КОМП'ЮТЕРНІ МЕРЕЖІ

Мультіплексування. Комутація даних. VPN технології. Мршрутизація

Лекція 14

Лектор: Володимир Саєнко
Харків, ХНУРЕ, каф. ІУС, 2013

Зміст

- Середовище передачі даних, що розділяється
- Мультиплексування
- Адресація вузлів мережі
- Комутація
- Комутація пакетів
- Методи просування пакетів
- Порівняння мереж із комутацією пакетів та каналів
- VPN
- СтруктураVPN
- Принцип роботи VPN
- Класифікація VPN
- Протоколи VPN

Введення

Мета лекції - вивчити особливості реалізації методів комутації та формування VPN.

Предмет вивчення – методи комутації та технології формування VPN

План лекції

1. Основні технологічні положення
2. Інформацінйі структури
3. Приклади
4. Обговорення питаннь

Перелік нових термінів

- Середовищем передачі даних, що розділяється, є спільно використовуваний декількома інтерфейсами фізичний канал (shared).
- Мультиплексування – технологія розділення засобів передачі даних між групами використовуючих їх об’єктів
- частотне мультиплексування(Frequency Division Multiplexing, FDM);
- хвильове мультиплексування (Wave Division Multiplexing, WDM).
- часове мультиплексування (Time Division Multiplexing, TDM);
- множинний доступ з кодовим розділенням(Code Division Multiple Access, CDMA).
- VPN (англ. Virtual Private Network - віртуальна приватна мережа)
- PPTP - Point - to - Point Tunneling Protocol)
- Multi - protocol label switching (MPLS)
- IPSec (IP security) - часто використовується поверх IPv4.
- PPTP (point - to - point tunneling protocol) - розроблявся спільними зусиллями декількох компаній, включаючи Microsoft.
- PPPoE (PPP (Point - to - Point Protocol) over Ethernet)
- L2TP (Layer 2 Tunnelling Protocol) - використовується в продуктах компаній Microsoft і Cisco.
- L2TPv3 (Layer 2 Tunnelling Protocol version 3)

Мультиплексування

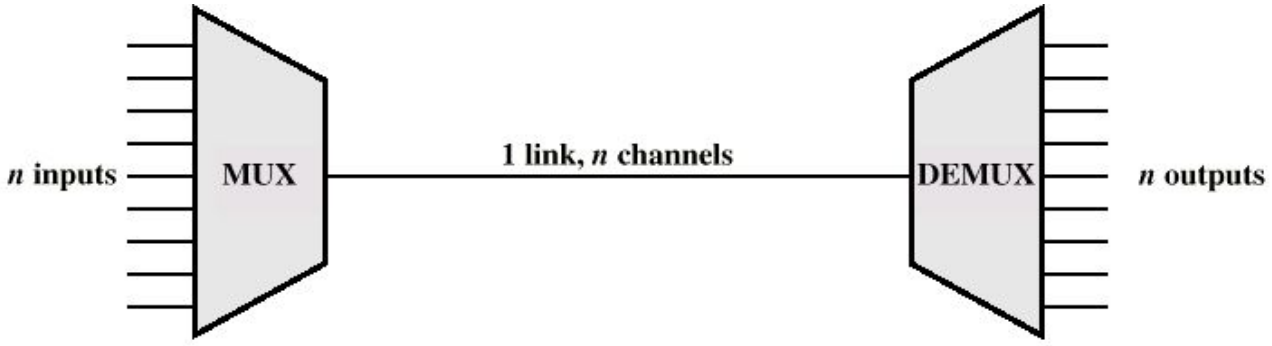
- **Мультиплексування –** **Multiplexing** технологія розділення засобів передачі даних між групами використовуючих їх об’єктів.

  В результате мультиплексирования в одном физическом канале создается группа логических каналов. Различают временное и частотное мультиплексирования.

- *В информационных технологиях и связи*, мультиплекси́рование (англ. multiplexing, muxing) — уплотнение канала, т. е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу.

- *В телекоммуникациях* мультиплексирование подразумевает передачу данных по нескольким логическим каналам связи в одном физическом канале. Под физическим каналом подразумевается реальный канал со своей пропускной способностью — медный или оптический кабель, радиоканал.

- *В информационных технологиях* мультиплексирование подразумевает объединение нескольких потоков данных (виртуальных каналов) в один. Примером может послужить видеофайл, в котором поток (канал) видео объединяется с одним или несколькими каналами аудио.



Мультиплексування

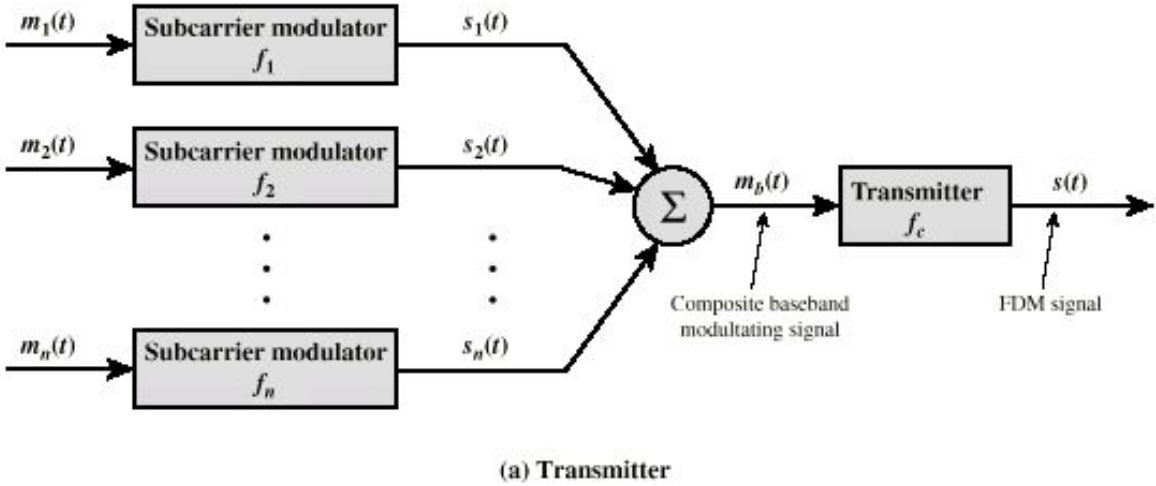
В даний час для мультиплексування абонентських каналів використовуються:

- частотне мультиплексування (**Frequency Division Multiplexing**, FDM);
- часове мультиплексування (**Time Division Multiplexing**, TDM);
- статистическое временное мультиплексирование Statistical time division multiplexing **(STDM);**
- хвильове мультиплексування (**Wave Division Multiplexing**, WDM);
- множинний доступ з кодовим **розділенням(Code Division Multiple Access,** CDMA).

