УДК 621.391

О.Л. Недашківський

ПРИНЦИПИ ПОБУДОВИ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ ДЛЯ НАДАННЯ VPN І ІНТЕРНЕТ ПОСЛУГ

В статті описані принципи побудови мереж передачі даних для надання VPN і Інтернет послуг на базі концепції Metro Ethernet. Запропоновано підходи до знаходження рішення, сформульовано ідеологію такої мережі та наведено архітектуру, параметри і властивості таких мереж. Синтезовано структуру мережі та ієрархію вузлів і обладнання. Докладно описана схема організації послуги доступу до мережі Інтернет в умовах автоматичного конфігурування та ідентифікації абонентського обладнання. Запропоновані способи обмеження швидкості доступу до різних сегментів мережі Інтернет, тобто управління профілями користувачів у відповідності до політики та вимог тарифних планів.

Ключові слова: Metro Ethernet мережі, послуга High-speed Internet access, послуга Virtual Private Networks.

Вступ і постановка проблеми

Останнім часом ринок телекомунікаційних послуг розширюється і вдосконалюється, запити в цій сфері неухильно зростають, як за якістю надаваних сервісів, так і по їх функціональній різноманітності. Ці обставини роблять необхідним пошук рішень по забезпеченню потреб користувачів послуг.

В даній статті описується принципове рішення для надання послуг приватних віртуальних мереж (VPN – virtual private networks) і Інтернет-послуг в рамках розгортання типових мультисервісних мереж для надання Triple-Play послуг в повному обсязі.

Серед послуг, які повинні бути доступні користувачам даної мережі, можна виділити основні:

- послуга високошвидкісного доступу в мережу Інтернет (HSI - High-speed Internet access);
- послуги по створенню віртуальних приватних мереж (VPN) другого рівня (LAYER2 моделі OSI);
- послуги електронної пошти.

Мета статті

Описати принципи побудови мереж передачі даних для надання VPN і Інтернет послуг. Запропонувати рішення, розробити ідеологія такої мережі; визначити архітектуру, параметри і властивості мережі. Синтезувати структуру мережі та ієрархію вузлів і обладнання. Визначити основні принципи надання послуг в таких мережах.

Ідеологія та структура мережі

В основу ідеології побудови мережі покладено дворівневий принцип – опорні вузли та мережа доступу (рис. 1).

В даному рішенні пропонується ієрархічна структура мережі, що складається з двох рівнів:

Вузли агрегації (опорні вузли для даної мережі) транспортної Metro Ethernet [1] мережі, яка працює на основі технологій 1G-Etherneti та 10G-Ethernet [2], об'єднані волоконно оптичними лініями зв’язку (ВОЛЗ), повинні забезпечувати:

- надійне надання сервісів з гарантіями якості;
- збіжність сегментів мережі на основі сімейства протоколів зв’язую чого дерева (STP).

Вузли доступу повинні забезпечувати:

- фізичне підключення абонентів, як мінімум через інтерфейс 100BASE-T [2];
- передачу інформації про точку підключення абонентів для подальшої аутентифікації абонентів за допомогою механізмів динамічного конфігурування обладнання з підтримкою опції 82, яка дозволяє ідентифікувати абонентське обладнання по MAC-адресі та ідентифікатору фізичного порта пристрою вузла доступу (DHCP OPTION 82) [3, 4];

- базовий рівень безпеки для запобігання нелегального (IP SOURCE GUARD) або небажаного (PORT ISOLATION) користування мережею;
- поділ сервісів для забезпечення безпеки і надійності роботи кожного з них, а саме виділення окремої віртуальної локальної мережі (VLAN) для кожного сервісу (послуги);
- підключення до опорних вузлів за допомогою ВОЛЗ на швидкості не менше1Гбіт/с.

