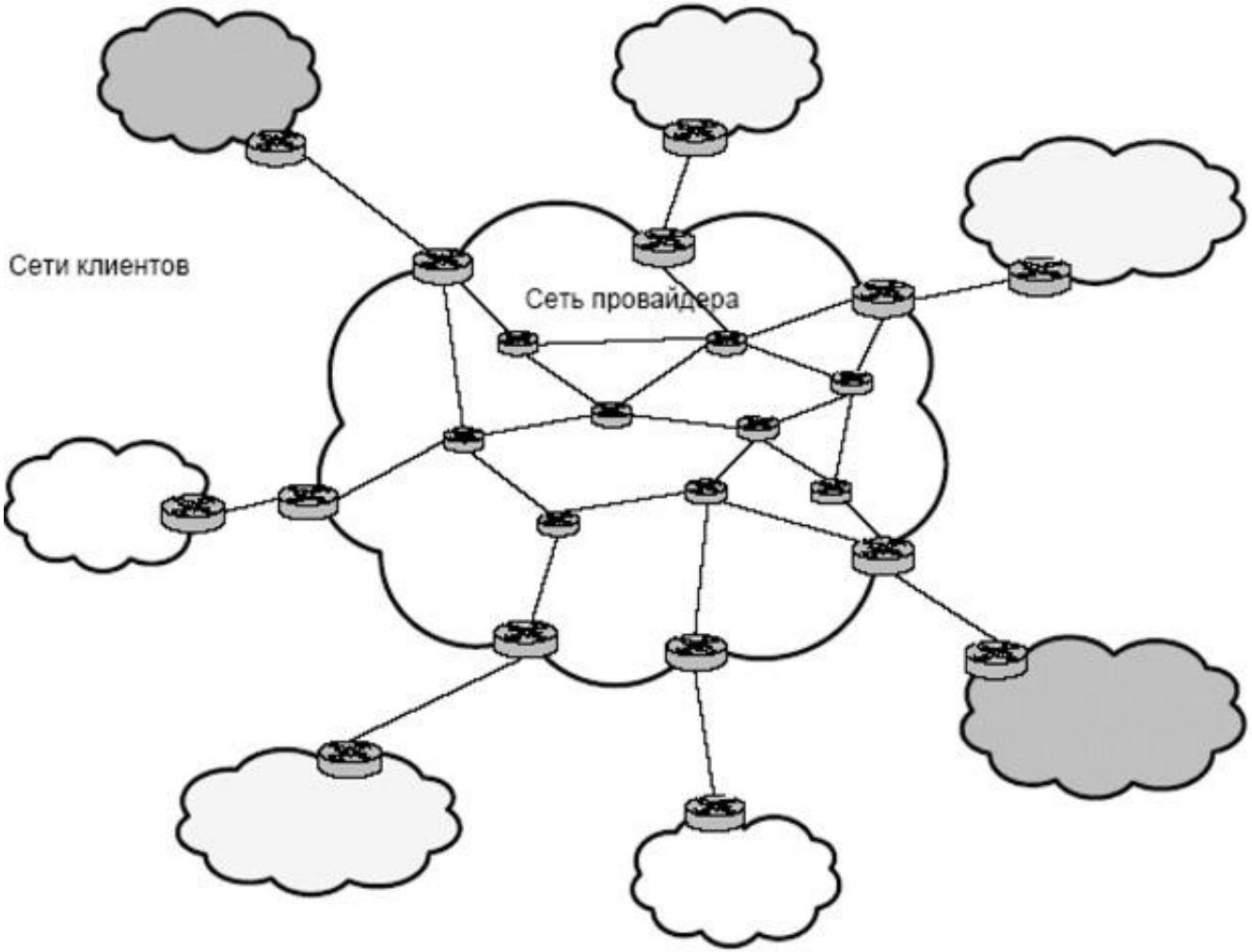
ПРОЕКТУВАННЯ ВІРТУАЛЬНОЇ ПРИВАТНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ МОСТІВ ПРОВАЙДЕРА

Виконав:ст. гр. ТСМ-14м
Заяць В.В.
Керівник: к.т.н., доц.
Гикавий В.А.

