目 录

1 NTP

1.1 NTP配置命令

说明

支持 NTP 的接口均为三层接口，包括三层以太网接口/子接口、VLAN 接口、Tunnel 接口等。

1.1.1 display ntp-service ipv6 sessions

display ntp-service ipv6 sessions 命令用来显示 NTP 服务的所有 IPv6 会话信息。

【命令】

display ntp-service ipv6 sessions [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

verbose：显示 NTP 服务的所有 IPv6 会话的详细信息。如果不指定该参数，则只显示所有 IPv6 会话的简要信息。

【举例】

显示 NTP 服务的所有 IPv6 会话的简要信息。

```
<Sysname> display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:   [125]3000::32
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 1               Poll interval: 64
 Last receive time: 6            Offset: -0.0
 Roundtrip delay: 0.0            Dispersion: 0.0

 Total sessions: 1
```

表1-1 display ntp-service ipv6 sessions 命令显示信息描述表

字段	描述
[12345]	1：系统选中的时间服务器，即当前与设备进行时间同步的时间服务器 2：该时间服务器的时钟层数小于等于15

字段	描述
	3：该时间服务器的时钟通过了时钟选择算法 4：该时间服务器的时钟为候选的时钟 5：该时间服务器是通过配置命令指定的
Source	时间服务器的IPv6地址。若该字段显示为::，表示时间服务器的IPv6地址尚未解析成功
Reference	时间服务器的参考时钟ID 当参考时钟为本地时钟时，本字段的显示情况和Clock stratum字段的取值有关： • 当 Clock stratum 字段为 0 或 1 时，本字段显示为 LOCL • 当 Clock stratum 字段为其他值时，本字段显示为 IPv6 地址前 32 位的 MD5 摘要值，摘要信息按照点分十进制形式显示 当参考时钟为网络中其他设备的时钟时，本字段显示为IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
Clock stratum	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1～16，层数取值越小，时钟的准确度最高，层数为16的时钟处于未同步状态
Reachabilities	时间服务器的可达性计数，0表示时间服务器不可达
Poll interval	轮询间隔，即两个连续NTP报文之间的时间间隔，单位为秒
Last receive time	最近一次接收到NTP报文或更新本地时间到当前时间的时间间隔 缺省单位为秒；如果时间间隔大于2048秒，则显示为分钟m；如果时间间隔大于300分钟，则显示为小时h；如果时间间隔大于96小时，则显示为天d；如果时间间隔大于999天，则显示为年y；如果最近一次接收到NTP报文或更新本地时间比当前时间晚，则显示为“-”
Offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
Roundtrip delay	本地设备到时间服务器的往返时延，单位为毫秒
Dispersion	系统时钟相对于参考时钟的最大误差，单位为毫秒
Total sessions	总的会话数目

显示 NTP 服务的所有 IPv6 会话的详细信息。

```
<Sysname> display ntp-service ipv6 sessions verbose

 Clock source: 1::1
 Session ID: 36144
 Clock stratum: 16
 Clock status:  configured, insane, valid, unsynced
 Reference clock ID: INIT
 VPN instance: Not specified
 Local mode: sym_active, local poll interval: 6
 Peer mode: unspec, peer poll interval: 10
 Offset: 0.0000ms, roundtrip delay: 0.0000ms, dispersion:  15937ms
 Root roundtrip delay: 0.0000ms, root dispersion: 0.0000ms
 Reachabilities:0, sync distance: 15.938
 Precision: 2^10, version: 4, source interface: Not specified
 Reftime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
```

```
Orgtime: d17cbb21.0f318106  Tue, May 17 2011  9:15:13.059
Rcvtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Xmttime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Roundtrip delay samples: 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
Offset samples: 0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
Filter order: 0     1     2     3     4     5     6     7

Total sessions: 1
```

表1-2 display ntp-service ipv6 sessions verbose 命令显示信息描述表

字段	描述
Clock source	时间服务器的IPv6地址。若该字段显示为::，表示时间服务器的IPv6地址尚未解析成功
Session ID	会话ID
Clock stratum	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1～16，层数取值越小，表示时钟的准确度最高，层数为16的时钟处于未同步状态
Clock status	会话的状态，该字段的取值及含义为： • configured：表示该会话是配置命令所建立的 • dynamic：表示该会话是动态生成的 • master：表示该会话对应的时间服务器是当前系统的主时间服务器 • selected：表示该会话对应时间服务器的时钟通过了时钟选择算法 • candidate：表示该会话对应时间服务器的时钟为候选时钟 • sane：表示该会话对应的时间服务器通过身份验证，该时间服务器的时钟将作为参考时钟 • insane：表示该会话对应的时间服务器未通过身份验证，或该时间服务器通过身份验证但其时钟不作为参考时钟 • valid：表示该会话对应的时间服务器是有效的（通过验证、处于同步状态、层数有效、根延时/离差未越界等） • invalid：表示该会话对应的时间服务器是无效的 • unsynced：表示该会话对应时间服务器的时钟未同步或层数非法
Reference clock ID	时间服务器的参考时钟ID 当参考时钟为本地时钟时，本字段的显示情况和Clock stratum字段的取值有关： • 当 Clock stratum 字段为 0 或 1 时，本字段显示为 LOCL • 当 Clock stratum 字段为其他值时，本字段显示为 IPv6 地址前 32 位的 MD5 摘要值，摘要信息按照点分十进制形式显示 当参考时钟为网络中其他设备的时钟时，本字段显示为IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
VPN instance	时间服务器所属的VPN实例的名称，如果时间服务器位于公网，则显示为Not specified（暂不支持）
Local mode	本地设备的工作模式，取值包括： • unspec：未指定模式 • sym_active：主动对等体模式

字段	描述
	• sym_passive：被动对等体模式 • client：客户端模式 • server：服务器模式 • broadcast：广播服务器模式或组播服务器模式 • bclient：广播客户端模式或组播客户端模式
local poll interval	本地设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Peer mode	对端设备的工作模式，取值包括： • unspec：未指定模式 • sym_active：主动对等体模式 • sym_passive：被动对等体模式 • client：客户端模式 • server：服务器模式 • broadcast：广播服务器模式或组播服务器模式 • bclient：广播客户端模式或组播客户端模式
peer poll interval	对端设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
roundtrip delay	本地设备到时间服务器的往返时延，单位为毫秒
dispersion	系统时钟相对于参考时钟的最大误差，单位为毫秒
Root roundtrip delay	本地设备到主时间服务器的往返时延，单位为毫秒
root dispersion	系统时钟相对主参考时钟的最大误差，单位为毫秒
Reachabilities	时间服务器的可达性计数，0表示时间服务器不可达
sync distance	表示相对上一级时间服务器的同步距离，由误差disper和往返时延delay计算而来，单位为秒
Precision	系统时钟的精度
version	NTP版本，取值为1～4
source interface	源接口，未指定源接口时，此字段显示为Not specified
Reftime	NTP报文中的参考时间戳
Orgtime	NTP报文中的起始时间戳
Rcvtime	NTP报文的接收时间戳
Xmttime	NTP报文的发送时间戳
Roundtrip delay samples	本地设备到时间服务器往返时延的抽样值
Offset samples	相对于参考时钟的时钟偏移的抽样值
Filter order	样本信息排序
Reference clock	本地时钟的工作状态，只有通过**ntp-service refclock-master**命令设置本地时钟作为参考时

字段	描述
status	钟时，才会显示该字段 当本地时钟的reach值等于255时，该字段取值为working normally；否则，该字段取值为working abnormally
Total sessions	总的会话数目

