

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Стандартная конфигурация](#)

[Рекомендации по конфигурации и настройке](#)

[Первоначальное планирование и настройка](#)

[Общая конфигурация системы](#)

[Конфигурация DHCP](#)

[Конфигурация DNS](#)

[Настройка TFTP](#)

[Конфигурация CNR LDAP](#)

[Параметры настройки сервера LDAP](#)

[Подпрограммы](#)

[Немедленные действия при возникновении проблемы](#)

[Анализ файлов журналов](#)

[Выявление проблем LDAP](#)

[Подтвердите внутренние базы данных сетевого регистратора Cisco \(CNR\)](#)

[Проверьте Данные DNS С nslookup](#)

[Дополнительные сведения](#)

Введение

У этой статьи две цели. Во-первых, в ней содержатся рекомендации по настройке оптимальной производительности и стабильности сетевого регистратора Cisco (CNR), а также по контролю за установкой CNR. Во-вторых, в ней содержатся рекомендации, что предпринять в случае возникновения неполадки. В идеальном случае вы прочтете эту статью и будете работать с конфигурацией и рекомендациями по отслеживанию до того, как встретятся какие-либо проблемы. Таким образом вы сможете избежать проблем. При чтении этой статьи впервые, потому что у вас есть проблема с CNR, пойдите сразу в [Срочные меры При Направлении с Разделом проблем](#). Для дальнейшего пояснения рекомендаций, см. [Руководства пользователя CNR](#) и [Справочники по командам](#).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Стандартная конфигурация

Рекомендации по конфигурации, предлагаемые здесь, представляют отправную точку. Если система имеет иную конфигурацию, пересмотрите свои настройки. Ваша конфигурация могла развиваться из предыдущих версий CNR. CNR 5.0 и более поздние версии обеспечивают намного большую производительность по сравнению с более ранними версиями, но для достижения максимального полезного эффекта следует внести изменения в параметры. Этот документ описывает в основном среды крупных поставщиков услуг, но большинство рекомендаций также применяется и к другим средам CNR. Этот документ предполагает что:

- Вы являетесь поставщиком услуг, использующим широкополосную сеть с 10000 абонентов или более.
- Вы используете CNR 5.0.3 или позже.
- Используется протокол упрощенного доступа к каталогам (LDAP). Выполнения CNR без LDAP, но много поставщиков услуг используют LDAP.
- Ваша сеть имеет среднюю насыщенность IP-адреса.
- CNR запускается на серверах UNIX. Большинство рекомендаций применяется одинаково к Windows NT, но используется большинство поставщиков услуг выполненный CNR на серверах UNIX, поэтому где UNIX и NT отличаются, пример Unix.
- Существуют восходящие подключения к другим системам (таким как системы выставления счетов, доступа к банковским счетам клиента или инициализации), работающим на других серверах.
- Динамическая система имен доменов (DDNS) не активна на вашем узле (большинство поставщиков услуг не использует DDNS).

Рекомендации по конфигурации и настройке

Первоначальное планирование и настройка

- План и документ IP - адрес размещения.
- Интенсивные действия отдельного диска: поместите свой основной сервер DHCP на другую машину, чем ваш Сервер LDAP и основной сервер DNS.
- ЗадOCUMENTИРУЙТЕ свою конфигурацию Системы терминиРОВАНИЯ кабельных модемов (CMTS); убедитесь в соответствии параметров конфигурации CMTS и CNR.
- Подготовьте планы аварийного восстановления.
- Зафиксируйте топологию сети.
- Обратите внимание на версии программного обеспечения Cisco IOS CMTSs.

Самые эффективные шаги в долгосрочное состояние вашей сети: а) планируют вашу

конфигурацию, b) делают запись тех планов, и c) делают запись изменений, когда изменения запланированы и внесены. Документирование причин выбора может помочь во время сеансов планирования.

Общая конфигурация системы

- Используйте безопасную обработку ситуаций отказов. Простое аварийное переключение, где один сервер является основным для всех областей и другого сервера, является резервной копией для всех областей (в противоположность симметричному аварийному переключению, где оба сервера являются основными и резервируют в то же время, в зависимости от индивидуального диапазона), настоятельно рекомендован, поскольку это *упрощает значительно* задачи администрирования.
- Включите Перехваты простого протокола управления сетью (SNMP). Эти примеры для рисунка:

```
nrcmd> trap enable address-conflict  
nrcmd> trap enable dhcp-failover-config-mismatch  
nrcmd> trap enable other-server-not-responding  
nrcmd> trap set free-address-low-threshold=15%  
nrcmd> trap set free-address-high-threshold=30%  
nrcmd> trap enable free-address-low
```
- Убедитесь, что у вас есть соответствующее ОЗУ (512 МБ или больше).
- Убедитесь, что разделение данных является достаточно большим (2.5 ГБ или больше).
- Используйте разные разделы для журналов и данных.
- Гарантируйте высокую скорость, соединения низкой задержки между серверами; проверьте настройки интерфейса.

