УДК 004.72, 004.738

Черкасов Д. І.

МАРШРУТИЗАЦІЯ В МЕРЕЖІ СУЧАСНОГО ПІДПРИЄМСТВА

У статті розглянуто оптимальні підходи до організації маршрутизації в мережі сучасного підприємства, до складу якої входить низка територіально розмежованих відділень. Використано поняття транспортної інфраструктури локальної мережі відділення. Підходи базуються на особливостях сучасної компонентної бази. Увагу приділено використанню технології віртуалізації мережних функцій (NFV).

Ключові слова: телекомунікації, підприємство, маршрутизація, VPN, віртуалізація, NFV.

Вступ

Для організації комунікацій у корпоративних мережах зазвичай використовують модель мережі сучасного підприємства [5]. Ця модель передбачає наявність у підприємства декількох територіально розмежованих відділень, одним з яких є головний кампус. Для взаємодії відділень між їхніми локальними мережами (Local Area Network, або LAN) використовують з'єднання, створені за технологіями так званих глобальних мереж (World Area Network, або WAN).

До WAN-технологій, які використовують у корпоративних мережах, належать зокрема [11]:

- орендовані канали 2-го або 3-го рівня через транспортну мережу оператора зв'язку;
- з'єднання через телефонну мережу загального користування;
- канали віртуальних приватних мереж (Virtual Private Network або VPN) через Інтернет.

VPN-з'єднання через Інтернет на сьогодні здобули значне поширення, оскільки суттєво дешевші, ніж орендовані канали, при цьому забезпечують достатньо високу якість передачі даних. Для побудови VPN-з'єднань між відділеннями кожне з відділень має бути підключене до Інтернет.

За наявності єдиного головного відділення, в якому розміщені основні інформаційні ресурси підприємства (наприклад, дата-центр), основні потоки даних передаються між головним і підпорядкованими відділеннями. Оптимальною топологією VPN-з'єднань у такому випадку є зірка з головним відділенням у центрі. При цьому можливе використання технології динамічних багатоточкових VPN-з'єднань (Dynamic Multipoint VPN або DMVPN), коли в головному відділенні встановлено DMVPN-концентратор і з'єднання між головним відділенням і будь-яким підпорядкованим здійснюється у разі потреби передачі даних між ними [3].

Якщо інформаційні ресурси розподілені між різними відділеннями, до того ж є потреба постійної взаємодії між відділеннями, доцільно використовувати постійно діючі VPN-з'єднання типу «точка–точка» (point-to-point), кожен з яких з'єднує між собою два відділення. Для надійності варто з'єднати кожне відділення з декількома іншими. Такий підхід дає можливість скоротити шлях передання пакетів, оскільки воно здійснюється безпосередньо між відділеннями відправника і отримувача, а також забезпечує стійкість мережі до відмови окремих VPN-з'єднань, – пакети можуть передаватися транзитом через інші відділення, оминаючи ділянку, на якій сталася відмова.

Якщо загальна кількість відділень не перевищує 4-5, можливе створення VPN-з'єднань між кожною парою відділень з утворенням «повної сітки» (full mesh) з'єднань. У разі наявності великої кількості відділень, наприклад, десятків, створення повної сітки з'єднань призводить до надмірного ускладнення конфігурації корпоративної мережі. В цьому випадку доцільно визначити 3-4 відділення як основні (магістральні) і створити повну сітку з'єднань між ними. Інші відділення під'єднуються кожне до двох магістральних для надійності. Така топологія відома під назвою «часткова сітка» (partial mesh) [6].

IP-адресація в корпоративній мережі

Об'єднання відділень в єдину корпоративну мережу – intranet [5] – передбачає використання спільного IP-адресного простору. Зазвичай використовують IP-адреси з так званих приватних діапазонів згідно з рекомендаціями RFC1918 [8]. За кожним відділенням закріплюється піддіапазон IP-адрес. У результаті створюється єдина IP-мережа, в якій є можливість обміну пакетами між будь-якою парою пристроїв із будь-яких відділень.

