УДК 681.35 DOI: 10.31673/2518-7678.2019.0301218

Ткаченко О.М., д.т.н.; **Лемешко А.В.,** аспірант; **Кращенко Д.В.,** аспірант;
Кадюк Р.С., студент; **Стельмах Т.М.,** студент

ОСОБЛИВОСТІ СТВОРЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ВЕЛИКОГО ПІДПРИЄМСТВА

Tkachenko O.M., Lemeshko A.V., Krashchenko D.V., Kadiuk R.S., Stelmakh T.M. Features of creating network infrastructures of a big enterprise. The article describes the stages of building a network infrastructure of a large enterprise with the possibility of expansion and further administration. The network infrastructure (NI) of the enterprise that is being created belongs to the category of service networks for the provision of data transmission services. The task of the service level boundary of the network infrastructure is the routing and processing of corporate traffic. The security system has been seized by switching on and off to a single information space, to the central data processing center in the central network and to the Internet. Securing the connectivity of the Internet segment is achieved through the use of infrastructure switches integrated in a fault-tolerant design using factory expansion technology.

Keywords: network infrastructure, secure connection, information and telecommunication systems, data centers, MPLS, redundancy.

Ткаченко О.М., Лемешко А.В., Кращенко Д.В., Кадюк Р.С., Стельмах Т.М. Особливості створення мережевої інфраструктури великого підприємства. В статті наведено опис етапів побудови мережевої інфраструктури великого підприємства з можливістю розширення та подальшого адміністрування. Мережева інфраструктура (МІ) підприємства, що створюється, відноситься до категорії сервісних мереж надання послуг передавання даних. Задача рівня сервісної межі мережевої інфраструктури маршрутизація та обробка корпоративного трафіку. Підсистема забезпечує захищене підключення співробітників до єдиного інформаційного простору, до відомчих ІТ сервісів, сервери яких розташовані в центрі обробки даних (ЦОД) в центральному вузлі і до мережі Інтернет.

Ключові слова: мережева інфраструктура, захищене підключення, інформаційно-телекомунікаційні системи, ЦОД, MPLS, резервування.

Ткаченко О.Н., Лемешко А.В., Кращенко Д.В., Кадюк Р.С., Стельмах Т.М. Особенности построения сетевой инфраструктуры большого предприятия. В статье приведено описание этапов построения сетевой инфраструктуры крупного предприятия с возможностью расширения и дальнейшего администрирования. Сетевая инфраструктура (СИ) предприятия, которая создается, относится к категории сервисных сетей предоставления услуг передачи данных. Задача уровня сервисного предела сетевой инфраструктуры маршрутизация и обработка корпоративного трафика. Подсистема обеспечивает защищенное подключение сотрудников к единому информационному пространству, к ведомственным ИТ сервисам, серверы которых расположены в центре обработки данных (ЦОД) в центральном узле и в сети Интернет.

Ключевые слова: сетевая инфраструктура, защищенное подключение, информационно-телекоммуникационные системы, ЦОД, MPLS, резервирование.

Вступ

Головним завданням Мережевої інфраструктури (МІ) є [1-3]:

-забезпечення транспортного середовища передавання трафіку різного типу каналами зв'язку між об'єктами та структурними підрозділами;

-надання послуг передавання даних та доступу в мережу Інтернет іншим підприємствам;

-надання послуг корпоративної поштової системи, сервісу уніфікованих комунікацій, програмних засобів для керування проектами, організації спільної роботи, веб-порталів;

-надання захищеного доступу до мережі Інтернет співробітникам;

-надання доступу співробітникам до відомчих ІТ сервісів;

-забезпечення комплексного функціонування усіх інформаційних (інформаційно-телекомунікаційних) систем, що використовують її ресурси, за рахунок вибору відповідного мережевого устаткування, оптимального поєднання технологій і протоколів передачі різнорідного трафіку (відео, голос, дані) з можливістю управління якістю обслуговування;

-захист інформації, що передається ЗТМ, сучасними програмними та апаратними засобами;

-забезпечення високого рівня надійності при цілодобовому режимі роботи;
-високу ефективність використання ресурсів мережі;
-забезпечення зручності експлуатації з урахуванням віддаленого моніторингу і управління;
-диференційоване обслуговування трафіку відповідно до заданих пріоритетів;
-можливість масштабування.