Захват SNMP позволяет вам управлять сервером DHCP с сетевого монитора. Проверьте конфигурирование прерываний в DHCP сервере, конфигурируйте монитор для их принятия и отображения и естественно обратите внимание на монитор.

Настройка производственная система требует компромиссов стоимости против эффективности системы. Мы предлагаем эти значения, принимающие приблизительно 100,000 абонентов в E250-системах-классов рабочее аварийное переключение. Использование многой политики, классов клиентов, областей, запроса и буферов ответа, расширений DHCP и других осложнений влияет на потребности памяти и производительность.

Раздел журнала (/var/nwreg2) необходимо увеличить, если число и размер журналов увеличивается.

Конфигурация DHCP

- Настройте буферы запроса и отклика для оптимальной пропускной способности. Учитывайте, что эти рекомендации изменились для CNR 5.0.

```
nrcmd> DHCP set max-dhcp-requests=500  
nrcmd> DHCP set max-dhcp-responses=2000
```
- Время аренды кабельного модема = 604800 (7 дней) или больше.
- Время аренды Customer Premises Equipment (CPE): максимально долго (см. примечание для компромиссов).
- DHCP увеличения и размеры журнала TFTP:

```
nrcmd> server DHCP serverLogs nlogs=15  
logsize=10M  
nrcmd> server DNS serverLogs nlogs=15 logsize=10M  
nrcmd> server TFTP serverLogs  
nlogs=10 logsize=10M
```
- Настройте настройки журнала, которые предоставляют достаточно подробности для определения проблем, но не генерируют излишнюю информацию (который мешает

отличать проблемы и создает ненужную нагрузку для сервера). Это рекомендуемые настройки, которые обычно применимы. Для решения проблем в вашей сети при необходимости откорректируйте установки: Сводка Activity По умолчанию No-failover-activity Делает доступными расширения отложенной аренды Набор last-transaction-time-granularity = 1/2 арендует интервал Отключите allow-client-lease-override для политики, предлагающей производственные арендные договоры. Включите fall-back-to-local; когда LDAP недоступен, CNR использует локальные данные:

```
nrcmd> session set visibility=3nrcmd> dhcp enable fallback-to-local-client-datanrcmd> session set visibility=5
```

- При использовании CNR 5.5 или позже, настройте возможность client-cache уменьшить запросы LDAP наполовину.

```
nrcmd> dhcp set client-cache-count=2000nrcmd> dhcp set client-cache-ttl=5
```

Для наиболее эффективного использования пропускной способности CNR число буферов ответа должно в три-четыре раза превышать число буферов запроса. Система только использует столько буферов, сколько ей нужно. Поскольку времена аренды испытывают недостаток, больше буферов ответа требуется.

Примечание: Следует устанавливать максимально возможное время аренды. Кабельный модем арендует адрес из частного адресного пространства (обычно net-10), при этом модемы редко перемещаются в другое место в сети. Эти аренды должны быть недельными или более длительными. Арендные договоры CPE, с другой стороны, прибывают из области общедоступных адресов, и CPE (в частности портативные ПК) действительно перемещаются. Здесь продолжительность аренды должна собираться совпасть с привычками к вашему кругу пользователей. При увеличении срока аренды снижается нагрузка на DHCP-сервер. В случае краткосрочной аренды (менее чем на 8 часов) увеличьте число буферов ответов до 2500.

Отключите allow-client-lease-override, чтобы гарантировать, что клиенты придерживаются времен аренды, заданных в вашей конфигурации CNR? некоторые клиенты пытаются отвергнуть указанную установку.

Сделайте доступным fall-back-to-local, чтобы сохранить работоспособность вашей сети в случае отказа сервера LDAP. С этой установкой сервер DHCP продолжает удовлетворять запросы арендного договора даже при том, что не отвечает Сервер LDAP. У сервера не будет доступа к определенным данным клиента, хранящимся на сервере LDAP, поэтому он будет отвечать на все запросы в соответствии с настройками по умолчанию. Необходимо настроить по умолчанию, который разумен для сети.