Для прикладу розглянемо корпоративну мережу, яка використовує для внутрішньої адресації блок 10.0.0.0/8 (рис. 1). Для розподілу IP-адрес застосовано такий принцип:

- 1-й байт IP-адреси є фіксованим і дорівнює 10;
- 2-й байт IP-адреси є ідентифікатором відділення (branch-id) і приймає значення від 1 до 200;
- 3-й байт є ідентифікатором сегмента локальної мережі у відділенні;
- 4-й байт є ідентифікатором пристрою в сегменті мережі (всі сегменти отримують діапазон адрес однакового розміру – /24);
- IP-адреси, 2-й байт яких приймає значення від 201 до 250, використовуються на каналах з'єднання між відділеннями, при цьому на кожний канал виділяється діапазон /30.

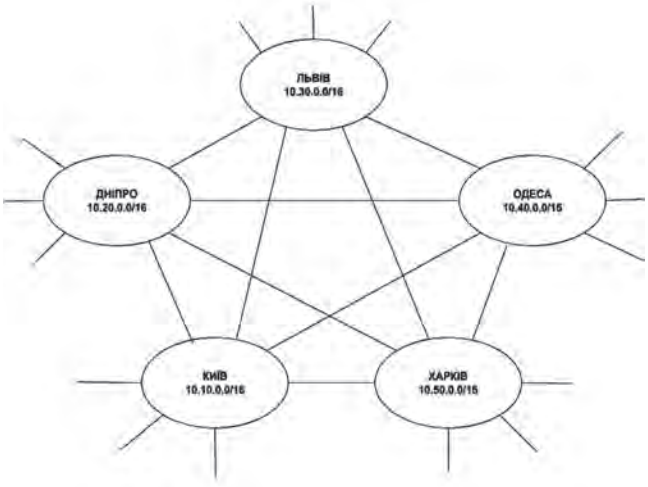

Рис. 1. Приклад розподілу IP-адрес у корпоративній мережі

Постановка задачі маршрутизації в мережі сучасного підприємства

Ефективність функціонування корпоративної мережі значною мірою залежить від упровадженої в ній системи маршрутизації. Для розгляду маршрутизації в корпоративній мережі внутрішня структура мережі відділення може бути представлена як логічна модель, яка містить такі компоненти (рис. 2):

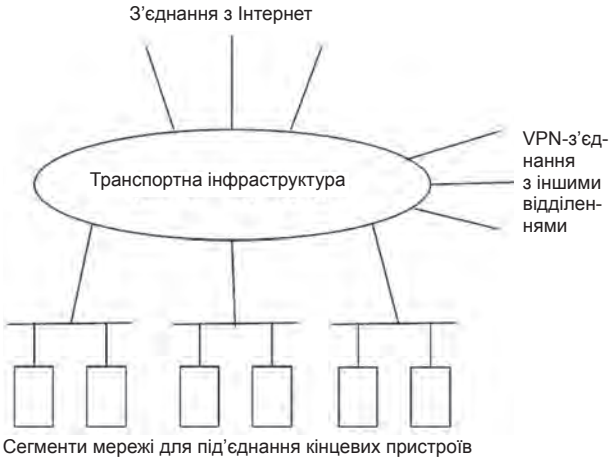

Рис. 2. Внутрішня структура мережі відділення

- сегменти мережі для під'єднання кінцевих пристроїв;
- з'єднання з іншими відділеннями;
- з'єднання з Інтернет;
- транспортна інфраструктура.

Транспортна інфраструктура забезпечує обмін даними між кінцевими пристроями в межах одного відділення, між кінцевими пристроями, що розташовані в різних відділеннях, та між кінцевими пристроями відділення Інтернет. З'єднання, які забезпечує транспортна інфраструктура, можуть бути віднесені до таких типів:

- з'єднання 2-го рівня моделі OSI (L2) – канального, для передачі даних між кінцевими пристроями, що належать одному сегменту локальної мережі;
- з'єднання 3-го рівня (L3) – мережного, для передачі даних між кінцевими пристроями, що належать різним сегментам локальної мережі одного відділення;
- тунельні L3-з'єднання для передачі даних між кінцевими пристроями з різних відділень;
- L3-з'єднання з використанням NAT для передачі даних між кінцевими пристроями і Інтернет.

