

ASTRA LINUX

GUIDE

БАЗОВЫЕ СЕТЕВЫЕ СЛУЖБЫ

Сеть TCP/IP

Пакеты и сегментация

Данные передаются по сети в форме сетевых пакетов, каждый из которых состоит из заголовка и полезной нагрузки. Заголовок содержит сведения о том, откуда прибыл пакет и куда он направляется. Заголовок, кроме того, может включать контрольную сумму, информацию, характерную для конкретного протокола, и другие инструкции по обработке.

Полезная нагрузка — это данные, подлежащие пересылке.

Адресация пакетов

Сетевые пакеты могут достичь пункта назначения только при наличии правильного сетевого адреса. Протокол TCP/IP использует сочетание нескольких схем сетевой адресации.

Самый нижний уровень адресации задается сетевыми аппаратными средствами. На следующем, более высоком, уровне используется адресация Интернет (которую чаще называют «IP-адресацией»). Каждому включенному в сеть устройству присваивается один четырехбайтовый IP-адрес (в соответствии с протоколом IPv4). IP-адреса глобально уникальны и не зависят от аппаратных средств.

IP-адреса идентифицируют компьютер, но не обеспечивают адресацию отдельных процессов и служб. Протоколы TCP и UDP расширяют IP-адреса, используя порты. Порт в данном случае представляет собой двухбайтовое число, добавляемое к IP-адресу и указывающее конкретного адресата той или иной сетевой службы. Все стандартные UNIX службы связываются с известными портами, которые определены в файле /etc/services.

Для того чтобы предотвратить попытки нежелательных процессов замаскироваться под эти службы, установлено, что порты с номерами до 1024 могут использоваться только суперпользователем. Описание файла /etc/services приведено в man services.

Маршрутизация

Таблица

Маршрутизация — это процесс направления пакета по ряду сетей, находящихся между источником и адресатом.

Данные маршрутизации хранятся в таблице маршрутизации. Каждый элемент этой таблицы содержит несколько параметров, включая поле надежности, которое расставляет маршруты по приоритетам, если таблица содержит противоречивую информацию. Для направления пакета по конкретному адресу подбирается наиболее подходящий маршрут.

Если нет ни такого маршрута, ни маршрута по умолчанию, то отправителю возвращается ошибка: «network unreachable» (сеть недоступна).

Таблицу маршрутизации компьютера можно вывести на экран монитора с помощью команды route.

Организация подсетей

Организация подсетей задается маской подсети, в которой биты сети включены, а биты компьютера выключены. Мaska подсети задается во время начальной загрузки, когда конфигурируется сетевой интерфейс командой ifconfig. Ядро, как правило, использует сам класс IP-адресов для того, чтобы выяснить, какие биты относятся к сетевой части адреса; если задать маску явно, то эта функция просто отменяется.

При организации подсетей необходимо учесть, что если вычислительная сеть имеет более одного соединения с сетью Интернет, то другие сети должны уметь отличать подсети сети пользователя, чтобы определить в какой маршрутизатор следует послать пакет.

Создание сети TCP/IP

Процесс создания сети TCP/IP состоит из следующих этапов:

- планирование сети;
- назначение IP-адресов;
- настройка сетевых интерфейсов;
- настройка статических маршрутов.

Планирование сети

Планирование сети включает:

- определение сегментов сети;
- определение технических и программных средств, с помощью которых сегменты объединяются в сеть;
- определение серверов и рабочих станций, которые будут установлены в каждом сегменте;
- определение типа среды (витая пара и др.).

Назначение IP-адресов

Адреса назначают сетевым интерфейсам, а не компьютерам. Если у компьютера есть несколько интерфейсов, у него будет несколько сетевых адресов.

Назначая компьютеру IP-адрес, следует указать соответствие между этим адресом и именем компьютера в файле /etc/hosts. Это соответствие позволит обращаться к компьютерам по их именам.

Настройка сетевых интерфейсов

Команда ifconfig используется для включения и выключения сетевого интерфейса, задания IP-адреса, широковещательного адреса и связанной с ним маски подсети, а также для установки других опций и параметров. Она обычно выполняется во время первоначальной настройки, но может применяться и для внесения изменений в дальнейшем. В большинстве случаев команда ifconfig имеет следующий формат:

```
ifconfig интерфейс [семейство] адрес up опция ...
```

Пример

```
ifconfig eth0 128.138.240.1 up netmask 255.255.255.0 broadcast 128.138.240.255
```

Здесь интерфейс обозначает аппаратный интерфейс, к которому применяется команда. Как правило, это двух-трехсимвольное имя устройства, за которым следует число. Примеры распространенных имен eth1, lo0, ppp0 образуются из имени драйвера устройства, используемого для управления им. Для того чтобы выяснить, какие интерфейсы имеются в системе, можно воспользоваться командой:

```
netstat -i
```

Ключевое слово up включает интерфейс, а ключевое слово down выключает его.

