무선 LAN 컨트롤러에서 NTP 구성

목차

소개

이 문서에서는 NTP(Network Time Protocol) 서버와 날짜 및 시간을 동기화하도록 AireOS WLC(Wireless LAN Controller)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco WLC 구성에 대한 기본 지식
- NTP에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.8.110을 실행하는 Cisco WLC 3504.

- Cisco IOS® 소프트웨어 릴리스 15.2(6)E2를 실행하는 Cisco Catalyst 3560-CX 시리즈 L3 스위치.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Wireless LAN Controller에서 시스템 날짜 및 시간 관리

WLC에서 시스템 날짜 및 시간을 WLC에서 수동으로 구성하거나 NTP 서버에서 날짜 및 시간을 가져오도록 구성할 수 있습니다.

시스템 날짜 및 시간은 CLI 컨피그레이션 마법사 또는 WLC GUI/CLI에서 수동으로 구성할 수 있습니다.

이 문서에서는 NTP 서버를 통해 WLC 시스템 날짜 및 시간을 동기화하는 컨피그레이션 예를 제공합니다.

NTP는 컴퓨터의 시계를 특정 시간 참조에 동기화하기 위해 가변 대기 시간 데이터 네트워크를 통해 컴퓨터 시스템 간의 시계 동기화를 위한 네트워크 프로토콜입니다. RFC 1305 및 RFC 5905는 각각 NTPv3 및 NTPv4 구현에 대한 자세한 정보를 제공합니다.

NTP 네트워크는 일반적으로 시간 서버에 연결된 라디오 클럭 또는 원자 클럭 등의 신뢰할 수 있는 시간 소스에서 시간을 수신합니다. 그런 다음 NTP는 이 시간을 네트워크 전체에 배포합니다.

NTP 클라이언트는 폴링 간격 동안 서버와 트랜잭션을 수행하며, 이 작업은 시간이 지남에 따라 동적으로 변경되며 NTP 서버와 클라이언트 간의 네트워크 상태에 따라 달라집니다.

NTP는 계층 개념을 사용하여 신뢰할 수 있는 시간 소스에서 시스템을 벗어난 NTP 홉의 수를 설명합니다. 예를 들어, 계층 1 시간 서버에는 무선 장치 또는 원자 클럭이 직접 연결되어 있습니다. 그런 다음 NTP 등을 통해 시간을 계층 2 시간 서버로 전송합니다.

NTP 구축의 모범 사례에 대한 자세한 내용은 Use Best Practices for Network Time Protocol을 참조하십시오.

이 문서의 예에서는 Cisco Catalyst 3560-CX Series L3 Switch를 NTP 서버로 사용합니다. WLC는 날짜 및 시간을 이 NTP 서버와 동기화하도록 구성됩니다.

구성

네트워크 다이어그램

WLC ---- 3560-CX L3 Switch ---- NTP server

설정

L3 스위치를 신뢰할 수 있는 NTP 서버로 구성

시스템이 외부 시간 소스에 동기화되지 않은 경우에도 시스템이 신뢰할 수 있는 NTP 서버가 되도록 하려면 글로벌 컨피그레이션 모드에서 이 명령을 사용합니다.

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

NTP 인증 구성

보안을 위해 다른 시스템과의 연결을 인증하려면 다음 명령을 사용합니다. 첫 번째 명령은 NTP 인증 기능을 활성화합니다.

두 번째 명령은 각 인증 키를 정의합니다. 각 키에는 키 번호, 유형 및 값이 있습니다. 현재 지원되는 유일한 키 유형은 md5입니다.

