NTP на примере конфигурации контроллеров беспроводной локальной сети

Содержание

Введение

Этот документ объясняет, как настроить контроллеры беспроводной локальной сети (WLC) для синхронизации даты и времени с сервером Протокола NTP.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Базовые знания о конфигурации облегченных точек доступа (LAP) и WLC Cisco
- Базовые знания о NTP

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WLC Cisco 4400, который работает под управлением ПО версии 7.0.116.0
- LAP Cisco 1230AG Series
- Маршрутизатор Cisco серии 2800, который выполняет выпуск 12.4 (11) T программного обеспечения Cisco IOS

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Управление системной датой и время на контроллере беспроводной локальной сети

На WLC системная дата и время может быть вручную настроена от WLC или настроена для получения даты и времи из сервера NTP.

Системная дата и время может быть вручную настроена с помощью мастера настройки CLI или GUI/CLI WLC. Этот документ предоставляет пример конфигурации для синхронизации системной даты WLC и время через сервер NTP.

NTP является Протокол Интернета, используемый для синхронизации часов компьютеров к некоторой ссылке времени. RFC 1305 предоставляет подробные сведения о реализации v3 NTP. Сеть NTP обычно получает свое время от надежного источника времени, такого как радиочасы или атомные часы, подключенные к временному серверу. NTP тогда распределяет на этот раз по сети. Клиент NTP делает транзакцию с ее сервером по интервалу опроса (с 64 до 1024 секунд), который динамично изменяется в течение долгого времени в зависимости от состояний сети между сервером NTP и клиентом. Когда маршрутизатор связывается с плохим сервером NTP (например, сервером NTP с большой дисперсией), другая ситуация происходит. Маршрутизатор также увеличивает интервал опроса. Не больше, чем одна транзакция в минуту NTP необходима для синхронизации двух машин. Не возможно отрегулировать интервал опроса NTP на маршрутизаторе.

NTP использует понятие страты для описания, сколько NTP скачкообразно перемещает далеко, машина от надежного источника времени. Например, страта 1 временной сервер имеет радиочасы или атомные часы, непосредственно подключенные к нему. Это тогда передает свое время к страте 2 временных сервера через NTP и т.д.

Для получения дополнительной информации об оптимальных методах для развертывания NTP обратитесь к Протоколу сетевого времени: Рекомендации и Описание технологических решений. пример в этом документе использует маршрутизатор Cisco 2800 в качестве сервера NTP. WLC настроен для синхронизации его даты и времи с этим сервером NTP.

Настройка

Настройка Cisco маршрутизатор серии 2800 как сервер NTP

Настройка маршрутизатор как авторитетный сервер NTP

Используйте эту команду в режиме глобальной конфигурации, если вы хотите, чтобы система была авторитетным сервером NTP, даже если система "not synchronized" внешнему

источнику времени:

```
ntp master
!--- Makes the system an authoritative NTP server
```

Аутентификация NTP Настройки

Если вы хотите аутентифицировать ассоциации с другими системами для целей обеспечения безопасности, используйте команды, которые придерживаются. Первая команда активирует опцию Аутентификации NTP. Вторая команда определяет каждый из ключей проверки подлинности. Каждый ключ имеет ключевой номер, тип и значение. В настоящее время единственный ключевой поддерживаемый тип является md5. В-третьих, список "доверяемых" ключей проверки подлинности определен. Если ключу будут доверять, то эта система будет готова синхронизироваться с системой, которая использует этот ключ в ее пакетах NTP. Для настройки Аутентификации NTP используйте эти команды в режиме глобальной конфигурации:

```
ntp authenticate
!--- Enables the NTP authentication feature ntp authentication-key number md5 value !--- Defines
the authentication keys ntp trusted-key key-number !--- Defines trusted authentication keys
```

