվյալների փոխանցման մակարդակից (forwarding functions) իրականացվող ղեկավարման գործառույթները ծրագրին փոխանցման հաշվին (երթուղիչներ, անջատիչներ և այլն), որն աշխատում է առանձին սերվերում(controller)։

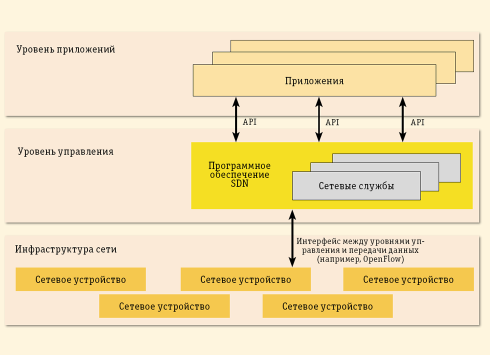
Արդյունքը պետք է լինի ճկուն, կառավարելի, հարմարվողական և ծախսարդյունավետ ճարտարապետություն, որը կարող է արդյունավետ կերպով հարմարվել տարասեռ երթևեկության մեծ հոսքերի փոխանցմանը:

SDN- ի հիմնական գաղափարները ներառում են՝

* տվյալների փոխանցման (data plane) և ղեկավարման մակարդակների (control plane) տարանջատումը,
* data plane մակարդակի ցանցային տարրերի զգալի պարզեցում,
* միակը, միասնական, մատակարարից անկախ ինտերֆեյս տվյալների փոխանցման (data plane) և ղեկավարման մակարդակների (control plane) միջև ,
* տրամաբանորեն կենտրոնացված ցանցի կառավարում, որն իրականացվում է տեղադրված ցանցի օպերացիոն համակարգով վերահսկիչի և դրա վերևում իրականացվող ցանցային ծրագրերի միջոցով,
* ֆիզիկական ցանցի ռեսուրսների վիրտուալիզացում։

SDN-ը փորձում է տարանջատել երկու հարթությունները` ցանցի կառավարում և տրանսպորտ, և ի վերջո կենտրոնացնել բաշխված ցանցի կառավարումը` ռեսուրսներն առավել արդյունավետ օգտագործելու և ցանցային ծառայությունների կառավարումը ավտոմատացնելու համար: NFV-ն կենտրոնանում է ցանցի ներսում ցանցային ծառայությունների օպտիմալացման վրա` տարանջատելով ցանցի գործառույթները (օրինակ՝ DNS, քեշավորում և այլն) իրական ապարատային իրականացումից: Ենթադրվում է, որ NFV- ն թույլ է տալիս ծրագրակազմի բազմակողմանիություն, արագացնել ցանցի նոր գործառույթների և ծառայությունների ներդրումը `առանց պահանջելու արդեն տեղակայված ցանցային ենթակառուցվածքից հրաժարվելը:

**SDN ճարտարապետության դիագրամը**

SDN-ը և NFV-ն թույլ են տալիս պարզեցնել ցանցի կազմաձևումը, ընդլայնել ցանցերն ու ծառայությունները ըստ պահանջի, ավտոմատացնել ցանցի կառավարումը, բարձրացնել ֆիզիկական ենթակառուցվածքի հզորությունը։

Գոյություն ունի SDN, NFV և ամպերի իրականացման երկու ռազմավարական ուղղություն: **Առաջինը** ցանցի արդյունավետության և ծառայությունների ճկունության բարձրացումն է: Հիմնական նպատակն է նվազեցնել ցանցի շահագործման արժեքը և կարճացնել շուկա դուրս գալու ժամանակը: **Երկրորդը** նպատակ ունի օգտվել նոր բիզնես հնարավորությունների համադրությունից: Նպատակն այս դեպքում այլ է` նոր տարբերակված ամպային ծառայությունների ձևավորում և դրանց դինամիկ մատուցում` կախված ներկայիս պահանջարկի պրոֆիլից: Առաջինը այս ճանապարհին հետևում են այնպիսի ընկերություններ, ինչպիսիք են գերմանական Deutsche Telekom- ը և իսպանական Telefonica- ն, երկրորդը`ճապոնական NTT- ն և ամերիկյան AT&T- ն:

**Մատակարարի համար NFV / SDN- ի ներդրման գործնական ազդեցությունը**

* Կապի նվազեցված ծախսեր՝ ծառայությունները վիրտուալացված են և չեն պահանջում հատուկ սարքավորում
* COTS սարքավորումների օգտագործում (ստանդարտ ապարատային x86 ճարտարապետություն)
* Հաճախորդի այցելությունների կրճատում կամ ամբողջական չեղարկում `լրացուցիչ ծառայություններ միացնելու համար:
* Մատչելիություն ծառայություններին 24/7 ռեժիմով, նույնիսկ երբ հաճախորդը տեղափոխվում է։
* Ժամանակի նվազեցում ինչպես նոր հաճախորդին միանալու, այնպես էլ նոր ծառայություններ ավելացնելու համար։
* Նվազեցված գործառնական ծախսեր։
* Ծառայությունների արագ և առաձգական մասշտաբավորում ` կախված կարիքներից։
* Ցանցի միասնական ներառումներ` տարբեր տեսակի տերմինալ սարքավորումների կրճատում։

**SDN-ի հիմնական առավելությունները**

1.SDN կարգավորիչը կարող է ուղղորդել ոչ կրիտիկական / մեծածավալ երթևեկությունը ավելի երկար երթուղիներով, որոնք ամբողջությամբ չեն օգտագործվում:

2. SDN կարգավորիչը կարող է ուղարկել սկզբնական զույգ փաթեթներ firewall-ին, և երբ firewall-ը հավանություն է տալիս՝ ընդունում է հոսքը, SDN կարգավորիչը կարող է շրջանցել firewall-ը՝ այդպիսով վերցնելով ծանրաբեռնվածությունը FW-ից և թույլ տալով, որ բազմաբիթանոց տվյալների կենտրոնները լինեն firewall՝ ;)պարսպապատված;)

3. SDN կարգավորիչը կարող է հեշտությամբ իրականացնել բեռի հավասարակշռում նույնիսկ տվյալների փոխանցման բարձր արագությամբ՝ ուղղակի ուղղելով տարբեր հոսքեր դեպի տարբեր հոսթեր՝ միայն կարգավորելով սկզբնական հոսքը:

4. Երթևեկությունը կարող է մեկուսացվել առանց vlan-ի անհրաժեշտության, SDN վերահսկիչը կարող է պարզապես մերժել որոշակի կապեր:

5. Հեշտությամբ է կարգավորում ցանցի TAP/Sniffer-ը ցանկացած պորտի կամ նույնիսկ հատուկ տրաֆիկի համար՝ ծրագրավորելով ցանցը՝ կրկնօրինակ հոսքեր ուղարկելով ցանցի մոնիթորինգի սարքին:

6. Սա թույլ է տալիս նոր ծառայություններ և գաղափարներ մշակել ամբողջությամբ SDN կարգավորիչի ծրագրային ապահովման մեջ OpenFlow-Actions։

https://docs.microsoft.com/ru-ru/azure-stack/hci/concepts/network-controller

Աշխարհում կան միլիոնավոր ցանցային սարքեր, որոնք պետք է կազմաձևվեն, թարմացվեն և հաստատվեն՝ աշխատելու համար: Սարքավորումների նման համակարգի պահպանումը բավականին դժվար է և պահանջում է շատ ժամանակ, ջանք և մարդկային ռեսուրսներ: Ժամանակակից միտումները, ինչպիսիք են ինտերնետին միացված սարքերի թվի աճը, տեղեկատվության ծավալների էքսպոնենցիալ աճը, ամպային տեխնոլոգիաների զարգացումը, BYOD-ը, մեծ տվյալները, փոխում են կորպորատիվ հեռահաղորդակցությունը մեր աչքի առաջ: Քանի որ ցանցի թրաֆիկի ծավալը շարունակում է աճել, բիզնեսը գնալով ավելի մեծ կարիք ունի լայնածավալ ցանցերի կազմաձևման: Քանի որ անցումը դեպի ամպային համակարգ շարունակվում է, ձեռնարկության հաճախորդները և նրանց հավելվածները ավելի ու ավելի են կախված ցանցի արդյունավետությունից, հետևաբար, ակնկալվում է, որ ցանցերը կունենան բարձր հուսալիություն՝ նվազագույն խափանումներով: Ցանցում սարքերի թվի աճին զուգընթաց մեծանում է դրանց միջև անխափան, ճկուն, արագ, արդյունավետ կապ ապահովելու անհրաժեշտությունը։ Դրա համար անհրաժեշտ է ձեռք բերել մեծ թվով ցանցային սարքեր, որոնք կլինեն որակով և կունենան մեծ հնարավորություններ ինչպիսիք են, օրինակ՝ մեծ հիշողությունը, շատ ինտերֆեյսները, հզոր պրոցեսորները, իսկ այս ամենը կապված է մեծ ծախսերի հետ, որն էլ ավտոմատիզացիա և վիրտուալացում հասկացությունների առաջացման հիմնական նախադրյալներից է:

Ծառայություններ մատուցողների համար ավտոմատիզացիան ցանցի ճկունությունն ու հուսալիությունը բարելավելու հիմնական ռազմավարությունն է՝ միաժամանակ վերահսկելով գործառնական և կապիտալ ծախսերը: Հետևաբար անհրաժեշտ է ավտոմատացնել ցանցային սարքավորումների հետ աշխատանքը։ Ցանցի ավտոմատացումը ցանցում ֆիզիկական և վիրտուալ սարքերի կազմաձևման, կառավարման, փորձարկման, տեղակայման և շահագործման ավտոմատացման գործընթաց է: Ավտոմատացնելով ամենօրյա ցանցային առաջադրանքները և գործառույթները, ինչպես նաև ավտոմատ մոնիթորինգով և հսկողությամբ կրկնվող գործընթացները՝ մեծանում է ցանցային ծառայությունների հասանելիությունը:

Ինչքան մեծանում են ցանցին միացված սարքերի թիվը, այնքան մեծանում է դրանց օգտագործման անհարմարավետությունը և ծախսերը։ Եվ քանի դեռ ցանցային համակարգը չի ավտոմատացվել, որը կարող է իրականացվել վիրտուալացման միջոցով այս խնդիրը լինելու է շարունակական։ Կազմակերպությունները մեծ թվով գումարներ են ծախսելու լավ ցանցային սարքերի վրա։

Մի շարք փորձագետներ ցանցային արդյունաբերության ներկա իրավիճակը բնութագրում են որպես «կրիտիկական և հեղափոխական»: Շուկայում գերիշխող փակ (գույքային) լուծումները ներկայացնում են ծրագրերի համար «սև արկղեր», իսկ տարբեր վաճառողների լուծումների փոխգործունակությունը լավագույն դեպքում ապահովվում է ինտերֆեյսի մակարդակում: Ցանցերը չափազանց բարդ են, ինչը դժվարացնում է դրանց մասշտաբավորումը, կառավարումը և հուսալիությունը: Ակնհայտ է, որ դա խոչընդոտում է դրանցում գործող ցանցերի և ծրագրերի հետագա զարգացմանը:

Ցանցի վիրտուալացման տեխնոլոգիաները վաղուց օգտագործվել են ՏՏ ենթակառուցվածքի կառուցման համար: Ցանկացած երթուղիչ գրեթե որոշակի չափով աջակցում է ցանցի վիրտուալացման գործառույթներին՝ կարգավորում VLAN (վիրտուալ տեղական ցանց), VPN (վիրտուալ մասնավոր ցանց): Իսկ հիպերվիզորները(ծրագիր կամ ապարատային սխեմա, որը հնարավորություն է տալիս կամ թույլ է տալիս մի քանի օպերացիոն համակարգերով զուգահեռ աշխատել նույն համակարգչի վրա:), օրինակ, կարող են վիրտուալացնել ֆիզիկական պորտերը և դրանք կիսել տասնյակ վիրտուալ մեքենաների միջև: SDN լուծումը ենթադրում է մասնավոր ցանցի ավտոմատ ձևավորում և տեղեկատվության փոխանցում բոլոր տեսակի հասանելի կապուղիներով՝ չկորցնելով հավելվածների արագությունն ու որակը: Օրինակ, նախկինում միայն թանկարժեք VPN ալիք էր օգտագործվում ձայնը կամ տեսանյութը առանց աղավաղումների փոխանցելու համար: Այժմ, շնորհիվ SDN-ի, մենք կարող եք օգտագործել միայն ինտերնետ ալիքը և LTE-ն որպես կրկնօրինակ: Այսպիսով, հաճախորդները կարող են խնայել հեռահաղորդակցության օպերատորներից հաշիվների վճարման վրա և լուծել VPN ալիքների ամրագրման հարցը պարզ և էժան եղանակով:

Ավելի գլոբալ մասշտաբով վիրտուալ ցանցեր կառուցելու համար, օրինակ՝ տվյալների կենտրոնների համար, երբ անհրաժեշտ են ճկուն ցանցի կառավարման և մատչելիության, ավտոմատացման և անվտանգության բարձր մակարդակի գործիքներ, անհրաժեշտ են մասնագիտացված լուծումներ, ինչպիսիք են.