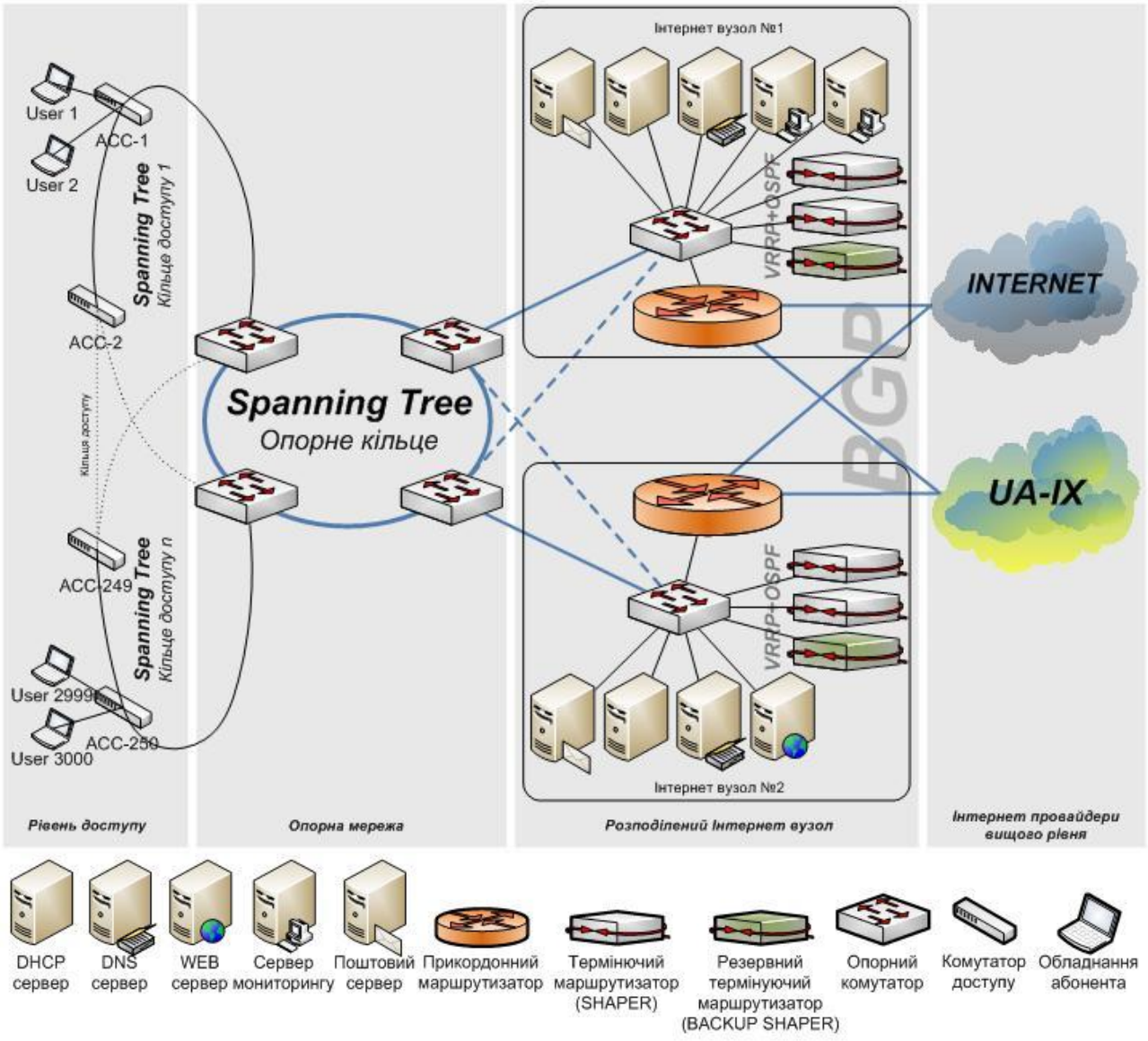

Рис.1. Ідеологія мережі

Ієрархія вузлів і обладнання

Мережа складається з опорних вузлів і вузлів доступу.

Опорні вузли розташовуються в центрах сегментів місцевих (районних) мереж доступу, кожен з яких повинен укомплектовуватись Ethernet комутатором (наприклад 3com 5500G-EI). З'єднання між опорними вузлами, в своїй більшості, можуть здійснюються на швидкості 1 Гбіт/с, але рекомендується кілька, наприклад три, вузлів (для надійності та концентрації навантаження) з'єднувати на швидкості 10 Гбіт/с. В загальному випадку, кількість вузлів та швидкості міжвузлових зав'язків повинні визначатися в кожному конкретному випадку окремо.

