УДК 004.9

Ірина Овчарук, к.т.н., доцент

(доцент кафедри інформаційних технологій, ДУІТ)

Костянтин Афанасьєв

(магістрант кафедри інформаційних технологій, ДУІТ)

ДОСЛІДЖЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ОРГАНІЗАЦІЇ ТА НАЛАГОДЖЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ НА ТРАНСПОРТІ

Актуальною задачею в наш час є забезпечення безперебійної роботи мережевого обладнання в транспортній галузі. В даній статті розглядаються технології, що застосовуються для налагодження стабільного та якісного інтернет-підключення та забезпечення необхідними ресурсами фізичного рівня мережі, розглянуто вимоги до обладнання, через яке підключається користувач, а саме конфігурацію портів, що використовуються для підключення комутаторів. Приділяється увага способам захисту ліній зв'язку. В роботі наведено приклад налаштування комп'ютерної мережі.

Ключові слова: технологія VLAN, NAT, STP, мережа, модель OSI, топологія, інтернет-ресурси, хости.

Вступ. Безперебійна робота мережевого обладнання є актуальною задачею особливо в транспортній галузі. Передача великих обсягів інформації, вчасне оновлення інформації, швидкий доступ до неї користувача в наш час неможливий без стабільної і якісної роботи комп'ютерних мереж в транспортних установах та підприємствах транспорту. Доволі часто виникає така ситуація, в якій у будь-якого користувача починає накопичуватися інформація, яку він бажає зберегти від випадкового видалення чи її втрати у будь-який спосіб. В наш час у користувачів виникає потреба зберігати інформацію у великих об'ємах, які не завжди можуть бути збережені на одному носії інформації, тому в нинішню епоху розвиток технологій все більш поглиблюється у інтернет-індустрію, внаслідок чого велику увагу слід приділяти налаштуванню комп'ютерних мереж.

Аналіз останніх досліджень і постановка проблеми. Питаннями організації комп'ютерних мереж займалися: Таненбаум Э., Узєролл Д., Оліфер В., Оліфер Н., Д. Куроуз, К. Росс, Сергєєв А. Н., Робачевський А. В їх роботах описано методи та принципи організації комп'ютерних мереж та застосування мережевих технологій [1-3,9-14]. Питання захисту фізичної складової мережі, організації підключення та створення логічної інфраструктури мережі висвітлені у роботах: Самойленко Н., Чубіна І., Таненбаума Э., Узєролла Д., Оліфера В., Оліфера Н., Куроуза Д.

Росса, де особливу увагу приділено технологіям VLAN, NAT, STP та фізичній організації мережі в межах корпорацій/локальних мереж [4, 9-11, 15].

DOI: 10.32703/2617-9040-2019-33-2-6

За результатами узагальнених досліджень, можна установити, що адекватного налаштування мережі для взаємодії хостів між собою недостатньо. Необхідно також передбачити захист підключення, його стабільність та правильну маршрутизацію. Об'єднання декількох комп'ютерів у загальну систему з вибіркоким наданням доступу до даних є більш зручною альтернативою постійному транспортуванню інформації за допомогою USB-носіїв та інших видів передачі даних.

Мета і завдання дослідження. В роботі досліджуються параметри підключення до мережі в транспортних установах, враховуючи топологію самої мережі. В першу чергу має бути визначеним тип підключення. У цьому випадку мова йде про метод, за яким будуть надаватися налаштування.

Матеріали та методи дослідження. Все, що раніше потрібно було зберігати на локальних носіях даних, у реаліях нинішнього часу вже можна зберігати у так званих «Хмарах». Хмарні сервіси дозволяють зберігати інформацію віддалено від техніки та засобів користувача і отримувати до них доступ з будь-якого пристрою, на якому користувач зможе себе ідентифікувати та пройти авторизацію. Щоб отримати доступ до «Хмар» або до будь-якого іншого інтернет-ресурсу, на якому можна знайти потрібну інформацію, необхідно організувати принаймні справне інтернет-підключення.

Для організації зазначеного інтернет-підключення є перелік вимог, що мають бути обов'язково виконанні і без яких доступ до всесвітньої мережі не буде можливим. В першу чергу має бути визначеним тип та методи підключення. На сьогоднішній день найвідомішими й найпоширенішими є такі типи підключення як Dynamic (DHCP) або Static: Dynamic (DHCP) – тип підключення, при якому прописувати налаштування на обладнанні користувача немає потреби; Static – тип підключення, при якому всі налаштування прописуються вручну [7].