* VMware NSX;
* Citrix NetScaler;
* Microsoft Windows Server Datacenter и System Center;
* Cisco Application Centric Infrastructure.

Ի տարբերություն մնացած վիրտուալացման տեխնոլոգիաների ըստ վերլուծաբանների SDN-ի բաց լուծումն ավելի խոստումնալից է համարվում: SDN-ն արդեն տրամադրում է ընկերություններին ընտրելու բազմաթիվ տարբերակներ՝ OpenFlow, NETCONF, OVSDB և ընդլայնվող API գրադարան աջակցող անջատիչներ, ինչպես նաև ձեռնարկության ծրագրակազմ, որն օգտվում է այս արձանագրություններից: Ինչպես ցանկացած այլ ենթակառուցվածքներ, SDN ենթակառուցվածքը նույնպես կառուցվում է բաց ստանդարտներով: Այս բաց էկոհամակարգը արագացնում է ցանցի նորարարությունը:

Չնայած մտածողության իներցիայի և ճգնաժամային երևույթների բացասական ազդեցության պատճառով ցանցային ենթակառուցվածքի կառուցման ավանդական մոտեցումը դեռ գերակշռում է, սակայն SDN-ն արդեն թույլ է տալիս արդյունավետորեն լուծել խնդիրները վիրտուալ և ֆիզիկական միջավայրերի հանգույցում: Ինտերնետային խոշոր ընկերությունների փորձը ցույց է տվել լայնածավալ ցանցային ենթակառուցվածքը մշտապես փոփոխվող պահանջներին հարմարեցնելու ունակությունը: Բայց ընկերություններից շատերը դանդաղել են իրենց SDN ռազմավարությունն իրականացնելու հարցում՝ հավատալով, որ պետք է ամբողջությամբ վերանախագծեն իրենց ցանցային սարքավորումները:

Այս մտահոգության մի մասը բխում է տարածված սխալ պատկերացումից, որ SDN-ն արտադրանք է: Իրականում սա ավելի շատ մոտեցում է ցանցի նախագծմանը, ինչպես նաև նոր պարադիգմ՝ դրանց կառավարման, մոնիտորինգի և, ի վերջո, հավելվածների կողմից իրականացվող բիզնես առաջադրանքներին հարմարվելու համար: SDN-ին անցնելը փուլային գործընթաց է, որը հաշվի է առնում ցանցի բիզնես օգտագործման դեպքերը: Թեև կան որոշակի ապրանքներ, ինչպիսիք են SDN անջատիչները, որոնք աջակցում են OpenFlow-ին, ցանցային ենթակառուցվածքն ամբողջությամբ փոխարինելու կարիք չկա:

Դեռ 2012 թվականին Google-ի տեխնիկական ենթակառուցվածքների ավագ փոխնախագահ Ուրս Հոլցլեն բաց ցանցային գագաթնաժողովի ժամանկ զեկուցեց, որ ընկերությունը օգտագործում է SDN տեխնոլոգիաներ: Նույն 2012 թվականին խոստումնալից մարքեթինգային հետազոտությունները սկսեցին խմբաքանակով հայտնել, որ SDN լուծումների շուկան հսկայական չափերի կհասնի հինգ տարում, և գրեթե բոլորը 2016 թվականն անվանեցին «զանգվածային ներդրման տարի»:Սակայն այն այնպես էլ չդարձավ «զանգվածային ներդրման տարի»: Փաստորեն, զանգվածային ներդրման փուլի փոխարեն մենք այժմ դիտարկում ենք տեխնոլոգիայի զանգվածային փորձարկման փուլը։ Հեռահաղորդակցության բոլոր խոշոր օպերատորները թիրախավորում են տեխնոլոգիաները, հավաքագրում են թիմեր, որոնք կարող են աշխատել նոր տեխնոլոգիաների հետ և պլանավորում են բիզնես գործընթացների վերակազմավորում:

Ոչ ոք այլևս չի վիճում, որ SDN-ն անհրաժեշտ է, և բոլոր հակասությունները տեղափոխվել են դեպի իրականացում։