Показники ефективності функціонування локальної мережі відділення визначаються саме її транспортною інфраструктурою. Розглянемо можливі підходи до її реалізації.

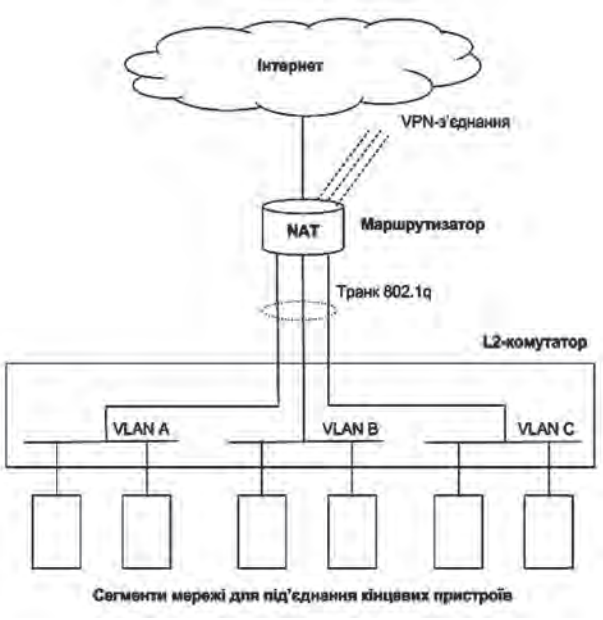

Рис. 3. Транспортна інфраструктура у вигляді одного маршрутизатора та L2-комутаторів

Підхід 1. Транспортна інфраструктура у вигляді одного маршрутизатора та L2-комутаторів

До транспортної інфраструктури надходить маршрутизатор і група L2-комутаторів (рис. 3). Типово маршрутизатор має окремі фізичні інтерфейси для під'єднання Інтернет та локальної мережі. На інтерфейсі з боку локальної мережі використовують транкове (trunk) з'єднання згідно зі стандартом IEEE 802.1q [1], при цьому на маршрутизаторі створюють під-інтерфейси (sub-interfaces) для всіх VLAN. Комутатори забезпечують під'єднання кінцевих пристроїв до різних VLAN.

Через інтерфейс підключення до Інтернет реалізуються VPN-з'єднання з іншими відділеннями. Для кожного VPN-з'єднання на маршрутизаторі створюється окремий під-інтерфейс. На інтерфейсі маршрутизатора в бік Інтернет також здійснюється трансляція мережних адрес (Network Address Translation або NAT).

Маршрутизатор виконує передачу таких типів трафіку:

- між кінцевими пристроями цього відділення та Інтернет;
- між кінцевими пристроями цього відділення та кінцевими пристроями інших відділень (через VPN);
- між кінцевими пристроями цього відділення, що належать різним VLAN;
- між кінцевими пристроями пар інших відділень у разі непрацездатності VPN-каналу безпосереднього зв'язку між ними (див. нижче).

Для передання пакетів між VLAN реалізується топологія «маршрутизатора на паличці» (router-on-a-stick) [4].

Таблиця маршрутизації маршрутизатора містить такі маршрути:

- маршрути до безпосередньо під'єднаних (directly connected) сегментів мережі, що пов'язані з VLAN під-інтерфейсами маршрутизатора;
- статичний маршрут поза вибором (default route) в бік Інтернет;
- маршрути до локальних мереж інших відділень через VPN-канали.

У разі застосування раніше розглянутої схеми розподілу IP-адрес (див. рис. 1) з кожним відділенням асоційовано постійний адресний префікс виду 10.<branch-id>.0.0/16.