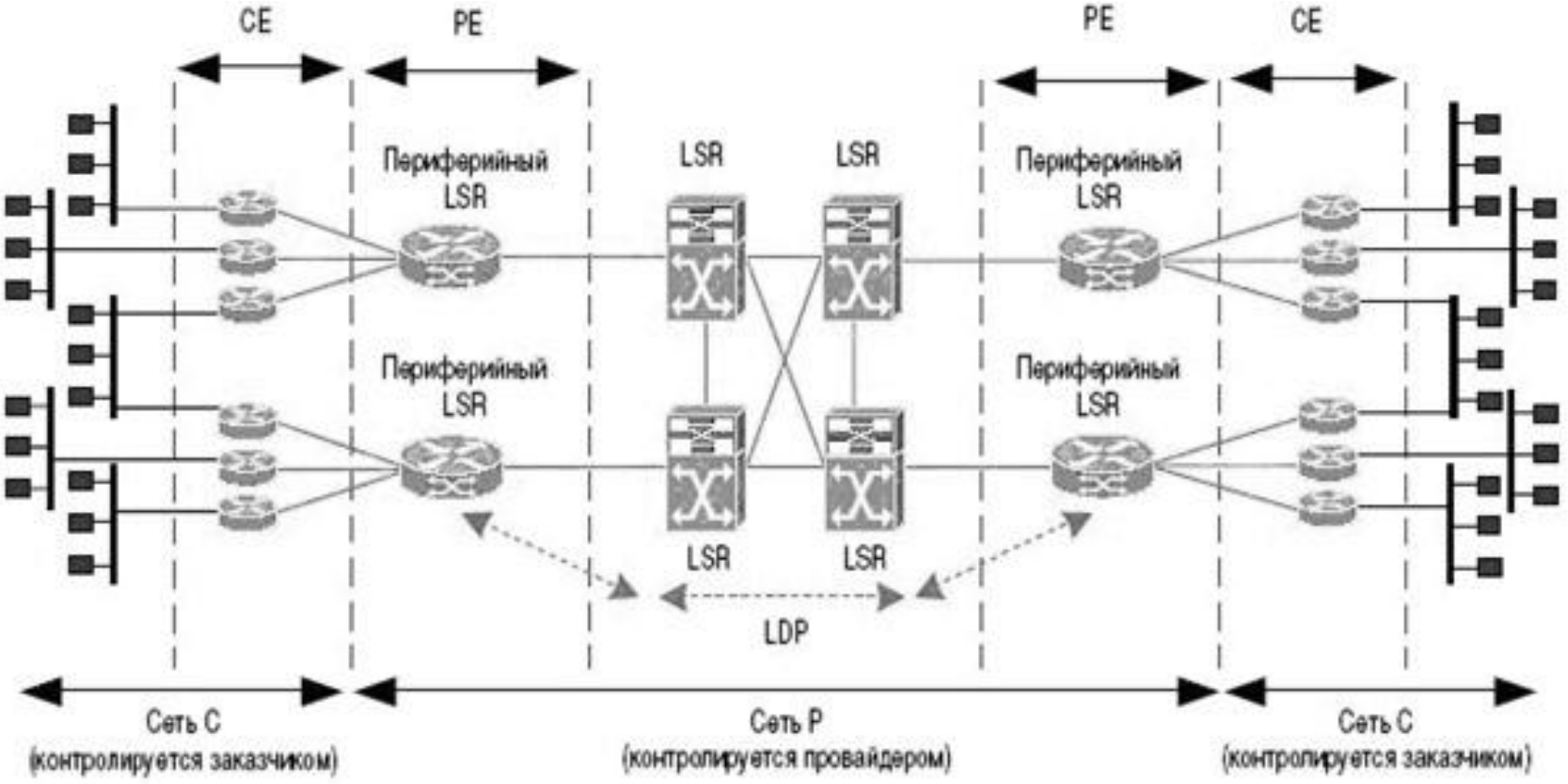
Властивості приватної мережі

- **Изольованість від інших мереж.**
- **Незалежний вибір смережевих технологій: вибір обмежується лише можливостями виробників обладнання.**
- **Незалежна система адресації. У приватних мережах немає обмежень на вибір адрес: вони можуть бути будь-якими.**
- **Передбачувана продуктивність. Власні канали зв'язку гарантують заздалегідь відому пропускну спроможність між вузлами підприємства (для глобальних з'єднань) або комунікаційними пристроями (для локальних з'єднань).**
- **Максимально можлива безпеку. Відсутність зв'язків із зовнішнім світом убезпечує від атак ззовні і істотно знижує ймовірність "прослуховування" трафіку по шляху слідування.**