Головною вимогою до типу підключення є відповідність його як на обладнанні користувача, так і на обладнанні, до якого користувач підключений. У випадку, коли тип підключення у користувача виставлено не той, що встановлено на обладнанні, наприклад, провайдера, то доступу до мережі не буде взагалі. Також, якщо тип підключення є статичним, то необхідна відповідність налаштуванням, за якими обладнання користувача ідентифікується в мережі. Ідентифікація користувача у мережі провайдера, та знаходження, необхідних йому налаштувань у таблиці відповідності, знаходиться по відповідності зазначеної *IP-адреси* та відповідної *MAC-адреси*.

MAC-адреса – унікальний ідентифікатор обладнання, що бажає підключитися до мережі [2].

IP-адреса – адреса, за якою обладнання ідентифікується в мережі [5].

Це єдина вимога, що безпосередньо стосується користувача. Але ще необхідно зазначити, що бажано обирати захищені лінії зв'язку, або застосовувати додаткові механізми захисту у вигляді проміжного обладнання (мережеві екрани, проксі-підключення, технології захисту підключення, наприклад, IPSec та захищені протоколи, наприклад, HTTPS, IMAPS, POP3S. Додатковий захист дозволяє не переживати за достовірність та цілісність відправлених даних, що є важливо для транспортної галузі. Все це реалізується за допомогою додаткового шифрування, інколи неодноразового, і для отримання та зчитування даних необхідно володіти ключем для розшифрування інформації.

Всі наступні вимоги можуть змінюватися, залежно від того, яке обладнання виступає провідником у наданні доступу, яким методом виконується підключення: по витій парі, оптоволоконним кабелем, бездротово, чи коаксіальним кабелем. Від цього критерія може залежати стабільність підключення та якість вхідного/вихідного сигналу.

Також необхідно зазначити перелік вимог, що стосуються безпосередньо обладнання, через яке підключається користувач, у цьому випадку – комутатори. Для здійснення стабільного якісного підключення, мають бути зконфігуровані порти належним чином, як на фізичному рівні, так і на логічному. Не зайвим буде трохи більше уваги приділити логічному рівню. Для забезпечення роботоспроможності підключення, порт має бути зконфігурований, як порт типу *access*, що відповідає конфігурації порту в режимі роботи з кінцевим обладнанням. Існує також конфігурація в режимі *trunk*, що використовується зазвичай для підключення комутаторів між собою. Оскільки у комутаторів також є свій максимально допустимий поріг роботи, бажано також створити та зконфігурувати *vlan*-и [8] для роботи з кінцевими користувачами та що будуть застосовуватися для роботи обслуговуючого персоналу. Для простоти їх можна назвати абонентським *vlan*-ом та *vlan* менеджменту.

Перший відповідає за роботу з кінцевими користувачами, їх можна створити декілька, наприклад, для розмежування всіх користувачів на окремі групи, в яких вони не «бачать» один одного.

Другий відповідає за наявність доступу до налаштувань комутатора без застосування абонентських *vlan*-ів, створюється для зручності використання та підвищення рівню захищеності.[14]

Для використання *vlan*-ів було створено межу, тому допустимий діапазон для творення «вланів» відповідає від 1-го до 4096-го. Частина з них може бути зарезервована виробником, ще на стадії програмування, зазвичай перший встановлюється як стандартний *vlan* повсюди. Тому коли обладнання починають конфігурувати вже на місці використання, то з більшості портів за необхідністю його видаляють [13]. Також можна зазначити, що вирішальну роль може мати навіть топологія мережі, що організовується на місці використання. У більшості випадків в наш час застосовується змішана топологія, на основі топологій кільце, зірка та шина. Кільцем підключаються комутатори, до яких підключають кінцеве обладнання, а зіркою – обладнання сполучення (рис.1).

Рис. 1. Приклад змішаної топології на основі топологій: зірка, кільце та шина

Зазвичай, для організації доступу до свого власного сховища, користувач організовує тунельне з'єднання між вузлом(комп'ютером) що використовує користувач в даний момент часу та комп'ютером, що виступає сховищем даних, створюючи таким чином однорангову мережу, за допомогою технології VPN, що реалізується за посередництвом протоколу PPP та його різновидів, типу PPPoE [15].

VPN (virtual private network) – віртуальна приватна мережа, що надбудовується над основною мережею. Така мережа має більший рівень довіри, аніж основна. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією [6].