Наконец, функция client-cache поддерживает в памяти данные клиента полученными из LDAP, так, чтобы сервер DHCP сделал запрос LDAP только однажды во время цикла discovery-offer-request-ack, ускорив производительность сервера DHCP.

Конфигурация DNS

1. Включите поддержку инкрементной передачи:

```
nrcmd> dns enable ixfr-enable
```
2. Включите уведомляют. См. [Ссылки команды CLI CNR](#) для аргументов необходимо включить, уведомляют.
3. Помещенный основной и дополнительные DNS - серверы на отдельных сегментах сети.
4. Настройте клиентов для запроса дополнительного DNS - сервера.

Дополнительные DNS - серверы получают свои данные от основного сервера один из двух путей: а) "полная передача зоны" или б) "notify/ixfr" (инкрементная передача).

Использование notify/ixfr сокращает количество записей, которые должны быть переданы от основного до дополнительных серверов. Когда пространство имен является относительно динамичным, это важно.

Настройка TFTP

- **Initial-packet-timeout** набора к 2:
`nrcmd> tftp set initial-packet-timeout = 2`
- При использовании CNR 5.5 или позже, позвольте кэшированию файлов TFTP улучшить производительность:
`nrcmd> tftp set home-directory=/var/nwreg2/data/tftp`
`nrcmd> tftp set file-cache-directory=CacheDir`
`nrcmd> tftp set file-cache-max-memory-size=32000`
`nrcmd> tftp enable file-cache`
`nrcmd> tftp reload`

Кэширование файлов TFTP поддерживает файлы настройки кабельного модема сохраненными в памяти, избегая чтений к диску каждый раз, когда кабельный модем запрашивает файл конфигурации. Каталог кэша файла должен быть создан в жестком диске (CacheDir в приведенном выше примере), и назначен максимальный размер. Выберите размер, принимающий во внимание общее количество ОЗУ в вашей системе и количестве других необходимых файлов конфигурации.

TFTP протокол не требует, чтобы клиент передал окончательное подтверждение (ACK) пакет по получении файла. Если никакой ACK не получен, сервер должен держать клиентское соединение для периода ожидания, который ограничивает его емкость обработать новые запросы. Если ваш сервер TFTP имеет емкость ресурса, можно также увеличить стоимость **Max-tftp-packets** для поддержки большего количества клиентских соединений. Значение по умолчанию для этого параметра равно 512. Максимальным значением является 1000.

Конфигурация CNR LDAP

Данные настройки соответствуют конфигурации, в которой CNR сохраняет обновления аренды в LDAP. По возможности спроектируйте свою сеть, но это не является обязательным условием. Если необходимо записать обновления арендного договора, это, как показывают, здесь предоставляет рекомендации. Оптимизируйте Соединения LDAP при помощи отдельно настраиваемых объектов LDAP READ/WRITE. (Каждый объект получает свою собственную группу потоков).

```
nrcmd> tftp set home-directory=/var/nwreg2/data/tftp
nrcmd> tftp set file-cache-directory=CacheDir
nrcmd> tftp set file-cache-max-memory-size=32000
nrcmd> tftp enable file-cache
nrcmd> tftp reload
```

Приведенная конфигурация включает обновления CNR к LDAP. Это может потребоваться, чтобы разрешить приложениям отправлять запросы на сервер LDAP для получения текущих сведений об аренде, но следует избегать структурирования приложения, чтобы в этом не возникала необходимость. Если необходимо обеспечить доступ к информации о состоянии аренды IP-адреса, можно использовать команду lease интерфейса NRCMD для получения MAC-адреса, времени окончания срока действия и другой информации о состоянии аренды.

Каталоги LDAP спроектированы для их быстрого и эффективного чтения, но запись в каталог LDAP малозэффективна. При настройке CNR для записи сведений аренды в LDAP, LDAP становится узким местом к общей производительности системы. Если необходимо конфигурировать записи аренды LDAP, используйте рекомендуемые настройки. Заметьте, что доступ CNR к LDAP был оптимизирован посредством использования отдельных объектов "read" и "update LDAP". Обратите внимание также на 30-секундный простой записи. С более коротким временем ожидания существует риск истечения времени записи

LDAP при высокой нагрузке LDAP. CNR осуществляет повторную попытку записи, что добавляет дополнительную нагрузку на LDAP.

