

1. [Обзор протокола DHCP.](#)
2. [Установка в сети протокола DHCP.](#)
3. [Функции и конфигурирование протокола DHCP](#)
4. [Различия между протоколами BOOTP и DHCP.](#)

### **Обзор протокола DHCP.**

DHCP (Dynamic Host Configuration Protocol) – это сетевая служба и протокол Прикладного уровня. TCP/IP, позволяющий сетевым администраторам настраивать серверы таким образом, чтобы они осуществляли распределение и управление группами IP-адресов рабочих станций, настольных компьютеров и других клиентских машин, не требующих присвоения фиксированных IP-адресов. По мере того, как организации растут и количество компьютеров, требующих администрирования, увеличивается, протокол DHCP быстро перестает быть предметом роскоши и становится необходимым инструментом.

Компания Microsoft всегда вкладывала в службу DHCP значительные средства, рассматривая ее как ключевой компонент управления конфигурационными данными протокола IP для большого количества систем. DHCP-серверы способны управлять одним или несколькими диапазонами IP-адресов, каждый из которых можно назвать адресным пулом или областью адресов. В пределах каждой отдельной области IP-адресов служба DHCP может выделить отдельные адреса или совокупности адресов, которые не должны распределяться между клиентскими машинами. Это позволяет DHCP координировать существующие диапазоны IP-адресов, некоторые из которых могут быть уже присвоены маршрутизаторам и серверам. По требованию клиентов служба DHCP может осуществлять распределение оставшихся неприсвоенных адресов, причем каждое такое присвоение называется выделением адреса или просто выделением.

### **Установка в сети протокола DHCP.**

Большинство сетевых проектов разрабатывают на основе протокола IP. Для работы с этим протоколом все компьютеры следует сконфигурировать соответствующим образом. При большом количестве компьютеров в сети повышается вероятность возникновения ошибок в конфигурации IP, а также увеличивается время на настройку и администрирование. Основная задача проекта обеспечить корректное конфигурирование IP на всех компьютерах частной сети организации. Прежде чем создавать проект, надо определить метод конфигурирования IP на каждом компьютере. Для этого разработано несколько методов:

а) конфигурирование вручную, годится для файловых серверов, серверов печати, маршрутизаторов, шлюзов и других сетевых устройств, предоставляющих ресурсы и службы клиентам. Автоматическая настройка IP применяется для компьютеров, которые не управляют сетевыми ресурсами, например, для настольных компьютеров. Это снижает вероятность ошибок в конфигурации и снижает административные издержки.

б) службы DHCP операционных систем сторонних производителей. DHCP-сервер входит в состав большинства современных операционных систем, в том числе Novell Netware и Unix.

в) службы DHCP в составе Windows 2000. Может поддерживать клиентов с другой операционной системой. Их используют, если:

- Windows 2000 является корпоративным стандартом;
- требуется исключить ошибки конфигурирования, обусловленные неавторизованными DHCP-серверами;
- в качестве службы каталогов необходимо использовать Active Directory;
- требуется интеграция с DNS-серверами и со службой RRAS.

Автоматическое конфигурирование IP - это важная часть любого проекта сетевых служб. Успех или провал проекта во многом зависит от ресурсов, необходимых для его поддержки. Поэтому снижение вероятности возникновения ошибок в конфигурации IP и сокращение времени на администрирование существенно повышает ценность проекта. Один из способов достичь этого результата - автоматическая настройка IP. DHCP - это протокол, представляющий собой отраслевой стандарт и позволяющий выполнять автоматическую настройку IP-конфигурации компьютеров. Служба DHCP в Windows 2000 состоит из трех компонентов:

а) клиент DHCP - это неотъемлемый компонент реализации протокола IP в Windows 2000. Он изменяет конфигурацию компьютера в соответствии с параметрами IP, полученными от DHCP-сервера, входит в состав любой операционной системы.

б) сервер DHCP - назначает параметры IP клиентам DHCP. Это обычная служба Windows 2000. Она управляет своей локальной базой данных IP адресов.