PPP (Point-to-Point Protocol) – Протокол канального рівня мережевої моделі OSI. Це механізм для створення й запуску IP (Internet Protocol) й інших мережевих протоколів на послідовних лініях зв'язку – прямий послідовний зв'язок (по нуль-модемному кабелю), зв'язок поверх Ethernet або модемний зв'язок по телефонних лініях [7].

Протокол PPP є основою для всіх протоколів другого рівня. Зв'язок по протоколу PPP складається із чотирьох стадій: встановлення зв'язку (здійснюється вибір протоколів аутентифікації, шифрування, стиснення і встановлюються параметри з'єднання), визначення аутентичності користувача (реалізуються алгоритми аутентифікації, на основі протоколів PAP, CHAP або MS-CHAP), контроль повторного виклику PPP (необов'язкова стадія, у якій підтверджується справжність віддаленого клієнта), виклик протоколу мережевого рівня (реалізація протоколів установлених на першій стадії). Протокол PPP включає IP, IPX й NetBEUI пакети всередині PPP кадрів [4].

Зазвичай, використовується для встановлення прямих з'єднань між двома вузлами. Широко застосовується для з'єднання комп'ютерів за допомогою телефонної лінії. Також використовується поверх широкосмугових з'єднань. Багато хто з провайдерів використовують PPP для надання комутованого доступу в Інтернет.

Link Control Protocol (LCP) забезпечує автоматичне налаштування інтерфейсів на кожному кінці (наприклад, установка розміру пакетів) і опціонально проводить аутентифікацію. Протокол LCP працює поверх PPP, тобто до роботи LCP повинен бути PPP зв'язок.[15]

RFC 1994 описує Challenge-handshake authentication protocol (CHAP), який є найкращим для з'єднань з провайдерами. Вже застарілий Password authentication protocol (PAP) все ще іноді використовується.[7]

Іншим варіантом аутентифікації через PPP є розширений протокол аутентифікації (EAP - Extensible Authentication Protocol).

Після того, як з'єднання було встановлено, поверх нього може бути налаштована додаткова мережа.

За результатами викладеного матеріалу реалізована робочої мережа, макет якої наведено на рис.2 і рис.3. На рис.2 і рис.3 зображено проміжне мережеве обладнання (маршрутизатори та комутатори), за допомогою якого забезпечується комутація пакетів даних між кінцевими хостами. Підписи під обладнанням несуть описовий характер і допомагають людині, що зайнята налаштуванням мережі швидше зрозуміти, до якого сегменту мережі відноситься обладнання та куди будуть спрямовані наступні підключення.

Рис. 2. Макет робочої мережі

Рис. 3. Макет робочої мережі (доповнення до рис.2)

Підключення було виконано згідно правил по правильному підключенню, а саме, однаковий тип обладнання підключається крос-кабелем (перехресним кабелем), різні типи обладнання підключаються прямим кабелем. Тепер необхідно додати кінцеві хости: користувачів і персонал, що буде обслуговувати мережу. На рис.4 – рис.7 зображена вся мережа, сегменти мережі з кінцевими хостами відповідно виділені прямокутниками: Київ район Позняків (kyiv-roznuaki), Дарниця (kyiv-darnytsya), Оболонь (вулиці Герої Дніпра (obl-dnh) та Героїв Сталінграду (obl-stlh)) та відділи (фінансово-економічний (FEO), бухгалтерія (Accounting), технічний відділ(PTO PC1-5) та підтримка(PTO PC6-12)).

Рис. 4. Результат додавання кінцевих хостів

Рис. 5. Результат додавання кінцевих хостів

Рис. 6. Результат додавання кінцевих хостів

Рис. 7. Результат додавання кінцевих хостів

Для забезпечення відмовостійкості серверів, було створено додаткове з'єднання між комутаторами Kyiv-roznyaki-dsw1, Kyiv-roznyaki-asw1 та kyiv-roznyaki-asw2. За допомогою протоколу STP у місці підключення серверів було забезпечено безперебійне з'єднання і, навіть, якщо одно зі з'єднань буде втрачено, то зв'язок буде встановлено по іншому шляху за декілька секунд.

В даній мережі було реалізовано декілька методів підключення кінцевих хостів і застосовано декілька методів маршрутизації. Наприклад, частина мережі підключена через L3-комутатор, який за замовчанням працює як маршрутизатор, але його можна перелаштувати у режим L2-комутатора і підключати пристрої як зазвичай. Завдяки тому, що порти працюють, як на маршрутизаторі, через нього можливо підключити користувачів і організувати підключення мережевого обладнання. Це дозволяє значно зберегти кошти, що могли бути витрачені на закупівлю більшої кількості обладнання(окремо маршрутизатора, окремо комутаторів).

Висновки. В результаті проведених досліджень було встановлено, що існують різні варіанти реалізації підключення між комп'ютерами, але в основному використовується найпростіша і найбільш захищена реалізація варіанту організації підключення. Даний тип налаштування підключення дозволяє створювати безліч підключень типу вузол – вузол (Point-to-Point), чого цілком достатньо для реалізації всіх необхідних функцій, що застосовує користувач. Але для належного функціонування даного типу підключення на великих відстанях чи, коли користувач не знаходиться в локальній мережі серверу-сховища інформації, то для отримання доступу до нього може знадобитися додаткове налаштування, що, на жаль, реалізувати віддалено без вже отриманого доступу є майже неможливою справою. А для отримання належного доступу є необхідним попереднє налаштування з'єднання зі сторони комп'ютера-сервера та надання дозволу на отримання запитів зі сторони комп'ютера-клієнта, що не знаходиться в локальній мережі.

Додатково було встановлено, що існують не тільки відомі проблеми з організацією комп'ютерних мереж, та доступу до мережі інтернет, а і деякі з невиявлених чи неоголошених особливостей обладнання, з яким працюють користувачі, також велику значимість має однорідність обладнання, оскільки при послідовному підключенні на одному й тому ж самому рівні обладнання, що

розроблюється різними компаніями може призвести до непередбачуваних наслідків: від простої неспроможності надати стабільний доступ до мережі інтернет, чи обмін даними між двома чи більше кінцевими пристроями до абсолютної втрати роботоспроможності обладнанням без можливості подальшого відновлення.

Описані у даній статті технології та методи мають на сьогоднішній день практичну значимість і можуть застосовуватися у транспортних установах та підприємствах транспорту, а також, як у локальних рішеннях для компаній різного масштабу, так і для глобальних рішень у підключенні як у межах однієї країни, так і на більш далекі відстані: від підключень між країнами, до підключення між континентами. Наочно було продемонстровано роботу мережі в межах одного міста, але розповсюджену по всій його площі, з декількома точками підключень кінцевих хостів, але з однією точкою виходу у світ.

ЛІТЕРАТУРА

1. *Топологія комп'ютерних мереж*. Режим доступу: http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6
2. *Serial Programming Guide for POSIX Operating Systems*. Режим доступу: http://cisco.opennet.ru/docs/RUS/serial_guide/index.html#2_3_2
3. *Dynamic Host Configuration Protocol*. Режим доступу: <https://tools.ietf.org/html/rfc2131>
4. *ANA Guidelines for IPv4 Multicast Address Assignments*. Режим доступу: <https://www.rfc-editor.org/rfc/rfc3171.txt>
5. *Internet Official Protocol Standards*. Режим доступу: <http://www.rfc-editor.org/rfc/rfc3330.txt>
6. *IEEE 802.3ad Link Bundling*. Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sbcelacp.html
7. *802.1Q*. Режим доступу <https://ieeexplore.ieee.org/document/8403927>
8. *VLAN Aggregation for Efficient IP Address Allocation*. Режим доступу: <https://www.rfc-editor.org/rfc/rfc3069.txt>
9. *Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд./ В.Олифер, Н.Олифер. – СПб.: Питер, 2016. – 992 с.*
10. *Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с. (2016)*
11. *Куроуз Д., Росс К. Компьютерные сети: Нисходящий подход(6-е издание). Москва: Издательство «Э», 2016. 912 с.*
12. *Сергеев А. Н. Основы локальных компьютерных сетей: Учебное пособие. СПб.: Издательство «Лань», 2016. 184 с.*
13. *Робачевский А. Интернет изнутри. Экосистема глобальной Сети. 2-е изд., перераб. и доп. М.: Альпина Паблишер, 2017. 271 с.*
14. *Benchmarking Methodology for Network Interconnect Devices*. Режим доступу : <https://tools.ietf.org/html/rfc2544>
15. *Internet Official Protocol Standards*. Режим доступу : <https://tools.ietf.org/html/rfc3000#appendix-B>

REFERENCES

1. *Topologiya komp'uternykh merezh* [Computer network topology]. Retrieved from http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 [in Russian].
2. *Serial Programming Guide for POSIX Operating Systems*. Retrieved from http://cisco.opennet.ru/docs/RUS/serial_guide/index.html#2_3_2.
3. *Dynamic Host Configuration Protocol*. Retrieved from <https://tools.ietf.org/html/rfc2131>.
4. *ANA Guidelines for IPv4 Multicast Address Assignments*. Retrieved from <https://www.rfc-editor.org/rfc/rfc3171.txt>.
5. *Special-Use IPv4 Addresses*. Retrieved from <http://www.rfc-editor.org/rfc/rfc3330.txt>.
6. *IEEE 802.3ad Link Bundling*. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sbcelacp.html.
7. *802.1Q*. Retrieved from <https://ieeexplore.ieee.org/document/8403927>.

8. VLAN Aggregation for Efficient IP Address Allocation. Retrieved from <https://www.rfc-editor.org/rfc/rfc3069.txt>
9. Olifer V., Olifer N. (2016). *Komp'yuternye seti. Principi, tehnologii, protokoly: Uchebnik dlya vyzov. 5-e izd.* [Computer networks. Technologies, principles and protocols. University textbook. 5-th edition]. Sankt-Peterburg, Piter Publ. [in Russian].
10. Tanenbaum A., Watherall D. (2012). *Komp'yuternye seti, 5-ye izdanye* [Computer networks. 5-th edition]. Sankt-Peterburg, Piter Publ. [in Russian].
11. D. Kurouz, K. Ross (2016). *Komp'yuternye seti: Niskhodyashchiy podkhod* (6-ye izdaniye) [Computer Networks: A Downward Approach (6th Edition)]. Moscow, «E» Publ. [in Russian].
12. Sergeev A. N. (2016) *Osnovy lokalnykh komp'yuternykh setey: uchebnoe posobie*. [Computer networks basics: study guide]. Sankt-Peterburg, «Lan'» Publ. [in Russian].
13. Robachevsky A. (2017). *Internet iznytri. Ekosistema globalnoi seti - 2-ye izdanye*. [Internet from inside. Global net ecosystem - 2-nd edition]. Moscow, Alpine Publ. [in Russian].
14. *Benchmarking Methodology for Network Interconnect Devices*. Retrieved from <https://tools.ietf.org/html/rfc2544>
15. *Internet Official Protocol Standards*. Retrieved from <https://tools.ietf.org/html/rfc3000.txt>

Ирина Овчарук, к.т.н., доцент

(доцент кафедры информационных технологий, ГУИТ)

Константин Афанасьев

(магистрант кафедры информационных технологий, ГУИТ)

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ОРГАНИЗАЦИИ И НАСТРОЙКИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ТРАНСПОРТЕ

Актуальной задачей в наше время является обеспечение бесперебойной работы сетевого оборудования в транспортной отрасли. В данной статье рассматриваются технологии, применяемые для налаживания стабильного и качественного интернет-подключения и обеспечения необходимыми ресурсами физического уровня сети, рассмотрены требования к оборудованию, через которое подключается пользователь, а именно конфигурацию портов, используемых для подключения коммутаторов. Уделяется внимание способам защиты линий связи. В работе приведен пример настройки компьютерной сети.

Ключевые слова: технология VLAN, NAT, STP, сеть, модель OSI, топология, интернет-ресурсы, хосты.

Iryna Ovcharuk, PhD

(Associate Professor of the Department of Information Technologies, SUIT)

Kostiantyn Afanasyev

(Master's degree student of the Department of Information Technologies, SUIT)

RESEARCH OF MODERN TECHNOLOGIES IN NETWORK CONFIGURATION ON TRANSPORT

Nowadays, the current topic is to ensure the smooth operation of network equipment in the transport industry. In this article reviews the technologies that are used to ensure stability and quality of Internet connection and prove resources needed to physical level of the network, described requirements to net equipment through which users are connected, especially ports configuration, which are used to establish connection via switches. Attention is paid to defence methods of communication lines.

For accomplishing the task set for the network it is required to configure a big list of technologies and methods. That list includes such technologies as VLAN, NAT and STP. Firstly, attention is paid to create an adequate network plan. For example, internet-provider has to know the amount of inputs, amount of subnets used, their numeration, count of possible connections. The next step should be in choosing network equipment and topology of connection, location and cable routing, cable type. Topology and structure of the net has to be chosen responsibly, because stability and durability depends on them. The paper gives an example of configuring computer network.

Keywords: *technology VLAN, NAT, STP, network, OSI model, topology, Internet-resources, host.*