Общее количество соединений с сервером LDAP не должно превышать максимальное число доступных потоков. Если ваш Сервер LDAP поддерживает многопроцессного для каждого подключения, оптимальное число соединений является общим числом потоков, разделенных на количество потоков для каждого подключения.

[Параметры настройки сервера LDAP](#)

- Создайте индексы для полей lookup.
- Настройте размер кэша для увеличения количества записей, содержащихся в памяти, при этом размер кэша не должен превышать одной трети доступной памяти.
- Настройте максимальное число потоков для увеличения количества одновременных соединений, которые могут поддерживаться, но не расходуйте на это более половины доступных ресурсов.
- Настройте настройки журнала, которые предоставляют достаточно подробности для определения проблем, но не генерируют излишнюю информацию (который мешает отличать проблемы и создает ненужную нагрузку для сервера).
- Используйте разные разделы для журналов и данных.

Варьируются определенные реализации Сервера LDAP. См. вашу документацию сервера для реализации этих предложений.

[Подпрограммы](#)

- Регулярно выполняйте резервное копирование базы данных CNR. См. [Руководства пользователя](#) для инструкций. Необходимо выполнить резервное копирование базы данных CNR, по крайней мере, один раз в день. Сохраняет резервные файлы в течение как минимум двух недель.
- Регулярно LDAP резервного копирования.
- Регулярно резервное копирование и архивации журналов.
- После того, как изменения внесены в CNR, гарантируют, что конфигурация главных серверов и серверы резервного копирования в сценарии аварийного переключения остаются последовательными. Используйте **cnrFailoverConfig** - **сравнивают** программное средство в version CNR 5.5 и ранее или сравнивают конфигурации с помощью WebUI в CNR 6.0 и позже.
- При планировании изменений топологии сети установите обновление DHCP и введите небольшие значения срока аренды.
- Использование IP-адреса монитора (используют trap-сообщения SNMP).
- Использование системы контроля (память, диск, ЦП и подкачка). Сервисная **вершина** полезна для этой цели.
- Периодически просматривайте журналы, чтобы ознакомиться с примерами сообщений при нормальной работе. Понимание обычных журналов позволяет вам решить проблемы более быстро.
- Периодически рассматривайте журналы для исключений: grep для "ошибки", "предупредите", или "подключение" (например, в UNIX, используйте **grep-i**, **предупреждают name_dhcp_1_log**).

Безопасное восстановление DHCP после отказа требует, чтобы параметры конфигурации

для диапазона на основном и резервном сервере этого диапазона совпадали. Убедитесь при внесении изменения в установку что вы вносите изменение на обоих серверах. Периодически используйте `cnrFailoverConfig` - **выдерживают сравнение** или WebUI в CNR 6.0 и выше проверять, чтобы удостовериться, что нет никаких различий.

Изменения топологии сети или изменения IP - адреса размещения могут заставить клиентов получать другой адрес. Необходимо планировать на промежуток времени, когда некоторые клиенты на подсети имеют адрес из старого диапазона, а некоторые обновили и получили адрес из нового диапазона. Вы можете сократить период активности обоих наборов адресов, уменьшив длину аренды до внесения изменений, чтобы у всех клиентов были краткосрочные аренды. Это гарантирует, что они должны возобновлять свои арендные договоры часто и поэтому поднимать арендный договор с нового диапазона после внесения изменения. Обязательно не установите время аренды, настолько короткое, что арендные договоры заканчиваются, в то время как вы останавливаете и запускаете сервер для внесения изменения. После внесения изменения убедиться восстановить период исходной аренды так, чтобы вы не увеличивали загрузку на сервере.

Самый эффективный способ решения проблем - это их недопущение. После рекомендаций, выделенных выше, поддерживает ваших администраторов в мелодии с вашей операцией и позволяет вам избежать серьезных проблем. Когда проблемы появляются (такие как увеличения времени ожидания ввода-вывода или увеличения использования памяти ни по какой бывшей известной причине), добиваются журналов. Просмотрите последние изменения в своей физической среде или конфигурации CNR, чтобы узнать могут ли они быть источником проблем.

Журналы CNR являются вашими друзьями. Начиная использовать CNR, обновляя CNR или изменяя его конфигурацию, пользуйтесь командой `grr`, которая предназначена для обнаружения ошибок путем просмотра журналов. Затем работайте назад в журнале, чтобы понять, когда и как проблема возникла, и решите проблему.