Описание команды приведено в man ifconfig.

Настройка статических маршрутов

Команда route определяет статические маршруты — явно заданные элементы таблицы маршрутизации, которые обычно не меняются даже в тех случаях, когда запускается серверный процесс маршрутизации.

Маршрутизация выполняется на уровне IP. Когда поступает пакет, предназначенный для другого компьютера, IP-адрес пункта назначения пакета сравнивается с маршрутами, указанными в таблице маршрутизации ядра. Если номер сети пункта назначения совпадает с номером сети какого-либо маршрута, то пакет направляется по IP-адресу следующего шлюза, связанного с данным маршрутом.

Существующие маршруты можно вывести на экран командой route.

Описание команды приведено в man route.

Проверка и отладка сети

ping

Команда ping служит для проверки соединений в сетях на основе TCP/IP. Она работает в бесконечном цикле, если не задан параметр -c, определяющий количество пакетов, после передачи которого команда завершает свое выполнение. Чтобы прекратить работу команды ping, необходимо нажать <Ctrl+C>.

Описание команды приведено в man ping.

netstat

Команда netstat выдает информацию о состоянии, относящуюся к сетям:

- проверка состояния сетевых соединений;
- анализ информации о конфигурации интерфейсов;
- изучение таблицы маршрутизации;
- получение статистических данных о различных сетевых протоколах.

Команда netstat без параметров выдает информацию о состоянии активных портов TCP и UDP. Неактивные серверы, ожидающие установления соединения, как правило, не показываются (их можно просмотреть командой netstat -a).

Основные параметры команды netstat:

- -i — показывает состояние сетевых интерфейсов;
- -r — выдает таблицу маршрутизации ядра;
- -s — выдает содержимое счетчиков, разбросанных по сетевым программам.

Описание команды приведено в man netstat.

arp

Команда arp обращается к таблице ядра, в которой задано соответствие IP-адресов аппаратным адресам. В среде Ethernet таблицы ведутся с помощью протокола ARP и не требуют администрирования.

Команда arp -a распечатывает содержимое таблицы соответствий.

Описание команды приведено в man arp.

Служба FTP

В ОС передача файлов обеспечивается с помощью интерактивной команды lftp, вызываемой на клиентской стороне, и сервера vsftpd, который запускается на компьютере, выполняющем функцию сервера службы FTP. Обе команды реализуют протокол передачи файлов FTP. Для копирования файлов клиенту обычно (хотя существует и вариант анонимного доступа) необходимо знание имени и пароля пользователя, которому принадлежат файлы на сервере службы FTP.

Клиентская часть

Вызов команды lftp осуществляется командой:

```
lftp имя_сервера
```

Интерактивный доступ к серверу службы FTP обеспечивается следующими основными внутренними командами lftp:

- open, user, close — связь с удаленным компьютером;
- lcd, dir, mkdir, lpwd — работа с каталогами в FTP-сервере;
- get, put, ftpcopy — получение и передача файлов;
- ascii, binary, status — установка параметров передачи.

Выход из команды lftp осуществляется по команде exit.

Описание команды приведено в man lftp.

Сервер VSFTPD

В ОС программный пакет vsftpd устанавливается командой:

```
apt-get install vsftpd
```

Пакет также может быть установлен в процессе установки ОС. Для этого следует в окне программы установки «Выбор программного обеспечения» отметить группу пакетов «Сетевые сервисы».

После установки следует обратить внимание на файлы документации в каталоге /usr/share/doc/vsftpd, где каталог EXAMPLE содержит различные примеры конфигурационного файла сервера vsftpd.conf. В руководстве man подробно описаны все возможности программы.

Команда располагается в каталоге /usr/sbin/vsftpd.

Конфигурационный файл

После установки сервера vsftpd он сразу готов к работе с параметрами по умолчанию. Если для работы сервера необходимы другие значения параметров, следует отредактировать конфигурационный файл /etc/vsftpd.conf.

В файле vsftpd.conf представлены три вида параметров:

- BOOLEAN — параметры, которые могут содержать значения YES и NO;
- NUMERIC — параметры, содержащие различные цифровые значения (например, время в секундах или номер порта соединения);
- STRING — параметры, содержащие текстовую строку (например, путь к каталогу на диске).