Для додання маршрутів у бік інших відділень до таблиці маршрутизації доцільно використовувати протокол динамічної маршрутизації. В цьому разі існує можливість у разі непрацездатності VPN-з'єднання, що безпосередньо сполучає відділення, передавати пакети між ними транзитом через маршрутизатори інших відділень.

Головною проблемою цього підходу є виконання всіх дій з маршрутизації пакетів єдиним маршрутизатором. За умов, коли домінуючим стандартом для створення локальних мереж є Gigabit Ethernet, передача потоків даних між VLAN створює значне навантаження на процесор (CPU) маршрутизатора, що може призвести до погіршення якості зв'язку з Інтернет та іншими відділеннями. Іншим «вузьким місцем» є фізичний інтерфейс маршрутизатора, під'єднаний до комутатора локальної мережі, оскільки його пропускна здатність спільно використовується всіма VLAN.

Підхід 2. Використання L3-комутатора для маршрутизації між сегментами локальної мережі відділення

Зазначених проблем 1-го підходу допоможе позбутися використання L3-комутатора для маршрутизації між VLAN (рис. 4). Маршрутизатор звільняється від функцій передачі трафіку між VLAN відділення, пропускна здатність його інтерфейсу, під'єднаного до локальної мережі, використовується лише для передачі трафіку між кінцевими пристроями відділення і Інтернет та кінцевими пристроями інших відділень.

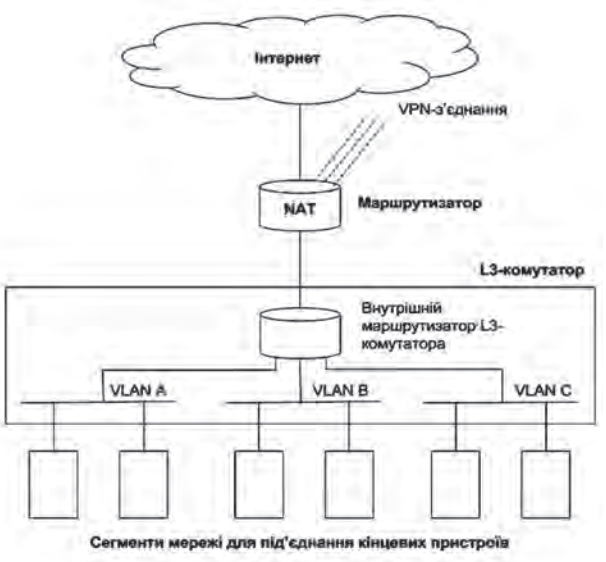

Рис. 4. Транспортна інфраструктура з використанням L3-комутатора

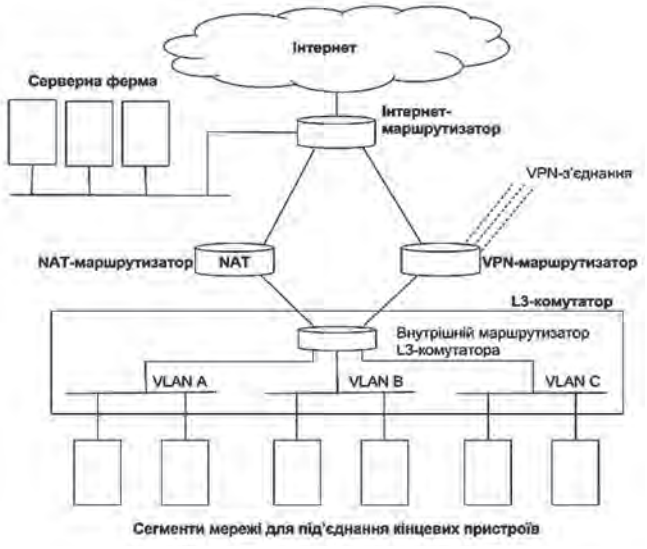

Рис. 5. Транспортна інфраструктура з розділенням функцій з'єднання з Інтернет, NAT та VPN

Порівняно з 1-м підходом у таблиці маршрутизації відбуваються такі зміни: замість маршрутів до безпосередньо під'єднаних VLAN-сегментів додається один маршрут до безпосередньо під'єднаного сегмента в бік L3-комутатора та один статичний маршрут для префіксу 10.<local-branch-id>.0.0/16 в бік L3-комутатора.