Загальний варіант проектування VPN



Компоненты MPLS VPN



Customer Edge Router, CE – граничний маршрутизатор клієнта
Provider Router, P – внутрішній маршрутизатор магістральної мережі провайдера
Provider Edge Router, PE – граничний маршрутизатор мережі провайдера

Протоколи маршрутизації PE

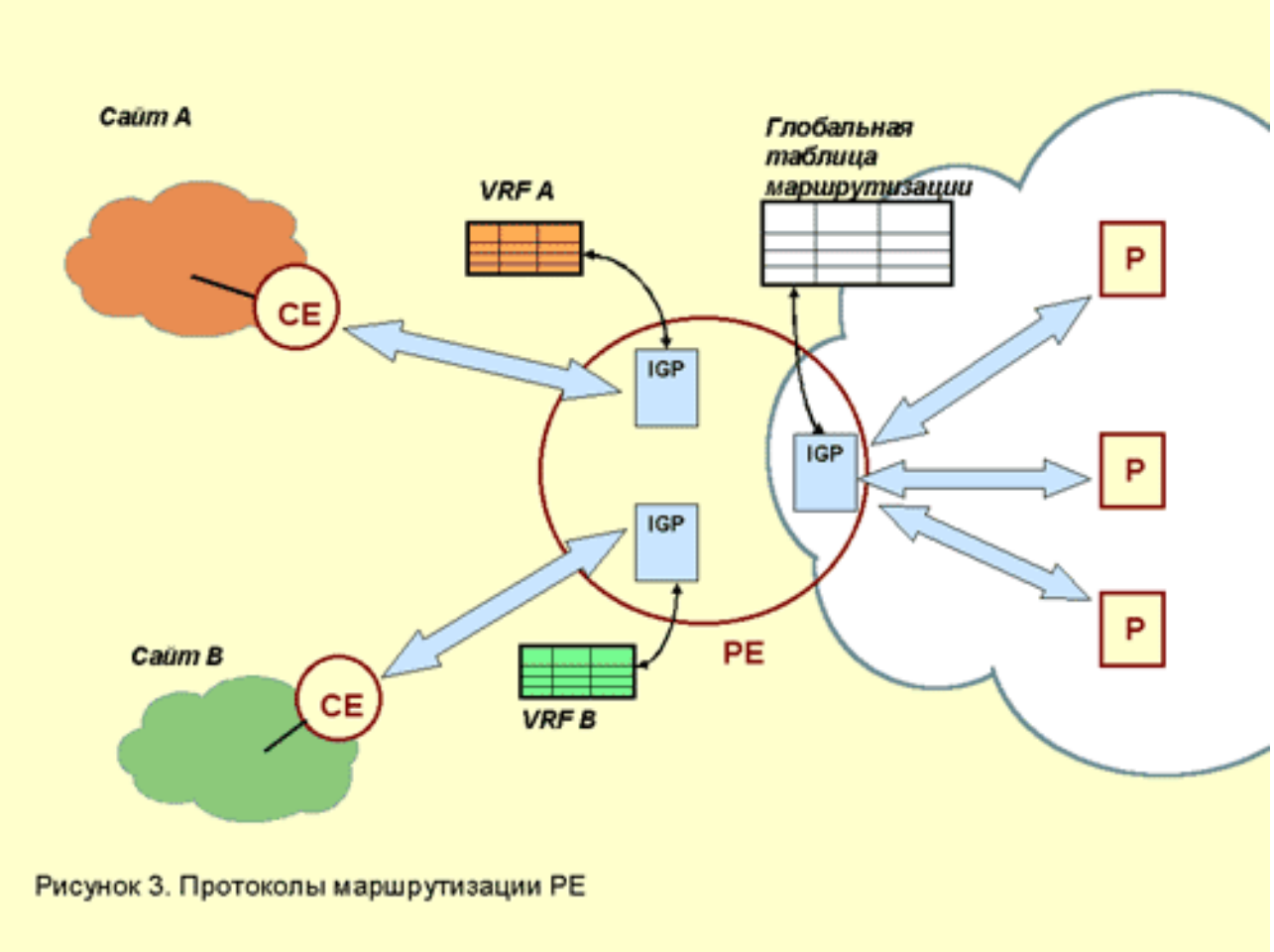


Рисунок 3. Протоколы маршрутизации PE

VRF - VPN Routing and Forwarding

Маршрут пакета VPN

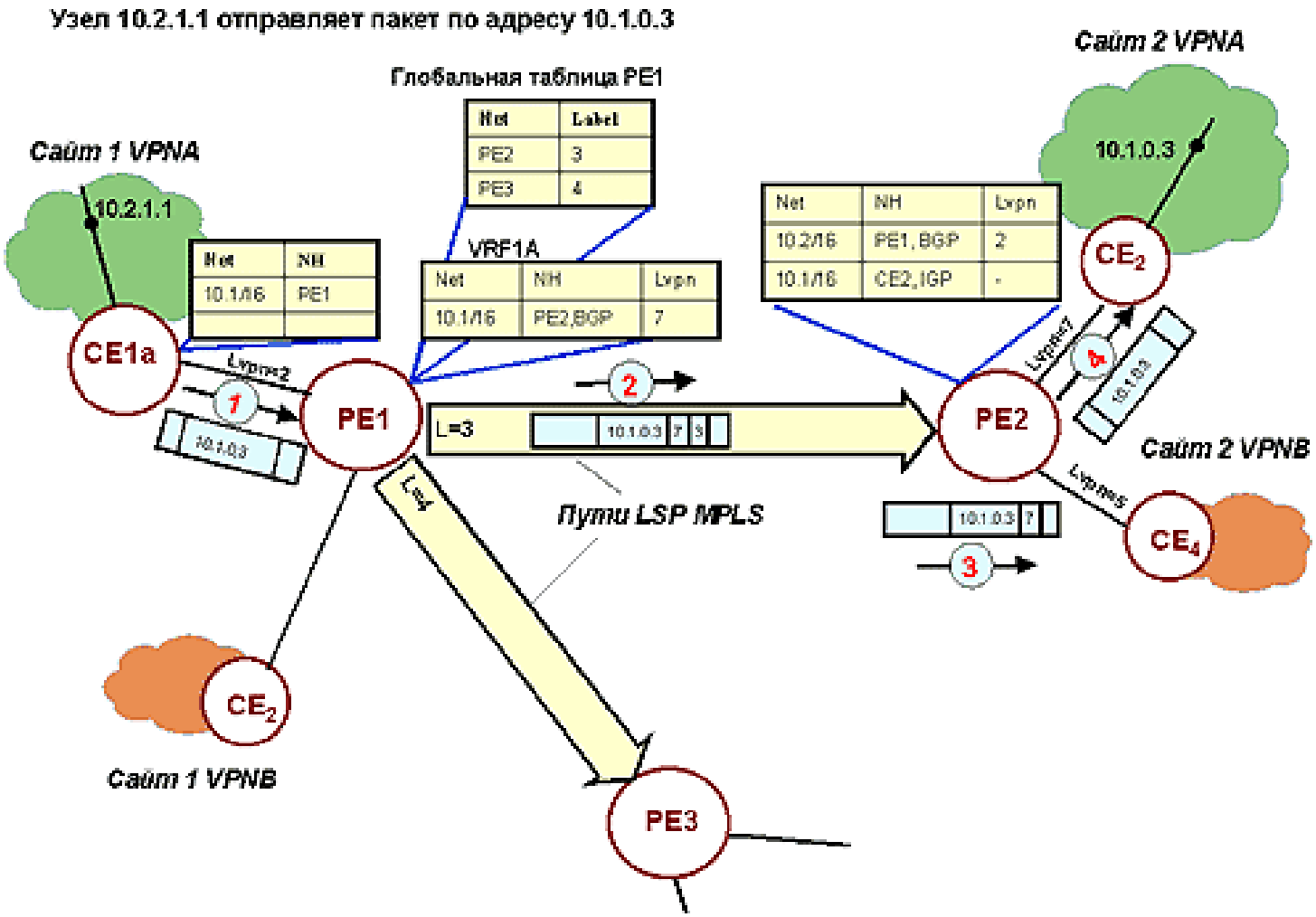


Рисунок 6. Путешествие пакета между сайтами VPN

Способи утворення захищених віртуальних каналів

- Будь-який з двох вузлів віртуальної мережі, між якими формується захищений тунель, може належати кінцевій чи проміжній точці потоку повідомлень, який захищають. Відповідно можливі різні способи утворення захищеного віртуального каналу.
  - кінцеві точки тунелю співпадають з кінцевими точками потоку повідомлень
  - кінцевою точкою захищеного тунелю обирають брандмауер або граничний маршрутизатор локальної мережі, захищений тунель утворюється лише у публічній мережі
  - в якості кінцевих точок захищеного тунелю виступають засоби, що встановлені не на комп'ютерах користувачів, а на площах провайдерів Інтернет

Кінцеві точки тунелю співпадають з кінцевими точками потоку повідомлень