Вузлу доступу будуються на основі Ethernet комутаторів другого рівня (LAYER2) і включаються в опорні вузли за допомогою ВОЛЗ. Можливі будь-які топології підключення як кільцеві, так і деревоподібні. При цьому, рекомендується обирати кільцеві топології з

«об'ємними», чи як мінімум «пласкими» кільцями, які дозволяють підвищити надійність і зв'язність мережі доступу. Для забезпечення ще більшої надійності вузлів доступу, їх слід замикати на два різних опорних вузла безпосередньо.Збіжність кільцевих, а в загальному випадку нелінійних, топологій в сегментах мереж доступу забезпечується сімейством протоколів зв'язуючого дерева (STP) [5], що гарантують відновлення мережі, в разі аварії, за час до 1 хв (в найгіршому випадку) та до 50 мс. в найкращому, що відповідає швидкості перемикання за зворотній захисний напрямок в кільцевих мережах синхронної цифрової ієрархії (SDH)).

Принципи надання послуг

Для реалізації пропонується концепція «загальний для всіх абонентів VLAN для кожного сервісу» (VLAN-PER-SERVICE). Різні абоненти, підписані на загальну послугу, підключаються в один VLAN, в рамках якого виконується її надання. Слід зауважити, що для послуги HSI віртуальна мережа (VLAN)може бути одна на сегмент (будинок, мікрорайон, район, але не більше географічного кластера) і залежить від схеми видачі IP-адрес.

Поділ сервісів в різні VLANи дає ряд переваг, що дозволяють побудувати мережу максимально ефективно. У представленому рішенні, функціонування кожного з сервісів не буде залежати від логічного стану інших сервісів (як, наприклад, послуги VPN в межах мережі не залежать від працездатності вузла Інтернет доступу), а тільки від фізичного стану мережі. Крім того, використання розділених віртуальних мереж дозволяє помітно спростити і зробити більш надійною класифікацію сервісів для забезпечення параметрів якості обслуговування (QoS):

- трафік від абонентів маркується відповідним ідентифікатором QoS на основі ідентифікатора VLAN, який однозначно визначає тип послуги. Маркер може бути встановлений на абонентському порту вузла доступу;
- трафік до абонентів послуг HSI маркується відповідним ідентифікатором QoS на вході першого ж комутатора сервісного вузла. Під сервісним вузлом розуміється вузол, на якому встановлено обладнання, яке формує трафік послуги у відповідності до тарифних планів;
- трафік до абонентів, при виході з обладнання вузла доступу позначається пріоритетами та обслуговується на підставі призначеного ідентифікатора QoS.

Транспортна мережа від комутаторів доступу і до стику з вузлом Інтернету працює на другому рівні (LAYER2), тобто на рівні Ethernet. Перехід на третій рівень (LAYER3), тобто на рівень IP, здійснюється вже на Інтернет вузлі.

Сервісний вузол Internet

Рекомендується для надійності та можливості балансування навантаження функції сервісного вузла Інтернет розподіляти між двома фізичними, географічно рознесеними, площадками. Логічна схема сервісного Інтернет вузла для забезпечення послуги HSI наведена на рис. 2. При цьому обидва вузли підключаються до мережі Інтернет. Типовий склад кожного з Інтернет вузлів такий:

- прикордонний маршрутизатор (апаратний або програмний), здатний (за допомогою спеціального програмного забезпечення) ефективно обробляти неповну таблицю маршрутизації BGP. Цього достатньо, щоб отримати список мереж, що входять в в український сегмент мережі Інтернет (UA-IX) [6], а також маршрут «за замовчуванням»;
- два основних клієнтських маршрутизатори - точки термі нації IP трафіку, необхідні для перенесення абонентського трафіку з LAYER2 на LAYER3, а також застосування до нього політик обмеження швидкості доступу до міжнародного сегменту Інтернет;
- один резервний клієнтський маршрутизатор, для перехоплення функцій основних, в разі збою в їх роботі;
- один сервер доменних імен (DNS сервер);

- один сервер конфігурування мережевих параметрів (DHCP сервер), необхідний для розподілу простору IP-адрес між абонентами. Відзначимо, що використання технології DHCP серйозно спрощує процес подальшого переходу до повноцінних мультисервісних мереж, в зв'язку з тим, що додаткова робота по налаштуванню телевізійних приставок (STB – Set Top Box) IP телебачення небудепроводитись. Додатково, використання DHCP дозволяє різко скоротити можливості нелегального доступу до ресурсів мережі.