Виклад основного матеріалу дослідження

МІ територіально складається з центрального вузла (ЦВ), та вузлів структурних підрозділів.

Створення мережевої інфраструктури передбачається на базі наступних функціональних підсистем:
-підсистема агрегації рівня ядра;
-підсистема рівня сервісної границі;
-підсистема захищеного доступу до Інтернет;
-підсистема рівня Інтернет доступу;
-підсистема рівня доступу;
-підсистема управління;
-підсистема загальних інформаційних сервісів.
Структурна схема розподілу системи наведена на рис.1.

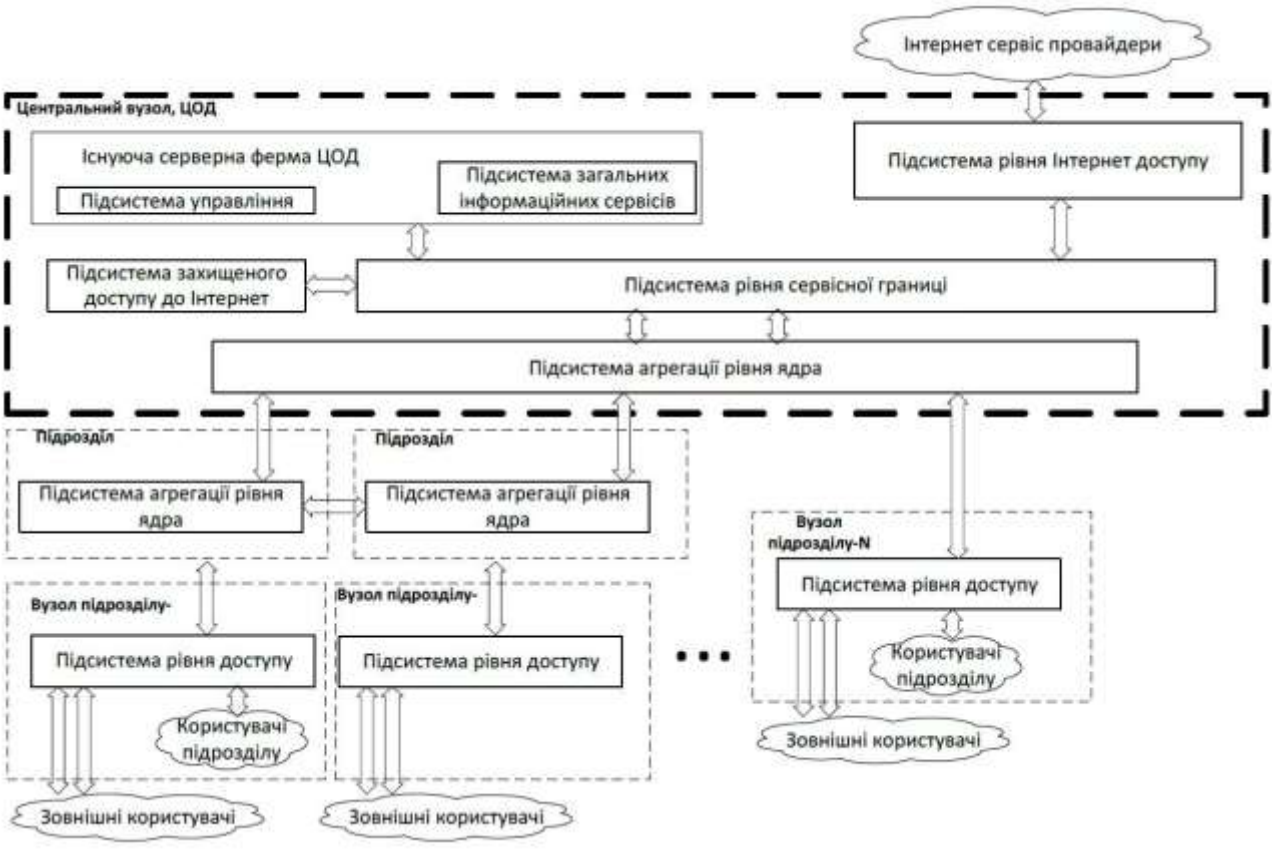

Рис.1. Структурна схема розподілу системи

В якості основних мережевих протоколів обміну інформацією в МІ пропонується використання набору протоколів TCP/IP.