в) агент ретрансляции DHCP - это протокол, который является компонентом службы RRAS. Он обеспечивает пересылку DHCP-сообщений через маршрутизатор. Компьютеру с агентом ретрансляции следует назначать постоянные IP-адреса. Нельзя устанавливать сервер DHCP и агент ретрансляции на одном компьютере.

### **Функции и конфигурирование протокола DHCP**

1) Определение сегментов, для которых требуется автоматическая настройка IP.

Автоматическую настройку IP следует применять во всех сетевых сегментах, за исключением:

- сегментов сети, в которых есть только компьютеры, управляющие сетевыми ресурсами. Управляющие сетевыми ресурсами компьютеры, такие, как файловые серверы, серверы печати, баз данных и Web-серверы, должны иметь постоянные IP-адреса. Они назначаются вручную.
- опорных сегментов, которые содержат только маршрутизаторы, соединяющие другие сегменты сети с опорной сетью.
- сегментов с соединениями через глобальные (WAN) сети. Для сохранения пропускной способности WAN-соединения необходимо избегать его перегрузки ненужным трафиком.

- защищенных подсетях. Они содержат ресурсы, доступные только определенным пользователям. В целях безопасности DHCP-серверы не размещаются в защищенных подсетях.

В остальных случаях для настольных компьютеров можно использовать автоматическую конфигурацию IP.

2) Определение метода автоматической настройки IP. чтобы обеспечить автоматическую настройку IP, для каждого сетевого сегмента необходимо выбрать один из методов:

а) DHCP-сервер. В каждом географическом сегменте должен быть хотя бы один сервер DHCP. Один сервер DHCP поддерживает 15000 количеств. Дополнительные серверы обычно ставят для повышения доступности и производительности.

б) Агенты ретрансляции DHCP. Они устанавливаются в сегментах, которые не соединены непосредственно с DHCP-сервером. Они принимают широковещательные пакеты, преобразуют запросы в одноадресные пакеты и пересылают конкретному DHCP-серверу. Один агент поддерживает 1000 компьютер клиентов.

в) Включение пересылки DHCP/BOOTP на маршрутизаторе. BOOTP - Bootstrap Protocol - протокол загрузки - обеспечивает бездисковым рабочим станциям возможность получения сетевого доступа и образа операционной системы во время загрузки. Пересылку DHCP/BOOTP включают на маршрутизаторах в сетевых сегментах, которые не соединены непосредственно с DHCP-сервером. Он минимизирует широковещательный трафик, тем, что передает только широковещательный трафик DHCP. Основное преимущество этого метода в том, что не надо приобретать дополнительное оборудование или программное обеспечение.

3) Определение областей DHCP и их параметров. Область - это диапазон IP-адресов, которым будет управлять DHCP-сервер. Особенность реализации DHCP в Windows 2000 - наличие суперобластей, которые являются объединителем нескольких областей DHCP-сервера. Они в проекте используются если:

- требуется поддержка сетевых сегментов, получающих параметры IP через агенты ретрансляции или маршрутизаторы с пересылкой DHCP/BOOTP;
- необходимо представить дополнительные диапазоны IP-адресов для сегментов, в которых существующие диапазоны уже исчерпаны;
- надо объединить несколько подсетей в одну с сохранением существующей схемы IP-адресации и масок подсетей.

Для области надо задать длительность аренды - промежуток времени, после которого разрешается переназначить IP-адрес. Она задается в зависимости от частоты перемещения компьютеров. Если часто, то длительность меньше. Если редко, то длительность больше. Параметры области - определяют конфигурацию клиентов DHCP. Из области DHCP надо исключить IP-адреса, назначаемые вручную. Это:

- IP маршрутизаторов;
- брандмауэров;
- серверов (файловых, печати, приложений);
- шлюзов;
- любых операционных систем или устройства, которые невозможно сконфигурировать средствами DHCP.

В параметрах области DHCP надо указать особенности конфигурации IP клиентов:

- маршрутизаторы;
- серверы DNS;
- имя домена DNS;
- тип узла WINS;
- сервер WINS.