1.1.2 display ntp-service sessions

display ntp-service sessions 命令用来显示 NTP 服务的所有 IPv4 会话信息。

【命令】

display ntp-service sessions [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

verbose：显示 NTP 服务的所有 IPv4 会话的详细信息。如果不指定该参数，则只显示所有会话的简要信息。

【使用指导】

设备作为 NTP 广播服务器或 NTP 组播服务器时，在设备上执行 **display ntp-service sessions** 命令不会显示与该广播服务器或组播服务器对应的 NTP 服务的 IPv4 会话信息，但是这些会话会统计在总的会话数中。

【举例】

显示 NTP 服务的所有 IPv4 会话的简要信息。

```
<Sysname> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]LOCAL(0)        LOCL              0     1   64    - 0.0000 0.0000 7937.9
    [5]0.0.0.0         INIT             16     0   64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

表1-3 display ntp-service sessions 命令显示信息描述表

字段	描述
source	参考时钟为本地时钟时，显示为LOCAL(*number*)，表示本地时钟的地址为127.127.1.*number*，其中*number*为NTP的进程号，取值范围为0～3 参考时钟为网络中其他设备的时钟时，显示为时间服务器的IP地址。若该字段显示为0.0.0.0，表示时间服务器的IP地址尚未解析成功
reference	时间服务器的参考时钟ID

字段	描述
	当参考时钟为本地时钟时，本字段的显示情况和stra字段的取值有关： • 当 stra 字段为 0 或 1 时，本字段将显示为 LOCL • 当 stra 字段为其他值时，本字段将显示为本地时钟的 IP 地址 当参考时钟为网络中其他设备的时钟时，本字段显示为该设备的IP地址，若该设备为IPv6设备，则本字段显示为该设备的IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
stra	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1～16，层数取值越小，表示时钟的准确度最高，层数为16的时钟处于未同步状态
reach	时间服务器的可达性计数，0表示时间服务器不可达
poll	轮询间隔，即两个连续NTP报文之间的时间间隔，单位为秒
now	最近一次接收到NTP报文或更新本地时间到当前时间的时间间隔 缺省单位为秒；如果时间间隔大于2048秒，则显示为分钟m；如果时间间隔大于300分钟，则显示为小时h；如果时间间隔大于96小时，则显示为天d；如果时间间隔大于999天，则显示为年y；如果最近一次接收到NTP报文或更新本地时间比当前时间晚，则显示为“-”
offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
delay	本地设备到时间服务器的往返时延，单位为毫秒
disper	系统时钟相对于参考时钟的最大误差，单位为毫秒
[12345]	1：系统选中的时间服务器，即当前与设备进行时间同步的时间服务器 2：该时间服务器的时钟层数小于等于15 3：该时间服务器的时钟通过了时钟选择算法 4：该时间服务器的时钟为候选时钟 5：该时间服务器的时钟是配置命令指定的
Total sessions	总的会话数目

显示 NTP 服务的所有 IPv4 会话的详细信息。

```
<Sysname> display ntp-service sessions verbose
 Clock source: 192.168.1.40
 Session ID: 35888
 Clock stratum: 2
 Clock status:  configured, master, sane, valid
 Reference clock ID: 127.127.1.0
 VPN instance: Not specified
 Local mode: client, local poll interval: 6
 Peer mode: server, peer poll interval: 6
 Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
 Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
 Reachabilities:31, sync distance: 0.0194
 Precision: 2^18, version: 3, source interface: Not specified
 Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
 Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
 Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
```

```
Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
Filter order: 7     5     2     6     0     4     1     3

Total sessions: 1
```

表1-4 display ntp-service sessions verbose 命令显示信息描述表

字段	描述
Clock source	时间服务器的IP地址。若该字段显示为0.0.0.0，表示时间服务器的IP地址尚未解析成功
Session ID	会话ID
Clock stratum	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1～16，层数取值越小，表示时钟的准确度越高，层数为16的时钟处于未同步状态
Clock status	会话的状态，该字段的取值及含义为： • configured：表示该会话是配置命令所建立的 • dynamic：表示该会话是动态生成的 • master：表示该会话对应的时间服务器是当前系统的主时间服务器 • selected：表示该会话对应时间服务器的时钟通过了时钟选择算法 • candidate：表示该会话对应时间服务器的时钟为候选时钟 • sane：表示该会话对应的时间服务器通过身份验证，该时间服务器的时钟将作为参考时钟 • insane：表示该会话对应的时间服务器未通过身份验证，或该时间服务器通过身份验证但其时钟不作为参考时钟 • valid：表示该会话对应的时间服务器是有效的（通过验证、处于同步状态、层数有效、根延时/离差未越界等） • invalid：表示该会话对应的时间服务器是无效的 • unsynced：表示该会话对应时间服务器的时钟未同步或层数非法
Reference clock ID	时间服务器的参考时钟ID 当参考时钟为本地时钟时，本字段的显示情况和Clock stratum字段的取值有关： • 当 Clock stratum 字段取值为 0 或 1 时，本字段将显示为 LOCL； • 当 Clock stratum 字段取值为其他值时，本字段将显示为本地时钟的 IP 地址 当参考时钟为网络中其他设备的时钟时，本字段显示为该设备的IP地址，若该设备为IPv6设备，则本字段显示为该设备的IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
VPN instance	时间服务器所属的VPN实例的名称，如果时间服务器位于公网，则显示为Not specified（暂不支持）
Local mode	本地设备的工作模式，取值包括： • unspec：未指定模式 • sym_active：主动对等体模式 • sym_passive：被动对等体模式 • client：客户端模式 • server：服务器模式

字段	描述
	• broadcast：广播服务器模式或组播服务器模式 • bclient：广播客户端模式或组播客户端模式
local poll interval	本地设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Peer mode	对端设备的工作模式，取值包括： • unspec：未指定模式 • sym_active：主动对等体模式 • sym_passive：被动对等体模式 • client：客户端模式 • server：服务器模式 • broadcast：广播服务器模式或组播服务器模式 • bclient：广播客户端模式或组播客户端模式
peer poll interval	对端设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
roundtrip delay	本地设备到时间服务器的往返时延，单位为毫秒
dispersion	系统时钟相对于参考时钟的最大误差
Root roundtrip delay	本地设备到主时间服务器的往返时延，单位为毫秒
root dispersion	系统时钟相对主参考时钟的最大误差，单位为毫秒
Reachabilities	时间服务器的可达性计数，0表示时间服务器不可达
sync distance	表示相对上一级时间服务器的同步距离，由误差disper和往返时延delay计算而来，单位为秒
Precision	系统时钟的精度
version	NTP版本，取值为1～4
source interface	源接口，未指定源接口时，此字段显示为Not specified
Reftime	NTP报文中的参考时间戳
Orgtime	NTP报文中的起始时间戳
Rcvtime	NTP报文的接收时间戳
Xmttime	NTP报文的发送时间戳
Roundtrip delay samples	本地设备到时间服务器往返时延的抽样值
Offset samples	相对于参考时钟的时钟偏移的抽样值
Filter order	抽样信息排序
Reference clock status	本地时钟的工作状态，只有通过**ntp-service refclock-master**命令设置本地时钟作为参考时钟时，才会显示该字段 当本地时钟的reach值等于255时，该字段取值为working normally；否则，该字段取值为working abnormally

字段	描述
Total sessions	总的会话数目

1.1.3 display ntp-service status

display ntp-service status 命令用来显示 NTP 服务的状态信息。

【命令】

display ntp-service status

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

时间已同步时，显示 NTP 服务的状态信息。