Таблиця маршрутизації L3-комутатора містить:

- маршрути до безпосередньо під'єднаних сегментів мережі – VLAN кінцевих пристроїв та до маршрутизатора;
- статичний маршрут поза вибором у бік маршрутизатора.

Цей підхід є оптимальним для випадків використання відділенням єдиної не-приватної IP-адреси, яку надає провайдер Інтернет і яка налаштовується на інтерфейсі маршрутизатора в бік Інтернет. Підключення до Інтернет з використанням єдиної не-приватної IP-адреси є типовим для малих та середніх офісів.

Підхід 3. Розділення функцій з'єднання з Інтернет, NAT та VPN

Для більших відділень, особливо у разі наявності в них інформаційних ресурсів, що використовуються користувачами Інтернет, можливе використання відділенням декількох не-приватних IP-адрес. Такими ресурсами можуть бути окремі сервіси на кшталт веб-сервера або сервера електронної пошти, а також повноцінні дата-центри.

З міркувань структурного відділення внутрішніх потоків трафіку Інтранет та Інтернет-трафіку з метою спрощення конфігурації та подальшого розподілення навантаження між пристроями транспортної інфраструктури функції з'єднання з Інтернет, NAT та VPN можуть бути розділені між різними пристроями (рис. 5):

- маршрутизатор доступу в Інтернет – Інтернет-маршрутизатор;
- NAT-маршрутизатор;
- VPN-маршрутизатор;

Таблиця маршрутизації Інтернет-маршрутизатора містить такі маршрути:

- маршрути до безпосередньо під'єднаних одного чи декількох сегментів локальної мережі, в яких використовуються лише не-приватні IP-адреси, зокрема – серверної ферми;
- маршрути в бік Інтернет – єдиний статичний маршрут поза вибором у разі використання одного провайдера Інтернет, або таблиця маршрутів, отримана за протоколом BGP у разі використання декількох провайдерів.

Таблиця маршрутизації NAT-маршрутизатора містить:

- маршрут до безпосередньо під'єднаного сегмента зв'язку з L3-комутатором;
- маршрут поза вибором у бік Інтернет-маршрутизатора.

Таблиця маршрутизації VPN-маршрутизатора містить:

- маршрут до безпосередньо під'єднаного сегмента зв'язку з L3-комутатором;
- маршрут поза вибором у бік Інтернет-маршрутизатора;
- маршрути до локальних мереж інших відділень через встановлені VPN-з'єднання.

Таблиця маршрутизації L3-комутатора містить:

- маршрути до безпосередньо під'єднаних сегментів мережі – VLAN кінцевих пристроїв та до маршрутизатора;

- статичний маршрут поза вибором у бік маршрутизатора;
- статичний маршрут для загального префіксу інтранет – 10.0.0.0/8, в бік VPN-маршрутизатора.

З погляду розподілу функцій і простоти конфігурації кожного з пристроїв цей підхід видається оптимальним серед розглянутих. Втім, його проблемою є велика кількість використовуваних пристроїв транспортної інфраструктури, яка може стати ще більшою у разі додання компонентів із метою впровадження відмовостійкості та балансування навантаження.

Підхід 4. Транспортна інфраструктура з віртуалізацією мережних функцій

Розглянемо транспортну інфраструктуру, в якій Інтернет-, NAT- та VPN-маршрутизатор реалізовані у вигляді віртуальних компонентів на єдиному сервері-носії (рис. 6). Цей підхід ілюструє концепцію віртуалізації мережних функцій (Network Function Virtualization або NFV) [7]. Для забезпечення відмовостійкості доцільно використовувати два сервери-носії.