Будівництво МІ передбачається з використанням технології MPLS. Підсистему агрегації рівня ядра формують шість маршрутизаторів, розміщених на центральному та двох агрегуючих вузлах структурних підрозділів, які включені за повнозв'язною схемою і в

мережі MPLS виконує роль P- маршрутизаторів. Для забезпечення резервування використовується по два шасі на кожній локації, об'єднані в логічний кластер за технологією розширення IRF (Intelligent Resilient Framework) (або аналогічною). Нарощування ємності з'єднань досягаються використанням балансування трафіку за допомогою механізмів MPLS через паралельні канали (від 2 до 8) ємністю 10G кожний. Ємність з'єднань між ЦВ та агрегуючими вузлами складає 40 Гбіт/с.

На опорній мережі застосовується ряд протоколів динамічної маршрутизації, що забезпечують розповсюдження маршрутної інформації, відмовостійкість та балансування трафіку. Ядро побудовано за принципом BGP-free CORE, для маршрутизації трафіку використовуються MPLS label switch path (LSP). Розповсюдження інформації про службові адреси, необхідні для формування повнозв'язної топології здійснюється за протоколом OSPF. Для передачі інформації про мітки застосовується протокол LDP. Маршрутизатори рівня сервісної межі (SE) використовують протокол iBGP для обміну маршрутами між собою.

Опорна мережа працює в прозорому режимі, забезпечуючи передачу трафіку між підключеними до неї вузлами в незмінному вигляді. Передача трафіку в опорній мережі виконується за допомогою технології IEEE 802.3ae (10G Ethernet). Управління мережею та трафіком забезпечується за допомогою механізмів та протоколів сімейства стандартів MPLS. Опорні маршрутизатори (P) підтримують наступні механізми передачі даних:

-комутація трафіка у відповідності до міток MPLS, призначених трафіку на вузлах межі надання сервісу;

-підтримка черг та пріоритетів відповідно до пріоритетів, наданих трафіку в усіх інших сегментах мережі;

-підтримка топологічної цілісності, відсутність замкнутих кілець (loop-free topology) та швидке відновлення цілісності у випадку аварійної ситуації.

Задача підсистеми агрегації рівня ядра - забезпечення підключень вузлів рівня доступу (за територіальною ознакою) і рівня сервісної межі в єдину транспортну мережу та передачу магістральних потоків трафіку MPLS між вузлами мережі найбільш оптимальним маршрутом.

Обладнання підсистеми рівня сервісної межі розміщується в ЦВ і будується на базі чотирьох маршрутизаторів, які в мережі MPLS виконують роль граничних транспортних пристроїв і виступають у ролі PE-маршрутизаторів.

Задача рівня сервісної межі мережевої інфраструктури – маршрутизація та обробка корпоративного трафіку. На цьому рівні працюють наступні сервіси, протоколи та технології: VPN, BGP, OSPF, ADVPN.

Підсистема рівня сервісної межі працює в прозорому режимі, забезпечуючи передачу трафіку від підсистеми доступу до підсистеми рівня сервісної межі в незмінному вигляді.

Підсистема рівня сервісної межі має підтримувати наступні механізми для передачі трафіку:

-ізоляція даних (L2 VPN "точка-точка" та "багатоточка", L3 VPN) у відповідності або з урахуванням ізоляції в підсистемі доступу;

-підтримка черг та пріоритетів відповідно до пріоритетів, наданих трафіку в підсистемі доступу;

-підтримка топологічної цілісності, відсутність замкнутих кілець (loop-free topology) та швидке відновлення цілісності у випадку аварійної ситуації.

Підсистема забезпечує захищене підключення співробітників до єдиного інформаційного простору, до відомчих IT сервісів, сервери яких розташовані в центрі обробки даних (ЦОД) в центральному вузлі і до мережі Інтернет.

Обладнання підсистеми рівня доступу розміщується на вузлах структурних підрозділів та будується на базі:

-L3 комутаторів - обладнання, яке в мережі MPLS виконує роль граничних транспортних пристроїв і є точкою підключення WAN-маршрутизаторів корпоративного сегменту;

-маршрутизатора - обладнання, яке виконує роль клієнтського обладнання та створює захищений WAN сегмент корпоративної мережі.