셋째, 신뢰할 수 있는 인증 키 목록이 정의됩니다. 키를 신뢰할 수 있는 경우 이 시스템은 NTP 패킷에서 이 키를 사용하는 시스템과 동기화할 준비가 됩니다. NTP 인증을 구성하려면 글로벌 컨피그레이션 모드에서 다음 명령을 사용합니다.

```
#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
```

다음은 3560-CX L3 스위치의 NTP 서버 컨피그레이션 예입니다. 스위치는 NTP입니다 master이는 라우터가 신뢰할 수 있는 NTP 서버 역할을 하지만 그 자체가 다른 NTP 서버 xxxx.xxx에서 시간을 가져온다는 의미입니다.

```
(config)#ntp authentication-key 1 md5 1511021F0725 7
(config)#ntp authenticate
(config)#ntp trusted-key 1
(config)#ntp master
(config)#ntp server xxxx.xxx
```

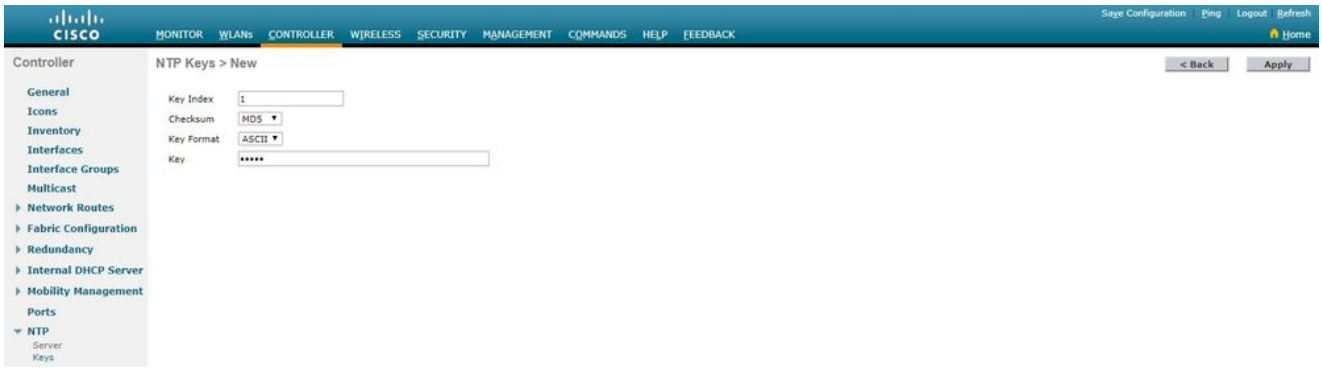
NTP 서버에 대한 WLC 구성

버전 8.6부터 NTPv4를 활성화할 수 있습니다. 컨트롤러와 NTP 서버 간에 인증 채널을 구성할 수도

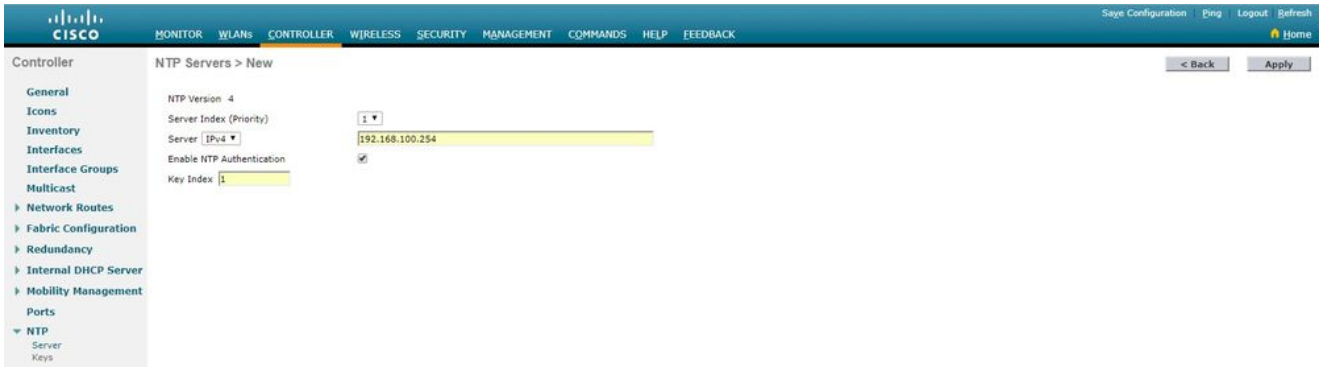
있습니다.

컨트롤러 GUI에서 NTP 인증을 구성하려면 다음 단계를 수행합니다.