Разрешается определять (а также создавать, изменять и удалять) параметры области DHCP, доступные для управления администратору DHCP. Для различных групп, или уровней, клиентов DHCP можно назначать различные параметры области DHCP. Причины назначения параметров области на различных уровнях:

Уровень	Причина назначения
Параметры сервера	Параметры действительны для всех областей DHCP-сервера. При назначении параметров на этом уровне необходимо проявлять осторожность, так как эти параметры влияют на конфигурацию всех клиентов данного DHCP-сервера
Параметры области	Действительны для всех клиентов DHCP. Параметры области в пределах диапазона IP-адресов (сетевого сегмента), определяемого областью DHCP.
Параметры класса	Параметры области для определенной категории клиентов DHCP. Можно сгруппировать клиентов DHCP в произвольные классы на основе определенных критериев. Например, класс для клиентов DHCP под управлением Windows 2000. Для этого класса разрешается назначать специальные параметры, устанавливаемые только в Windows 2000.
Параметры клиента	Параметры области для отдельных клиентских компьютеров. Например, определенный тип узла WINS только для одного компьютера в организации.

1) Защита конфигурации в проектах с DHCP. Обеспечение целостности конфигурации IP - наиболее важная задача при создании проекта с DHCP. Ведь любые посторонние DHCP-серверы в сети организации, автоматически конфигурирующие клиентов DHCP, способны вызвать ошибки и несогласованность в конфигурации IP компьютеров-клиентов и, как результат, нарушить сетевые подключения. Способ защиты в этом случае - предотвращение появления неавторизованных DHCP-серверов.

Если сервер DHCP в сети один:

- Служба сервера DHCP направляет в локальную подсеть запрос DHCPINFORM, пытаясь получить у DHCP-серверов сведения, о корневом домене Active Directory. Так как этот сервер единственный, ответа на запрос он не получит.
- Не получив ответа, служба сервера DHCP запрашивает у Active Directory подтверждение своей авторизации.
- Получив разрешение, DHCP-сервер переходит к выполнению функций конфигурирования протокола IP клиентов DHCP.

г) Если DHCP-сервер разрешения не получает, то служба сервера DHCP записывает соответствующее событие в журнал событий и останавливается.

Если DHCP-серверов в сети несколько

а) Служба сервера DHCP направляет в локальную подсеть запрос DHCPINFORM, пытаясь получить у существующих DHCP-серверов сведения о корневом домене Active Directory. б) Действующие DHCP-серверы отвечают на запрос сообщением-подтверждением DHCPACK и возвращают информацию о корневом домене (разные DHCP-серверы могут вернуть сведения о разных корневых доменах).

в) Создается список корневых доменов и список активных DHCP-серверов.

г) Если служба сервера DHCP установлена на контроллере домена или рядовом сервере, DHCP-сервер запрашивает в Active Directory подтверждение своей авторизации в корневом домене своего компьютера.

д) Если служба сервера DHCP выполняется на автономном компьютере, то DHCP сервер запрашивают у Active Directory подтверждение своей авторизации поочередно во всех корневых доменах по списку, пока не получит подтверждения.

е) Получив разрешение, DHCP-сервер переходит к выполнению функций конфигурирования протокола IP клиентов DHCP.

ж) Если DHCP-сервер разрешения не получает, служба сервера DHCP записывает соответствующее событие в журнал событий Windows 2000 и останавливается.

Авторизация DHCP-серверов под управлением Windows 2000 в службе каталогов Active Directory позволяет предотвратить появление в сети посторонних серверов DHCP. Для распознавания и блокировки неавторизованных DHCP-серверов следует предпринять ряд мер:

- Предусмотрите в проекте установку одной или нескольких служб сервера DHCP на контроллер домена или рядовой сервер (несколько DHCP-серверов, установленных на контроллеры домена или рядовые серверы, обеспечат отказоустойчивость на случай выхода из строя компьютера, являющегося DHCP-сервером контроллером домена).
- Составьте список DHCP-серверов, которым разрешено авторизоваться в Active Directory (не указанные в списке DHCP-серверы не запустятся).
- Установите агенты ретрансляции DHCP или включите пересылку DHCP/BOOTP на маршрутизаторах (сообщения DHCPINFORM, DHCPACK - это широковещательные сообщения, поэтому необходимо обеспечить, чтобы они беспрепятственно принимались и отправлялись во все сегменты сети).