Փաստորեն, բոլորն այժմ հասկացել են, թե ինչ կարելի է ակնկալել SDN-ից և՛ SDN / OpenFlow-ի գործնականում ներդրման, և՛ նոր սարքավորումների առաջացման, և՛ նոր ծառայությունների առաջացման առումով: Հաստատ է, որ SDN-ի կիրառման ոլորտներն այլևս չեն փոխվի։ Օրինակ, կարելի է պնդել, որ քանի որ այս ընթացքում OpenFlow անջատիչները չեն հայտնվել, նրանք, ամենայն հավանականությամբ, չեն հայտնվի, քանի որ քանի դեռ խոշոր վաճառողները չեն փոխել իրենց սարքավորումների արտադրությունը, ապա այս ոլորտում առաջընթաց չի լինի: Ամենայն հավանականությամբ, OpenFlow արձանագրությունը կամաց-կամաց կզարգանա այնպիսի ուղղությամբ, որը կհամապատասխանի ինչպես վաճառողներին, այնպես էլ նրանց հաճախորդներին:

Բոլոր վաճառողները բոլորովին այլ կերպ են հասկանում SDN-ն: Բոլորովին տարբեր արձանագրություններ, իրականացման տարբեր մոտեցումներ, հետո այս կամ այն ​​կերպ հայտնվեց կենտրոնացված հսկողություն, կա ծառայություններ ինքնուրույն ստեղծելու հնարավորություն և այլն, բայց սարքերի բաց և դյուրակիր չեն: Սակայն 2015 թվականից ի վեր, SDN-ի բոլոր խոշոր վաճառողները սկսել են ագրեսիվ կերպով հորիզոնական կապեր ստեղծել՝ վերջնական հաճախորդների ուզած վերջնական արտադրանքները ստեղծելու համար:

Կարծում ենք, որ առաջիկա 2-3 տարիներին հնարավոր կլինի խոսել իրականացման փուլի մեկնարկի մասին։

«Ծագրային ապահովմամբ սահմանված» ցանցերի ( SDN) և ցանցային գործառույթների վիրտուալացման (NFV) հասկացությունների առաջացման հիմնական նախադրյալներն են՝ տվյալների տրաֆիկի և ցանցին միացված սարքերի արագ աճ:

Վիրտուալացումն այսօր տարածվում է ոչ միայն սերվերների, այլև ցանցերի և պահեստավորման համակարգերի վրա. Դա պահանջում է այն բիզնեսը, որը պատրաստ չէ վճարել չօգտագործվող ՏՏ ռեսուրսների համար, և նույնիսկ դրա տեղադրման համար պահանջվում է շատ ժամանակ:

Ցանցի ավտոմատացումը կարող է իրականացվել անկախ դրա տեսակից:

Օգտագործելով արհեստական ​​ինտելեկտը (AI) և մեքենայական ուսուցումը, ցանցային ավտոմատացման առաջադեմ լուծումները վերլուծում են մետատվյալները և օգտագործում մոդելների վրա հիմնված ցանցային ծրագրավորման հնարավորությունները՝ ծանոթանալու ցանցի վարքագծին, տրամադրելու ակտիվ պատկերացումներ և ուղղորդում տրամադրելու ցանցային օպերատորներին: Ավտոմատացման այս առաջադեմ լուծումները կարող են կազմաձևվել այնպես, որ ուղղիչ գործողություններ կատարեն ինքնուրույն՝ թույլ տալով ցանցի խնդիրները շտկել փակ օղակում, երբեմն նույնիսկ մինչ դրանք տեղի ունենալը: Այսպիսով, ցանցի ավտոմատացումը բարելավում է գործառնական արդյունավետությունը, նվազեցնում է մարդկային սխալի հավանականությունը, մեծացնում է ցանցային ծառայությունների հասանելիությունը և ապահովում է հաճախորդների սպասարկման ավելի լավ մակարդակ:

Այսօր ցանցային ավտոմատացման լուծումները թույլ են տալիս կատարել առաջադրանքների լայն շրջանակ, մասնավորապես.