Следует заметить, что некоторые параметры могут явно отсутствовать в конфигурационном файле. Это означает, что для них используется значение, заданное по умолчанию и обозначаемое как Default: в руководстве man.

Не все параметры следует указывать напрямую, иначе конфигурационный файл может достичь очень больших размеров. В большинстве случаев достаточно записать в файл несколько строк, а для остальных настроек использовать значения по умолчанию.

Многие настройки зависят от других параметров. Если параметры, от которых они зависят, отключены, то и данные настройки будут отключены. Некоторые параметры являются взаимоисключающими и, следовательно, не будут работать в паре с такими включенными параметрами.

Описание службы vsftpd и файла vsftpd.conf приведено на страницах руководства man.

Служба DHCP

На компьютере, выполняющем роль сервера динамической конфигурации сети, должна быть установлена служба dhcpcd. Настройки этой службы хранятся в файле /etc/dhcpcd.conf. Файл настройки содержит инструкции, которые определяют, какие подсети и узлы обслуживает сервер и какую информацию настройки он им предоставляет.

Сервер динамически назначает IP-адреса DHCP-клиентам обеих подсетей и осуществляет поддержку нескольких клиентов БООТР. Первые несколько активных строк файла определяют ряд параметров и режимов, действующих для всех обслуживаемых сервером подсетей и клиентов. Конструкция каждой строки есть реализация шаблона «параметр — значение». «Параметр» может быть общим или стоять перед ключевым словом option. Параметры, следующие за словом option, — это ключи настройки. Они также состоят из имени ключа и его значения.

Кроме общих параметров, существуют т. н. «операторы топологии сети» или «объявления».

Описание некоторых параметров настройки сервера dhcpcd, содержащихся в файле dhcpcd.conf, приведено в таблице.

Параметр	Описание
max-lease-time	Определяет максимально допустимое время аренды. Независимо от длительности аренды, фигурирующей в запросе клиента, этот срок не может превышать значение, заданное данным параметром
get-lease-hostnames	Предписывает dhcpcd предоставлять каждому клиенту наряду с динамическим адресом имя узла. Имя узла должно быть получено от DNS. Данный параметр — логический. При значении FALSE назначается адрес, но не имя узла. Значение TRUE используется только в сетях с небольшим количеством хостов, которым выделяются имена, т. к. поиск имен в DNS замедляет запуск демона
hardware type address	Параметр определяет аппаратный адрес клиента. Значение type может быть ethernet или token-ring. address должен быть соответствующим устройству физическим адресом. Параметр должен быть связан с оператором host. Он необходим для распознавания клиента БООТР

<code>filename file</code>	Указывает файл загрузки для бездисковых клиентов. <code>file</code> – это ASCII-строка, заключенная в кавычки
<code>range [dynamic-bootp]</code>	Данный параметр указывает диапазон адресов. После него через пробел указывается нижний адрес диапазона и опционально верхний адрес. Если верхний адрес не указан, занимается весь теоретически возможный диапазон от нижнего адреса. Этот параметр всегда связан с оператором <code>subnet</code> . Все адреса должны принадлежать этой подсети. Флаг <code>dynamic-bootp</code> указывает, что адреса могут автоматически назначаться клиентам BOOTP также, как и клиентам DHCP. Если оператор <code>subnet</code> не содержит параметра <code>range</code> , для такой подсети динамическое распределение адресов не действует
<code>server-name name</code>	Имя сервера DHCP, передаваемое клиенту. <code>name</code> – это ASCII-строка, заключенная в кавычки
<code>next-server name</code>	Имя узла или адрес сервера, с которого следует получить загрузочный файл
<code>fixed-address</code>	Назначает узлу один или несколько фиксированных адресов. Действителен только в сочетании с параметром <code>host</code> . Если указано несколько адресов, выбирается адрес, корректный для данной сети, из которой выполняет загрузку клиент. Если такого адреса нет, никакие параметры не передаются
<code>dynamic-bootp-lease-cuttof date</code>	Устанавливает дату завершения действия адресов, назначенных клиентам BOOTP. Клиенты BOOTP не обладают способностью обновлять аренду и не знают, что срок аренды может истечь. Этот параметр меняет поведение сервера и используется только в особых случаях
<code>dynamic-bootp-lease-length</code>	Длительность аренды в секундах для адресов, автоматически назначаемых клиентам BOOTP. Данный параметр используется в особых ситуациях, когда клиенты используют образ загрузки BOOTP PROM. В ходе загрузки клиент действует в качестве клиента BOOTP, а после загрузки работает с протоколом DHCP и умеет обновлять аренду
<code>use-host-decl-names</code>	Предписывает передавать имя узла, указанное в операторе <code>host</code> , клиенту в качестве его имени. Логический параметр, может иметь значения <code>TRUE</code> или <code>FALSE</code>
<code>server-identifier hostname</code>	Определяет значение, передаваемое в качестве идентификатора сервера. По умолчанию передается первый IP-адрес сетевого интерфейса
<code>authoritative not authoritative</code>	Указывает, является ли сервер DHCP компетентным. <code>not authoritative</code> используется, когда в компетенцию сервера не входит распределение адресов клиентам
<code>use-lease-addr-for-default-route</code>	Логический параметр (<code>TRUE</code> или <code>FALSE</code>). Предписывает передавать клиенту арендованный адрес в качестве маршрута по умолчанию. Параметр используется только тогда, когда локальный маршрутизатор является сервером-посредником ARP. Оператор настройки <code>routers</code> имеет более высокий приоритет
<code>always-replay-rfc1048</code>	Логический параметр. Предписывает посыпать клиенту BOOTP ответы в соответствии с RFC 1048