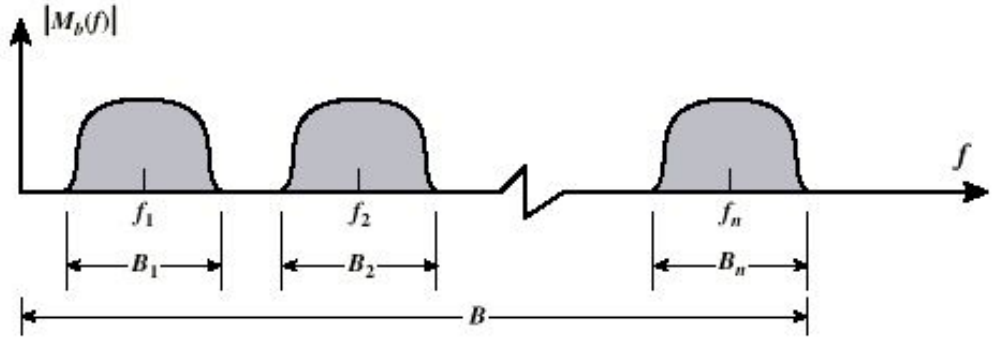
Мультиплексирование с разделением по частоте (FDM)

- **Технология**
- Мультиплексирование с разделением по частоте (англ. FDM, Frequency Division Multiplexing) предполагает размещение в пределах полосы пропускания канала нескольких каналов с меньшей шириной.
- Каждый поток передается по выделенному частотному диапазону. Пропускная способность делится на равные части, подканалы.
- Наглядным примером может послужить радиовещание, где в пределах одного канала (радиоэфира) размещено множество радиоканалов на разных частотах (в разных частотных полосах).
- **Основные применения**
- Используется в сетях мобильной связи (FDMA) для разделения доступа, в волоконно-оптической связи аналогом является мультиплексирование с разделением по длине волны (WDM, Wavelength Division Multiplexing) (где частота — это цвет излучения излучателя), в природе — все виды разделений по цвету (частота электромагниных колебаний) и тону (частота звуковых колебаний).

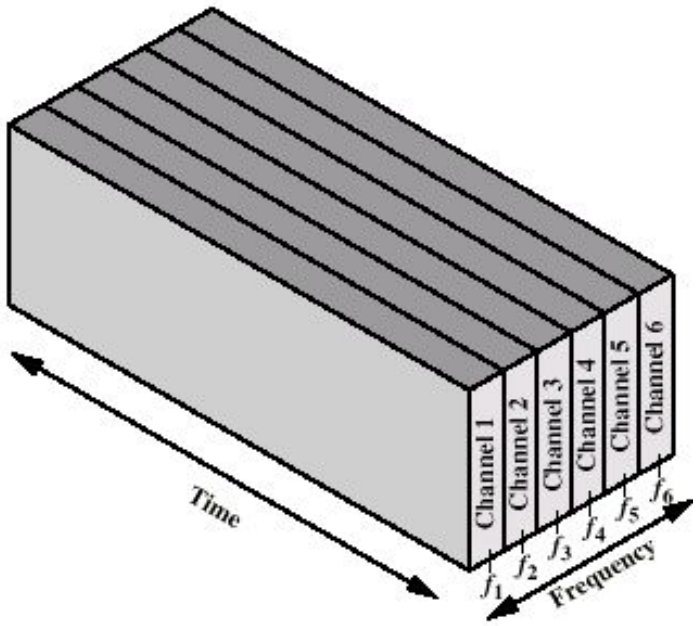
FDM System

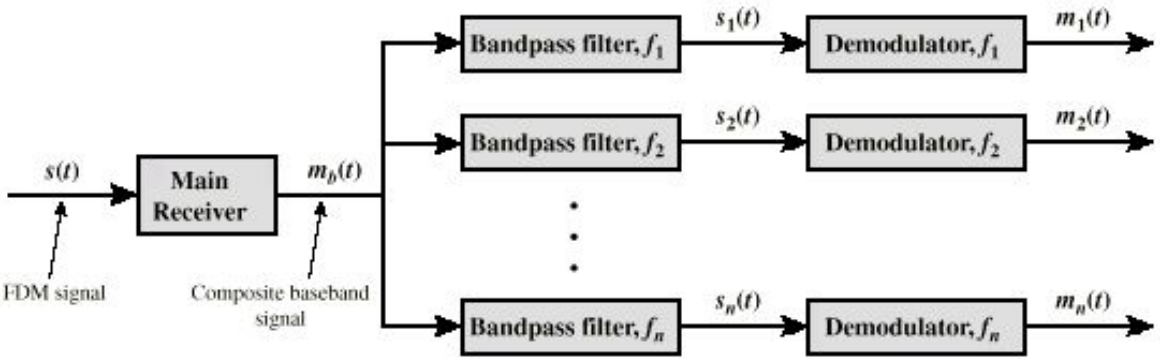


(a) Transmitter



(b) Spectrum of composite baseband modulating signal

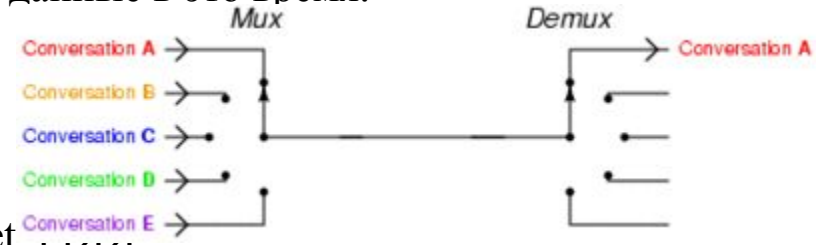




(c) Receiver

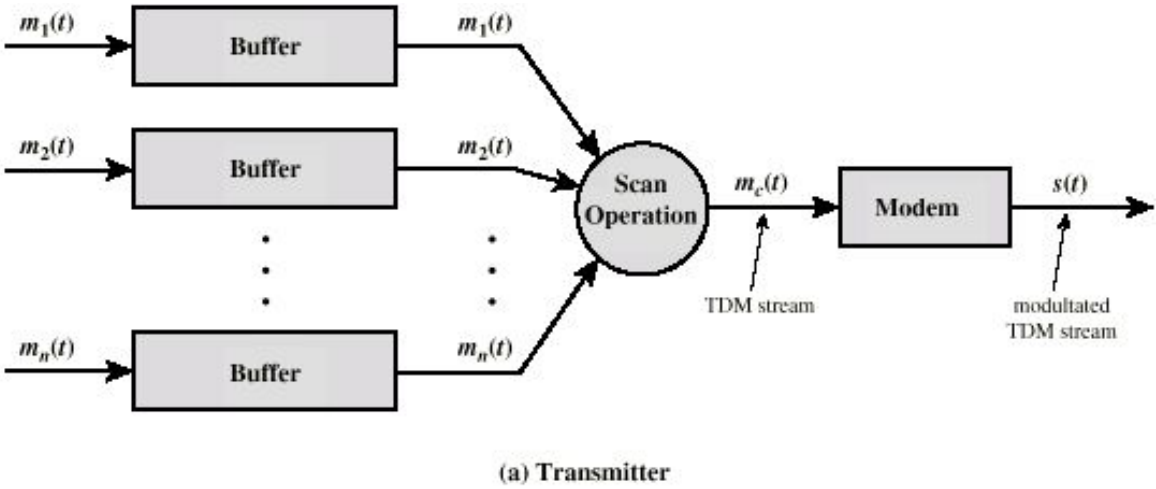
Мультиплексирование с разделением по времени (TDM, STDM)

- **Технология**
- **Временное мультиплексирование - Time division multiplexing (TDM)**
- Временное мультиплексирование - метод мультиплексирования, при котором канал предоставляется всем системам по очереди независимо от наличия у них данные для передачи. Временное мультиплексирование предусматривает использование мультиплексора.
- *Недостаток:* даже если какой-то входной канал не использует для передачи выделенный ему интервал, другие каналы не могут передавать данные в это время.