Маршрутизатори локацій доступу мають підключення до центрального вузла або агрегуючих вузлів ємністю 10 Гбіт/с які може бути збільшено за необхідності та наявності технічної можливості до залежності від об'єму трафіку до 40 Гбіт/с.

Підсистема рівня Інтернет доступу складається з двох виділених маршрутизаторів з функціоналом граничних маршрутизаторів та з двох виділених комутаторів, що здійснюють підключення до Інтернет сервіс-провайдерів та/або точок обміну трафіком.

Підключення комутаторів здійснюється за допомогою технології IEEE 802.3ae (10G Ethernet) до двох незалежних upstream провайдерів. Зовнішнє підключення використовує протокол динамічної маршрутизації eBGP між пограничним маршрутизатором та upstream провайдерами для обміну маршрутною інформацією. Необхідною передумовою є наявність публічної автономної системи та блоку публічних адрес IPv4 для забезпечення описаного підключення.

Граничні маршрутизатори мають забезпечити можливість тримати два повних BGP full view кожен (не менш 2 мільйона IPv4 маршрутів). Підключення підсистеми рівня сервісної межі до комутаторів доступу до Інтернет здійснюється за допомогою технології IEEE 802.3ae (10G Ethernet). Необхідна кількість інтерфейсів 10G Ethernet по два на кожному пристрої. Забезпечення зв'язності сегменту доступу до Інтернет досягається за рахунок використання інфраструктурних комутаторів, об'єднаних у відмовостійку конструкцію з використанням технології розширення фабрики IRF (Intelligent Resilient Framework) або аналогічної. Підключення здійснюється до інтерфейсів, що можуть працювати у комбінованому режимі 1/10G з використанням оптичних модулів. Кількість інтерфейсів має становити не менше 24 на кожен комутатор. Комутатори працюють в L2 режимі та не надають L3 сервісів (окрім управління). Протокол BGP призначений для обміну інформацією про досяжності підмереж між автономними системами (АС), тобто групами маршрутизаторів під єдиним технічним і адміністративним управлінням, що використовують протокол внутрішньодоменої маршрутизації для визначення маршрутів всередині себе і протокол міждоменої маршрутизації для визначення маршрутів доставки пакетів в інші АС. Передана інформація включає в себе список АС, до яких є доступ через дану систему. Вибір найкращих маршрутів здійснює виходячи з правил, прийнятих в мережі. З метою динамічного управління Інтернет трафіком через двох провайдерів для МІ виділяється своя АС. Підсистема забезпечує відмовостійке підключення мережевої інфраструктури до мережі Інтернет.

Обладнання підсистеми захищеного доступу до Інтернет розміщується на центральному вузлі і будується на базі трьох пар пристроїв захисту з різною функціональністю, а саме: міжмережевого екрану, захист WEB трафіку, захист e-mail трафіку.

Задача підсистеми захищеного доступу до Інтернет:

-захист периметру мережі від зовнішніх Інтернет загроз;

-визначення та забезпечення роботи політик доступу до Інтернет і взаємодії різного трафіку корпоративної мережі;

-контроль і фільтрацію мережевих пакетів, що проходять через нього відповідно до заданих правил;

-забезпечення захищеного доступу до серверного обладнання ЦОД;

-трансляцію адрес – динамічну заміну внутрішньо-мережевих (приватних) адрес або портів на зовнішні (публічні), що використовуються за межами локальної мережі.

В підсистемі пропонується використовувати міжмережеві екрани нового покоління з функціоналом протидії мережевим атакам, з можливістю контролю додатків, захисту від вторгнень, захисту від вразливостей в ПЗ. Передбачається реалізувати відмовостійку архітектуру рішення в режимі кластера, що складається з двох пристроїв з сумарною пропускною здатністю не менше 52 Gbit/s (для функціоналу міжмережевого екрану), з можливістю збільшення. Для управління передбачається використовувати систему керування пристроями.

Підключення міжмережевих екранів нового покоління планується здійснювати двома інтерфейсами 10G Ethernet кожного до комутаторів підсистеми.