<pre>allow keyword deny keyword</pre>	<p>Определяет необходимость отвечать на запросы различных типов. Ключевое слово <code>keyword</code> указывает тип разрешенных и запрещенных запросов. Существуют следующие ключевые слова:</p> <ul style="list-style-type: none"> – <code>unknown-clients</code> – определяет возможность динамического назначения адресов неизвестным клиентам; – <code>bootp</code> – определяет необходимость отвечать на запросы BOOTP (по умолчанию обрабатываются); – <code>booting</code> – используется внутри объявления <code>host</code> для указания необходимости отвечать тому или иному клиенту. По умолчанию сервер отвечает всем клиентам
---------------------------------------	--

Операторы определяют иерархическую структуру. Операторы топологии, встречающиеся в файле `dhcp.conf`, приведены в таблице.

Оператор	Описание
<code>group {[parameters] [options]}</code>	Группирует операторы <code>shared-network</code> , <code>subnet</code> , <code>host</code> и другие операторы <code>group</code> . Позволяет применять наборы параметров и опций ко всем элементам группы
<code>shared-network name {[parameters] [options]}</code>	Используется только в случае, когда несколько подсетей находятся в одном физическом сегменте. В большинстве случаев различные подсети находятся в различных физических сетях. В качестве имени <code>name</code> может использоваться любое описательное имя. Оно используется только в отладочных сообщениях. Параметры и опции, связанные с общей сетью, объявляются внутри фигурных скобок и действуют на все подсети общей сети. Каждый оператор <code>shared-network</code> содержит не менее двух операторов <code>subnet</code> , в противном случае нет необходимости использовать группирование

Общеупотребительные опции, следующие за ключевым словом `option` в файле `dhcp.conf`, приведены в таблице.

Опция	Описание
<code>subnet-mask</code>	Определяет маску подсети в формате десятичной записи через точку. Если <code>subnet-mask</code> отсутствует, <code>dhcpd</code> использует маску подсети из оператора <code>subnet</code>
<code>time-offset</code>	Указывает разницу данного часового пояса с временем UTC в секундах
<code>routers</code>	Перечисляет адреса доступных клиентам маршрутизаторов в порядке предпочтения
<code>domain-name-servers</code>	Перечисляет адреса доступных клиентам серверов DNS в порядке предпочтения
<code>lpr-servers</code>	Перечисляет адреса доступных клиентам серверов печати LPR в порядке предпочтения
<code>host-name</code>	Указывает имя узла для клиента
<code>domain-name</code>	Определяет имя домена
<code>interface-mtu</code>	Определяет значение MTU для клиента в байтах. Минимально допустимое значение – 68
<code>broadcast-address</code>	Определяет широковещательный адрес для подсети клиента
<code>static-routes destination gateway</code>	Перечисляет доступные клиенту статические маршруты. Маршрут по умолчанию не может быть указан таким способом. Для его указания используется опция <code>routers</code>

Опция	Описание
<code>trailer-encapsulation</code>	Определяет, следует ли клиенту выполнять инкапсуляцию завершителей (оптимизация, основанная на изменении порядка данных). Значение 0 означает, что инкапсуляцию выполнять не следует, 1 имеет противоположный смысл
<code>nis-domain string</code>	Строка символов, определяющая имя домена NIS
<code>dhcp-client-identifier string</code>	Используется в операторе <code>host</code> для определения идентификатора клиента DHCP. <code>dhcpd</code> может использовать данное значение для идентификации клиента вместо аппаратного адреса

Запуск службы `dhcpd` можно осуществить с помощью команды:

```
systemctl start isc-dhcp-server
```

Или включить в список служб, запускаемых при старте системы. Описание службы `dhcpd` и файла `dhcp.conf` приведено на страницах руководства тан.