На одному з Інтернет вузлів необхідне встановлення додаткового сервера для забезпечення WEB-ресурсів таких систем, як система обробки скарг (Trouble-ticketing система [7]), а система інвентаризації ресурсів мережі і послуг, що надаються (Inventory система).

Крім усього іншого, потрібна установка, як мінімум двох (для дублювання) серверів, для організації на них функцій мережевого моніторингу. Вони необхідні для стеження за навантаженням на мережу, а також за працездатністю її окремих елементів.

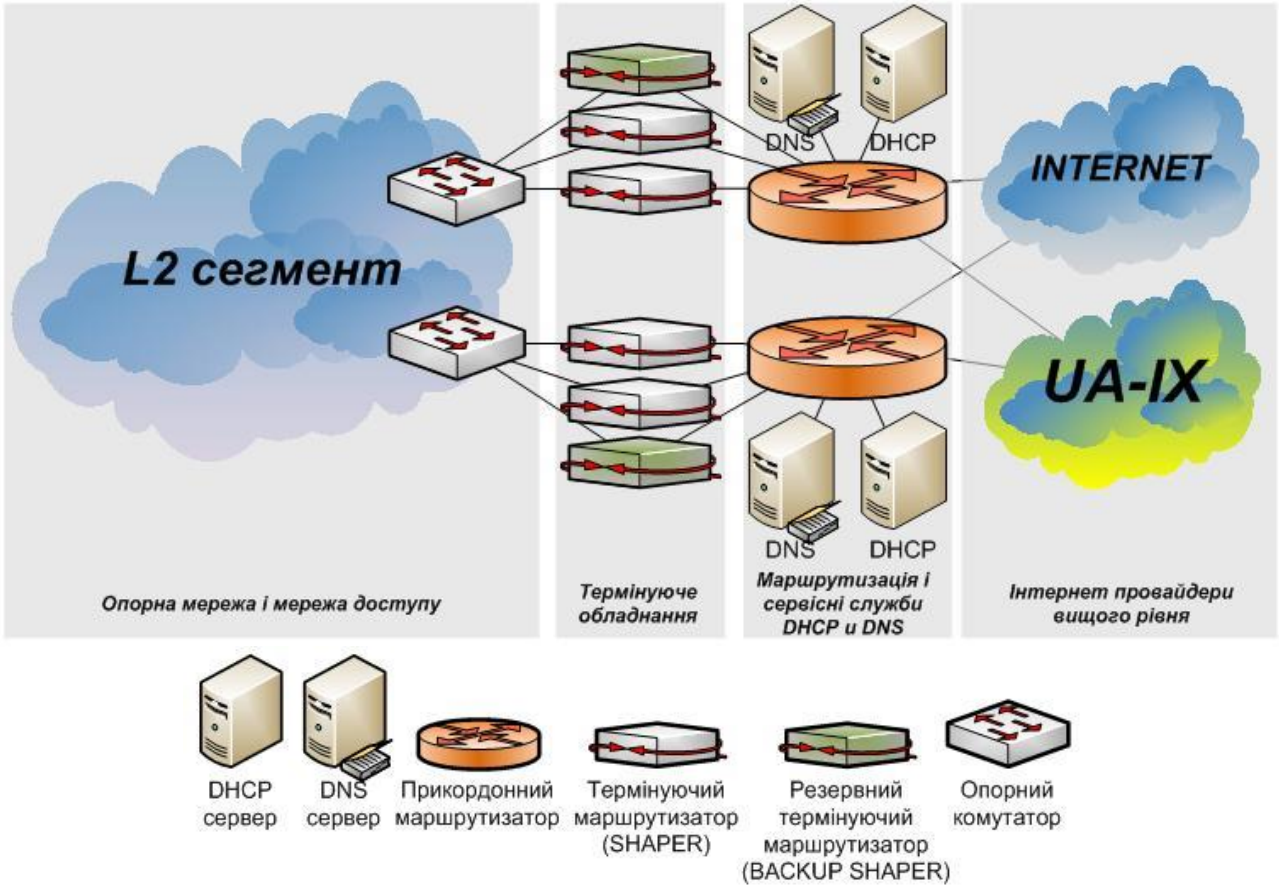

Рис.2. Логічна схема сервісного вузла забезпечення послуги HSI

Сервісний вузол пошти

В якості апаратної платформи для організації поштового сервісу з метою забезпечення безперервної і гарантованої роботи послуги, рекомендується використовувати від двох серверів в режимі «активний-резервний» (Active-Standby) з синхронізацією конфігурації кожні 10 хвилин.