Міжмережеві екрани нового покоління створюють демілітаризовану зону (DMZ) для забезпечення можливості публікації в мережу Інтернет як визначених ресурсів

корпоративного сегменту. При цьому розділ та ізоляція вказаних ресурсів здійснюється на логічному рівні.

Окремо для захисту корпоративного сегменту передбачаються пристрої для захисту веб-ресурсів та електронної пошти.

Для захисту інформації, переданої по мережевій інфраструктурі між вузлами підрозділів та ЦОД доцільно використовувати технології побудови віртуальних приватних мереж. Віртуальні приватні мережі виконують такі функції:

-динамічне визначення несправностей на шляху проходження трафіку;

-захист інформації, що передається відкритими каналами передачі даних;

-можливість використання протоколів динамічної маршрутизації між маршрутизаторами корпоративної мережі;

-логічний поділ трафіку між підмережами корпоративної мережі, мережі управління, гостьових мереж та інших на третьому рівні моделі OSI.

З огляду на вимоги до масштабування, а також до організації виділених логічних мереж для різних сегментів передачі даних в мережі використовується технологія ADVPN спільно з технологією MPLS L3VPN.

Технологія ADVPN розрахована на застосування у дизайнах HUB-and-Spoke, dynamic full-mesh і dynamic partial-mesh. Одним з головних переваг є підтримка VPN вузлів з IP адресами, що призначаються динамічно.

ADVPN використовує multipoint GRE тунелі, для організації VPN пристроями, а також технологію VAM (VPN Address Management) для динамічного зіставлення "реальних" адрес, і адрес тунельних інтерфейсів. Для забезпечення безпеки передачі даних, за загальними каналами, використовується шифрування даних за допомогою протоколу IPSec.

До переваг технології можна віднести:

-підтримку передачі мультикаст трафіку;

-підтримку динамічних протоколів маршрутизації;

-підтримку QoS;

-можливість створення динамічних VPN тунелів для обміну трафіком між VPN Spoke вузлами.

З метою логічного розподілу відокремлених мереж (VRF) корпоративного сегмента, сегмента управління, гостьових сегментів та інших використовується функціонал MPLS L3VPN. Логічні інтерфейси, які підключаються до мереж з різних VRF включаються в попередньо створені віртуальні таблиці маршрутизації. Для передачі маршрутної інформації між вузлами використовується протокол динамічної маршрутизації.

На центральному вузлі Мережевої інфраструктури передбачається встановлення наступного обладнання:

-два маршрутизатора - HPE HSR6802 підсистеми рівня Інтернет доступу;

-два комутатора - HPE 5700 40XG 2QSFP+ підсистеми рівня Інтернет доступу;

-два комутатора - HPE 5700 32XGT 8XG 2QSFP+ підсистеми рівня сервісної межі;

-чотири маршрутизатора - HPE HSR 6804 підсистеми рівня сервісної границі, які в мережі IP/MPLS виконують функції граничних пристроїв (PE);

-два міжмережевих екрана в режимі відмовостійкого кластеру - Fortinet FG-1000D підсистеми захищеного доступу до Інтернет;

-два пристрої захисту електронної пошти в режимі відмовостійкого кластеру - Fortinet FML-400E підсистеми захищеного доступу до Інтернет;

-два пристрої захисту WEB трафіку в режимі відмовостійкого кластеру - Fortinet FWB-600D підсистеми захищеного доступу до Інтернет;

-два комутатора - HPE 5930 4-slot підсистеми агрегації рівня ядра, які в мережі IP/MPLS виконують функції магістральних пристроїв (P);

-підсистема управління і моніторингу - HPE IMC Standart;

-підсистема управління і моніторингу - Fortinet FMG-VM-Base (FortiManager-VM);

-підсистема загальних інформаційних сервісів.

Слід зазначити, що підсистеми управління і моніторингу, загальних інформаційних сервісів – це, в свою чергу, програмні засоби, що розгортаються на серверному обладнанні Замовника та розміщення яких передбачається в центральному вузлі.

Передбачається формування ІТ інфраструктури на базі продуктів Microsoft з використанням платформи віртуалізації.

Технічне рішення 1-ої Черги передбачає розгортання на технічних потужностях ЦОД з використанням платформи віртуалізації VMware, наступних інфраструктурних сервісів Майкрософт (далі – ІТ-сервіси):

-базові мережеві сервіси (Active Directory, DNS, DHCP)

-корпоративна електронна пошта на базі Exchange Server 2016

-система уніфікованих комунікацій на базі Skype for Business Server 2015.

