Комп’ютерні мережі, проміжний контроль

**I-рівень**

1.Головними різницями між 2.4 і 5.0 GHz це є:

1) Швидкість передачі сигналу.

2)Площа покриття.

Якщо говорити про швидкість , то тут повністю виграє 5-ти герцова частота. Завдяки малій завантаженості радіоефіру і 17-ти каналам ( як мінімум) сигнал швидше "йде" до користувача.

А ось діапазон в 2.4 Ггц має лише три канали і тому сигнали точок доступу часто плутаються та заважають один одному.

А вот у плані площі покриття, то тут 2.4Ггц має значно більшу дальність розповсюдження сигналу. Їй, на відмінну від сигналу на частоті 5Ггц, не заважають стіни,стелі, двері або щось інше. На частоті 5Ггц сигнал залежить не тільки від товщини перешкоди , а й від кута між перешкодою та роутером. Через те , що 5Ггц сигнал далеко не йде, він не плутається з іншими сигналами.

2. NAT - це технологія, яка забезпечує зв'язок між глобальною та локальною мережею за допомогою пристрою маршрутизації, який дозволяє перетворювати IP-пакети. За допомогою цього група комп’ютерів може функціонувати по одній зовнішній адресі. NAT також допомагає поліпшити комп'ютерну безпеку та спростити адміністрацію. Іншими словами NAT переводить приватні адреси в загальнодоступні.

3.iptables - це утиліта для настройки програмного firewall'а (брандмауера) Linux, яка встановлюється за замовчуванням в усі збірки Linux, починаючи з версії 2.4. Запускається iptables з командного рядка (CLI) під користувачем з правами root і налаштовується там же.

4. TCP/IP – це абревіатура терміну Transmission Control Protocol / Internet Protocol (Протокол керування передачею / міжмережевий протокол) . Фактично TCP/IP не один протокол, а декілька. Саме тому його часто називають набором, або комплектом (стеком) протоколів, серед яких TCP і IP – два основні. Фактично TCP/IP представляє цей базовий набір протоколів, відповідальний за розбивання вихідного повідомлення на пакети (TCP), доставку пакетів на вузол адресата (IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP).

5. Модель Open Systems Interconnection (OSI) - це скелет, фундамент та база даних всіх мережевих об'єктів. Модель визначає мережеві протоколи шляхом розповсюдження до 7 логічних рівнів.

1. Прикладний рівень
2. Рівень представлення
3. Сеансовий рівень
4. Транспортний рівень
5. Мережевий рівень
6. Канальний рівень
7. Фізичний рівень

Важливо відзначити, що в будь-якому процесі, управління мережевою передачею переходить від рівня до рівня, послідовно підключаючи протоколи на кожному з рівнів.

6. Відмінності між моделлю OSI та tcp/ip протоколом:

1) TCP / IP є клієнт-серверною моделлю, тобто коли клієнтські запити на обслуговування надаються сервером. Тоді як OSI є концептуальною моделлю.

2) TCP/IP - чотиришарова модель, а OSI має сім шарів.

3) TCP/IP - це стандартний протокол, який використовується для кожної мережі, включаючи Інтернет, тоді як OSI не є протоколом, а еталонна модель, яка використовується для розуміння та розробки архітектури системи.

4) TCP / IP слідує за вертикальним підходом , а модель OSI підтримує горизонтальний підхід.

5) TCP / IP матеріальна, а ISO ні.

6) TCP / IP наближається до підходу зверху вниз, тоді як модель OSI має підхід знизу-вгору.

7) TCP / IP це протокол керування передачею / Інтернет-протокол, модель OSI це відкрита система Interconnect.

8) TCP / IP наданний момент використовується, ISO ні.

7. MAC-адреса - це один двійковий код, який має доступ до мережі. Його присвоюють мережевій карті в ході виготовлення, тому це адреса карти, а не всього комп'ютера.

Коли провайдер підключає нового користувача, він закріплює його MAC-адресу в системі і поставляє трафік згідно встановленого пакета саме на нього. Прив'язка до MAC-адресу потрібна для побудови мережі і стане в нагоді, якщо якась жадна людина захоче скористатися інтернетом сусіда.

8. Default gateway(основний шлюз) – часто називаємий маршрутизатором IP шлюз, що з'єднує дві або більше мережі або підмережі і дозволяє передавати дані з однієї мережі в іншу. Використаний по замовчуванні шлюз являється маршрутизатором для локальної підмережі. Шлюз задається записом в таблиці маршрутизації виду «мережа 0.0.0.0 з маскою мережі 0.0.0.0».

**II-рівень**

1. Спочатку клієнт робить запит на локальний DNS сервер, наприклад, в адресному рядку браузера ви набрали адресу сайту. Потім якщо локальний DNS містить даний запис, то він дає відповідь, тобто браузер отримає IP адресу сайту, і звернеться до нього. Якщо в локальному DNS, немає потрібного запису, то він звертається до наступного DNS сервера, і так, до тих пір, поки запис не знайдеться.

2. Це можливо зробити за допомогою Resubnetting. Це рекомендована процедура для збільшення області DHCP, коли поточна область повністю споживає поточну маску підмережі. Цей метод вимагає зміни всіх хостів і шлюзів підмереж. Всі області або області DHCP спочатку повинні бути видалені, а потім повторно створені за допомогою нової підмережі маски. Конфігурація повторної мережі не створює додаткових накладних витрат на маршрутизатори або шлюзи підмережі і зберігає всі хости на одному і тому ж адресу трансляції.

Приклад:

Адреса підмережі: 192.168.1.0

Маска subnet: 255.255.255.0

Вона дає мережу з 254 хостів з адресами від 192.168.1.1 до 1921.68.1.254.

У наступному прикладі показаний результат при використанні параметра resubnetting:

Адреса підмережі: 192.168.1.0

аска subnet: 255.255.254.0

Тепер у вас є мережа з 510 хостів з адресами від 192.168.0.1 до 192.168.1.254 (для області 192.168.0.0) або 256 знову доступних адрес DHCP