Тема 15. Технологія пасивних оптичних мереж PON. Віртуалізація мережевих функцій

PON (Passive optical network) – технологія пасивних оптичних мереж, заснована на деревоподібній волоконно-кабельній архітектурі з пасивними оптичними розгалужувачами на вузлах. Зазвичай є досить економічним способом забезпечення широкосмугової передачі інформації. При цьому архітектура PON володіє необхідною ефективністю нарощування як вузлів мережі, так і пропускної здатності, залежно від поточних та майбутніх потреб абонентів.

Перші кроки в технології PON були зроблені в 1995 році, коли впливова група з семи компаній (British Telecom, France Telecom, Deutsche Telecom, NTT, KPN, Telefonica і Telecom Italia) створила консорціум для того, щоб втілити в життя ідеї множинного доступу по одному волокну. Ця організація отримала назву FSAN (full service access network). Багато нових членів, як операторів, так і виробників обладнання увійшло до неї наприкінці 90-х років. Метою FSAN була розробка загальних рекомендацій та вимог до обладнання PON для того, щоб виробники устаткування та оператори могли співіснувати разом на конкурентному ринку систем доступу PON. На сьогодні FSAN налічує 40 операторів та виробників, і працює в тісній співпраці з такими організаціями з стандартизації як ITU-T, ETSI та ATM форум.

15.1 Принцип роботи PON

Основна ідея архітектури PON – використання лише одного модуля в оптичному терміналі OLT (optical line terminal) для передачі інформації великій кількості абонентських пристроїв ONT (optical network terminal), які називаються ONU (optical network unit) і прийому інформації від них. ONU –пристрій, що перетворює середовище передачі даних з оптично волоконного кабелю до витої пари та використовується в технології пасивної оптичної мережі PON.

Число абонентських вузлів, підключених до одного модуля OLT, може бути настільки великим, наскільки дозволяє бюджет потужності і максимальна швидкість апаратури. Для передачі потоку інформації від OLT до ONT – прямого (низхідного) потоку, як правило, використовується довжина хвилі 1490 нм. Навпаки, потоки даних від різних абонентських вузлів у центральний вузол спільно утворюють зворотний (висхідний) потік, передаються на довжині хвилі 1310 нм. В OLT та ONT вбудовані мультиплексори WDM, що розділяють вихідні і вхідні потоки.

Прямий потік на рівні оптичних сигналів, є широкомовним. Кожен абонентський вузол ONT, зчитуючи адресні поля, виділяє з цього загального потоку призначену тільки йому частину інформації. Фактично, ми маємо справу з розподіленим демультиплексором.

Всі абонентські вузли ONT ведуть передачу у зворотному потоці на одній і тій же довжині хвилі, використовуючи концепцію множинного доступу з часовим поділом TDMA (time division multiple access). Для того, щоб виключити можливість перетину сигналів від різних ONT, для кожного з них встановлюється свій індивідуальний розклад по передачі даних із врахуванням поправки на затримку, пов’язану з відстанню від даного ONT від OLT. Це завдання вирішує протокол TDMA MAC.

15.2 Переваги та недоліки PON

Переваги технології PON:

- більші швидкості, ніж при використанні витої пари в класичній топології багатоабонентської мережі;
- відсутність проміжних активних вузлів (надійність та економічність);
- довговічність та стійкість до зовнішніх випромінювань оптоволокна;
- фінансові плюси: економія оптичних приймачів у центральному вузлі, економія волокон, одне оптичне волокно на 64 абоненти (у нових станціях до 128);
- зручність проектування для приватного сектору житлових будинків.

Деревоподібна топологія P2MP дозволяє оптимізувати розміщення оптичних розгалужувачів, виходячи з реального розташування абонентів, витрат на прокладання оптичних кабелів та експлуатацію кабельної мережі.

Недоліки мережі PON:

- збільшена складність технології PON;
- фінансові мінуси: високі вимоги до якості матеріалів та монтажу волоконно-оптичних мереж (при недотриманні – обриви зв'язку), високотехнологічність та витратність ремонту, непоодинокість стандартів обладнання та технології з неясною перспективністю їх експлуатації через це;
- часто використовуються оптичні розгалужувачі, що збільшують згасання. Через високе згасання сигналу, передбаченого технологією PON, фізично неможлива побудова мережі деревоподібної структури з радіусом понад 10 км від оптичного лінійного терміналу (OLT).