Впровадження рішення дозволить закласти базу для формування та створення комплексної інформаційної системи, яка підвищить ефективність функціонування структурних підрозділів, створить базу для взаємодії з інформаційними системами.

Результат буде досягнуто за рахунок:

-впровадження інфраструктурних ІТ-сервісів, що відповідають сучасним вимогам (тенденціям, методикам, рекомендаціям, тощо)

-впровадження базової платформи комунікацій та колективної роботи та взаємодії співробітників

-оптимізації використання апаратних потужностей завдяки віртуалізації ІТ-інфраструктури.

Загальна схема організації зв‘язку МІ наведена на рис. 2.

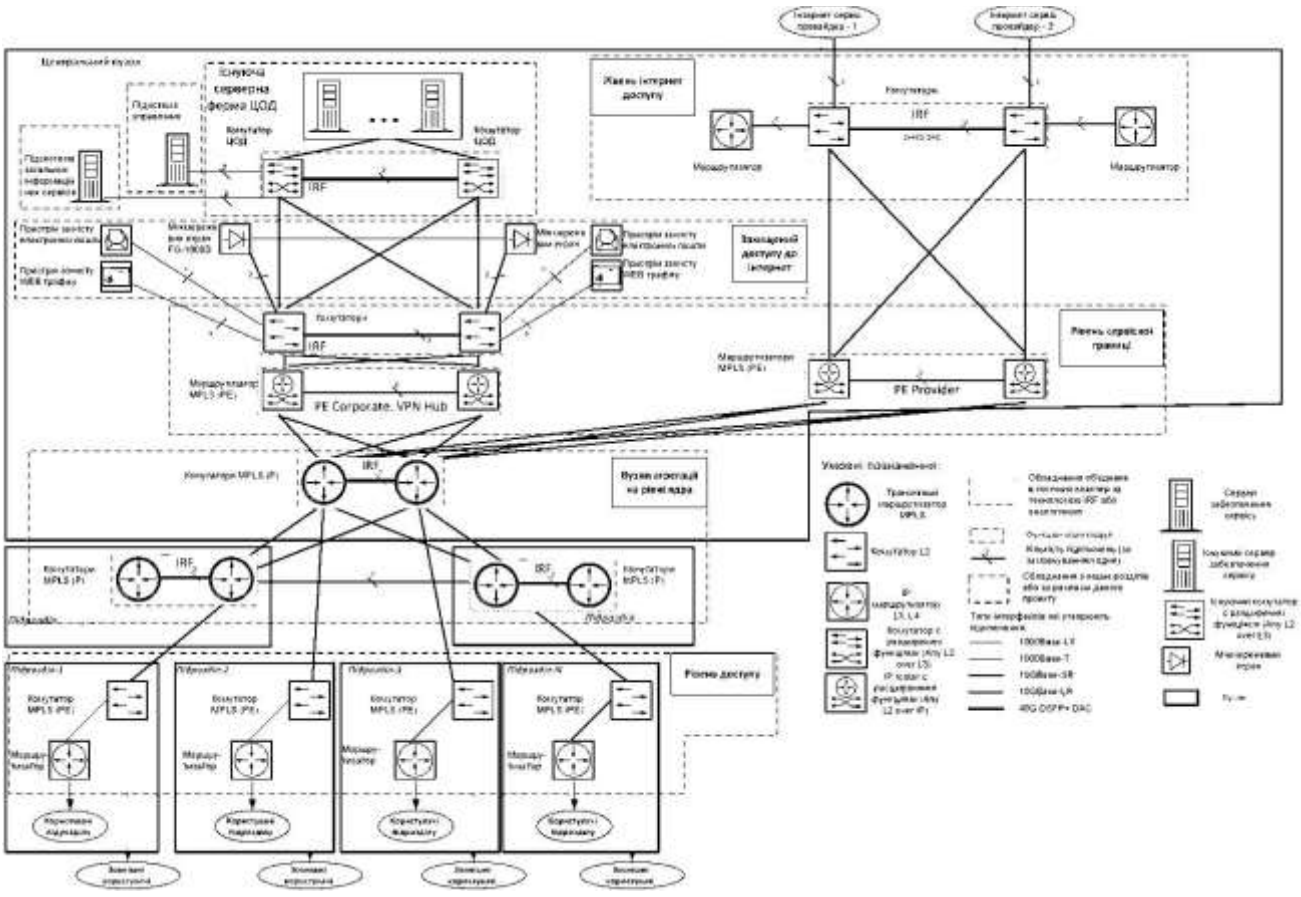

Рис. 2. Загальна схема організації зв‘язку МІ

Відмовостійкість та резервування пристроїв основних вузлів мережі у повному обсязі передбачається впровадити у наступних чергах модернізації мережі. У рамках І-Черги планується використовувати резервування блоків живлення обладнання та резервовані (подвійні) мережеві з’єднання при підключенні маршрутизаторів та комутаторів рівня ядра

Транспортна мережа складається з декількох логічних блоків (модулів), кожен з яких націлений на виконання відповідних функцій:

1) Модуль інтернет-доступу – зв'язок з провайдерами верхнього рівня та маршрутизація трафіку назовні.

2) Модуль сервісної мережі – контроль та термінування внутрішніх мережевих сервісів (MPLS, ADVPN);

3) Модуль ядра – високошвидкісний та відмовостійкий зв'язок між всіма компонентами мережі;

4) Модуль доступу користувачів – підключення кінцевих користувачів;

5) Модуль ЦОД – розміщення корпоративних сервісів та сервісів захисту доступу до мережі Інтернет.

Висновки

Таким чином реалізація розглянутої мережевої інфраструктури забезпечить створення єдиної транспортної пакетної мережі, яка призначена для обслуговування існуючих і в перспективі нових клієнтів.

Надання будь-яких транспортних пакетних сервісів передачі даних, таких як точка-точка, точка-мультиточка, багатоадресна розсилка, на основі технологій L2 MPLS VPN, VPLS, L3 MPLS VPN, Multicast. Надання доступу до корпоративних сервісів для підрозділів, аудіо та відео-зв'язок (включаючи конференції за участю трьох та більше учасників), телебачення шляхом Unicast-мовлення та широкомовне (шляхом Multicast- мовлення).