1. Controller(컨트롤러) > NTP > Keys(키)를 선택합니다.
2. 키를 생성하려면 New(새로 만들기)를 클릭합니다.
3. 키 인덱스 텍스트 상자에 키 인덱스를 입력합니다.
4. Key Checksum (MD5 또는 SHA1) 및 Key Format 드롭다운 목록을 선택합니다.
5. 키 텍스트 상자에 키를 입력합니다.

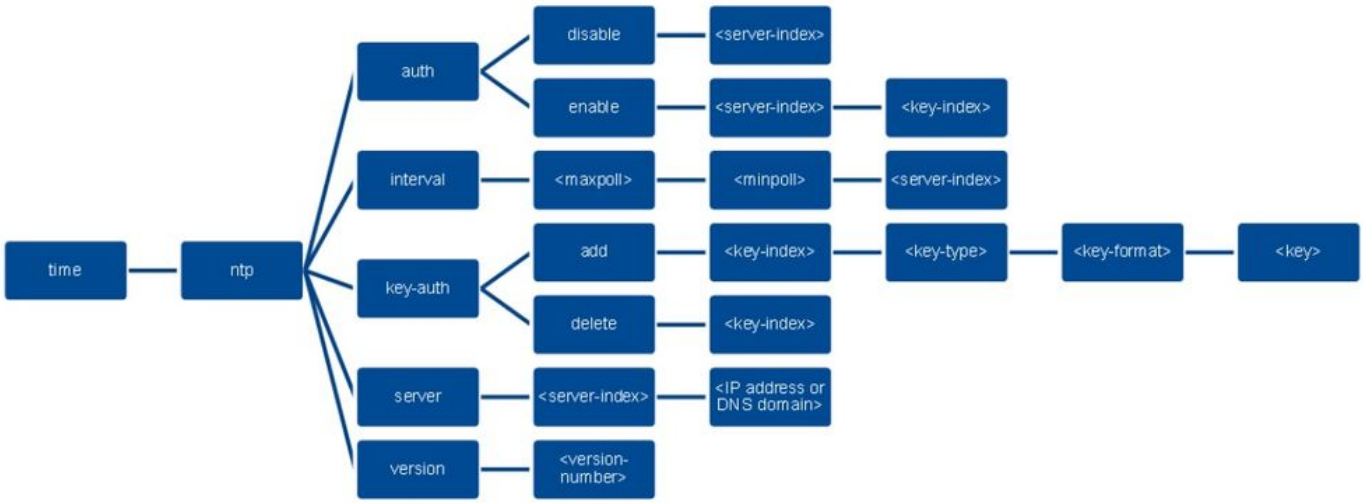


6. Controller(컨트롤러) > NTP > Servers(서버)를 선택하여 NTP Servers(NTP 서버) 페이지를 엽니다. 버전 3 또는 4를 선택한 다음 New(새로 만들기)를 클릭하여 NTP 서버를 추가합니다. NTP Servers(NTP 서버) > New(새) 페이지가 나타납니다.
7. Server Index(Priority)를 선택합니다.
8. Server IP Address(서버 IP 주소) 텍스트 상자에 NTP 서버 IP 주소를 입력합니다.
9. Enable NTP server authentication(NTP 서버 인증 활성화), NTP Server Authentication(NTP 서버 인증) 확인란을 선택하고 이전에 구성한 Key Index(키 인덱스)를 선택합니다.



10. 적용을 클릭합니다.

컨트롤러 CLI를 통해 NTP 인증을 구성하려면 다음 명령 트리를 추적합니다.




```
>config time ntp version 4
>config time ntp key-auth add 1 md5 ascii cisco
>config time ntp server 1 192.168.100.254
>config time ntp auth enable 1 1
```

다음을 확인합니다.

NTP 서버에서

```
#show ntp status
Clock is synchronized, stratum 3, reference is x.x.x.x
nominal freq is 286.1023 Hz, actual freq is 286.0901 Hz, precision is 2**21
ntp uptime is 6591900 (1/100 of seconds), resolution is 3496
reference time is E007C909.80902653 (09:23:21.502 UTC Fri Feb 8 2019)
clock offset is 0.3406 msec, root delay is 59.97 msec
root dispersion is 25.98 msec, peer dispersion is 1.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000042509 s/s
system poll interval is 128, last update was 7 sec ago.

#show ntp associations

 address ref clock st when poll reach delay offset disp
*~x.x.x.x y.y.y.y 2 20 1024 17 13.634 0.024 1.626
 ~127.127.1.1 .LOCL. 7 9 16 377 0.000 0.000 0.232
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

#show ntp information
Ntp Software Name : Cisco-ntpv4
Ntp Software Version : Cisco-ntpv4-1.0
Ntp Software Vendor : CISCO
Ntp System Type : Cisco IOS / APM86XXX
```

WLC에서

GUI

WLC가 통신을 설정하는 동안:

연결이 설정된 후:

WLC CLI에서

```
(Cisco Controller) >show time

Time..................................... Fri Feb 8 10:14:47 2019

Timezone delta..................................... 0:0
Timezone location.................................

NTP Servers
 NTP Version..................................... 4

Index NTP Key NTP Server NTP Key Polling Intervals
 Index Type Max Min
 ------------------------------------------------------------
 1 1 192.168.100.254 MD5 10 6

NTPQ status list of NTP associations

assoc
 ind assid status conf reach auth condition last_event cnt src_addr
 ================================================================================
```

```
 1 1385 f63a yes yes ok sys.peer sys_peer 3 192.168.100.254


(Cisco Controller) >
```

문제 해결

Cisco IOS를 실행하는 NTP 서버 측에서 debug ntp all enable 명령을 사용합니다:

```
#debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
#
(communication between SW and NTP server xxxx.xxx)
Feb 8 09:52:30.563: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:52:30.577: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:53:10.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:10.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:53:10.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).

(communication between SW and NTP server xxxx.xxx)
Feb 8 09:53:37.566: NTP message sent to x.x.x.x, from interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP message received from x.x.x.x on interface 'Vlan1' (192.168.1.81).
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:53:37.580: NTP Core(DEBUG): ntp_receive: peer is 0x0D284B34, next action is 1.

(communication between SW and WLC)
Feb 8 09:54:17.421: NTP message received from 192.168.100.253 on interface 'Vlan100' (192.168.100.254).
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: message received
Feb 8 09:54:17.421: NTP Core(DEBUG): ntp_receive: peer is 0x00000000, next action is 3.
Feb 8 09:54:17.421: NTP message sent to 192.168.100.253, from interface 'Vlan100' (192.168.100.254).
```