Апаратна конфігурація серверів повинна підтримувати дискові сховища понад 1 Тбайт. Сервера повинні підключатися до опорної мережі по інтерфейсам Ethernet на швидкості 100 Мбіт/с і вище.

Поштовим серверам необхідно виділити зовнішню IP-адресу і доменні імена під такі поштові сервіси як SMTP, POP, IMAP.

Як програмне забезпечення можливе використання безкоштовних продуктів під операційними системами (ОС) Freebsd:

- SMTP - EXIM 4.x;
- POP/IMAP – DBMAIL;
- DB - MYSQL 5.x;
- WEB - APACHE 2.x, PHP 5.x;
- WEB-MAIL - HORDE IMP 4.x.

Доступ в мережу Інтернет

Схема організації послуги доступу до мережі Інтернет наведена на рис. 3.

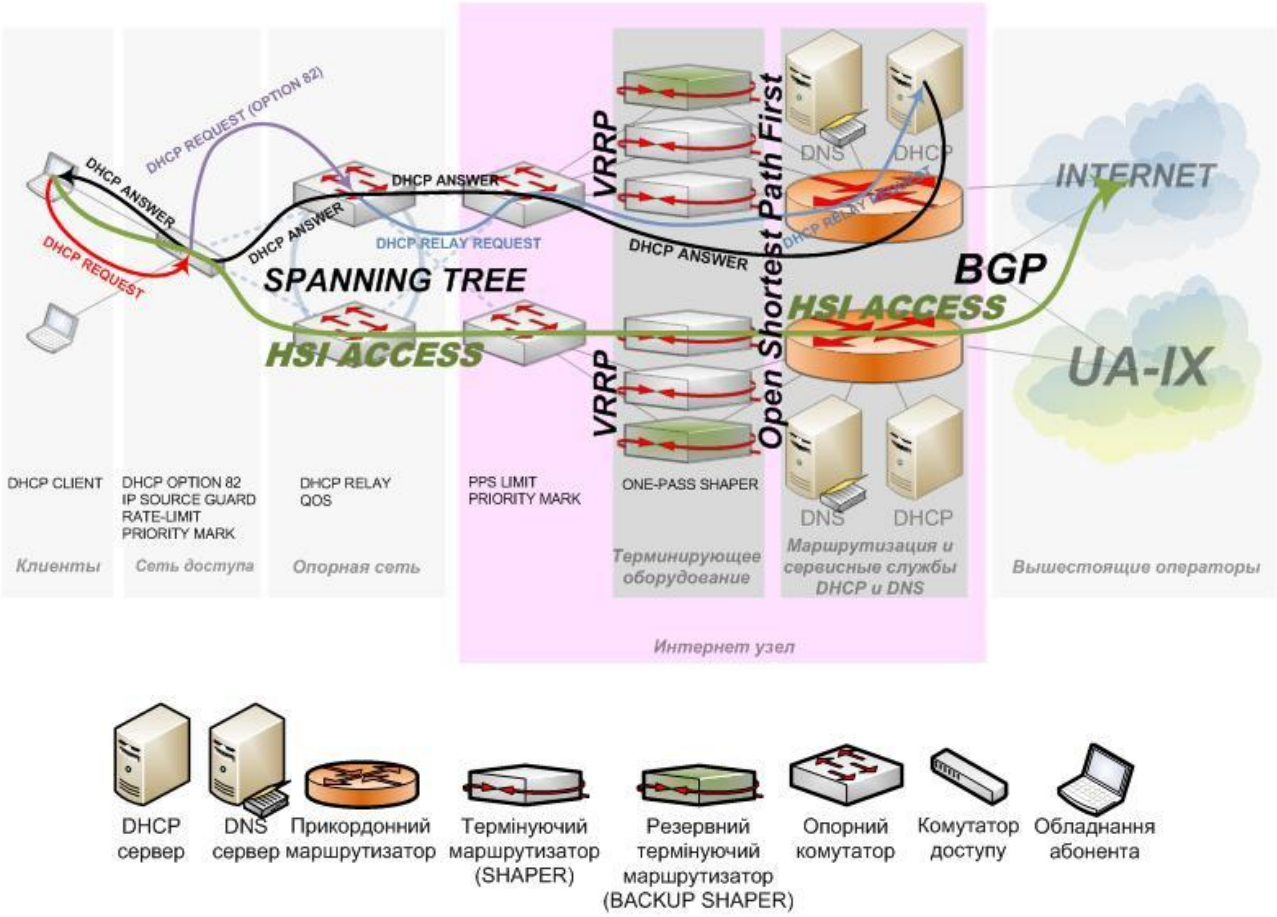

Рис.3. Схема організації послуги доступу до мережі Інтернет

Доступ до мережі інтернет здійснюється наступним чином:

- абонент робить запит на отримання Інтернет адреси за протоколом DHCP;
- комутатор доступу перехоплює широкомовний DHCP запит, доповнює його опцією 82 і направляє на порти, підключені до опорних комутаторів;
- запит доходить до опорного комутатора, перехоплюється повторно і відправляється на DHCP сервер;
- DHCP сервер, керуючись своїм файлом конфігурації, аналізує дані опції 82, і, відповідно до них, реєструє для абонента статичну адресу і посилає DHCP відповідь;
- відповідь безперешкодно проходить до комутатора доступу, який розпізнає його, і перебудує свою таблицю дозволів:
  - оскільки абонент отримав адресу по DHCP то база даних DHCP Snooping модифікується, і на порту дозволяється трафік від цієї IP-адреси і до неї;

– оскільки адреса була отримана цілком визначеним пристроєм, з конкретною апаратною адресою (MAC адреса) - то ця адреса не може бути використана іншим пристроєм;

- після отримання IP адреси дані від користувача направляються на порт комутатора доступу, де проводиться перевірка його відповідності із записами в базі DHCP Snooping, а також застосовується обмеження сумарної смуги пропускання (швидкості передачі);