* Ցանցի պլանավորում և նախագծում, ներառյալ սցենարների պլանավորում և պահուստային կառավարում։
* Սարքերի փորձարկում և կոնֆիգուրացիայի ստուգում։
* Տեղակայված ֆիզիկական սարքերի և ծառայությունների սկզբնավորում, ինչպես նաև վիրտուալ սարքերի տեղակայում և տրամադրում։
* Սարքերի, համակարգերի, ծրագրերի, ցանցի տոպոլոգիայի, տրաֆիկի և ծառայությունների հետ կապված ցանցային տվյալների հավաքագրում իրական ժամանակում։
* Տվյալների վերլուծություն, ներառյալ ակտիվ արհեստական բանականության և մեքենայական ուսուցման վերլուծություն, ցանցի ներկայիս և ապագա վարքագծի վերաբերյալ պատկերացում կազմելու համար։
* Ստուգել կոնֆիգուրացիայի համապատասխանությունը բոլոր ցանցային սարքերի և ծառայությունների ճիշտ շահագործումն ապահովելու պահանջներին։
* Ծրագրային ապահովման թարմացում, ներառյալ անհրաժեշտության դեպքում ծրագրակազմի վերադարձ։
* Ցանցային խնդիրների փակ հանգույցի ուղղում, ներառյալ անսարքությունների վերացումը, ինչպես նաև բարդ և դժվար հայտնաբերվող խափանումների ուղղումը։
* Հաշվետվությունների, վահանակների, ահազանգերի և նախազգուշացումների մանրամասն վերլուծություն։
* Անվտանգության պահանջների իրականացում։
* Ցանցի և նրա ծառայությունների մոնիթորինգ՝ սպասարկման մակարդակը և հաճախորդների գոհունակությունը պահպանելու համար:

Կազմակերպությունները ստանում են հետևյալ առավելությունները՝ ավտոմատացնելով իրենց ցանցերը և ծառայությունները.

* Խնդիրների քանակի կրճատում.

Ցածր կոդերի աշխատանքային հոսքերի օգտագործումը՝ հիմնված մի շարք սցենարների վրա, և մտադրության վրա հիմնված փակ գործողությունների արդյունավետությունը, թույլ է տալիս հեշտությամբ լուծել ցանցի ընդհանուր խնդիրները: Այն նաև նվազեցնում է ձեռքով աշխատանքային հոսքերի հետ կապված սխալների հավանականությունը, ինչպիսիք են կազմաձևման սխալները, տառասխալները և այլն:

* Ծախսերի կրճատում.

Քանի որ ավտոմատացումը հեշտացնում է հիմքում ընկած ենթակառուցվածքը, զգալիորեն ավելի քիչ աշխատաժամանակ է պահանջվում ծառայություններն ու ցանցը կարգավորելու, տրամադրելու և կառավարելու համար: Պարզեցնելով գործառնությունները, համախմբելով ցանցային ծառայությունները, նվազեցնելով տարածքը և չօգտագործված ծառայությունները ցանցից դուրս հանելով՝ մենք նվազեցնում եք անսարքությունները վերացնելու և վերանորոգելու համար պահանջվող մարդկանց թիվը և խնայում էներգիան:

* Ցանցի ճկունության բարձրացում.

Իրադարձության դեպքում ծառայությունները ձեռքով անջատելու անհրաժեշտությունը բացառելով՝ ընկերությունները կարող են ավելի լավ և հետևողական ծառայություններ մատուցել մասնաճյուղերում և աշխարհագրություններում:

* Ցանցի խափանումների կրճատում.

Վերացնելով մարդկային սխալի հավանականությունը՝ ընկերությունները կարող են ավելի լավ և հետևողական ծառայություններ մատուցել տարբեր վայրերում և աշխարհագրություններում: Օրինակ՝ Service Now-ը՝ Juniper Networks-ի անսարքությունների վերացման հեռակառավարման և ավտոմատացված հաճախորդը, թույլ է տալիս արագ և ակտիվորեն հայտնաբերել ցանցի խնդիրները, նախքան հաճախորդները կիմանան դրանց մասին:

* Բարձրացնել ռազմավարական նշանակություն ունեցող աշխատակիցների թիվը.

Ավտոմատացնելով կրկնվող առաջադրանքները, որոնք ներառում են մարդկային սխալ, ընկերությունները մեծացնում են արտադրողականությունը, ինչը նրանց օգնում է ավելի շատ կատարելագործում և նորարարություն առաջացնել բիզնեսում: Արդյունքում նոր աշխատատեղերը հասանելի են դառնում գործող աշխատակիցներին:

* Ընդլայնված վերլուծություն և ցանցի կառավարման հնարավորություններ. Ավտոմատացումը բարելավում է ՏՏ գործառնությունների արագագործությունը՝ ի պատասխան անալիտիկ փոփոխության: Գործողությունները վերահսկելու և անհրաժեշտության դեպքում հարմարեցնելու ունակությունը ապահովում է ցանցի ավելի մեծ տեսողական վերահսկողություն և դրա ներսում տեղի ունեցող գործընթացների թափանցիկություն:

Կանխատեսվում էր, որ Եվրոպայում և ԱՄՆ-ում SDN-ի զանգվածային ընդունումը կսկսվի 2016 թվականին: Այս պահին SDN-ի համաշխարհային շուկայի ծավալը կարող է գերազանցել, ըստ IDC-ի կանխատեսումների, 3,7 միլիարդ դոլարը։ Շուրջ 670 մլն դոլարը կգա SDN հավելվածներից։ Քանի որ ներդրման տեմպերը մեծանում են, գործիքներն ու հնարավորությունները նույնպես կզարգանան: SDN-ը որպես տեխնոլոգիա հասել է կրիտիկական զանգվածի, և այժմ կան բազմաթիվ տարբեր տարբերակներ այն ընկերությունների համար, որոնք նախընտրում են օգտվել դրանից:

**OpenFLow արձանագրություն**

Ժամանակակից ցանցային տեխնոլոգիաները զարգանում են շուրջ 40 տարի: Կա ցանցերի ղեկավարման 7 մակարդակ՝ OSI ցանցային մոդելy: Այս մոդելի յոթ մակարդակներից չորսից ավելին երբեք գործնականում չի իրականացվել: Այս տարիների ընթացքում առաջադրանքներն ավելի ու ավելի են դժվարացել։ Դա պայմանավորված է տեղեկատվական գործընթացների մարդկային կյանքի բոլոր ոլորտներում ավելի խորը ներթափանցմամբ: Հատուկ պահանջներ են դրվում ցանցի և այնտեղ պահվող տվյալների անվտանգությունն ապահովելու անհրաժեշտության նկատմամբ։ Առաջանում է Firewall-ի կարիք, որը ոչ միայն պաշտպանում է ցանցի պարագիծը, այլ նաև տեղաբաշխում է անվտանգության հատուկ գոտիներ տեղական կամ կորպորատիվ ցանցի ներսում: Հատուկ պահանջներ են առաջանում, երբ անհրաժեշտ է ապահովել պահանջվող QoS մակարդակը ոչ միայն ծառայություն մատուցողից, այլ նաև տեղական ցանցում։ Քիչ-քիչ ավելի ու ավելի են դրվում ցանցային ռեսուրսների դինամիկ վերաբաշխման խնդիրները (թողունակություն, ուշացում և այլն): Ավանդական ցանցային տեխնոլոգիաների շրջանակներում այս բոլոր խնդիրներն այլևս հնարավոր չէ լուծել։ OpenFlow (կամ SDN - Software Defined Network) տեխնիկան նախատեսված է այս մարտահրավերներին պատասխանելու համար:

OpenFlow-ն բաց ստանդարտ է, որը թույլ է տալիս ծրագրավորողներին աշխատել լոկալ ցանցում՝ փորձարարական արձանագրություններով: OpenFlow-ն ավելացվել է՝ որպես նոր հատկություն առևտրային Ethernet անջատիչների, երթուղիչների և անլար մուտքի կետերի համար, որպեսզի թույլ տա փորձարկել ցանցը՝ առանց ցանցային սարքերի ներքին մասերը բացահայտելու: OpenFlow ստանդարտը ներկայումս ընդունված է ցանցային սարքավորումներ արտադրողների մեծ մասի կողմից: OpenFlow անջատիչներն այսօր հասանելի են ցանցային շուկայում: OpenFlow արձանագրությունը հիմնված է SDN (Software Defined Networking) տեխնոլոգիայի վրա և կարող է օգտագործվել լարային և անլար ցանցերում: Արձանագրության ներկայիս նոր տարբերակը OpenFlow 1.3-ն է:

Դասական երթուղիչում կամ անջատիչում փաթեթների արագ վերահասցեավորումը (տվյալների վերահասցեավորում) և բարձր մակարդակի երթուղավորման որոշումները (վերահսկման գործողություններ) կատարվում են նույն սարքում: OpenFlow անջատիչը առանձնացնում է այս երկու գործառույթները: Տվյալների վերահասցեավորումն իրականացվում է հենց անջատիչի կողմից, մինչդեռ երթուղավորման որոշումները վստահված են առանձին վերահսկիչի(SDN), սովորաբար ստանդարտ սերվերի: Վերահսկիչի հետ կապի ալիքը պետք է ծածկագրված լինի: OpenFlow անջատիչն ու վերահսկիչը միմյանց հետ շփվում են OpenFlow արձանագրության միջոցով, որը սահմանում է այնպիսի հաղորդագրություններ, ինչպիսիք են packet-received(փաթեթների ստացում), send-packet-out (փաթեթների ուղարկում),modify-forwarding-table(փոխանցման աղյուսակի փոփոխում) և get-stats (ստանում վիճակագրություն):