15.3 Технологія GPON

GPON (Gigabit Passive Optical Network) – представник сімейства пасивних технологій оптичних мереж доступу PON. Серед переваг GPON можна відзначити найбільшу швидкість, синхронний формат кадру, інтеграцію з ATM та TDM технологіями та визначені плани розвитку.

Мережа GPON складається з:

- станційного терміналу OLT, якій містить у собі певну кількість портів GPON (від 4 до 112) та порти Gigabit Ethernet або 10Gigabit Ethernet для підключення до транспортної IP мережі.
- абонентського терміналу ONT. ONT може бути розрахованим на одного користувача та мати порти Ethernet, POTS та RF TV, або на групу користувачів, або на організацію, та мати порти Ethernet, xDSL, POTS, E1, RF TV.

– повністю пасивної оптичної розподільчої мережі між ними, яка складається зі сплітерів з коефіцієнтом розділення від 1:2 до 1:64, що розташовані централізовано, або розподілено.

Передача з OLT ведеться на довжині хвилі 1490 нм зі швидкістю 2,5 Гбіт/с, а прийом – на довжині хвилі 1310 нм зі швидкістю 1,25 Гбіт/с. Таким чином забезпечується робота системи по одному волокну за принципом WDM. Асиметричність швидкостей потоку обумовлена характером трафіку низхідного протоку (завантаження файлів, передача відео).

Стабільна та гнучка робота досягається завдяки повній синхронізації мережі разом з динамічним розподілом пропускної смуги.

15.4 Віртуалізація мережевих функцій

Віртуалізація – створення віртуального, тобто штучного, об’єкту чи середовища.

Термін часто використовується в комп’ютерних технологіях для позначення абстракції комп’ютерних ресурсів. Відповідно, він може стосуватися різних випадків:

– мережева віртуалізація, створення віртуалізованого адресного простору мережі всередині або через існуючі підмережі
– віртуальна приватна мережа (VPN), комп’ютерна мережа, в якій деякі канали зв’язку між вузлами створені через відкриті канали передачі даних або віртуальні канали у більших мережах, таких як Інтернет

14.5.1 VPN

VPN (Virtual Private Network – віртуальна приватна мережа) – загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передачі інформації через

загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. 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 за клієнт-серверною технологією.

VPN класифікують за типом використовуваного середовища таким чином:

– Захищені. Найпоширеніший варіант віртуальних приватних мереж. З його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, зазвичай, Інтернету. Прикладом захищених протоколів VPN є: IPsec, SSL та PPTP. Прикладом використання протоколу SSL є програмне забезпечення OpenVPN.
– Довірчі. Використовують у випадках, коли середовище, яким передають дані, можна вважати надійним і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN рішень є: Multi-protocol label switching (MPLS) і L2tp (Layer 2 Tunnelling Protocol).

Захист інформації в розумінні VPN включає в себе шифрування (encryption), підтвердження справжності (authentication) та контроль доступу (access control). Найбільш часто використовуваними в VPN-рішеннях алгоритмами кодування в наш час є DES, Triple DES і різні реалізації AES. Підтвердження справжності включає в себе перевірку цілісності даних та ідентифікацію осіб та об`єктів, задіяних у VPN. Перша гарантує, що дані дійшли до адресата саме в тому вигляді, в якому були надіслані. Найпопулярніші алгоритми перевірки цілісності даних на сьогодні – MD5 і SHA1.

Зазвичай, при створенні VPN, використовують підключення типу точка-точка до певного сервера, або встановлення Ethernet-тунелю з певним сервером, при якій тунелю призначають певну підмережу. Сервер VPN при цьому виконує

функції маршрутизації та фільтрування трафіку для доступу до локальної мережі через VPN.

При використанні такого підходу ми все ще маємо можливість фільтрувати трафік на підставі способу підключення (наприклад, використовувати для локальної мережі та для віддалених користувачів різні фільтри), але виключається необхідність налаштування маршрутизації, а віддалені машини включаються прямо в локальну мережу, бачать ресурси, навіть здатні використовувати широкосмугові посилки взагалі без додаткового налаштування.