```
<Sysname> display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 System peer: LOCAL(0)
 Local mode: client
 Reference clock ID: 127.127.1.0
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-10
 Root delay: 0.00000 ms
 Root dispersion: 3.96367 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

时间未同步时，显示 NTP 服务的状态信息。

```
<Sysname> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Clock jitter: 0.000000 s
 Stability: 0.000 pps
 Clock precision: 2^-10
 Root delay: 0.00000 ms
 Root dispersion: 0.00002 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

表1-5 display ntp-service status 命令显示信息描述表

字段	描述
Clock status	系统时间的状态，取值为： • synchronized：系统时间已同步 • unsynchronized：系统时间未同步
Clock stratum	系统时钟的层数
System peer	系统时钟选中的时间服务器的IP地址
Local mode	相对于选中的时间服务器，本地设备的工作模式，取值包括： • unspec：未指定模式 • sym_active：主动对等体模式 • sym_passive：被动对等体模式 • client：客户端模式 • server：服务器模式 • broadcast：广播服务器模式或组播服务器模式 • bclient：广播客户端模式或组播客户端模式
Reference clock ID	参考时钟ID (1) 对于 IPv4 NTP 服务器： 本地设备从远程时间服务器获取时间同步时，表示远程服务器的IP地址 本地设备从本地时钟获取时间同步时，表示本地时钟的标识： • 本地时钟的层数为 1 时，显示为 LOCL • 本地时钟的层数为其他值时，显示为本地时钟的 IP 地址 (2) 对于 IPv6 NTP 服务器： 本地设备从远程时间服务器获取时间同步时，表示远程服务器的IPv6地址前32位的MD5摘要值 本地设备从本地时钟获取时间同步时，表示本地时钟的标识： • 本地时钟的层数为 1 时，显示为 LOCL • 本地时钟的层数为其他值时，显示为本地时钟的 IPv6 地址前 32 位的 MD5 摘要值
Leap indicator	告警状态，取值包括： • 00：正常状态 • 01：闰秒标志，表示一天中的最后一分钟有 61 秒 • 10：闰秒标志，表示一天中的最后一分钟有 59 秒 • 11：时间未被同步的告警状态
Clock jitter	系统时钟相对于参考时钟的偏移量，单位为秒
Stability	时钟频率的稳定性，取值越小，时钟频率越稳定
Clock precision	系统时钟的精度
Root delay	本地设备到主时间服务器的往返时延，单位为毫秒
Root dispersion	系统时钟相对主参考时钟的最大误差，单位为毫秒
Reference time	参考时间戳

1.1.4 display ntp-service trace

display ntp-service trace 命令用来显示从本地设备回溯到主时间服务器的各个 NTP 时间服务器的简要信息。

【命令】

display ntp-service trace [**source** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

source *interface-type interface-number*：指定回溯主时间服务器时发送 NTP 报文的源接口，*interface-type interface-number* 表示接口类型和接口编号。本地设备向时间服务器发送 NTP 报文时，报文的源地址为指定源接口的主 IPv4 地址或接口的 IPv6 地址；如果 NTP 时间服务器地址是链路本地地址时，报文的源地址为报文出接口的链路本地地址。如果不指定本参数，则以报文发送接口作为回溯主时间服务器时发送 NTP 报文的源接口。

【使用指导】

指定源接口回溯主时间服务器时，需要保证主时间服务器已及各个 NTP 时间服务器均和源接口之间路由可达，否则将导致回溯失败。

【举例】

显示从本地设备回溯到主时间服务器的各个 NTP 时间服务器的简要信息。

```
<Sysname> display ntp-service trace
Server     127.0.0.1
Stratum    3, jitter  0.000, synch distance 0.0000.
Server     3000::32
Stratum    2 , jitter 790.00, synch distance 0.0000.
RefID      127.127.1.0
```

以上信息显示了服务器 127.0.0.1 的同步链：服务器 127.0.0.1 同步到服务器 3000::32，服务器 3000::32 从本地时钟得到同步。

表1-6 display ntp-service trace 命令显示信息描述表

字段	描述
Server	时间服务器的IP地址
Stratum	表示相应服务器的时钟层数
jitter	表示相对上一级时钟的时钟偏差的均方根，单位为秒
synch distance	表示相对上一级时间服务器的同步距离，由误差disper和往返时延delay计算而来，单位为秒

字段	描述
RefID	主时间服务器的标识，主参考时钟的层数为0时，显示为LOCL；为其他值时，显示为主参考时钟的IP地址

【相关命令】

- **ntp-service source**
- **ntp-service unicast-server**
- **ntp-service unicast-peer**
- **ntp-service ipv6 source**
- **ntp-service ipv6 unicast-server**
- **ntp-service ipv6 unicast-peer**

1.1.5 ntp-service acl

ntp-service acl 命令用来设置对端设备对本地设备 NTP 服务的访问控制权限。

undo ntp-service acl 命令用来取消设置的访问控制权限。

【命令】

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

【缺省情况】

对端设备对本地设备 NTP 服务的访问控制权限为 **peer**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

peer：完全访问权限。该权限既允许对端设备向本地设备的时间同步，对本地设备进行控制查询（查询 NTP 的一些状态，比如告警信息、验证状态、时间服务器信息等），同时本地设备也可以向对端设备的时间同步。

query：仅具有控制查询的权限。该权限只允许对端设备对本地设备的 NTP 服务进行控制查询，但是不能向本地设备的时间同步。

server：服务器访问与查询权限。该权限允许对端设备向本地设备的时间同步，对本地设备进行控制查询，但本地设备不会向对端设备的时间同步。

synchronization：仅具有访问服务器的权限。该权限只允许对端设备向本地设备的时间同步，但不能进行控制查询。

ipv4-acl-number：通过编号指定应用的 ACL（Access Control List，访问控制列表）。通过 ACL 过滤的对端设备具有本命令中指定的访问控制权限。*ipv4-acl-number* 为 IPv4 基本或高级 ACL 的编号，取值范围为 2000～2999 和 3000～3999。

【使用指导】

NTP 服务的访问控制权限从高到低依次为 **peer**、**server**、**synchronization**、**query**。当设备接收到一个 NTP 服务请求时，会按照权限从高到低的顺序依次进行匹配，第一个匹配的权限为此设备具有的访问控制权限。如果没有匹配的权限，则不允许对端设备与本地设备进行时间同步、对本端进行控制查询，也不允许本端设备与对端设备进行时间同步。

当引用的 ACL 不存在时，配置不生效。

ntp-service acl 命令提供了一种最小限度的安全措施，更安全的方法是进行身份验证。

【举例】

配置 10.10.0.0/16 网段的对端设备对本地设备具有完全访问权限。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ntp-service peer acl 2001
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.6 ntp-service authentication enable

ntp-service authentication enable 命令用来使能 NTP 身份验证功能。

undo ntp-service authentication enable 命令用来关闭 NTP 身份验证功能。

【命令】

ntp-service authentication enable

undo ntp-service authentication enable

【缺省情况】

NTP 身份验证功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用 NTP 身份验证功能。通过客户端和服务器端的身份验证，保证客户端只与通过验证的设备进行时间同步，避免客户端从非法的服务器获得错误的时间同步信息。

使能 NTP 身份验证功能后，还需要设置身份验证密钥，并将其设置为可信密钥，才能正确地进行身份验证。

【举例】

使能 NTP 身份验证功能。

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

【相关命令】

- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.7 ntp-service authentication-keyid

ntp-service authentication-keyid 命令用来设置 NTP 身份验证密钥。

undo ntp-service authentication-keyid 命令用来取消 NTP 身份验证密钥。

【命令】

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *

undo ntp-service authentication-keyid *keyid*

【缺省情况】

未设置 NTP 身份验证密钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keyid：密钥编号，用来标识身份验证密钥，取值范围为 1～4294967295。

authentication-mode md5：表示采用 MD5 算法进行身份验证。

cipher：以密文形式设置密钥。

simple：以明文形式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥为 1～32 个字符的字符串，密文密钥为 1～73 个字符的字符串。

acl *ipv4-acl-number*：对对端设备进行 ACL 过滤。通过 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。*ipv4-acl-number* 为 IPv4 基本 ACL 的编号，取值范围为 2000～2999。

ipv6 acl *ipv6-acl-number*：对对端设备进行 IPv6 ACL 过滤。通过 IPv6 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。*ipv6-acl-number* 为 IPv6 基本 ACL 的编号，取值范围为 2000～2999。

【使用指导】

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用身份验证功能。通过客户端和服务器端的身份验证，保证客户端只与通过验证的设备进行时间同步，提高了时间同步的安全性。

NTP 协议采用哪个密钥对对端进行身份验证由对端报文中携带的密钥 ID 决定。这会导致如下安全问题：对对端进行身份验证时只关心密钥是否正确而不关心对端是否有权使用该密钥 ID。**acl** 和 **ipv6 acl** 参数用于指定有权在本端使用该密钥 ID 进行身份验证的对端设备。需要注意的是：

- 当引用的 ACL 或 IPv6 ACL 不存在时，任何设备都能在本端使用该密钥 ID 进行验证。
- 当引用的 ACL 或 IPv6 ACL 下没有配置规则时，任何设备都不能在本端使用该密钥 ID 进行验证。

客户端和服务器上需要配置相同的密钥 ID 及密钥值，并且保证对端有权在本端使用该密钥 ID 进行身份验证，否则无法实现时间同步。

配置 NTP 验证密钥后，还需要通过 **ntp-service reliable authentication-keyid** 命令将该密钥设置为可信密钥。如果 NTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo ntp-service reliable authentication-keyid** 命令。

通过重复执行本命令，可以配置多个 NTP 身份验证密钥。设备上最多可以配置 128 个 NTP 身份验证密钥。

【举例】

设置 MD5 身份验证密钥，密钥 ID 号为 10，密钥为 BetterKey，以明文形式输入。

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

1.1.8 ntp-service broadcast-client

ntp-service broadcast-client 命令用来配置设备工作在 NTP 广播客户端模式，并使用当前接口接收 NTP 广播报文。

undo ntp-service broadcast-client 命令用来取消 NTP 广播客户端模式的配置。

【命令】

ntp-service broadcast-client

undo ntp-service broadcast-client

【缺省情况】

设备没有工作在任何 NTP 模式。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

配置设备工作在 NTP 广播客户端模式后，设备将在接口上监听 NTP 广播服务器发送的 NTP 广播报文，根据接收到的报文实现时间同步。

如果在接口上配置了设备工作在广播客户端模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 广播客户端配置。

【举例】

配置设备工作在广播客户端模式，在 VLAN 接口 1 上接收 NTP 广播报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

【相关命令】

- **ntp-service broadcast-server**

1.1.9 ntp-service broadcast-server

ntp-service broadcast-server 命令用来配置设备工作在 NTP 广播服务器模式，并使用当前接口发送 NTP 广播报文。

undo ntp-service broadcast-server 命令用来取消 NTP 广播服务器模式的配置。

【命令】

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

【缺省情况】

设备没有工作在任何 NTP 模式。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

authentication-keyid *keyid*：指定向广播客户端发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备无法同步使能了身份验证功能的广播客户端。

version *number*：指定 NTP 版本号。*number* 取值范围为 1～4，缺省值为 4。

【使用指导】

配置设备工作在 NTP 广播服务器模式后，设备将通过该接口周期性地向广播地址 255.255.255.255 发送 NTP 报文。

如果在接口上配置了设备工作在广播服务器模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 广播服务器配置。

【举例】

配置设备工作在广播服务器模式，在 VLAN 接口 1 上发送 NTP 广播报文，用 4 号密钥进行加密，设置 NTP 版本号为 4。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4
```