Служба NFS

Служба сетевого доступа к ФС NFS позволяет использовать ФС удаленных серверов и компьютеров.

Доступ к ФС удаленных компьютеров обеспечивается с помощью нескольких программ на сторонах сервера и клиента.

На стороне сервера существуют следующие программы, используемые для обеспечения службы NFS:

- `rpc.idmapd` — перенаправляет обращения, сделанные с других компьютеров к службам NFS;
- `rpc.nfsd` — переводит запросы к службе NFS в действительные запросы к локальной ФС;
- `rpc.svcgssd` — поддерживает создание защищенного соединения;
- `rpc.statd` — поддерживает восстановление соединения при перезагрузке сервера;
- `rpc.mountd` — запрашивается для монтирования и размонтирования ФС.

Описание программ приведено на страницах руководства тан.

На стороне сервера выполняется экспортация ФС. Это означает, что определенные поддеревья, задаваемые каталогами, объявляются доступными для клиентских компьютеров. Информация об экспортированных ФС заносится в файл `/etc(exports`, в котором указывается, какие каталоги доступны для указанных клиентских компьютеров и какими правами доступа обладают клиентские компьютеры при выполнении операций на сервере. Запросы монтирования поступают от клиентских компьютеров к серверу монтирования `mountd`, который проверяет правильность клиентского запроса на монтирование и разрешает серверу службы NFS (`nfsd`) обслуживать запросы клиента, выполнившего монтирование. Клиенту разрешается выполнять различные операции с экспортированной ФС в пределах своих полномочий. Для получения хорошего качества обслуживания клиентов рекомендуется на сервере службы NFS одновременно запускать несколько копий процесса `nfsd`.

На стороне клиента для поддержки службы NFS4 используется модифицированная команда mount (если указывается ФС NFS4, то автоматически вызывается команда mount.nfs4). Дополнительно команда модифицирована таким образом, чтобы она могла понимать запись:

имя_компьютера: каталог

где имя_компьютера — имя сервера NFS,
каталог — экспортированный каталог сервера службы NFS.

Для удаленных ФС, которые являются частью постоянной конфигурации клиента, записи о монтируемых ФС службы NFS должны быть перечислены в файле /etc/fstab для автоматического монтирования во время начальной загрузки клиентского компьютера.

Кроме того, для поддержки защищенных соединений на клиентской стороне должна запускаться команда rpc.gssd.

При работе с сетевой ФС любые операции над файлами, производимые на локальном компьютере, передаются через сеть на удаленный компьютер.

Служба DNS

Система доменных имен DNS (Domain Name System) представляет собой иерархическую распределенную систему для получения информации о компьютерах, сервисах и ресурсах, входящих в глобальную или приватную компьютерную сеть. Чаще всего используется для получения IP-адреса по имени компьютера или устройства, получения информации о маршрутизации почты и т.п.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Распределенная база данных DNS поддерживается с помощью иерархии DNS серверов, взаимодействующих по определенному протоколу. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Основными важными понятиями DNS являются:

- домен (область) — именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается справа налево от младших доменов к доменам высшего уровня (в порядке повышения значимости);
- полное доменное имя (FQDN) — полностью определенное доменное имя. Включает в себя имена всех родительских доменов иерархии DNS;
- зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен;

DNS-запрос — запрос от клиента (или сервера) серверу для получения информации. Служба доменных имен named предназначена для генерации ответов на DNS-запросы. Существуют два типа DNS-запросов:

- прямой — запрос на преобразование имени компьютера в IP-адрес;
- обратный — запрос на преобразование IP-адреса в имя компьютера.

Настройка сервера службы доменных имен named

Конфигурационные параметры службы named хранятся в файлах каталога /etc/bind/, в первую очередь, в файле /etc/bind/named.conf.