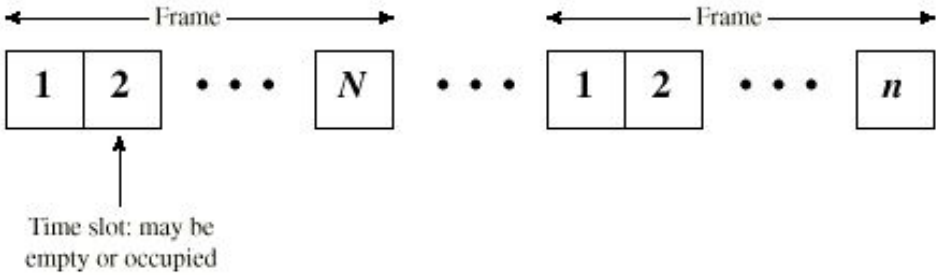


- **Основные применения**
- беспроводные TDMA-сети, Wi-Fi, WiMAX;
- канальная коммутация в PDH и SONET/SDH;
- пакетная коммутация в ATM, Frame Relay, Ethernet, PBB;
- коммутация в телефонных сетях;
- последовательные шины: PCIe, USB.

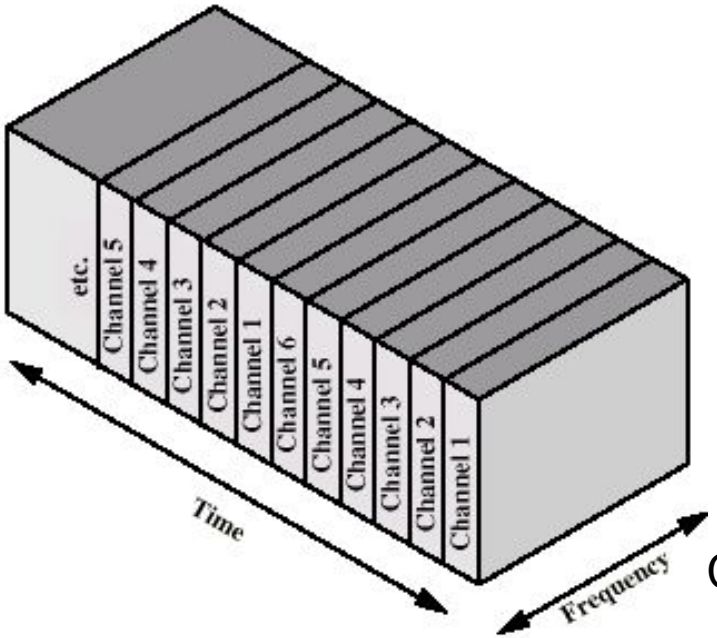
TDM System



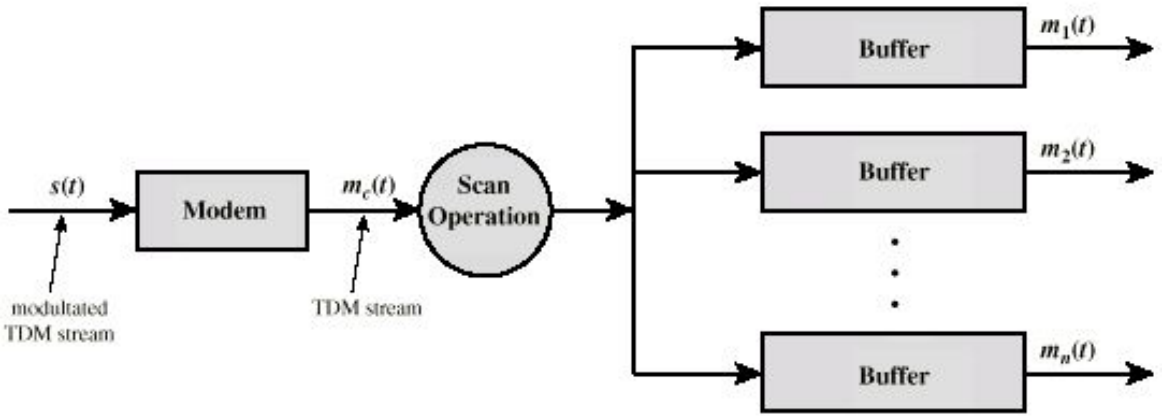
(a) Transmitter



(b) TDM Frames



C



(c) Receiver

Комутація каналів на основі WDM

- У методі **хвилевого мультиплексування** (WDM- *Wavelength-division multiplexing,*) інформаційним сигналом є світло
- У магістральному каналі зазвичай мультіплексирується декілька спектральних каналів — до 16, 32, 40, 80 або 160, причому, починаючи з 16 каналів, така техніка мультиплексування називається **ущільненим хвилевим мультиплексуванням** (DWDM -Dense WDM).
- Усередині такого спектрального каналу дані можуть кодуватися як дискретним способом, так і аналоговим.

Мультиплексирование (уплотнение) с кодовым разделением (Code Division Multiplexing, CDM).

- В схеме CDM каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ — кодовую последовательность длиной в 11, 16, 32, 64 и т.п. бит (их называют чипами).
- Кодовая последовательность уникальна для каждого передатчика, причем их подбирают так, чтобы корреляция двух любых CDM-кодов была минимальна (а в ряде случаев — чтобы автокорреляция CDM-кода при фазовом сдвиге была максимально возможной). Как правило, если для замены «1» в исходном потоке данных используют некий CDM-код, то для замены «0» применяют тот же код, но инвертированный.

Мультиплексування

- В разі мультиплексування в мережі з комутацією каналів встановлений при з'єднанні складений канал складається з ліній зв'язку з однаковою пропускною здатністю, лише роль ліній зв'язку грають підканали.

- мультиплексування підвищує ефективність роботи мережі, тому що користувач може точніше підібрати швидкість з'єднання відповідно до своїх реальних потреб.

- **Коефіцієнт пульсації трафіку** окремого користувача мережі визначається як відношення пікової швидкості на якому-небудь невеликому інтервалі часу до середньої швидкості обміну даними на тривалому інтервалі часу і може досягати значень 100:1

Комутація

- **Комутація-** це з'єднання кінцевих вузлів через мережу транзитних вузлів. Послідовність вузлів утворює **логічний канал**.

- **Задачі комутації:**
  - Визначення інформаційних потоків, для яких потрібно прокладати логічні канали.
  - Створювання логічних каналів потоків.
  - Просування потоків, тобто розпізнавання потоків і їх локальна комутація на кожному транзитному вузлі.
  - Мультиплексування і демультиплексування потоків.

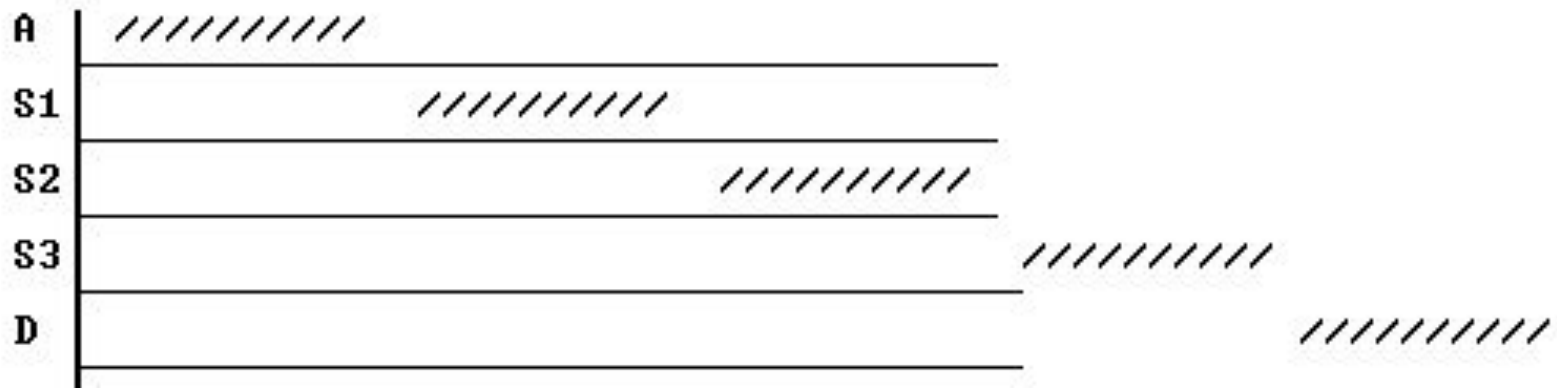
Комутація каналів

Комутаційна мережа складається з комутаторів, зв'язаних між собою **лініями зв'язку**. Кожна лінія має одну і ту ж пропускну спроможність.

- У транзитних комутаторах *немає необхідності буферизовувати дані* користувачів.

Передача повідомлень

- Все данные от пользователя передаются цельными частями – сообщениями.
- В течение передачи сообщения узел (коммутатор) и один сегмент канала полностью занят.
- Чем больше размер сообщения, тем дольше занят узел (коммутатор)



Комутація пакетів

- При комутації пакетів всі дані, які передаються користувачем мережі, розбиваються у вихідному вузлі на порівняно невеликі частини, що називаються пакетами. Кожен пакет забезпечується заголовком, в якому вказується адреса, необхідна для доставки пакету вузлу призначення.

- Кінцевик - поле, яке розміщується у кінці пакета

- Контрольна сума дає змогу перевірити, чи була змінена інформація

Комутація пакетів

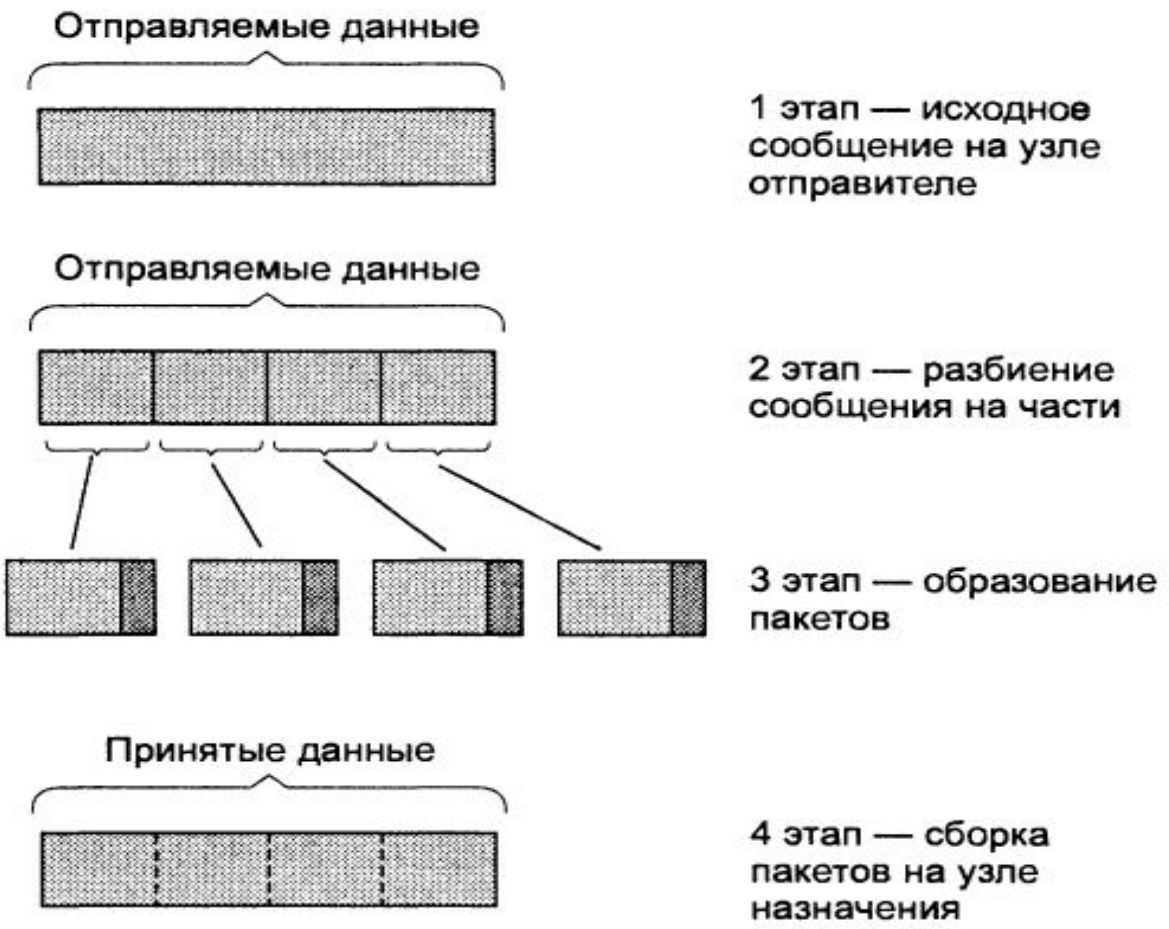


Рис. 3.4. Разбиение потока данных на пакеты

Комутація пакетів

- Пакети надходять в мережу без попереднього резервування лінія зв’язку й не з зафіксованою наперед заданою швидкістю.

Методи просування пакетів

- *При дейтаграммній передачі* з'єднання не встановлюється, і всі пакети, що передаються, просуваються незалежно один від одного на підставі одних і тих самих правил

- *Передача зі встановленням логічного з'єднання* розпадається на так звані сеанси, або логічні з'єднання. Процедура обробки визначається для всієї множини пакетів, що передаються в рамках кожного з'єднання.

- *Передача зі встановленням віртуального каналу*. Якщо до числа параметрів з'єднання входить маршрут, то всі пакети, що передаються в рамках даного з'єднання, повинні проходити за вказаним маршрутом

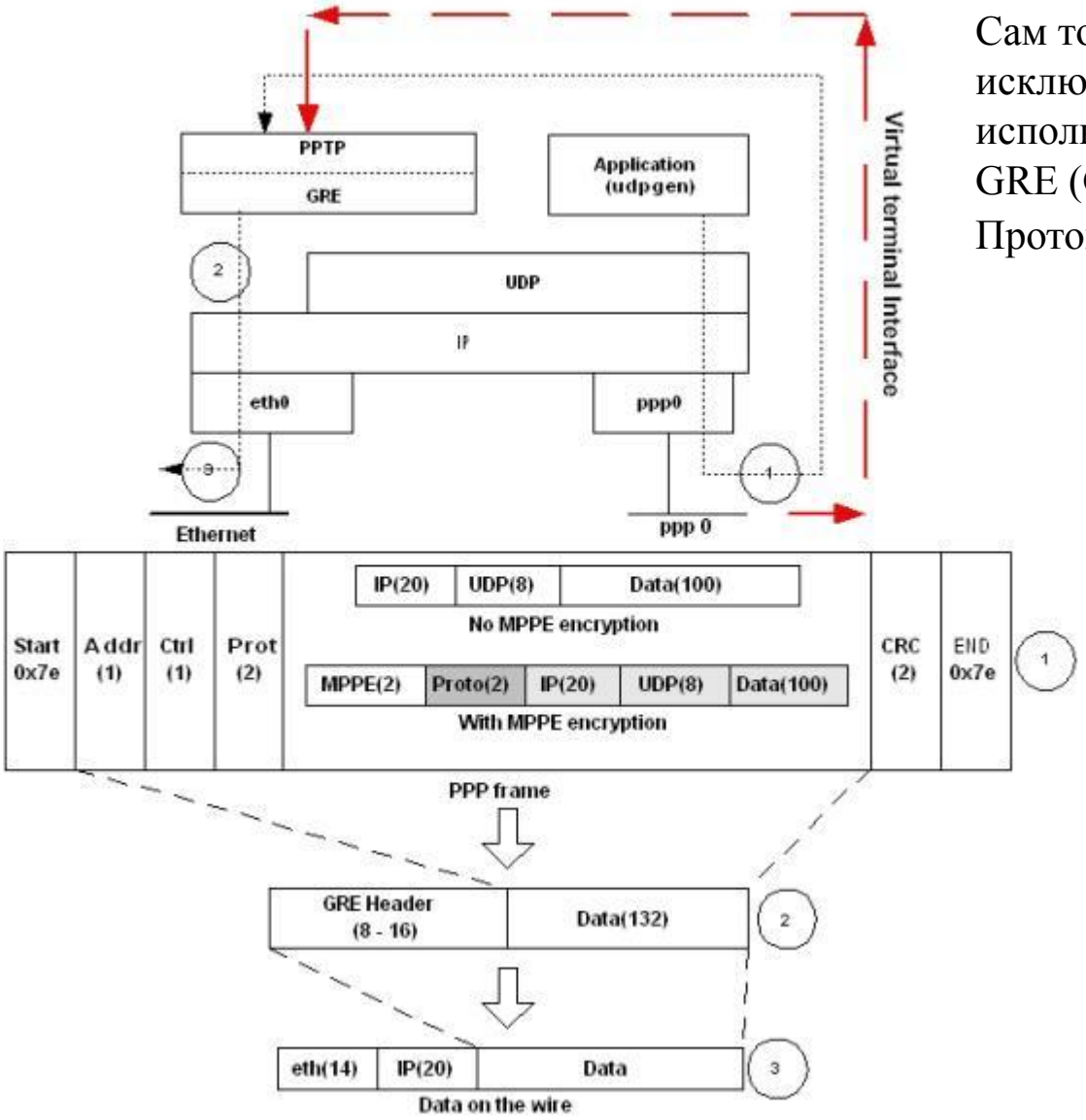
Порівняння мереж з комутацією каналів та пакетів:

Комутація каналів	Комутація пакетів
Необхідно заздалегідь встановлювати з’єднання	Відсутній етап встановлення з’єднання (дейтаграмний спосіб)
Адреса необхідна лише на етапі встановлення з’єднання	Адреса та інша службова інформація передається з кожним пакетом
Мережа може відмовити абоненту у встановлені з’єднання	Мережа завжди готова прийняти дані від абонента
Гарантована пропускна здатність для взаємодіючих абонентів	Пропускна здатність мережі для абонентів невідома, затримки передачі мають випадковий характер
Трафік реального часу передається без затримок	Ресурси мережі використовуються ефективно при передачі пульсуючого трафіка
Висока надійність передачі	Можливі втрати даних через переповнення буферів
Нераціональне використання пропускної здатності каналів, яка знижує загальну ефективність мережі	Автоматичний динамічний розподіл пропускної здатності фізичних каналів у відповідності до фактичної інтенсивності трафіку абонентів

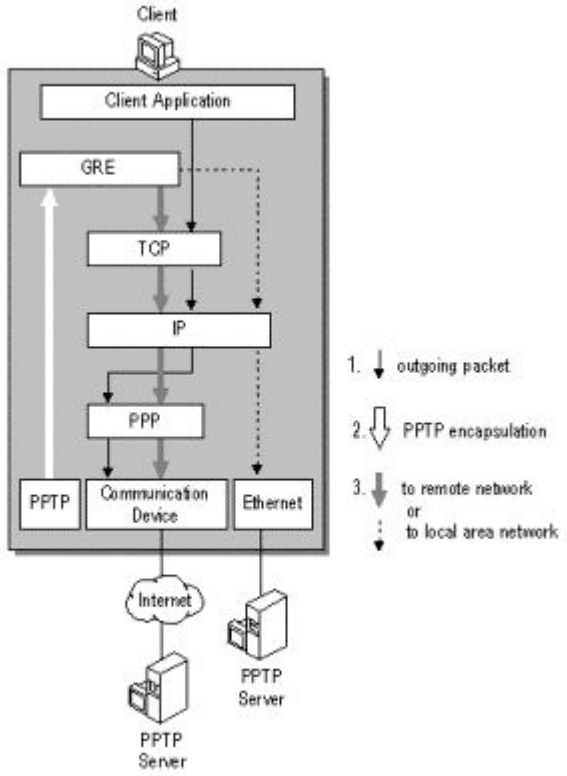
VPN

- VPN (англ. Virtual Private Network - віртуальна приватна мережа) - узагальнена назва технологій, що дозволяють забезпечити одне або декілька мережевих з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет).
- Використовуються засоби криптографії (шифрування, аутентифікації, інфраструктури відкритих ключів, засоби для захисту від повторів і змін передаваних по логічній мережі повідомлень).
- Залежно від вживаних протоколів і призначення, VPN може забезпечувати з'єднання трьох видів : вузол-вузол, вузол-мережа і мережа-мережа.
- Найбільш універсальним способом побудови VPN є використання технології ***туннелирования, або інкапсуляції***. Ця технологія дозволяє передавати пакети однієї мережі (первинною) по каналах зв'язку інший (вторинною). Для цього пакет первинної мережі (дані і протоколи) інкапсулюється в пакет вторинної мережі і стає видний, як дані. Взагалі кажучи, інкапсуляція не передбачає кодування. Якщо для підвищення рівня безпеки воно потрібне, то повинно виконуватися засобами приватної мережі до процедури інкапсуляції

VPN



Сам тоннель не использует TCP и работает исключительно на IP уровне с использованием протокола инкапсуляции GRE (Generic Encapsulation Protocol - Общий Протокол Инкапсуляции).



Принцип роботи VPN

- Для створення L2TP -туннеля служать два пристрої: концентратор доступу L2TP (L2TP Access Concentrator -- LAC) і мережевий сервер L2TP (L2TP Network Server -- LNS).

- LAC є однією з кінцевих точок L2TP -туннеля. Він розташовується між видаленою системою (користувачем або філією) і LNS. LAC приймає виклики від видалених систем і інкапсулює PPP -фреймы в пакети L2TP. Потім він направляє їх по L2TP -туннелю на один або декілька LNS по мережі з комутацією пакетів (Internet, Frame Relay, ATM).

- LNS -- друга кінцева точка тунеля, цього разу з боку корпоративної мережі. Він є логічною кінцевою точкою PPP -сессии. LNS деинкапсулирует L2TP -пакеты, обробляє PPP -фреймы і направляє їх в корпоративну мережу

Протоколи VPN

- **PPTP** (point - to - point tunneling protocol) - розроблявся спільними зусиллями декількох компаній, включаючи Microsoft.
- **L2TP (**Layer 2 Tunnelling Protocol) - використовується в продуктах компаній Microsoft і Cisco.
- **L2TPv3** (Layer 2 Tunnelling Protocol version 3).
- **OpenVPN** SSL/TLS VPN з відкритим початковим кодом, підтримує режими PPP, bridge, point - to - point, multi - client serve

- **PPPoE** (PPP (Point - to - Point Protocol) over Ethernet)
- **IPSec** (IP security) - часто використовується поверх IPv4.

Протоколи VPN. Шифрование

- IPSec (IP security) - (сокращение от **IP Security**) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. Протоколы IPsec работают на сетевом уровне (уровень 3 модели OSI). Другие широко распространённые защищённые протоколы сети Интернет, такие как SSL и TLS, работают на транспортном уровне (уровни OSI 4 — 7). Это делает IPsec более гибким, поскольку IPsec может использоваться для защиты любых протоколов базирующихся на TCP и UDP. В то же время увеличивается его сложность из-за невозможности использовать протокол TCP (уровень OSI 4) для обеспечения надёжной передачи данных.
- SSL (*Secure Sockets Layer* — уровень защищённых сокетов). криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером.
- Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причём для шифрования используется асимметричный алгоритм с открытым ключем. При шифровании с открытым ключом используются два ключа, причем любой из них может использоваться для шифрования сообщения. Тем самым, если используется один ключ для шифрования, то соответственно для расшифровки нужно использовать другой ключ. В такой ситуации можно получать защищённые сообщения, публикуя открытый ключ, и храня в тайне секретный ключ.
- TLS - Впоследствии на основании протокола SSL 3.0 был разработан и принят стандарт RFC, получивший имя TLS. (*Transport Layer Security* — безопасность транспортного уровня) — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет. TLS предоставляет возможности аутентификации и безопасной передачи данных через Интернет с использованием криптографических средств. Часто происходит лишь аутентификация сервера, в то время как клиент остается неаутентифицированным. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытого ключа (PKI), которая позволяет защитить клиент-серверные приложения от перехвата сообщений, редактирования существующих сообщений и создания поддельных.

Класифікація алгоритмів маршрутизації

Класифікація 1
Статичні: прості, фіксовані,
Динамічні: адаптивні.

Класифікація 2
Однорівними або ієрархічними
З інтелектом у головній обчислювальній машині або в роутері
Внутрідоменними й междоменними
Алгоритмами стану каналу або вектора відстаней

Алгоритми маршрутизації

Прості алгоритми маршрутизації.

алгоритм випадкової маршрутизації;

алгоритм із лавинною маршрутизацією;

алгоритм маршрутизації по попередньому досвіді.

Алгоритми маршрутизації з фіксованим маршрутом

- Одношляховий алгоритм із фіксованою маршрутизацією (ФМ): попередньо формується таблиця найкращого досягнення будь-якого вузла й, відповідно, будь-якого абонента.
- Багатодорожний алгоритм із фіксованою маршрутизацією: існує розширена таблиця, коли для досягнення абонента пропонується кілька маршрутів. У цьому випадку виникає проблема вибору конкретного маршруту залежно від ситуації, що створилася, у мережі.

Алгоритми маршрутизації

Адаптивні алгоритми маршрутизації (1)

1. Локальний адаптивний алгоритм маршрутизації: пакет, що потрапив у вузол, буде відправлений по маршруту відповідно до додаткової інформації, наявної в ньому:
- таблицею маршрутів, що визначає всі напрямки;
- даними про технічний стан всіх каналів,
- довжиною черги пакетів, що очікують передачу по вихідних каналах.

2. Алгоритм розподіленої адаптивної маршрутизації: кожний вузол формує таблицю маршрутів по всіх вузлах призначення. Для будь-якого маршруту враховується фактичний час передачі пакета у вузол призначення. Цей час ураховує довжини черг і час доставки. Інформація з вузла розсилається в сусідні вузли.

Алгоритми маршрутизації

Адаптивні алгоритми маршрутизації (2)

3. Алгоритм із централізованою адаптивною маршрутизацією: створюється центр маршрутизації, що розсилає таблиці всім вузлам. Таблиці формуються на підставі інформації, що йде від будь-якого вузла й враховуючої довжини черг, і працездатність лінії. Вся інформація про маршрути втримується в одному з. Достоїнство даного методу - з рівномірного завантаження мережі, тому що вибір маршруту кожного пакета здійснює єдина центральна станція.

4. Алгоритм із комбінованою централізованою адаптивною маршрутизацією, у мережі існує сервер, що розсилає таблиці маршрутів, але вибір маршруту здійснює сам вузол..

Алгоритми стека TCP\IP

дистанційно-векторний алгоритм (Distance Vector Algorithms, DVA), алгоритм стану зв'язків (Link State Algorithms, LSA).

Найпоширенішим протоколом, заснованим на дистанційно-векторному алгоритмі, є протокол RIP.

Алгоритми стану зв'язків забезпечують кожний маршрутизатор інформацією, достатньої для побудови точного графа зв'язків мережі. Всі маршрутизатори працюють на підставі однакових графів, що робить процес маршрутизації більше стійким до змін конфігурації. Широкомовне розсилання використовується тут тільки при змінах стану зв'язків, що відбувається в надійних мережах не так часто. Протоколом, заснованим на алгоритмі стану зв'язків, у стеці TCP/IP є протокол OSPF.

Дистанційно - векторний протокол RIP

Протокол *RIP (Routing Information Protocol)* являє собою один з найстарших протоколів обміну маршрутною інформацією, однак він дотепер надзвичайно розповсюджений в обчислювальних мережах.

Крім версії RIPдля мереж TCP/IP, існує також версія RIP для мереж IPX/SPX компанії Novell

У цьому протоколі всі мережі мають номера (спосіб утворення номера залежить від використовуваного в мережі протоколу мережного рівня), а всі маршрутизатори - ідентифікатори. Протокол RIP широко використовує поняття "вектор відстаней". Вектор відстаней являє собою набір пар чисел, що є номерами мереж і відстанями до них у хопах.
Вектора відстаней итерационно поширюються маршрутизаторами по мережі, і через кілька кроків кожний маршрутизатор має дані про досяжні для нього мережах і про відстані до них. Якщо зв'язок з якою-небудь мережею обривається, то маршрутизатор відзначає цей факт тим, що привласнює елементу вектора, що відповідає відстані до цієї мережі, максимально можливе значення, що має спеціальний сенс - "зв'язку ні". Таким значенням у протоколі RIP є число 16.

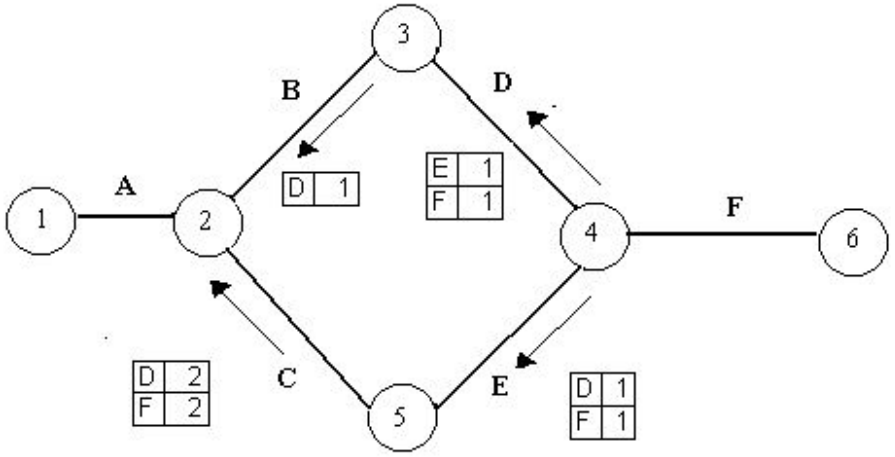
Дистанційно - векторний протокол RIP

Протокол *RIP (Routing Information Protocol)* являє собою один з найстарших протоколів обміну маршрутною інформацією.
RIPдля мереж TCP/IP
RIP для мереж IPX/SPX компанії Novell

У цьому протоколі всі мережі мають номера (спосіб утворення номера залежить від використовуваного в мережі протоколу мережного рівня), а всі маршрутизатори - ідентифікатори.

Протокол RIP широко використовує поняття "вектор відстаней". Вектор відстаней являє собою набір пар чисел, що є номерами мереж і відстанями до них у хопах.
Вектора відстаней итерационно поширюються маршрутизаторами по мережі, і через кілька кроків кожний маршрутизатор має дані про досяжні для нього мережах і про відстані до них.