【相关命令】

- **ntp-service broadcast-client**

1.1.10 ntp-service dscp

ntp-server dscp 命令用来配置 NTP 报文的 DSCP 优先级。

undo ntp-server dscp 命令用来恢复缺省情况。

【命令】

ntp-service dscp *dscp-value*

undo ntp-service dscp

【缺省情况】

NTP 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value：NTP 报文的 DSCP 优先级，取值范围为 0～63。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 NTP 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

1.1.11 ntp-service enable

ntp-service enable 命令用来开启 NTP 服务。

undo ntp-service enable 命令用来关闭 NTP 服务。

【命令】

ntp-service enable

undo ntp-service enable

【缺省情况】

没有开启 NTP 服务。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

开启 NTP 服务。

```
<Sysname> system-view
[Sysname] ntp-service enable
```

1.1.12 ntp-service inbound enable

ntp-service inbound enable 命令用来配置接口处理收到的 NTP 报文。

undo ntp-service inbound enable 命令配置接口不处理收到的 NTP 报文。

【命令】

ntp-service inbound enable

undo ntp-service inbound enable

【缺省情况】

接口处理收到的 NTP 报文。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

如果不允许设备为某个接口对应网段内的对端设备提供时间同步，或不允许设备从某个接口对应网段内的对端设备获得时间同步，则可以在该接口上执行 **undo ntp-service inbound enable** 命令，使该接口不处理收到的 NTP 报文。

【举例】

配置 VLAN 接口 1 不处理收到的 NTP 报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] undo ntp-service inbound enable
```

1.1.13 ntp-service ipv6 acl

ntp-service ipv6 acl 命令用来设置对端设备对本地设备 IPv6 NTP 服务的访问控制权限。

undo ntp-service ipv6 acl 命令用来取消设置的访问控制权限。

【命令】

ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } **acl** *ipv6-acl-number*

undo ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } **acl** [*ipv6-acl-number*]

【缺省情况】

对端设备对本地设备 IPv6 NTP 服务的访问控制权限为 **peer**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

peer：完全访问权限。该权限既允许对端设备向本地设备的时间同步，对本地设备进行控制查询（查询 NTP 的一些状态，比如告警信息、验证状态、时间服务器信息等），同时本地设备也可以向对端设备的时间同步。

query：仅具有控制查询的权限。该权限只允许对端设备对本地设备的 NTP 服务进行控制查询，但是不能向本地设备的时间同步。

server：服务器访问与查询权限。该权限允许对端设备向本地设备的时间同步，对本地设备进行控制查询，但本地设备不会向对端设备的时间同步。

synchronization：仅具有访问服务器的权限。该权限只允许对端设备向本地设备的时间同步，但不能进行控制查询。

ipv6-acl-number：通过编号指定应用的 IPv6 ACL（Access Control List，访问控制列表）。通过 IPv6 ACL 过滤的对端设备具有本命令中指定的访问控制权限。*ipv6-acl-number* 为 IPv6 基本或高级 ACL 的编号，取值范围为 2000～2999 和 3000～3999。

【使用指导】

IPv6 NTP 服务的访问控制权限从高到低依次为 **peer**、**server**、**synchronization**、**query**。当设备接收到一个 IPv6 NTP 服务请求时，会按照权限从高到低的顺序依次进行匹配，第一个匹配的权限为此设备具有的访问控制权限。如果没有匹配的权限，则不允许对端设备与本地设备进行时间同步、对本端进行控制查询，也不允许本端设备与对端设备进行时间同步。

当引用的 IPv6 ACL 不存在时，配置不生效。

ntp-service ipv6 acl 命令提供了一种最小限度的安全措施，更安全的方法是进行身份验证。

【举例】

配置 2001::1 网段的对端设备对本地设备具有完全访问权限。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ntp-service ipv6 peer acl 2001
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.14 ntp-service ipv6 dscp

ntp-server ipv6 dscp 命令用来配置 IPv6 NTP 报文的 DSCP 优先级。

undo ntp-server ipv6 dscp 命令用来恢复缺省情况。

【命令】

ntp-service ipv6 dscp *dscp-value*

undo ntp-service ipv6 dscp

【缺省情况】

IPv6 NTP 报文的 DSCP 优先级为 56。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value：IPv6 NTP 报文的 DSCP 优先级，取值范围为 0～63。

【使用指导】

DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 IPv6 NTP 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ntp-service ipv6 dscp 30
```