- Цей варіант є найкращим з міркувань безпеки
- Приклади кінцевих точок:
  - сервер у центральному офісі компанії і робоча станція користувача у віддаленій філії
  - портативний комп’ютер співробітника, який перебуває у відрядженні
- Перевагою такого варіанту є те, що захист інформаційного обміну забезпечується на всьому шляху пакетів повідомлень
- Суттєвий недолік цього варіанту – децентралізація керування
  - Засоби утворення захищених тунелів повинні встановлюватись і належним чином налаштовуватись на кожному клієнтському комп’ютері, що у великих мережах є занадто трудомісткою задачею

Кінцева точка захищеного тунелю – брандмауер або граничний маршрутизатор локальної мережі

- Захищений тунель утворюється лише у публічній мережі
- Якщо відмовитись від захисту трафіка всередині локальної мережі (або локальних мереж), що входить до складу VPN, можна досягти помітного спрощення задач адміністрування
  - Захист трафіка всередині локальної мережі може забезпечуватись іншими засобами, такими, як, наприклад, реєстрація дій користувачів і організаційні заходи

Рівні реалізації VPN

- Реалізація VPN можлива засобами протоколів
  - Сеансового рівня (SSL/TLS, SOCKS)
  - Мережного рівня (IPsec)
  - Канального рівня (PPTP, L2TP)