Якщо зв'язок з якою-небудь мережею обривається, то маршрутизатор відзначає цей факт тим, що привласнює елементу вектора, що відповідає відстані до цієї мережі, максимально можливе значення – 16 , що має спеціальний сенс - "зв'язку ні".



Начальная информация в узле 2

Сеть	Расстояние	Сосед
A	1	-
B	1	-
C	1	-

После 2 шагов

Сеть	Расстояние	Сосед
A	1	-
B	1	-
C	1	-
D	2	3
E	2	5
D	3	5
F	3	5

Протокол OSPF

Протокол OSPF (Open Shortest Path First - вибір найкоротшого шляху першим) - сучасна реалізація стану зв'язків (прийнятий в 1991 році) і має багато особливостей, орієнтованих на застосування у великих гетерогенних мережах

Етап 1 Кожен маршрутизатор будує граф зв'язків мережі, в якому вершинами графа є маршрутизатори і IP -сети, а ребрами- інтерфейси маршрутизаторів. Сусідні маршрутизатори обмінюються сполученнями з топологічною інформацією - оголошеннями про стан зв'язків мережі(Link State Advertisements, LSA). При передачі повідомлень топологічна інформація не модифікується OSPF -маршрутизаторами, у відмінності від RIP -маршрутизаторов.Відомості про графу, які мають усі маршрутизатори, зберігаються в базі даних про топологію мережі.

Етап 2 Полягає в знаходженні оптимальних маршрутів за допомогою отриманого графа. Для вирішення цього завдання використовується ітеративний алгоритм Дейкстри. Кожен маршрутизатор вважає себе центром мережі і шукає оптимальний маршрут до кожної відомої йому мережі. При цьому використовується принцип однокрокової маршрутизації і саме дані про цей крок і подаються в таблицю маршрутизації.

Протокол OSPF

Метрика - те число, яке говорить про те, наскільки хороший цей маршрут. Це число дозволяє порівняти його з іншими маршрутами, ведучими до того ж місцю призначення і що забезпечує той же рівень QoS.

Метрики для протокола OSPF:
- пропускна спроможність, це метрика, використовувана за умовчанням;
- затримки;
- надійність передачі пакетів каналами зв'язку.

Для кожної метрики протокол OSPF будує окрему таблицю.При виборі оптимального шляху на графі з кожним ребром графа пов'язана метрика, яка додається до шляху, якщо це ребро в нього входить. Обчислювальна складність протоколу OSPF швидко росте із збільшенням розмірності мережі. Для подолання цього недоліку в протоколі OSPF вводитися поняття - **області мережі (или аутономні системи).**

Протокол BGP, EGP

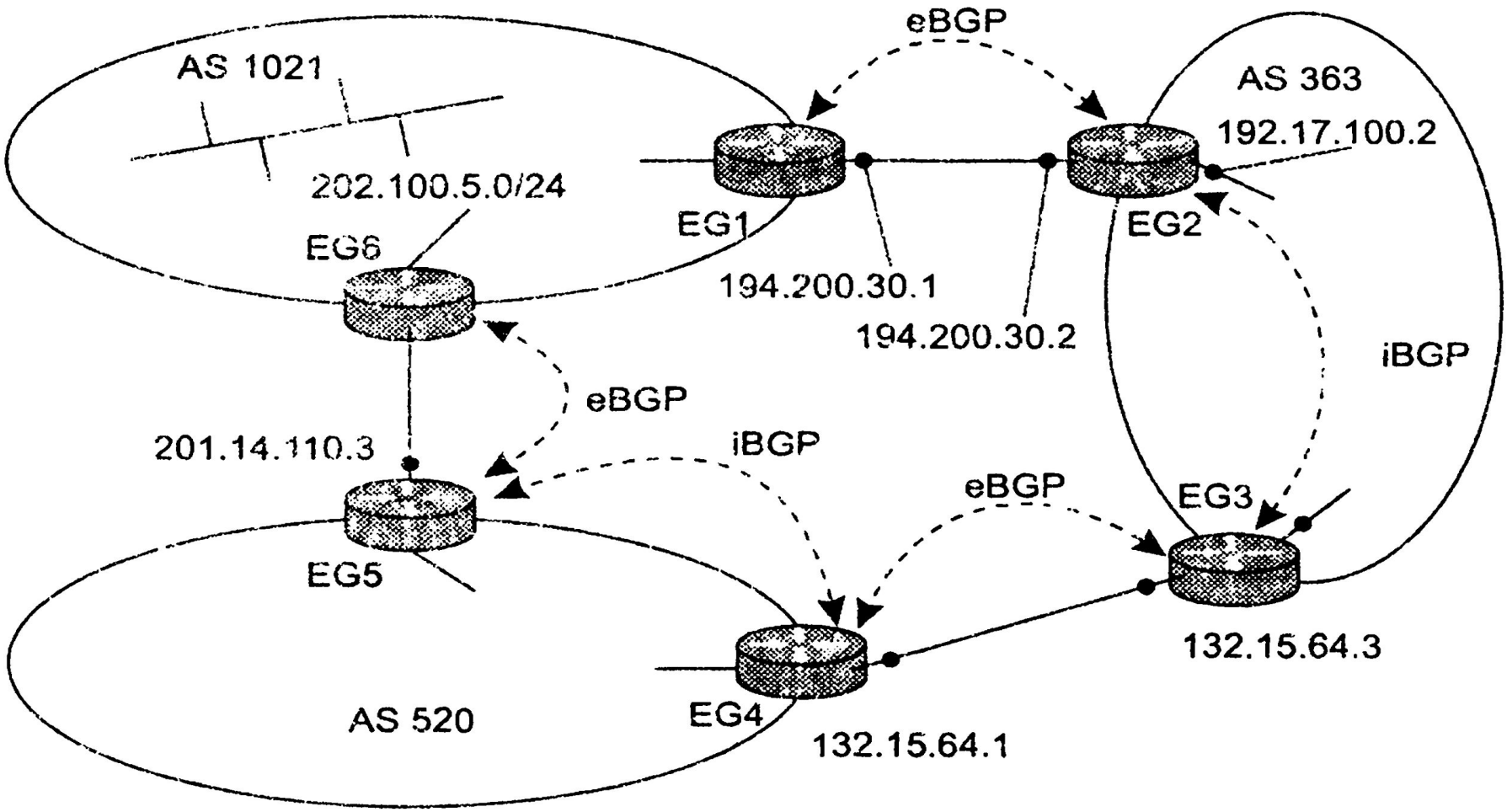
EGP (сокр. від англ. Exterior Gateway Protocol, протокол зовнішнього шлюзу) - застарілий протокол обміну інформації між маршрутизаторами декількох автономних систем. Розроблений в 82-84 роках. Згодом був замінений на BGP.

BGP є протоколом прикладного рівня і функціонує поверх протоколу транспортного рівня TCP (порт 179).
BGP, разом з DNS, є одним з головних механізмів, що забезпечують функціонування Internet.

BGP не використовує технічні метрики, а здійснює вибір найкращого маршруту виходячи з правил, прийнятих в мережі.
BGP підтримує безкласову адресацію і використовує підсумовування маршрутів для зменшення таблиць маршрутизації. З 1994 року діє четверта версія протоколу, усі попередні версії є застарілими.

Протокол BGP

Протокол BGP:



Таблиця маршрутизації. Маршрутизація у IP мережах на базі ОС Windows xx

Два способи модифікації запису в таблицях маршрутизації на IP – маршрутизаторах

■ Вручну. На статичних IP -маршрутизаторах таблиці залишаються незмінними до тих пір, поки їх не модифікує мережевий адміністратор. Статична маршрутизація заснована на адмініструванні таблиць маршрутизації вручну. Статичні маршрутизатори не забезпечують стійкість до збоїв.