**OpenDaylight**

OpenDaylight վերահսկիչը JVM ծրագրաշար է և կարող է գործարկվել ցանկացած օպերացիոն համակարգից և սարքաշարից, քանի դեռ այն աջակցում է Java-ին: Վերահսկիչը ծրագրային ապահովման սահմանված ցանցի (SDN) հայեցակարգի իրականացումն է և օգտագործում է հետևյալ գործիքները՝

**Maven** - OpenDaylight-ն օգտագործում է Maven-ը ավելի հեշտ կառուցելու ավտոմատացման համար: Maven-ն օգտագործում է pom.xml (Project Object Model)՝ փաթեթների միջև կախվածությունը գրելու և նաև նկարագրելու, թե ինչ փաթեթներ պետք է բեռնել և սկսել:

**OSGi** - Այս շրջանակը OpenDaylight-ի հետնամասն է, քանի որ այն թույլ է տալիս դինամիկ կերպով բեռնել փաթեթներ և փաթեթներ JAR ֆայլեր և կապել փաթեթները՝ տեղեկատվության փոխանակման համար:

**JAVA ինտերֆեյսներ** - Java ինտերֆեյսները օգտագործվում են իրադարձությունների ունկնդրման, բնութագրերի և ձևավորման օրինաչափությունների համար: Սա այն հիմնական միջոցն է, որով հատուկ փաթեթներն իրականացնում են հետադարձ կապի գործառույթներ իրադարձությունների համար, ինչպես նաև ցույց տալու կոնկրետ վիճակի մասին իրազեկվածությունը:

**REST API-ներ** - Սրանք հյուսիսային API-ներ են, ինչպիսիք են տոպոլոգիայի կառավարիչը, հյուրընկալող որոնիչը, հոսքի ծրագրավորողը, ստատիկ երթուղիչը և այլն:

Վերահսկիչը բացահայտում է բաց հյուսիսային API-ները, որոնք օգտագործվում են հավելվածների կողմից: OSGi շրջանակը և երկկողմանի REST-ը աջակցվում են հյուսիսային API-ների համար: OSGi շրջանակն օգտագործվում է հավելվածների համար, որոնք աշխատում են նույն հասցեի տարածքում, ինչ վերահսկիչը, մինչդեռ REST (վեբ վրա հիմնված) API-ն օգտագործվում է այն հավելվածների համար, որոնք չեն աշխատում նույն հասցեի տարածքում (կամ նույնիսկ նույն համակարգում), ինչ վերահսկիչը: Բիզնեսի տրամաբանությունը և ալգորիթմները գտնվում են հավելվածներում: Այս հավելվածներն օգտագործում են վերահսկիչը ցանցի հետախուզություն հավաքելու, դրա ալգորիթմը անալիտիկ անելու համար և այնուհետև նոր կանոնները ամբողջ ցանցում կազմակերպելու համար: Հարավային կողմում մի քանի արձանագրություններ աջակցվում են որպես հավելումներ, օրինակ. OpenFlow 1.0, OpenFlow 1.3, BGP-LS և այլն: OpenDaylight կարգավորիչը սկսվում է OpenFlow 1.0 հարավային պլագինով: OpenDaylight-ի մյուս մասնակիցները սկսում են ավելացնել վերահսկիչի կոդը: Այս մոդուլները դինամիկ կերպով կապված են ծառայության աբստրակցիոն շերտի (SAL):

SAL-ը ցուցադրում է ծառայություններ, որոնց վրա գրված են մոդուլները դեպի հյուսիս: SAL-ը պարզում է, թե ինչպես կատարել պահանջվող ծառայությունը՝ անկախ վերահսկիչի և ցանցային սարքերի միջև օգտագործվող հիմքում ընկած արձանագրությունից: Սա ապահովում է ներդրումների պաշտպանություն հավելվածներին, քանի որ OpenFlow-ը և այլ արձանագրությունները ժամանակի ընթացքում զարգանում են: Որպեսզի վերահսկիչը կառավարի իր տիրույթում գտնվող սարքերը, նա պետք է իմանա սարքերի, դրանց հնարավորությունների, հասանելիության և այլնի մասին: Այս տեղեկատվությունը պահվում և կառավարվում է Topology Manager-ի կողմից: Մյուս բաղադրիչները, ինչպիսիք են ARP handler-ը, Host Tracker-ը, Device Manager-ը և Switch Manager-ը, օգնում են Topology Manager-ի համար տոպոլոգիայի տվյալների բազայի ստեղծմանը:

