

NTP no exemplo de configuração dos controladores do Wireless LAN

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Controlando a data do sistema e o tempo no controlador do Wireless LAN](#)

[Configurar](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento explica como configurar os controladores do Wireless LAN (WLC) para sincronizar a data e hora com um server do Network Time Protocol (NTP).

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico da configuração do Lightweight Access Points (regações) e do Cisco WLC
- Conhecimento básico do NTP

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 4400 WLC que executa a versão de software 7.0.116.0
- Regações do Cisco 1230AG Series
- Cisco 2800 Series Router que executa o Software Release 12.4(11)T de Cisco IOS®

As informações neste documento são baseadas nestas versões de software e hardware:

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

[Controlando a data do sistema e o tempo no controlador do Wireless LAN](#)

Em um WLC, a data do sistema e o tempo podem manualmente ser configurados do WLC ou ser configurados para obter a data e hora de um servidor de NTP.

A data do sistema e o tempo podem manualmente ser configurados usando o assistente da configuração de CLI ou o WLC GUI/CLI. Este documento fornece um exemplo de configuração sincronizando a data do sistema e o tempo WLC através de um servidor de NTP.

O NTP é um protocolo de internet usado para sincronizar os pulsos de disparo dos computadores a alguma referência de tempo. [O RFC 1305](#) fornece a informação detalhada na aplicação NTP v3. [Uma rede NTP recebe geralmente seu tempo de uma fonte de tempo autoritária, tal como um relógio de rádio ou um relógio atômico anexado a um Time Server. O NTP distribui então esta vez através da rede. Um cliente de NTP faz uma transação com seu server sobre o intervalo de polling \(64 a 1024 segundos\), que muda dinamicamente ao longo do tempo segundo as condições de rede entre o servidor de NTP e o cliente. A outra situação ocorre quando o roteador se comunica a um servidor de NTP ruim \(por exemplo, servidor de NTP com grande dispersão\). O roteador igualmente aumenta o intervalo de votação. Não mais de uma transação NTP pelo minuto é precisada de sincronizar duas máquinas. Não é possível ajustar o intervalo de votação NTP em um roteador.](#)

O NTP usa o conceito de um estrato para descrever quantos saltos NTP afastado uma máquina é de uma fonte de tempo autoritária. Por exemplo, um Time Server do estrato 1 tem um rádio ou um relógio atômico anexado diretamente a ele. Envia então seu tempo a um Time Server do estrato 2 com o NTP, e assim por diante.

Para obter mais informações sobre dos melhores prática para a distribuição de NTP, refira o [protocolo Network Time Protocol: White Paper dos melhores prática](#). O exemplo neste documento usa um Cisco 2800 Router como um servidor de NTP. O WLC é configurado para sincronizar sua data e hora com este servidor de NTP.

[Configurar](#)

[Configurando o Cisco 2800 Series Router como um servidor de NTP](#)

Configurando o roteador como um servidor de NTP competente

Use este comando no modo de configuração global se você quer o sistema ser um servidor de NTP competente, mesmo se o sistema não está sincronizado a um origem de tempo exterior:

```
ntp master
```

!--- Makes the system an authoritative NTP server

Configurando a autenticação de NTP

Se você quer autenticar para efeitos de segurança as associações com outros sistemas, use os comandos que seguem. O primeiro comando permite a característica da autenticação de NTP. O comando `second` define cada um das chaves de autenticação. Cada chave tem um número chave, um tipo, e um valor. Atualmente, o único tipo chave apoiado é md5. Em terceiro lugar, uma lista de chaves de autenticação “confiadas” é definida. Se uma chave é confiada, este sistema estará pronto para sincronizar a um sistema que use esta chave em seus pacotes de NTP. A fim configurar a autenticação de NTP, use estes comandos no modo de configuração global:

```
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*

Está aqui uma configuração de servidor de NTP do exemplo no 2800 Series Router. O roteador é o mestre NTP, que significa que o roteador atua como o servidor de NTP competente.