- Поза розглядом залишаються системи шифрування на прикладному рівні, які реалізуються у деяких протоколах (SHTTP тощо), або просто деякими спеціальними прикладними програмами (наприклад, PGP)
  - Зазначені засоби здатні забезпечити захист інформаційного обміну, але вони
    - не є прозорими для прикладних програм
    - як правило, вони не забезпечують усіх необхідних функцій
    - вони не відносяться до засобів утворення VPN

Захист віртуальних каналів на канальному рівні

- Утворення захищених тунелів на канальному рівні моделі OSI забезпечує незалежність від протоколів мережного рівня і всіх вищих рівнів
  - Таким чином досягається максимальна прозорість VPN
- Недоліки:
  - Ускладнюються задачі конфігурації і підтримки віртуальних каналів
  - Ускладнюється керування криптографічними ключами
  - Зменшується набір реалізованих функцій безпеки
- В якості протоколів на цьому рівні використовуються:
  - PPTP (англ. – *Point-to-Point Tunneling Protocol*)
  - L2F (англ. – *Layer-2 Forwarding*)
  - L2TP (англ. – *Layer-2 Tunneling Protocol*)
- Усі названі протоколи не специфікують протоколи автентифікації та шифрування

Висновок

Створена мережа є дещо ідеалізованою, так як не враховує всіх особливостей елементів і їх параметрів та не враховує фактори зовнішнього середовища.