1.1.15 ntp-service ipv6 inbound enable

ntp-service ipv6 inbound enable 命令用来配置接口处理收到的 IPv6 NTP 报文。

undo ntp-service ipv6 inbound enable 命令用来配置接口不处理收到的 IPv6 NTP 报文。

【命令】

ntp-service ipv6 inbound enable

undo ntp-service ipv6 inbound enable

【缺省情况】

接口处理收到的 IPv6 NTP 报文。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

如果不允许设备为某个接口对应网段内的对端设备提供时间同步，或不允许设备从某个接口对应网段内的对端设备获得时间同步，则可以在该接口上执行 **undo ntp-service ipv6 inbound enable** 命令，使该接口不处理收到的 IPv6 NTP 报文。

【举例】

配置 VLAN 接口 1 不处理收到的 IPv6 NTP 报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] undo ntp-service ipv6 inbound enable
```

1.1.16 ntp-service ipv6 multicast-client

ntp-service ipv6 multicast-client 命令用来配置设备工作在 IPv6 NTP 组播客户端模式，并使用当前接口接收 IPv6 NTP 组播报文。

undo ntp-service ipv6 multicast-client 命令用来取消 IPv6 NTP 组播客户端模式的配置。

【命令】

ntp-service ipv6 multicast-client *ipv6-multicast-address*

undo ntp-service ipv6 multicast-client *ipv6-multicast-address*

【缺省情况】

设备没有工作在任何 NTP 模式。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-multicast-address：NTP 报文的 IPv6 组播地址，取值范围为 FFxy::/16，其中 x 和 y 均代表 0～F 的任意一个十六进制数。IPv6 组播客户端和 IPv6 组播服务器上配置的组播地址必须相同。

【使用指导】

配置设备工作在 IPv6 NTP 组播客户端模式后，设备将在接口上监听目的地址为指定 IPv6 组播地址的 IPv6 NTP 报文，根据接收到的报文实现时间同步。

如果在接口上配置了设备工作在 IPv6 组播客户端模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 IPv6 NTP 组播客户端配置。

【举例】

配置设备工作在 IPv6 组播客户端模式，在 VLAN 接口 1 上接收目的地址为组播地址 FF21::1 的 NTP 报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-client ff21::1
```

【相关命令】

- **ntp-service ipv6 multicast-server**

1.1.17 ntp-service ipv6 multicast-server

ntp-service ipv6 multicast-server 命令用来配置设备工作在 IPv6 NTP 组播服务器模式，并使用当前接口发送 IPv6 NTP 组播报文。

undo ntp-service ipv6 multicast-server 命令用来取消 IPv6 NTP 组播服务器模式的配置。

【命令】

ntp-service ipv6 multicast-server *ipv6-multicast-address* [**authentication-keyid** *keyid* | **ttl** *ttl-number*] *

undo ntp-service ipv6 multicast-server *ipv6-multicast-address*

【缺省情况】

设备没有工作在任何 NTP 模式。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-multicast-address：NTP 报文的 IPv6 组播地址，取值范围为 FFxy::/16，其中 x 和 y 均代表 0～F 的任意一个十六进制数。IPv6 组播客户端和 IPv6 组播服务器上配置的组播地址必须相同。

authentication-keyid *keyid*：指定向组播客户端发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备无法同步使能了身份验证功能的组播客户端。

ttl *ttl-number*：指定组播报文的生存期。*ttl-number* 取值范围为 1～255，缺省值为 16。

【使用指导】

配置设备工作在 IPv6 NTP 组播服务器模式后，设备将通过该接口周期性地向指定的 IPv6 组播地址发送 NTP 报文。

如果在接口上配置了设备工作在 IPv6 组播服务器模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 IPv6 NTP 组播服务器配置。

【举例】

配置设备工作在 IPv6 组播服务器模式，在 VLAN 接口 1 上向 IPv6 组播地址 FF21::1 发送 NTP 报文，用 4 号密钥加密 NTP 报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-server ff21::1 authentication-keyid 4
```

【相关命令】

- **ntp-service ipv6 multicast-client**

1.1.18 ntp-service ipv6 source

ntp-service ipv6 source 命令用来指定 IPv6 NTP 报文的源接口。

undo ntp-service ipv6 source 命令用来恢复缺省情况。

【命令】

ntp-service ipv6 source *interface-type interface-number*

undo ntp-service ipv6 source

【缺省情况】

没有指定 IPv6 NTP 报文的源接口，设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：接口类型和接口编号。

【使用指导】

如果指定了 IPv6 NTP 报文的源接口，则设备在主动发送 IPv6 NTP 报文时，将采用源接口的 IPv6 地址作为发送报文的源 IPv6 地址，从而保证 IPv6 NTP 应答报文的目的地址均为此地址。

设备对接收到的 IPv6 NTP 请求报文进行应答时，应答报文的源 IPv6 地址始终为接收到 IPv6 NTP 请求报文的目的 IPv6 地址。

如果不想让本地设备上其他接口的 IPv6 地址成为应答报文的目的地址，可以使用本命令。

- 如果在命令 **ntp-service ipv6 unicast-server** 或 **ntp-service ipv6 unicast-peer** 中指定了 IPv6 NTP 报文的源接口，则以 **ntp-service ipv6 unicast-server** 或 **ntp-service ipv6 unicast-peer** 命令指定源接口的为准。
- 如果在接口视图下配置了 **ntp-service ipv6 multicast-server** 命令，则 NTP 组播报文的源接口为配置了 **ntp-service ipv6 multicast-server** 命令的接口。
- 如果指定的 NTP 源接口处于 down 状态，则设备不再发送 IPv6 NTP 报文。

【举例】

配置 IPv6 NTP 报文的源接口为 VLAN 接口 1。