Для обеспечения целостности базы данных DHCP необходимо запретить прямой доступ неавторизованных пользователей к DHCP-серверу. Существует несколько способов предотвращения компрометации базы данных DHCP неавторизованными пользователями:

- Ограничение круга пользователей, которым разрешено управлять DHCP-серверами в организации.
- Изоляция DHCP-серверов от общей сети. DHCP-серверы следует размещать в сетевых сегментах, недоступных из открытых сетей, например из Интернета.

2) Повышение доступности DHCP. Способы повышения доступности в проектах DHCP:

а) кластеры серверов Windows Clustering. Служба сервера DHCP поддерживает работу в кластерах серверов Windows Clustering. Кластер состоит по крайней мере из двух компьютеров, использующих общий диск кластера. Диск кластера подключен к общей SCSI-шине компьютеров кластера или узлов кластера. Например, в каждый момент времени служба DHCP работает только на одном из узлов. База данных хранится на общем диске кластера. Кластерный узел, на котором в данный момент выполняется служба сервера DHCP, называется активным узлом. При отказе активного узла автоматически подключается неактивный узел.

б) распределение областей между несколькими DHCP-серверами. Иногда диапазон IP-адресов одной области DHCP распределяется между двумя (или более) DHCP-серверами. В этом случае каждая часть этого диапазона управляется на одном из серверов. При выходе из строя одного из DHCP-серверов второй сервер берет функции по конфигурации IP на себя, предоставляя адреса из оставшегося (своего) диапазона. Например, дан диапазон 172.16.0.1-172.16.0.254. На один сервер задается диапазон 172.16.0.1-172.16.0.128. На другой сервер - 172.16.0.129-172.16.0.254. Основное преимущество этого метода в том, что для его реализации не требуются дополнительные аппаратные и программные ресурсы. В случае выхода одного DHCP-сервера, его адреса станут недоступны, но остальные адреса можно назначить.

в) DHCP-сервер на выделенном компьютере. В этом случае нестабильная работа других приложений или служб не приведет к необходимости перезагрузки компьютера.

3) Повышение производительности DHCP. Способы повышения производительности DHCP:

а) балансировка нагрузки между несколькими DHCP-серверами. Если существующие DHCP-серверы перегружены и их модернизация невозможна, то стоит разместить дополнительные DHCP-серверы, DHCP-запросы распределяются между дополнительными серверами, а значит, время выполнения конфигурирования IP уменьшится.

б) изменение длительности аренды. Период времени, по истечении которого клиенты обновляют аренду IP-адресов, зависит от длительности аренды. При его увеличении клиенты обращаются к DHCP-серверу реже, что снижает DHCP-трафик.

в) размещение DHCP-сервера на специально выделенном компьютере. Производительность повышается, т.к. системные ресурсы не потребляются одновременно выполняющимися с ним приложениями и службами.

### **Различия между протоколами BOOTP и DHCP.**

Протокол DHCP является расширением BOOTP (Bootstrap Protocol, протокол загрузки). Он изначально предназначен для обеспечения возможности начальной загрузки бездисковых рабочих станций с программируемых постоянных запоминающих устройств (PROM) и стираемой программируемой постоянной памяти (EPROM), расположенной на сетевых интерфейсных платах. Запущенный код начальной загрузки выполняет жестко закодированную процедуру, которая позволяет таким машинам немедленно получать доступ к сети для загрузки данных конфигурации операционных систем и сетевой конфигурации с сервера, находящегося в другом месте в этой сети.

По сравнению со своим предшественником, протокол DHCP предоставляет значительно больше возможностей, однако форматы протоколов DHCP и BOOTP сохраняют совместимость