WLC 측:

```
 >debug ntp ?

detail Configures debug of detailed NTP messages.
low Configures debug of NTP messages.
packet Configures debug of NTP packets.

(at the time of writte this doc there was Cisco bug ID CSCvo29660
on which the debugs of ntpv4 are not printed in the CLI. The below debugs are using NTPv3.)
(Cisco Controller) >debug ntp detail enable
(Cisco Controller) >debug ntp packet enable
```

```
(Cisco Controller) >*emWeb: Feb 08 11:26:53.896: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = -1

*emWeb: Feb 08 11:26:58.143: Key Id = 1 found at Local Index = 0

*sntpReceiveTask: Feb 08 11:26:58.143: Initiating time sequence

*sntpReceiveTask: Feb 08 11:26:58.143: Fetching time from:192.168.100.254

*sntpReceiveTask: Feb 08 11:26:58.143: Started=3758614018.143350 2019 Feb 08 11:26:58.143

*sntpReceiveTask: Feb 08 11:26:58.143: hostname=192.168.100.254 hostIdx=1 hostNum=0
*sntpReceiveTask: Feb 08 11:26:58.143: Looking for the socket addresses

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6. Outgoing packet on NTP Server on socket 0:

*sntpReceiveTask: Feb 08 11:26:58.143: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000

*sntpReceiveTask: Feb 08 11:26:58.143: ori=0.000000 rec=0.000000
*sntpReceiveTask: Feb 08 11:26:58.143: tra=3758614018.143422 cur=3758614018.143422

*sntpReceiveTask: Feb 08 11:26:58.143: Host Supports NTP authentication with Key Id = 1

*sntpReceiveTask: Feb 08 11:26:58.143: NTP Auth Key Id = 1 Key Length = 5

*sntpReceiveTask: Feb 08 11:26:58.143: MD5 Hash and Key Id added in NTP Tx packet

*sntpReceiveTask: Feb 08 11:26:58.143: 00000000: 1b 0f 08 00 00 00 00 00 00 00 00 00 00 00 00 00 ......
*sntpReceiveTask: Feb 08 11:26:58.143: 00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ......
*sntpReceiveTask: Feb 08 11:26:58.143: 00000020: 00 00 00 00 00 00 00 00 e0 07 e6 02 24 b7 50 00 ......
*sntpReceiveTask: Feb 08 11:26:58.143: 00000030: 00 00 00 01 e4 35 f3 1a 89 f0 93 c5 51 c7 c5 23 .....5
*sntpReceiveTask: Feb 08 11:26:58.143: 00000040: 01 dd 67 e0 ..g.
*sntpReceiveTask: Feb 08 11:26:58.143: Flushing outstanding packets

*sntpReceiveTask: Feb 08 11:26:58.143: Flushed 0 packets totalling 0 bytes

*sntpReceiveTask: Feb 08 11:26:58.143: Packet of length 68 sent to ::ffff:192.168.100.254 UDPport=123
*emWeb: Feb 08 11:26:58.143: ntp Auth key Info = 0

*emWeb: Feb 08 11:26:58.143: idx != 0 : ntp key Id = 1 Msg auth Status = 66

*sntpReceiveTask: Feb 08 11:26:58.146: Packet of length 68 received from ::ffff:192.168.100.254 UDPport
*sntpReceiveTask: Feb 08 11:26:58.146: Incoming packet on socket 0: has Authentication Enabled
*sntpReceiveTask: Feb 08 11:26:58.146: 00000000: 1c 04 08 eb 00 00 0e a0 00 00 0b 2e c3 16 11 07 ......
*sntpReceiveTask: Feb 08 11:26:58.146: 00000010: e0 07 e5 f8 d3 21 bf 57 e0 07 e6 02 24 b7 50 00 .....!
*sntpReceiveTask: Feb 08 11:26:58.146: 00000020: e0 07 e6 02 24 e5 e3 b4 e0 07 e6 02 24 f3 c7 5a ....$.
*sntpReceiveTask: Feb 08 11:26:58.146: 00000030: 00 00 00 01 32 e4 26 47 33 16 50 bd d1 37 63 b7 ....2.
*sntpReceiveTask: Feb 08 11:26:58.146: KeyId In Recieved NTP Packet 1

*sntpReceiveTask: Feb 08 11:26:58.146: KeyId 1 found in recieved NTP packet exists as part of the trust

*sntpReceiveTask: Feb 08 11:26:58.146: The NTP trusted Key Id 1 length = 5

*sntpReceiveTask: Feb 08 11:26:58.146: NTP Message Authentication - SUCCESS

*sntpReceiveTask: Feb 08 11:26:58.146: sta=0 ver=3 mod=4 str=4 pol=8 dis=0.043671 ref=3758614008.824734

*sntpReceiveTask: Feb 08 11:26:58.146: ori=3758614018.143422 rec=3758614018.144133
```

```
*sntpReceiveTask: Feb 08 11:26:58.146: Offset=-0.000683+/-0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: best=-0.000683+/-0.002787

*sntpReceiveTask: Feb 08 11:26:58.146: accepts=1 rejects=0 flushes=0

*sntpReceiveTask: Feb 08 11:26:58.146: Correction: -0.000683 +/- 0.002787 disp=1.937698

*sntpReceiveTask: Feb 08 11:26:58.146: Setting clock to 2019 Feb 08 11:26:58.145 + 0.001 +/- 1.940 secs
*sntpReceiveTask: Feb 08 11:26:58.146: correction -0.001 +/- 1.938+0.003 secs - ignored


(Cisco Controller) >
```

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.