Особливості маршрутизації такої транспортної інфраструктури:

- один з Інтернет-маршрутизаторів є основним, другий – резервним;
- на інтерфейсах Інтернет-маршрутизаторів з боку NAT- та VPN-маршрутизаторів, а також серверної ферми налаштовується протокол відмовостійкості віртуального маршрутизатора (Virtual Router Redundancy Protocol або VRRP) [9];

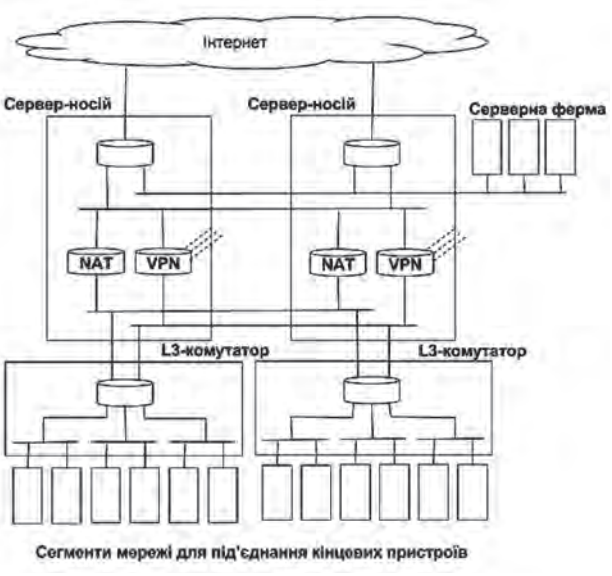

Рис. 6. Транспортна інфраструктура з віртуалізацією мережних функцій

- на інтерфейсах NAT- та VPN-маршрутизаторів з боку L3-комутатора налаштовується протокол VRRP.

Таблиці маршрутизації всіх пристроїв транспортної інфраструктури незмінні порівняно з описаними для 3-го підходу.

NFV-підхід має такі переваги:

- використання серверів загального призначення замість спеціалізованих пристроїв – маршрутизаторів;
- ефективне балансування навантаження між віртуальними компонентами в межах сервера-носія;
- відмовостійкість.

Вочевидь, компоненти серверної ферми також можуть бути реалізовані у вигляді віртуальних машин на серверах-носіях, щоб надалі зменшити кількість пристроїв.

Маршрутизація між відділеннями

Слід зазначити, що в усіх розглянутих підходах немає використання протоколів динамічної маршрутизації в локальній мережі відділення. Це значно спрощує конфігурацію і супровід. Втім, для відмовостійкої передачі трафіку між відділеннями через VPN-з'єднання використання динамічної маршрутизації є необхідним.

Особливості динамічної маршрутизації між відділеннями:

- у процесі динамічної маршрутизації беруть участь лише VPN-маршрутизатори;
- інформація про маршрути, якою обмінюються VPN-маршрутизатори відділень, містить лише загальні префікси відділень виду 10.<local-branch-id>.0.0/16;
- на процес маршрутизації між відділеннями впливає лише стан VPN-з'єднань між ними, натомість зміни топології, які відбуваються в локальних мережах відділень, не впливають взагалі;
- обмін маршрутною інформацією здійснюється VPN-маршрутизаторами за принципом «партнер-партнер» (peer-to-peer).

З огляду на зазначені особливості оптимальним для реалізації динамічної маршрутизації між відділеннями є протокол eBGP [2]. Кожному з відділень призначається номер автономної системи (Autonomous System або AS) з діапазону приватних номерів AS – 64512-65534 [10]. Для зручності доцільно обирати номер AS відділення як суму: 65000+<local-branch-id>.

Для передачі трафіку між кожною парою відділень автоматично обиратиметься VPN-з'єднання безпосередньо між ними, оскільки відповідні маршрути матимуть найменшу довжину шляху, вимірювану в AS (AS-path). У разі втрати працездатності цього каналу трафік може передаватися транзитом через інші відділення. Для ефективного впровадження політик маршрутизації між відділеннями використовують стандартний набір атрибутів протоколу BGP.