Немедленные действия при возникновении проблемы

- **Не** перезагружайте CMTS, пока не запрошено сделать так Персоналом службы технической поддержки Cisco (применяется к только кабельным средам).
- **Не перезапускайте CNR до получения соответствующего требования персонала технической поддержки Cisco.**
- **Не отключайте безопасное восстановление при отказе, если это не было рекомендовано службой поддержки Cisco.**
- **Не** повторно загружайте, перезапускайте или разрушайте CNR в любом случае с происходящей пересинхронизацией безопасного аварийного переключения.
- **Копируйте файлы журналов в каталог, где они не будут перезаписаны.** Если CNR вызвал сбой, скопируйте файлы ядра в такой каталог, где они не будут перезаписаны.
- **Используйте** `inrcmd> server dhcp getRelatedServers` изолировать неверную конфигурацию безопасного аварийного переключения.
- **Ищите исключения в журналах.** Проверьте особенно последовательность запуска (это может быть в старом журнале): **быстро пройдите по программе grr по ключевым словам "error", "warn" и "connect" (например, grr -i error name_dhcp_1_log*).**

При направлении с проблемой крайне важно, чтобы вы не наносили дальнейшего ущерба при изоляции и решении начальной проблемы. Когда система уже хрупка, перезагрузка CMTS или перезапуск CNR создают непосредственные скачки загрузки в течение времени.

Цель – полностью восстановить работоспособность системы за минимальное время. Время работы (астрономическое) до вашего последнего количества действия; время к вашему первому действию не рассчитывает. Другими словами, не берите быстрое действие только ради быстрого действия. Тщательно обдумайте любые действия, которые предполагается выполнить.

Запустите журнал всех сделанных шагов и всех изменений, внесенных где угодно в системе: DHCP, DNS, или серверы TFTP и изменения, внесенные в любой CMTS или кабельный модем. Опишите проблему и журнал в подробностях, просто как рассматриваемое поведение.

[Анализ файлов журналов](#)

Соберите журналы (/var/nwreg2/logs). Проанализируйте их, проверьте на наличие ошибок и предупреждений. Используйте текстовый редактор для дальнейшего анализа ошибок интереса. Просмотрите содержимое журнала, предшествующее сообщению об ошибке, и найдите все записи, относящиеся к упоминаемому в нем MAC-адресу, IP-адресу или имени домена.

Возможно, потребуется включить дополнительную регистрацию для диагностики проблем DHCP. Сервер DHCP поддерживает широкий диапазон возможностей регистрации. См. [Ссылки команды CLI CNR](#) для списка параметров регистрации и пояснения каждого. Будьте внимательны, так как каждое сообщение журнала загружается на сервер. Необходимо сделать компромисс между количеством данных, которое вы просите, чтобы CNR регистрировал и производительность сервера.

[Выявление проблем LDAP](#)

Проблема может быть связана с сервером LDAP. CNR создает очередь из запросов к Серверу LDAP. Если Сервер LDAP не может не отставать от загрузки, очередь растет. Посмотрите в /var/nwreg2/data/dhcpreventstore каталоге. Событие хранит файлы, исправлены в размере, поэтому если очередь растет, CNR создает больше файлов. Если существует несколько файлов в каталоге, это указывает, что очередь выполняет резервное копирование. Та же очередь используется к запросам очереди к серверу DNS, поэтому если очередь выполняет резервное копирование, и вы используете DDNS, это могло бы заполняться запросами к серверу DNS. Чтобы определить, является ли проблема с LDAP, включите дополнительную регистрацию Интерфейса LDAP CNR. **Включите флаги журнала ldap-create-detail, ldap-query-detail и ldap-update-detail.** Сообщение журнала включает штампы времени, которые помогают вам определять, является ли LDAP системным узким местом.

[Подтвердите внутренние базы данных сетевого регистратора Cisco \(CNR\)](#)

Если вы подозреваете, что проблема может состоять в том, что один или больше внутренних баз данных CNR потерял целостность, обратитесь к [Руководствам пользователя](#) CNR, чтобы изучить, как выполнить утилиты проверки достоверности базы данных. Если одна из этих утилит указывает на проблему, продолжите придерживаться направлений в [Руководствах пользователя](#) для решения его.

[Проверьте Данные DNS С nslookup](#)

Служебная программа `nslookup` включена и с системами UNIX и с Windows NT. Это может быть использовано для опроса DNS сервера и поэтому полезно в проверке данных, хранимых сервером. Документация операционной системы содержит подробные сведения по ее возможностям.

Дополнительные сведения

- [Технические примечания о продукте Cisco CNS Network Registrar](#)
- [Техническая поддержка - Cisco Systems](#)