- в залежності від типу послуги (L2 VPN, HSI) або типу сервісу (HTTP, FTP, P2P і т.і.) застосовується маркер QoS [8, 9], і дані відправляються до опорних комутаторів;
- опорні комутатори прозоро транспортують дані (з урахуванням QoS) до вузла Інтернет. Вони являють собою LAYER2 сегмент, і ніяких LAYER3 функцій не виконують;
- через комутатори сервісного вузла дані потрапляють на один з серверів термінації, де з'ясовується їх напрямок і виконується додаткове обмеження швидкості в кожному конкретному напрямку;
- після цього дані передаються до прикордонних маршрутизаторів і відправляються в зовнішні канали.

Існує три варіанти обмеженняшвидкості (управління профілями користувачів) у відповідності до політики та вимог тарифних планів:

- швидкість доступу абонента до мережі обмежується по загальній смузі на клієнтському порту комутатора доступу;
- обмеження швидкості доступу абонента до мережі по загальній смузі на комутаторі доступу, з можливістю виділення з неї меншою смуги для доступу до світового сегменту Інтернету. При цьому, додаткове обмеження може бути здійснено на сервісному вузлі Інтернет;
- виділення окремої смуги для кожного з напрямків на сервісному вузлі Інтернет), наприклад:
  – світової сегмент Інтернет;
  – український сегментІнтернет;
  – внутрішньо-мережевий сегмент Інтернет.

Кожен з варіантів передбачає можливість обмежувати або не обмежувати сумарну смугу на обладнанні вузлів доступу.

Останній варіант може бути досить вимогливим до апаратних ресурсів, в залежності від кількості абонентів, а також від кількості обраних напрямків. Якщо кількість абонентів перевищила 2000, знадобиться установка додаткового терміную чого обладнання – так званого Shaper (Формувач/Обмежувач), що зазвичай розрахований на 500 абонентів на пристрій при класифікації трафіку за трьома напрямками.