Таблица – Конфигурационные файлы службы доменных имен named

Файл	Описание
/etc/bind/named.conf	Основной конфигурационный файл. Содержит значения конфигурационных параметров для всего сервера и включения других конфигурационных файлов
named.conf.default-zones	Конфигурационный файл зон по умолчанию. В большинстве случаев не требует правки
named.conf.options	Конфигурационный файл основных параметров сервера, важным из которых является параметр directory, содержащий каталог конфигурационных файлов зон. Значение по умолчанию /var/cache/bind
/etc/bind/named.conf.local	Конфигурационный файл описания локальных зон сервера. Для каждой зоны указываются пути к конфигурационным файлам для прямого и обратного разыменования (как правило, в указанном ранее каталоге /var/cache/bind)

Настройка сервера доменных имен является сложной задачей. Перед использованием DNS следует ознакомиться с существующей документацией, файлами помощи и страницами руководства man сервиса named, конфигурационного файла named.conf и сопутствующих утилит.

Далее приведен типовой пример настройки службы доменных имен named, обслуживающей одну доменную зону. Пример достаточен для демонстрации функционирующего домена ЕПП ОС «Astra Linux Special Edition».

Пример

Настройка сервера DNS домена my.dom подсети 192.168.1.

В конфигурационный файл /etc/bind/named.conf.local необходимо добавить следующие строки:

```
zone "my.dom" {
    type master;
    file "/var/cache/bind/db.my.dom";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.192.168.1";
};
```

Примечание.

Имена конфигурационных файлов следует выбирать так, чтобы было понятно для какой конфигурации они используются. В приведенном примере имя конфигурационного файла для зоны обратного просмотра может быть, например:

/var/cache/bind/1.168.192.in-addr.arpa.zone

или

/var/cache/bind/db.my.dom.inv.

Конфигурационный файл /var/cache/bind/db.my.dom содержит информацию зоны прямого просмотра:

```
;;
; BIND data file for my.dom zone
;;
$TTL 604800
@ IN SOA my.dom. root.my.dom. (
2014031301 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@ IN NS server.my.dom.
@ IN A 192.168.1.100
@ IN MX 1 server.my.dom.
server IN A 192.168.1.100
client1 IN A 192.168.1.101
client2 IN A 192.168.1.102
client3 IN A 192.168.1.103

ns IN CNAME server
;gw CNAMEs
ftp IN CNAME server
repo IN CNAME server
ntp IN CNAME server
_https._tcp IN SRV 10 10 443 server.my.com.
client1 IN TXT "MAKS"
```

Конфигурационный файл /var/cache/bind/db.192.168.1 содержит информацию зоны обратного просмотра:

```
; BIND reverse data file for my.dom zone
;
$TTL 86400
@ IN SOA my.dom. root.my.dom. (
2014031301 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
86400 ) ; Negative Cache TTL
;
@ IN NS server.my.dom.
100 IN PTR server.my.dom.
101 IN PTR client1.my.dom.
102 IN PTR client2.my.dom.
103 IN PTR client3.my.dom.
```

Описание зон может содержать следующие основные типы записей:

- NS — имя DNS сервера;
- A — связь имени с IP-адресом;
- CNAME — связь псевдонима с другим именем (возможно псевдонимом);
- PTR — обратная связь IP-адреса с именем;
- SRV — запись о сетевом сервисе;
- TXT — текстовая запись.

ВНИМАНИЕ! Перевод строки в конце конфигурационных файлов зон обязателен. В большинстве применений необходимо указание точки в конце имен компьютеров для предотвращения вывода корневого суффикса имени вида «1.168.192.in-addr.arpa». Могут оказаться полезными следующие DNS утилиты (из состава пакетов bind9utils и dnsutils):

- named-checkconf — проверка синтаксиса, но не семантики конфигурации службы доменных имен named;
- nslookup — интерактивный терминал запросов к службе доменных имен;
- rndc — утилита управления службы доменных имен named.

Примечание. Обновление конфигурации сервера может выполняться без перезапуска самой службы доменных имен named вызовом:

```
rndc reload
```

Настройка клиентов для работы со службой доменных имен

Для работы со службой доменных имен на компьютерах необходимо наличие конфигурационного файла /etc/resolv.conf, содержащего информацию о доменах и именах серверов DNS, например:

```
domain my.dom
search my.dom
nameserver 192.168.1.100
```

Также может быть рассмотрена установка системы поддержки работы со службой доменных имен, содержащейся в пакете resolvconf.

ВНИМАНИЕ! Для взаимодействия DNS-сервера с клиентами, функционирующими в разных мандатных контекстах, требуется дополнительная настройка механизма privsock.