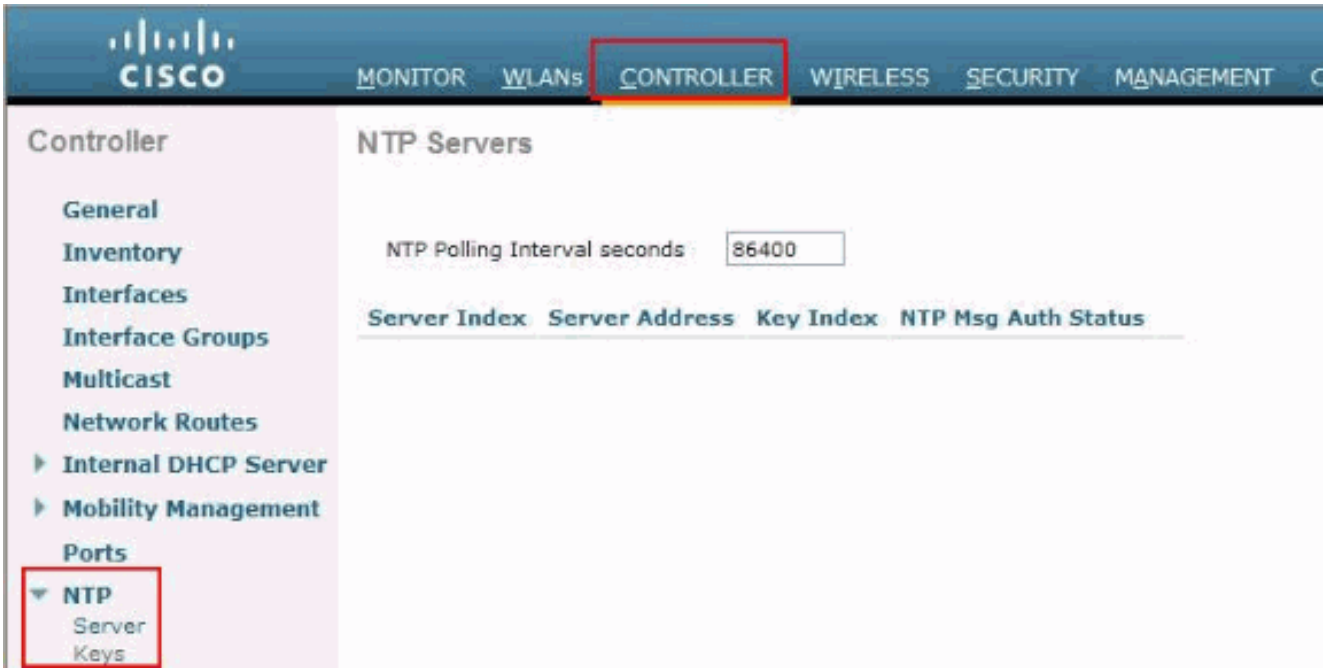
Вот конфигурация Сервера NTP в качестве примера на маршрутизаторе серии 2800. Маршрутизатором является NTP master, что означает действия маршрутизатора как авторитетный сервер NTP.

```
ntp master
ntp authenticate
ntp authentication-key 1 md5 0305480F0008 7
ntp trusted-key 1
```

Настройка WLC для сервера NTP

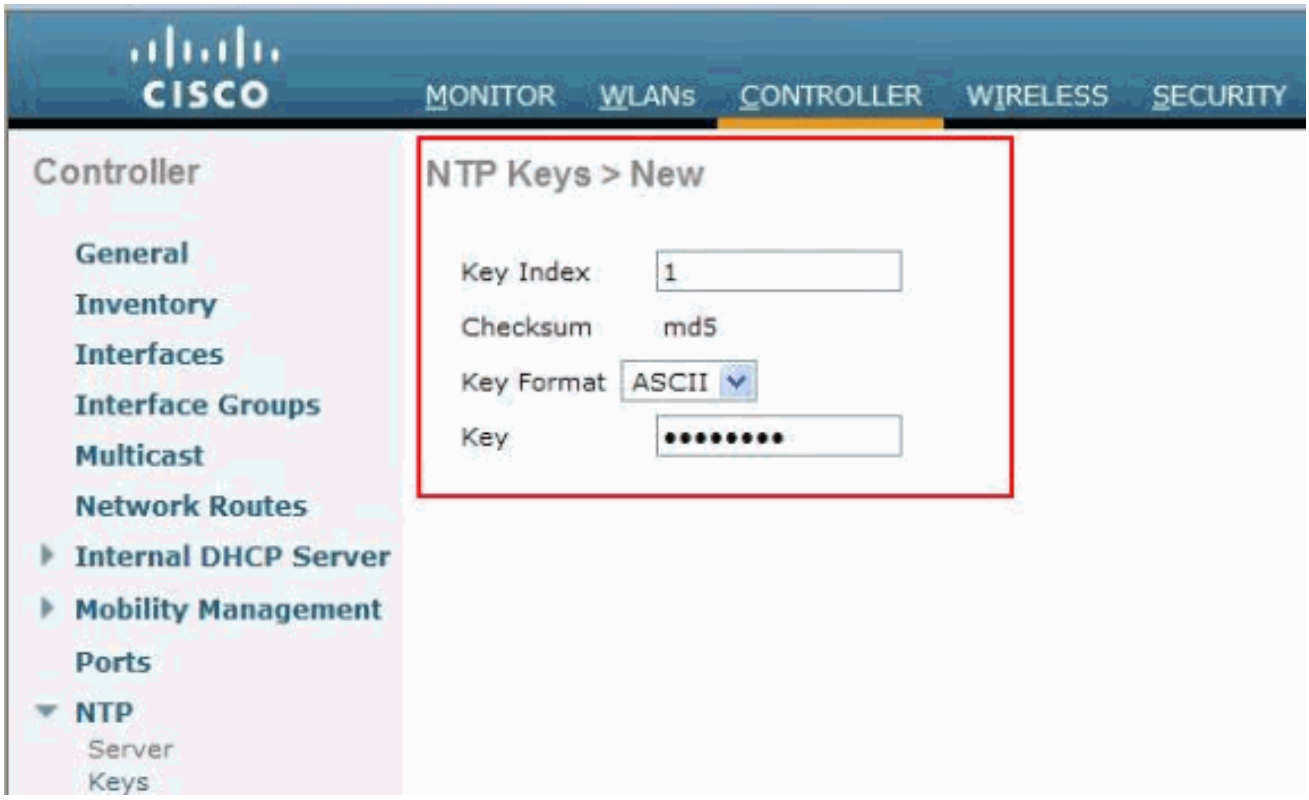
Начиная с этих 7.0.116.0 выпусков можно также настроить опознавательный канал между контроллером и сервером NTP. Для настройки Аутентификации NTP с помощью графического интерфейса контроллера выполните эти шаги:

1. Выберите **Controller> NTP> Servers** для открытия страницы NTP Servers. Нажмите **New** для добавления сервера NTP.**Страница NTP Servers> New** появляется.



2. Выберите приоритет сервера из **Индекса Сервера (Приоритетный)** выпадающий список.
3. Введите IP-адрес сервера NTP в **Сервер** текстовое поле **IPAddress**.
4. Включите аутентификацию сервера NTP путем установки опции NTP Server Authentication.

5. **Щелкните "Применить".**
6. Выберите **Controller> NTP> Keys**.
7. Нажмите **New** для создания ключа.
8. Введите ключевой индекс в **Ключевую** коробку **Текста указателя**.
9. Выберите формат ключа из выпадающего списка **Формата ключа**.
10. Введите Ключ в коробке **Ключевого текста**.



Проверка

Можно использовать эти команды от CLI WLC для проверки конфигурации:

```
(Cisco Controller) >show time Time..................................... Wed Nov 23
15:31:27 2011 Timezone delta.............................. 0:0 Timezone
location.............................. (GMT -6:00) Central Time (US and Canada) NTP Servers
NTP Polling Interval..................... 86400 Index NTP Key Index NTP Server NTP Msg Auth
Status ------- ------------------------------------------------------------------ 1 1 10.78.177.30
AUTH SUCCESS
```

Устранение неполадок

Можно использовать **команду debug ntp detail enable** для просмотра последовательности событий, которые происходят, как только конфигурация сервера NTP реализована на WLC.

```
*sntpReceiveTask: Nov 23 15:08:24.360: Started=3531049704.360568 2011 Nov 23 15:08:24.360

*sntpReceiveTask: Nov 23 15:08:24.360: Looking for the socket addresses

*sntpReceiveTask: Nov 23 15:08:24.360: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6.
 Outgoing packet on NTP Server on socket 0:

*sntpReceiveTask: Nov 23 15:08:24.360: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000

*sntpReceiveTask: Nov 23 15:08:24.361: ori=0.000000 rec=0.000000
*sntpReceiveTask: Nov 23 15:08:24.361: tra=3531049704.360889 cur=3531049704.360889

*sntpReceiveTask: Nov 23 15:08:24.361: Host Supports NTP authentication with Key Id = 1

*sntpReceiveTask: Nov 23 15:08:24.361: NTP Auth Key Id = 1 Key Length = 5

*sntpReceiveTask: Nov 23 15:08:24.361: MD5 Hash and Key Id added in NTP Tx packet
```

```
*sntpReceiveTask: Nov 23 15:08:24.361: Flushing outstanding packets

*sntpReceiveTask: Nov 23 15:08:24.361: Flushed 0 packets totalling 0 bytes

*sntpReceiveTask: Nov 23 15:08:24.361: Packet of length 68 sent to 10.78.177.30 UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: Packet of length 68 received from 10.78.177.30
UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: KeyId In Recieved NTP Packet 1

*sntpReceiveTask: Nov 23 15:08:24.363: KeyId 1 found in recieved NTP packet exists as part of
the trusted Key/s

*sntpReceiveTask: Nov 23 15:08:24.363: The NTP trusted Key Id  1 length = 5

*sntpReceiveTask: Nov 23 15:08:24.363: NTP Message Authentication - SUCCESS *sntpReceiveTask:
Nov 23 15:08:24.363: sta=0 ver=3 mod=4 str=8 pol=8 dis=3.875031 ref=3531071269.384065
*sntpReceiveTask: Nov 23 15:08:24.363: ori=3531049704.360889 rec=3531071270.103183
*sntpReceiveTask: Nov 23 15:08:24.363: tra=3531071270.103387 cur=3531049704.363251
```

Дополнительные сведения

- Протокол NTP (Network Time Protocol, протокол сетевого времени): Рекомендации и Описание технологических решений
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 7.0.116.0
- Cisco Systems – техническая поддержка и документация