```
ntp master
```

```
ntp authenticate
```

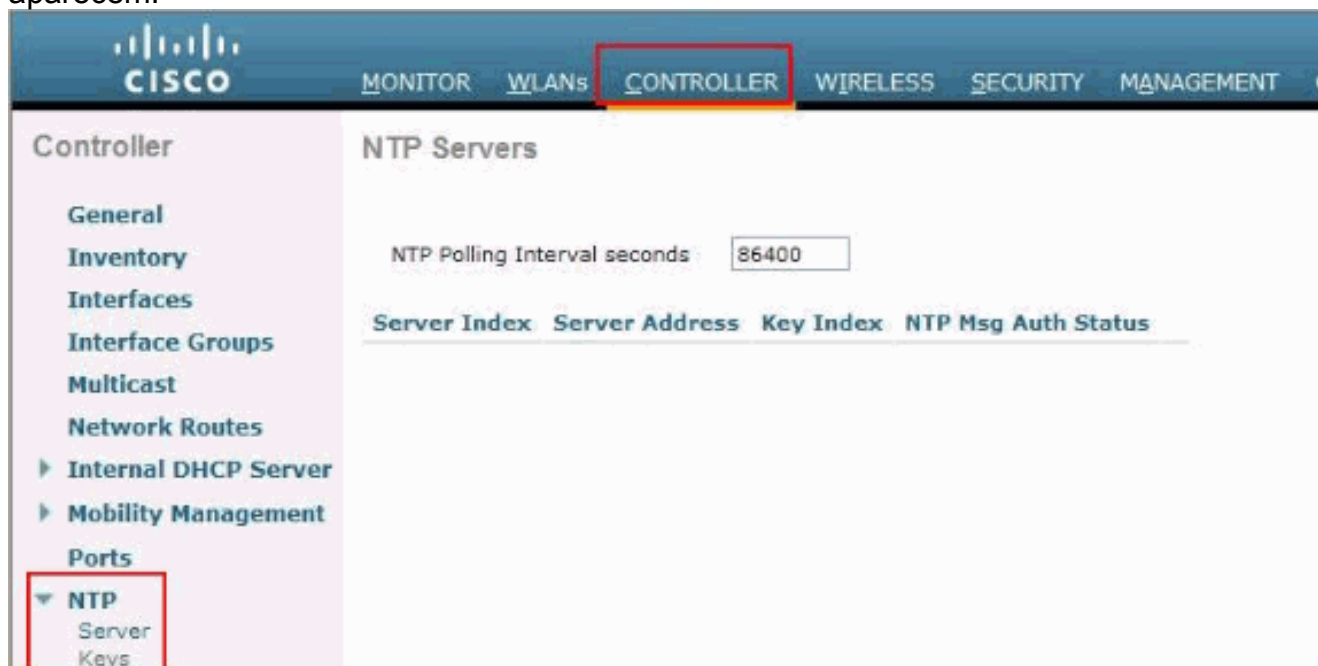
```
ntp authentication-key 1 md5 0305480F0008 7
```

```
ntp trusted-key 1
```

Configurando o WLC para o servidor de NTP

Começando com a liberação de 7.0.116.0, você pode igualmente configurar um canal da autenticação entre o controlador e o servidor de NTP. A fim configurar a autenticação de NTP usando o controlador GUI, execute estas etapas:

1. Escolha o **controlador > o NTP > os server** para abrir a página dos servidores de NTP. Clique **novos** para adicionar um servidor de NTP. **Os servidores de NTP > página nova** aparecem.



2. Escolha uma prioridade do server da lista de drop-down do **deslocamento predeterminado do server (prioridade)**.
3. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de NTP à caixa de texto do **IP address do server**.
4. Permita a autenticação de servidor de NTP selecionando a caixa de verificação da

autenticação de servidor de NTP.

The screenshot shows the Cisco Controller web interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Controller' and lists various configuration sections: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, and NTP (expanded to show Server and Keys). The main content area is titled 'NTP Servers > New' and contains the following fields:

- Server Index (Priority): 1 (dropdown)
- Server IP Address: 10.78.177.30 (text box)
- Enable NTP Authentication:
- Key Index: 1 (text box)

5. Clique em Apply.
6. Escolha o **controlador > o NTP > as chaves**.
7. Clique **novo** para criar uma chave.
8. Incorpore o deslocamento predeterminado chave à caixa de texto do **deslocamento predeterminado chave**.
9. Escolha o formato chave da lista de drop-down **chave do formato**.
10. Incorpore a chave à caixa de texto **chave**.

The screenshot shows the Cisco Controller web interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Controller' and lists various configuration sections: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, and NTP (expanded to show Server and Keys). The main content area is titled 'NTP Keys > New' and contains the following fields:

- Key Index: 1 (text box)
- Checksum: md5 (text box)
- Key Format: ASCII (dropdown)
- Key: [Redacted with dots] (text box)

Verificar

Você pode usar estes comandos do WLC CLI verificar a configuração:

```
(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
```

Troubleshooting

Você pode usar o comando **enable do detalhe NTP debug** ver a sequência de evento que ocorre a configuração de servidor de NTP é feito uma vez no 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
```

Informações Relacionadas

- [Protocolo Network Time Protocol: White Paper de práticas recomendadas](#)
- [Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0.116.0](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)