```
<Sysname> system-view
[Sysname] ntp-service ipv6 source vlan-interface 1
```

1.1.19 ntp-service ipv6 unicast-peer

ntp-service ipv6 unicast-peer 命令用来为设备指定 IPv6 被动对等体。

undo ntp-service ipv6 unicast-peer 命令用来取消为设备指定的 IPv6 被动对等体。

【命令】

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* }

【缺省情况】

没有为设备指定 IPv6 被动对等体。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

peer-name：被动对等体的主机名字，为 1～253 个字符的字符串，不区分大小写。

ipv6-address：被动对等体的 IPv6 地址。该地址只能是一个单播地址，不能为组播地址。

authentication-keyid *keyid*：指定向对等体发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备与对等体之间不会进行身份验证。

priority：在同等条件下，优先选择 *ip-address* 或 *peer-name* 指定的对等体为同步对等体。

source *interface-type interface-number*：指定 IPv6 NTP 报文的源接口。如果指定的被动对等体地址不是链路本地地址，则本地设备给对端发送 IPv6 NTP 报文时，报文的源 IPv6 地址为指定源接口的 IPv6 地址。如果指定的被动对等体地址是链路本地地址，则 IPv6 NTP 报文从指定的源接口发送，并且报文的源地址为该接口的链路本地地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【使用指导】

为设备指定 IPv6 被动对等体后，主动对等体和被动对等体的时间可以互相同步。如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步。

【举例】

配置设备工作在主动对等体模式，被动对等体的 IPv6 地址为 2001::1，NTP 报文的源接口为 VLAN 接口 1。

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-peer 2001::1 source vlan-interface 1
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.20 ntp-service ipv6 unicast-server

ntp-service ipv6 unicast-server 命令用来为设备指定 IPv6 NTP 服务器。

undo ntp-service ipv6 unicast-server 命令用来取消为设备指定的 IPv6 NTP 服务器。

【命令】

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* }

【缺省情况】

没有为设备指定 IPv6 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name：NTP 服务器的主机名字，为 1～253 个字符的字符串，不区分大小写。

ipv6-address：NTP 服务器的 IPv6 地址。该地址只能是一个单播地址，不能为组播地址。

authentication-keyid *keyid*：指定向 NTP 服务器发送报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备与 NTP 服务器之间不会进行身份验证。

priority：指定在同等条件下，优先选择该服务器。

source *interface-type interface-number*：指定 IPv6 NTP 报文的源接口。如果指定的 IPv6 NTP 服务器地址不是链路本地地址，则本地设备给服务器发送 IPv6 NTP 报文时，报文的源 IPv6 地址为指定源接口的 IPv6 地址。如果指定的 IPv6 NTP 服务器地址是链路本地地址，则 IPv6 NTP 报文从指定的源接口发送，并且报文的源地址为该接口的链路本地地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【使用指导】

为设备指定 IPv6 NTP 服务器后，设备可以与该服务器的时间同步，但是服务器不会与设备的时间同步。

【举例】

配置设备的 IPv6 NTP 服务器为 2001::1。

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-server 2001::1
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.21 ntp-service max-dynamic-sessions

ntp-service max-dynamic-sessions 命令用来配置 NTP 动态会话的最大数目。

undo ntp-service max-dynamic-sessions 命令用来恢复缺省情况。

【命令】

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

【缺省情况】

NTP 动态会话的最大数目为 100。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

number：NTP 动态会话的最大数目，取值范围为 0～100。

【使用指导】

同一设备同一时间内存在的会话数目最多为 128 个，其中包括静态会话数和动态会话数。静态会话是用户手动配置 NTP 相关命令而建立的会话；动态会话是 NTP 运行过程中建立的临时会话。

本配置用来限制动态会话的数目，以避免设备上维护过多的动态会话，占用过多的系统资源。

【举例】

设置 NTP 动态会话的最大数目为 50 个。

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

【相关命令】

- **display ntp-service sessions**

1.1.22 ntp-service multicast-client

ntp-service multicast-client 命令用来配置设备工作在 NTP 组播客户端模式，并使用当前接口接收 NTP 组播报文。

undo ntp-service multicast-client 命令用来取消 NTP 组播客户端模式的配置。

【命令】

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

【缺省情况】

设备没有工作在任何 NTP 模式。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address：NTP 报文的组播 IP 地址，取值范围为 224.0.0.0～239.255.255.255，缺省值为 224.0.1.1。组播客户端和组播服务器上配置的组播地址必须相同。

【使用指导】

配置设备工作在 NTP 组播客户端模式后，设备将在接口上监听目的地址为指定组播地址的 NTP 报文，根据接收到的报文实现时间同步。

如果在接口上配置了设备工作在组播客户端模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 组播客户端配置。

【举例】

配置设备工作在组播客户端模式，在 VLAN 接口 1 上接收目的地址为 224.0.1.1 的 NTP 报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

【相关命令】

- **ntp-service multicast-server**

1.1.23 ntp-service multicast-server

ntp-service multicast-server 命令用来配置设备工作在 NTP 组播服务器模式，并使用当前接口发送 NTP 组播报文。

undo ntp-service multicast-server 命令用来取消 NTP 组播服务器模式的配置。

【命令】

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

【缺省情况】

设备没有工作在任何 NTP 模式。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address：NTP 报文的组播 IP 地址，取值范围为 224.0.0.0～239.255.255.255，缺省值为 224.0.1.1。组播客户端和组播服务器上配置的组播地址必须相同。

authentication-keyid *keyid*：指定向组播客户端发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备无法同步使能了身份验证功能的组播客户端。

ttl *ttl-number*：指定组播报文的生存期。*ttl-number* 取值范围为 1～255，缺省值为 16。

version *number*：指定 NTP 版本号。*number* 取值范围为 1～4，缺省值为 4。

【使用指导】

配置设备工作在 NTP 组播服务器模式后，设备将通过该接口周期性地向指定的组播地址发送 NTP 报文。

如果在接口上配置了设备工作在组播服务器模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 组播服务器配置。

【举例】

配置设备工作在组播服务器模式，在 VLAN 接口 1 上发送 NTP 报文，NTP 报文的目的地址为组播地址 224.0.1.1，用 4 号密钥加密 NTP 报文，并设置 NTP 版本号为 4。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4
authentication-keyid 4
```

【相关命令】

- **ntp-service multicast-client**

1.1.24 ntp-service refclock-master

ntp-service refclock-master 命令用来设置本地时钟作为参考时钟。

undo ntp-service refclock-master 命令用来取消本地时钟作为参考时钟。

【命令】

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

【缺省情况】

设备未采用本地时钟作为参考时钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address：本地时钟的 IP 地址 127.127.1.u。u 的取值范围为 0～3，表示 NTP 的进程号。如果不指定 *ip-address*，则系统默认值是 127.127.1.0。

stratum：本地时钟所处的层数，取值范围为 1～15，缺省值为 8。时钟的层数定义了时钟的准确度，层数取值越小，时钟的准确度越高。

【使用指导】

实际网络中，通常将从权威时钟（如原子时钟）获得时间同步的 NTP 服务器的层数设置为 1，并将其作为主时间服务器同步网络中其他设备的时钟。网络中的设备与主时间服务器的 NTP 距离，即 NTP 同步链上 NTP 服务器的数目，决定了设备上时钟的层数。

在某些网络中，例如无法与外界通信的孤立网络，网络中的设备无法与权威时钟进行时间同步。此时，可以从该网络中选择一台时钟较为准确的设备，指定该设备与本地时钟进行时间同步，即采用本地时钟作为参考时钟，使得该设备的时钟处于同步状态。该设备作为时间服务器为网络中的其他设备提供时间同步，从而实现整个网络的时间同步。