Бізнес-послуги для клієнтів сервісів (L2 / L3 VPN). Підвищення безпеки послуг, транспортних сервісів і послуг за рахунок використання технологій сегментування і тунелювання. Покращення керованості, як окремими елементами інфраструктури, так і мережі в цілому, а також захищений доступ до мережі Інтернет.

Список використаної літератури

1. Гольдштейн А. Б., Гольдштейн Б. С. Технология и протоколы MPLS СПб.: БХВ-Петербург, 2014. — 304 с.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2001. – 672 с.

3. Технологія ADVPN [Електронний ресурс] // Режим доступу: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/ADVPN/ADVPN.htm

Автори статті

Ткаченко Ольга Миколаївна – доктор технічних наук, доцент, завідувач кафедри Комп'ютерної інженерії, Державний університет телекомунікацій, Київ, Україна.

Лемешко Андрій Вікторович – старший викладач кафедри Комп'ютерної інженерії, Державний університет телекомунікацій, Київ, Україна.

Кращенко Денис Васильович – аспірант кафедри Комп'ютерної інженерії, Державний університет телекомунікацій, Київ, Україна.

Кадюк Ростислав Сергійович – студент Навчально-наукового інституту інформаційних технологій, Державний університет телекомунікацій, Київ, Україна.

Стельмах Тарас Михайлович – студент Навчально-наукового інституту телекомунікацій, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Tkachenko Olha Mykolaivna – doctor of Science (technic), associate professor, head of Department of Computer engineering, State University of Telecommunications, Kyiv, Ukraine.

Lemeshko Andriy Viktorovich – Senior lecturer of computer engineering department, State University of Telecommunications, Kyiv, Ukraine.

Krashchenko Denys Vasylovych – post-graduate student, State University of Telecommunications, Kyiv, Ukraine.

Kadiuk Rostyslav Serhiiovych – student, State University of Telecommunications, Kyiv, Ukraine.

Stelmakh Taras Mykhailovych – student, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 05.08.2019 р. Рецензент: д.т.н., доцент А.О. Макаренко