Технологія трансляції IP адрес (NAT) не використовується. Кожному абоненту видається «реальна» («біла») IP-адреса.

Послуги для бізнес-абонентів

Під послугами для бізнес-абонентів розуміються наступні:

- віртуальна виділена лінія (E-LINE: P2P Ethernet VPN) - канал передачі даних типу «точка-точка» [10, 11];
- віртуальні приватна мережа (E-LAN: MP2MP Ethernet VPN) - канал передачі даних типу «багатоточка-багатоточка» [10, 11].

Для надання бізнес-послуги для кожного абонента виділяється один (або більше, в залежності від вимог абонента) сервісний VLAN, який логічно поєднує точки підключення на другому рівні моделі OSI (LAYER2) тобто на рівні Ethernet.

При цьому зазначимо, що бізнес-абонентами такої мережі можуть бути оператори мобільного зв’язку та мобільного Інтернет доступу, для яких вона стане транспортною мережею [12].

Висновки

Мережі передачі даних, що надають послуги високошвидкісного доступу до мережі Інтернет та послуги по створенню приватних віртуальних мереж можуть будуватися на основі концепції Metro Ethernet.

Дворівневий принцип побудови дозволяє використовувати мінімальну номенклатуру мережевих пристроїв при забезпеченні високої надійності.

Існує і запропоновано рішення, що дозволяє автоматично конфігурувати та ідентифікувати абонентське обладнання, яке мінімізує можливі шахрайські дії та підвищує продуктивність праці обслуговуючого персоналу.

Показані точки мережі, де можуть бути застосовані обмеження швидкості доступу до різних сегментів мережі Інтернет, тобто управління профілями користувачів у відповідності до політики та вимог тарифних планів.

Список використаної літератури

1. MEF 22 (MetroEthernetForum версия 22) [Електронний ресурс] // - Режим доступу: https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_22.1.pdf (18.04.2017).
2. IEEE Std 802.3™-2015I [Електронний ресурс] // - Режим доступу: http://standards.ieee.org/getieee802/download/802.3-2015.zip (18.04.2017).
3. RFC 3046 [Електронний ресурс] // - Режим доступу: https://tools.ietf.org/html/rfc3046 (18.04.2017).
4. Understanding DHCP Option 82 for Protecting Switching Devices Against Attacks [Електронний ресурс] // - Режим доступу: https://www.juniper.net/techpubs/en_US/junos/topics/concept/port-security-dhcp-option-82.html (18.04.2017).
5. IEEE 802.1Q-2014 - Bridges and Bridged Networks3046 [Електронний ресурс] // - Режим доступу: http://www.ieee802.org/1/pages/802.1Q-2014.html (18.04.2017).
6. Технічний опис Українська мережа обміну трафіком [Електронний ресурс] // - Режим доступу: http://www.ix.net.ua/pro-kompaniyu/tehnichnyy-opys (18.04.2017).
7. Issue tracking system [Електронний ресурс] // - Режим доступу: https://en.wikipedia.org/wiki/Issue_tracking_system (18.04.2017).
8. Рекомендація МСЕ Y.1540 [Електронний ресурс] // - Режим доступу: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11079&lang=ru (18.04.2017).
9. Рекомендація МСЕ Y.1541 [Електронний ресурс] // - Режим доступу: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11462&lang=ru (18.04.2017).
10. MEF 33 (MetroEthernetForum. Technical Specification MEF 33 Ethernet Access Services Definition January 2012) [Електронний ресурс] // - Режим доступу: https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_33.pdf (18.04.2017).
11. MEF 6.2 (EVC Ethernet Services Definitions Phase 3, August, 2014) 1541 [Електронний ресурс] // - Режим доступу: https://www.mef.net/resources/technical-specifications/download?id=8&fileid=file1 (18.04.2017).
12. Недашковский А.Л. Применение Metro Ethernet сетей как транспортных в 4G/5G / А.Л. Недашковский // Региональний семинар МСЭ «Тенденции развития конвергентных сетей: Решения пост-NGN, 4G, 5G», Тезисы докладов, МСЭ/ГУТ, Киев, 17-18 ноября 2016г. – С. 89-90.

Надійшла 23.04.2017 р. Рецензент: д.т.н., доцент Семко В.В.