请谨慎使用本配置，以免导致网络中设备的时间错误。在执行本命令之前，建议先调整本地系统时间。

【举例】

设置本地设备时钟作为参考时钟，层数为 2。

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 2
```

1.1.25 ntp-service reliable authentication-keyid

ntp-service reliable authentication-keyid 命令用来指定已创建的密钥是可信的。

undo ntp-service reliable authentication-keyid 命令用来取消可信密钥。

【命令】

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

【缺省情况】

没有配置可信密钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keyid：密钥编号，取值范围为 1～4294967295。

【使用指导】

- 使能身份验证功能后，客户端只会与提供可信密钥的服务器进行时间同步；如果服务器提供的密钥不是可信的，那么客户端不会与其同步。
- 配置本命令前，请确保认证开关已经打开并且配置了密钥，即保证该密钥的存在性后才能设定它是否可信。如果 NTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo ntp-service reliable authentication-keyid** 命令。
- 本命令可以多次配置，最多可以配置 128 个可信密钥。

【举例】

使能 NTP 身份验证功能，配置编号为 37 的密钥采用 MD5 算法进行身份验证，密钥值为 BetterKey。

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey
# 指定该密钥为可信密钥。
[Sysname] ntp-service reliable authentication-keyid 37
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

1.1.26 ntp-service source

ntp-service source 命令用来指定 NTP 报文的源接口。

undo ntp-service source 命令用来恢复缺省情况。

【命令】

ntp-service source *interface-type interface-number*

undo ntp-service source

【缺省情况】

没有指定 NTP 报文的源接口，设备根据路由表查找报文的出接口，并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：接口类型及接口编号。

【使用指导】

如果指定了 NTP 报文的源接口，则设备在主动发送 NTP 报文时，将报文的源 IP 地址设置为指定接口的主 IP 地址，从而保证 NTP 应答报文的目的地址均为此地址。

设备对接收到的 NTP 请求报文进行应答时，应答报文的源地址始终为接收到 NTP 请求报文的目的地址。

如果不想让本地设备上其他接口的 IP 地址成为应答报文的目的地址，可以使用本命令。

- 当 NTP 工作在客户端/服务器模式时，如果在命令 **ntp-service unicast-server** 中指定了 NTP 报文的源接口，则以 **ntp-service unicast-server** 命令指定的源接口为准。
- 当 NTP 工作在对等体模式时，如果在命令 **ntp-service unicast-peer** 中指定了 NTP 报文的源接口，则以 **ntp-service unicast-peer** 命令指定源接口的为准。
- 当 NTP 工作在组播模式时，如果在接口视图下配置了 **ntp-service multicast-server** 命令，则 NTP 组播报文的源接口为配置了 **ntp-service multicast-server** 命令的接口。
- 当 NTP 工作在广播模式时，如果在接口视图下配置了 **ntp-service broadcast-server** 命令，则 NTP 广播报文的源接口为配置了 **ntp-service broadcast-server** 命令的接口。
- 如果指定的 NTP 源接口处于 down 状态，则设备不再发送 NTP 报文。

【举例】

配置 NTP 报文的源接口为 VLAN 接口 1。

```
<Sysname> system-view
[Sysname] ntp-service source vlan-interface 1
```

1.1.27 ntp-service unicast-peer

ntp-service unicast-peer 命令用来为设备指定被动对等体。

undo ntp-service unicast-peer 命令用来取消为设备指定的被动对等体。

【命令】

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* }

【缺省情况】

没有为设备指定被动对等体。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

peer-name：被动对等体的主机名字，为 1～253 个字符的字符串，不区分大小写。

ip-address：被动对等体的 IP 地址。该地址只能是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。

authentication-keyid *keyid*：指定向对等体发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备与对等体之间不会进行身份验证。

priority：在同等条件下，优先选择 *ip-address* 或 *peer-name* 指定的对等体为同步对等体。

source *interface-type interface-number*：指定 NTP 报文的源接口。本地设备给对端发送 NTP 报文时，报文的源地址为指定源接口的主 IP 地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则根据路由表查找报文的出接口，并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

version *number*：指定 NTP 版本号。*number* 取值范围为 1～4，缺省值为 4。

【使用指导】

为设备指定被动对等体后，主动对等体和被动对等体的时间可以互相同步。如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步。

【举例】

配置设备工作在主动对等体模式，被动对等体的 IP 地址为 10.1.1.1，NTP 版本号为 4，NTP 报文的源接口为 VLAN 接口 1。

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 4 source vlan-interface 1
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.28 ntp-service unicast-server

ntp-service unicast-server 命令用来为设备指定 NTP 服务器。

undo ntp-service unicast-server 命令用来取消为设备指定的 NTP 服务器。

【命令】

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* }

【缺省情况】

没有为设备指定 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name：NTP 服务器的主机名字，为 1～253 个字符的字符串，不区分大小写。

ip-address：NTP 服务器的 IP 地址。该地址只能是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。

authentication-keyid *keyid*：指定向 NTP 服务器发送报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备与 NTP 服务器之间不会进行身份验证。

priority：指定在同等条件下，优先选择该服务器。

source *interface-type interface-number*：指定 NTP 报文的源接口。本地设备给服务器发送 NTP 报文时，报文的源地址为指定源接口的主 IP 地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则根据路由表查找报文的出接口，并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

version *number*：指定 NTP 版本号。*number* 取值范围为 1～4，缺省值为 4。

【举例】

配置设备的 NTP 服务器为 10.1.1.1，版本号为 4。

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 4
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

2 SNTP

2.1 SNTP配置命令

2.1.1 display sntp ipv6 sessions

display sntp ipv6 sessions 命令用来显示 SNTP 服务的所有 IPv6 会话信息。

【命令】

display sntp ipv6 sessions

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示 IPv6 SNTP 服务的所有 IPv6 会话信息。

```
<Sysname> display sntp ipv6 sessions
SNTP server: 2001::1
Stratum: 16
Version: 4
Last receive time: No packet was received.

SNTP server: 2001::100
Stratum: 3
Version: 4
Last receive time: Fri, Oct 21 2011 11:28:28.058 (Synced)
```

表2-1 display sntp ipv6 sessions 命令显示信息描述表

字段	描述
SNTP server	SNTP服务器，即NTP服务器。若该字段显示为::，表示NTP服务器的IPv6地址尚未解析成功
Stratum	时钟的层数 时钟层数决定了时钟的准确度，取值范围为1～16，层数取值越小，表示时钟的准确度越高，层数为16的时钟处于未同步状态
Version	版本号
Last receive time	最后一次接收到SNTP会话消息的时间 • Synced 表示设备的本地时钟从该服务器获得同步 • No packet was received.表示设备未从该服务器接收到 SNTP 会话消息

2.1.2 display sntp sessions

display sntp sessions 命令用来显示 SNTP 服务的所有 IPv4 会话信息。

【命令】

display sntp sessions

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示 SNTP 服务的所有 IPv4 会话信息。

```
<Sysname> display sntp sessions
SNTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Tue, May 17 2011  9:11:20.833 (Synced)
```

表2-2 display sntp sessions 命令显示信息描述表

字段	描述
SNTP server	SNTP服务器，即NTP服务器。若该字段显示为0.0.0.0，表示NTP服务器的IP地址尚未解析成功
Stratum	时钟的层数 时钟层数决定了时钟的准确度，取值范围为1～16，层数取值越小，表示时钟的准确度越高，层数为16的时钟处于未同步状态
Version	SNTP版本号
Last receive time	上一次接收到消息的时间，Synced标识本地时钟从该服务器获得同步

2.1.3 sntp authentication enable

sntp authentication enable 命令用来使能 SNTP 身份验证功能。

undo sntp authentication enable 命令用来关闭 SNTP 身份验证功能。

【命令】

sntp authentication enable

undo sntp authentication enable

【缺省情况】

SNTP 身份验证功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在一些对安全性要求较高的网络中，运行 SNTP 协议时需要启用身份验证功能。通过客户端和服务器端的身份验证，保证客户端只与通过验证的服务器进行时间同步，避免客户端从非法的服务器获得错误的时间同步信息。

使能 SNTP 身份验证功能后，还需要设置身份验证密钥，并将其设置为可信密钥，才能正确地进行身份验证。

【举例】

使能 SNTP 身份验证功能。