■ Автоматично. На динамічних IP -маршрутизаторах таблиці змінюються автоматично за рахунок обміну інформацією з іншими маршрутизаторами. Використовуються маршрутизуючі протоколи, наприклад RIP і OSPF,Динамічні маршрутизатори забезпечують стійкість до збоїв.

Таблиця маршрутизації.
Значення записів в таблиці маршрутизації
Host 157.55.27.90/20, - Шлюз – 157.55.16.1/20

Мережевий адрес	**Маска мережи**	**Адрес шлюза**	**Інтерфейс**	**Метрика Описа**
0.0.0.0	0.0.0.0	157.55.16.1	157.55.27.90	1 Маршрут за умовчанням
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1 Поворотнамережева адреса
157.55.16.0	255.255.240.0	157.55.27.90	157.55.27.90	1 Напрямую підключена мережа
157.55.27.90	255.255.255.255	127.0.0.1	127.0.0.1	1 Локальний хост
157.55.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1 Адреса широкомовної розсилки
224.0.0.0	224.0.0.0	157.55.27.90	157.55.27.90	1 Адреса групової розсилки
255.255.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1 Адреса обмеженої широкомовної розсилки

Таблиця маршрутизації. Значення записів в таблиці маршрутизації

Мережева адреса. Як цей параметр може бути вказаний ідентифікатор мережі (на основі класу, а також з ідентифікатором підмережі або надсети) або IP - адреса хоста-получателя**.**

Маска мережі. Використовується для порівняння IP -адреса призначення з ідентифікатором мережі.
Наступний перехід (чи шлюз). Наступний проміжний IP -адрес.

Інтерфейс. IP -адрес, відповідний мережевому інтерфейсу (мережевому адаптеру), по якому треба переслати IP -пакет.

Метрика. Значення, що показує "ціну" маршруту; зазвичай виражається числом переходів (тобто кількістю маршрутизаторів, що перетинаються) до кінцевої мережі. Якщо до адресата веде декілька маршрутів, вибирається той, у якого мінімальна метрика.

Таблиця маршрутизації.
Значення записів в таблиці маршрутизації

Ідентифікатор безпосередньо підключеної мережі. Маршрут до мережі, підключеної безпосередньо. Для таких мереж поле наступного переходу може бути порожнім або со- тримати IP -адрес локального мережевого адаптера.

Ідентифікатор видаленої мережі. Маршрут до мережі, не підключеної безпосередньо, але доступною через інші маршрутизатори. Для таких мереж поле наступного переходу може містити IP -адрес локального маршрутизатора, що знаходиться між пересилаючим вузлом і видаленою мережею.

Маршрут до хосту. Шлях до конкретному IP -адресу. У маршрутах до хостам ідентифікатор мережі являється IP -адресом вказаного хоста, а маска мережі дорівнює 255.255.255.255.

Маршрут за умовчанням. Використовується в тих випадках, коли знайти конкретний ідентифікатор мережі або маршрут до хосту не вдається. У маршрутах за умовчанням ідентифікатор мережі є значенням 0.0.0.0, а маска - 0.0.0.0.

Висновки

- Найбільш поширеними видами мультиплексування є TDM, WDM, FDM.
- Найбільш поширеними видами комутації є канальна, повідомлень, пакетна.
- Найефективніша комутація будується на основі пакетної.
- Існує два способи передачі даних по усій мережі: віртуальний канал, дейтаграммный.
- Технологія VPN використовується для захисту приватної мережі від зовнішнього доступу при використанні загальних каналів в Інтернет.
- Найбільш використовуваними протоколами для VPN є L2TP і PPTP.
- Безпека мереж VPN забезпечується іншими протоколами, наприклад, IPSec.

Висновки

- Основним методологічним рішенням для доставки повідомлень в складній мережі являється маршрутизація.
- Маршрут - це ланцюжок пов'язаних послідовно вузлів.
- У більшості мереж існую т альтернативні маршрути
- Маршрути вибираються на підставі певних показників.
- Алгоритми маршрутизації діляться на прості, з фіксованим маршрутом, адаптивні.
- Практичні реалізації алгоритмів ділять на дистанційно-векторних і алгоритми стану зв'язків.
- Найбільш поширеним є алгоритм RIP
- При складних метриках використовують протоколи OSPF.
- Додаткові алгоритми і протоколи - BGP, EGP, IGRP, EIGRP.
- Основним елементів маршрутизації на локальному комп'ютері являється таблиця маршрутизації.

Питання

- Що таке комутація?
- Що таке мультиплексування?
- По яких параметрах здійснюють розподіл для мультиплексування?
- Що таке частотне мультиплексування? Де воно використовується?
- Що таке статистичне мультиплексування? Де воно використовується?
- Що таке тимчасове мультиплексування? Де воно використовується?
- Що таке хвильове мультиплексування? Де воно використовується?
- Чим відрізняється синхронні і асинхронний режим мультиплексування? Приклад.
- Перерахуєте завдання комутації.
- Що таке комутація каналів?
- Що таке комутація повідомлень?
- Що таке комутація пакетів?
- Що таке дейтаграмная передача?
- Що таке передача "віртуальний канал"?
- Порівняти комутацію каналів і комутацію пакетів.
- Що таке VPN?
- Які протоколи використовуються для організації VPN?
- Наведіть приклад класифікації з'єднань по VPN.

Питання за лекційним матеріалом

Класифікація алгоритмів маршрутизації
Адаптивні алгоритми
Алгоритм RIP
Які методи маршрутизації використовуються?
Як працює протокол RIP?
Що таке маршрут?
Що таке таблиця маршрутизації?
Чому в процесі просування пакету по мережі MAC адреса міняється, а IP адреса залишається незмінною?
На які параметри передачі даних впливає вибір маршруту передачі?
Від чого може змінитися стан комп'ютерної мережі?
Наведіть приклад класифікації алгоритмів маршрутизації.
Охарактеризуйте прості алгоритми маршрутизації і алгоритми з фіксованими маршрутами.
У яких завданнях або випадках використовують прості алгоритми маршрутизації. Наведіть приклад.
У яких завданнях або випадках використовують адаптивні алгоритми маршрутизації. Наведіть приклад.
Охарактеризуйте адаптивні алгоритми маршрутизації і алгоритми з фіксованими маршрутами.
У чому перевага і недолік використання адаптивних алгоритмів?

Література

1. Олифер В., Олифер Н. Комп’ютерні мережі. Принципи, технології, протоколи.\ - ред. 3, ред.4, СПб.: Пітер. 2005, 2010 - 672 с.
2. Сталлингс В. Комп’ютерні мережі, протоколи та технології Інтернету. – СПб.: БХВ-Петербург, 2005. -832 с
3. Спортак М., Паппас Ф. Комп’ютерні мережі та мережеві технології. СПб: ООО"ДИА-СОФТ", 2005. - 720 с
4. Палмер М., Синклер Р. Проектування та впровадження комп’ ютерних мереж. Уч. Пособ. – 2е вид. – СПб.: БХВ-Петербург, 2005. -752 с
5. Столлингс В. Комп’ютерні системи передачі даных\6-е видання - М.: Видавничий дім Вільямс, 2002. - 928 с.

Інтернет ресурси

http://citforum.univ.kiev.ua/nets/glossary/_terms.shtml

http://citforum.univ.kiev.ua/nets/tpns/contents.shtml

http://citforum.univ.kiev.ua/nets/semenov/

http://citforum.univ.kiev.ua/nets/protocols/index.shtml