**Лабораторная работа № 3. Настройка отказоустойчивого DHCP-сервера на базе ОС Windows Server 2019.**

**Цель:** освоить навык организации отказоустойчивой динамической адресации в сетевых информационных системах на базе операционных систем Windows.

**Задачи:**

1. назначить сетевым адаптерам двух ОС Windows Server IP-адреса в соответствии с вариантом (см. табл.);
2. внимательно проверьте подключение кабелей и в параметры сети в настройках виртуальных машин – **ни в коем случае не включайте DHCP-серверы в общеуниверситетскую сеть**;
3. установить роль DHCP-сервера на две ОС Windows Server;
4. выбрать главный DHCP-сервер и создать на нем область с соответствии с вариантом (см. табл.); второй DHCP-сервер будет резервным;
5. создать на двух ОС Windows Server одинаковые учетные записи пользователя с именем и паролем, состоящими из латинских букв и цифр;
6. назначить одинаковые настройки времени на двух ОС Windows Server;
7. войти на главный DHCP-сервер под созданной учетной записью и создать резервирование области на резервный DHCP-сервер;
8. подключить в сеть еще одну ОС семейства Windows, которая будет выполнять роль клиентской; для этого в свойствах сетевого адаптера должно быть указанно автоматическое получение сетевых параметров; убедиться в успешном получении IP-адреса утилитой ipconfig.

Таблица

**Варианты заданий для лабораторной работы № 3**

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Имя хоста | Scope (диапазон IP-адресов) | IP-адрес хоста |
| 1 | Server1\_1 | 10.90.90.3–10.90.90.9  маска 255.255.255.0 | 10.90.90.1 |
| Server1\_2 | 10.90.90.2 |
| Client1\_1 | любой из scope |
| Client1\_2 | любой из scope |
| 2 | Server2\_1 | 10.90.90.12–10.90.90.19  маска 255.255.255.0 | 10.90.90.10 |
| Server2\_2 | 10.90.90.11 |
| Client2\_1 | любой из scope |
| Client2\_2 | любой из scope |
| 3 | Server3\_1 | 10.90.90.22–10.90.90.29  маска 255.255.255.0 | 10.90.90.20 |
| Server3\_2 | 10.90.90.21 |
| Client3\_1 | любой из scope |
| Client3\_2 | любой из scope |
| 4 | Server4\_1 | 10.90.90.32–10.90.90.39  маска 255.255.255.0 | 10.90.90.30 |
| Server4\_2 | 10.90.90.31 |
| Client4\_1 | любой из scope |
| Client4\_2 | любой из scope |
| 5 | Server5\_1 | 10.90.90.42–10.90.90.49  маска 255.255.255.0 | 10.90.90.40 |
| Server5\_2 | 10.90.90.41 |
| Client5\_1 | любой из scope |
| Client5\_2 | любой из scope |
| 6 | Server6\_1 | 10.90.90.52–10.90.90.59  маска 255.255.255.0 | 10.90.90.50 |
| Server6\_2 | 10.90.90.51 |
| Client6\_1 | любой из scope |
| Client6\_2 | любой из scope |

**Порядок защиты лабораторной работы.**

1. Продемонстрировать в сниффере передаваемые между DHCP-сервером и DHCP-клиентом пакеты.
2. Определить, какие пакеты являются широковещательными.
3. Определить, в каких свойствах каких пакетов передается назначаемый клиенту IP-адрес и маска подсети.
4. С помощью утилиты ipconfig определить DHCP-сервер, назначивший адрес DHCP-клиенту.
5. Отключить DHCP-сервер, назначивший адрес DHCP-клиенту, запросить и получить адрес от второго DHCP-сервера.