Маршрутизація в локальних мережах відділень

Згідно з розглянутими підходами у локальних мережах відділень може бути використана або лише статична маршрутизація, або динамічна маршрутизація з простою конфігурацією типу OSPF з єдиною областю (single-area) [12]. У здійсненні обміну маршрутами (redistribution) процесів маршрутизації між відділеннями та в локальних мережах відділень потреби немає.

Список літератури

1. 802.1Q-Virtual LANs [Electronic resource]. – Mode of access: http://www.ieee802.org/1/pages/802.1Q.html. – Title from the screen.
2. BGP Case Studies [Electronic resource]. – Mode of access: http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html. – Title from the screen.
3. Dynamic Multipoint VPN (DMVPN) [Electronic resource]. – Mode of access: http://www.cisco.com/c/en/us/products/security/dynamic-multipoint-vpn-dmvpn/index.html. – Title from the screen.
4. Fundamentals of VLAN's – Router on a stick [Electronic resource]. – Mode of access: https://learningnetwork.cisco.com/docs/DOC-23481. – Title from the screen.
5. John Tiso. Designing Cisco Network Service Architectures (ARCH). Foundation Learning Guide. Third Edition. Cisco Press, 800 East 96th Street, Indianapolis, IN 46240 USA.
6. Mesh Versus Hierarchical Mesh Topologies [Electronic resource]. – Mode of access: http://www.ccexpert.us/network-design-2/mesh-versus-hierarchicalmesh-topologies.html. – Title from the screen.
7. Network function virtualization [Electronic resource]. – Mode of access: https://en.wikipedia.org/wiki/Network_function_virtualization. – Title from the screen.
8. Request for Comments: 1918. Address Allocation for Private Internets [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc1918. – Title from the screen.
9. Request for Comments: 3768. Virtual Router Redundancy Protocol (VRRP) [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc3768. – Title from the screen.
10. Request for Comments: 6996. Autonomous System (AS) Reservation for Private Use [Electronic resource]. – Mode of access: https://tools.ietf.org/html/rfc6996. – Title from the screen.
11. Sean Wilkins. Designing for Cisco Internetwork Solutions (DESGN). Foundation Learning Guide. Third Edition. Cisco Press, 800 East 96th Street, Indianapolis, IN 46240 USA.
12. Stelios Antoniou. Cisco Routing Study Guide: Configuring OSPF in a Single Area [Electronic resource]. – Mode of access: https://www.pluralsight.com/blog/it-ops/cisco-ccnp-ospf. – Title from the screen.

D. Cherkasov

IP ROUTING IN THE NETWORK OF MODERN ENTERPRISE

The paper overviews optimal approaches for IP routing in an enterprise network that includes multiple remote branches, each having the Internet connection. The article briefly discusses the topology of VPN interconnection between branches. For the number of branches more than 4-5, it is recommended to choose several branches as an intranet backbone with full-mesh of interconnection channels. Other branches connect to any 2 of backbone ones for redundancy.

The discussion focuses on a typical modern branch network structure. Due to the usage of high performance routers and switches, the branch network structure is growing simpler. A model of branch network is suggested as a set of components, one of which – transport infrastructure – is the most significant for optimal IP-routing. Several approaches for transport implementation are discussed, proceeding from the simplest ones based on a single multi-functional router to using L3-switches and specialized Internet, NAT and VPN routers. The approach based on the network function virtualization (NFV) is suggested as the most flexible and promising, which also enables implementation of high-availability.

Special attention is brought to dynamic routing in the enterprise network. It is based on IP-address distribution. A simple IP-addressing scheme is shown as an example that ensures IP-address aggregation using a single prefix per branch. It is shown that eBGP is the most appropriate protocol for IP-routing implementation between branches. At the same time, static routing may be quite sufficient inside of branch network.

Keywords: telecommunications, enterprise routing, VPN, Virtualization, NFV.

Матеріал надійшов 30.09.2016