```
<Sysname> system-view
[Sysname] sntp authentication enable
```

【相关命令】

- **sntp authentication-keyid**
- **sntp reliable authentication-keyid**

2.1.4 sntp authentication-keyid

sntp authentication-keyid 命令用来设置 SNTP 身份验证密钥。

undo sntp authentication-keyid 命令用来取消 SNTP 身份验证密钥。

【命令】

sntp authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *

undo sntp authentication-keyid *keyid*

【缺省情况】

没有设置 SNTP 身份验证密钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keyid：密钥编号，用来标识身份验证密钥，取值范围为 1～4294967295。

authentication-mode md5：表示采用 MD5 算法进行身份验证。

cipher：以密文形式设置密钥。

simple：以明文形式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥为 1～32 个字符的字符串，密文密钥为 1～73 个字符的字符串。

acl *ipv4-acl-number*：对对端设备进行 ACL 过滤。通过 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。*ipv4-acl-number* 为 IPv4 基本 ACL 的编号，取值范围为 2000～2999。

ipv6 acl *ipv6-acl-number*：对对端设备进行 IPv6 ACL 过滤。通过 IPv6 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。*ipv6-acl-number* 为 IPv6 基本 ACL 的编号，取值范围为 2000～2999。

【使用指导】

在一些对安全性要求较高的网络中，运行 SNTP 协议时需要启用身份验证功能。通过客户端和服务器端的身份验证，保证客户端只与通过验证的服务器进行同步，提高了网络安全性。

SNTP 协议采用哪个密钥对对端进行身份验证由对端报文中携带的密钥 ID 决定。这会导致如下安全问题：对对端进行身份验证时只关心密钥是否正确而不关心对端是否有权使用该密钥 ID。acl 和 ipv6 acl 参数用于指定有权在本端使用该密钥 ID 进行身份验证的对端设备。需要注意的是：

- 当引用的 ACL 或 IPv6 ACL 不存在时，任何设备都能在本端使用该密钥 ID 进行验证。
- 当引用的 ACL 或 IPv6 ACL 下没有配置规则时，任何设备都不能在本端使用该密钥 ID 进行验证。

客户端和服务器上需要配置相同的密钥 ID 及密钥值，并且保证对端有权在本端使用该密钥 ID 进行身份验证，否则无法实现时间同步。

配置 SNTP 验证密钥后，还需要通过 **sntp reliable authentication-keyid** 命令将该密钥设置为可信密钥。如果 SNTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo sntp reliable authentication-keyid** 命令。

通过重复执行本命令，可以配置多个 SNTP 身份验证密钥。设备上最多可以配置 128 个 SNTP 身份验证密钥。

【举例】

设置 MD5 身份验证密钥，密钥 ID 号为 10，密钥为 BetterKey，以明文形式输入。

```
<Sysname> system-view
[Sysname] sntp authentication enable
[Sysname] sntp authentication-keyid 10 authentication-mode md5 simple BetterKey
```

【相关命令】

- **sntp authentication enable**
- **sntp reliable authentication-keyid**

2.1.5 sntp enable

sntp enable 命令用来开启 SNTP 服务。

undo sntp enable 命令用来关闭 SNTP 服务。

【命令】

sntp enable

undo sntp enable

【缺省情况】

没有开启 SNTP 服务。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

开启 SNTP 服务。

```
<Sysname> system-view
[Sysname] sntp enable
```

2.1.6 sntp ipv6 unicast-server

sntp ipv6 unicast-server 命令用来为设备指定 IPv6 NTP 服务器。

undo sntp ipv6 unicast-server 命令用来取消为设备指定的 IPv6 NTP 服务器。

【命令】

sntp ipv6 unicast-server { *server-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **source** *interface-type interface-number*] *

undo sntp ipv6 unicast-server { *server-name* | *ipv6-address* }

【缺省情况】

没有为设备指定 IPv6 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name：NTP 服务器的主机名字，为 1～253 个字符的字符串，不区分大小写。

ipv6-address：NTP 服务器的 IPv6 地址。

authentication-keyid *keyid*：指定向 NTP 服务器发送报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备与 NTP 服务器之间不会进行身份验证。

source *interface-type interface-number*：指定 IPv6 NTP 报文的源接口。如果指定的 IPv6 NTP 服务器地址不是链路本地地址，则本地设备给服务器发送 IPv6 NTP 报文时，报文的源 IPv6 地址为指定源接口的 IPv6 地址。如果指定的 IPv6 NTP 服务器地址是链路本地地址，则 IPv6 NTP 报文从指定的源接口发送，并且报文的源地址为该接口的链路本地地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【使用指导】

为设备指定 IPv6 NTP 服务器后，设备可以与该服务器进行时间同步。设备的时间获得同步后，不能作为服务器为其他设备提供时间同步。

【举例】

配置设备的 NTP 服务器为 2001::1。

```
<Sysname> system-view
[Sysname] sntp ipv6 unicast-server 2001::1
```

【相关命令】

- **sntp authentication enable**
- **sntp authentication-keyid**
- **sntp reliable authentication-keyid**

2.1.7 sntp reliable authentication-keyid

sntp reliable authentication-keyid 命令用来指定已创建的密钥是可信的。

undo sntp reliable authentication-keyid 命令用来取消可信密钥。

【命令】

sntp reliable authentication-keyid *keyid*

undo sntp reliable authentication-keyid *keyid*

【缺省情况】

没有配置可信密钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keyid：密钥编号，取值范围为 1～4294967295。

【使用指导】

使能身份验证功能后，客户端只会同步到提供可信密钥的服务器；如果服务器提供的密钥不是可信的，那么客户端不会与其同步。

本命令的使用前提是认证开关已经打开并且配置了密钥，即保证该密钥的存在性后才能设定它是否可信。如果 SNTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo sntp reliable authentication-keyid** 命令。

【举例】

使能SNTP身份验证功能，配置编号为37的密钥采用MD5算法进行身份验证，密钥值为BetterKey。

```
<Sysname> system-view
[Sysname] sntp authentication enable
[Sysname] sntp authentication-keyid 37 authentication-mode md5 simple BetterKey
```

指定该密钥为可信密钥。

```
[Sysname] sntp reliable authentication-keyid 37
```

【相关命令】

- **sntp authentication-keyid**
- **sntp authentication enable**

2.1.8 sntp unicast-server

sntp unicast-server 命令用来为设备指定 NTP 服务器。

undo sntp unicast-server 命令用来取消为设备指定的 NTP 服务器。

【命令】

sntp unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **source** *interface-type interface-number* | **version** *number*] *

undo sntp unicast-server { *server-name* | *ip-address* }

【缺省情况】

没有为设备指定 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name：NTP 服务器的主机名字，为 1～253 个字符的字符串，不区分大小写。

ip-address：NTP 服务器的 IP 地址。该地址只能是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。

authentication-keyid *keyid*：指定向 NTP 服务器发送报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1～4294967295。如果未指定本参数，则本端设备与 NTP 服务器之间不会进行身份验证。

source *interface-type interface-number*：指定 NTP 报文的源接口。本地设备给服务器发送 NTP 报文时，报文的源地址为指定源接口的主 IP 地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数，则根据路由表查找报文的出接口，并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

version *number*：指定 NTP 版本号。*number* 取值范围为 1～4，缺省值为 4。

【使用指导】

为设备指定 NTP 服务器后，设备可以与该服务器进行时间同步。设备的时间获得同步后，不能作为服务器为其他设备提供时间同步。

【举例】

配置设备的 NTP 服务器为 10.1.1.1，版本号为 4。

```
<Sysname> system-view
[Sysname] sntp unicast-server 10.1.1.1 version 4
```

【相关命令】

- **sntp authentication enable**
- **sntp authentication-keyid**
- **sntp reliable authentication-keyid**