

S5600带身份验证的NTP服务器模式的配置

一、组网需求:

1. Switch1设置本地时钟作为NTP主时钟，层数为2。
2. S5600以Switch1作为时间服务器，将自己设置为客户端模式，则Switch1自动工作在服务器模式，同时两端配置NTP验证。

二、组网图



三、配置步骤:

1. 配置S5600

- 1) 进入系统视图。

```
<S5600> system-view
```

- 2) 设置Switch1为时间服务器。

```
[S5600] ntp-service unicast-server 1.0.1.11
```

- 3) 配置NTP验证。

```
[S5600] ntp-service authentication enable
```

- 4) 设置编号为42的MD5密钥，内容为“aNiceKey”。

```
[S5600] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

- 5) 指定密钥为可信密钥。

```
[S5600] ntp-service reliable authentication-keyid 42
```

```
[S5600] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

以上配置将S5600向Switch1进行时间同步，但由于Switch1没有使能NTP身份验证，所以S5600还是无法向Switch1同步。

2. 现在，向Switch1增加以下配置:

- 1) 在Switch1上启动身份验证。

```
[Switch1] system-view
```

```
[Switch1] ntp-service authentication enable
```

- 2) 设置编号为42的MD5密钥，内容为“aNiceKey”。

```
[Switch1] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

- 3) 指定此密钥为可信密钥。

```
[Switch1] ntp-service reliable authentication-keyid 42
```

此时，S5600可以向Switch1同步，同步后观测S5600的状态为:

```
[S5600] display ntp-service status
```

```
Clock status: synchronized
```

```
Clock stratum: 3
```

```
Reference clock ID: 1.0.1.11
```

```
Nominal frequency: 250.0000 Hz
```

```
Actual frequency: 249.9992 Hz
```

```
Clock precision: 2^19
```

```
Clock offset: 0.66 ms
```

```
Root delay: 27.47 ms
```

```
Root dispersion: 208.39 ms
```

```
Peer dispersion: 9.63 ms
```

```
Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

可以看出，S5600已经与Switch1同步，层数为3，比Switch1大1。

- 4) 查看S5600的NTP会话信息，可以看到S5600与Switch1建立了连接。

```
<S5600> display ntp-service sessions
```

```
source      reference  stra reach poll now offset delay disper
*****
```

```
[5]1.0.1.11 127.127.1.0 2 1 64 1 350.1 15.1 0.0
```

```
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

四、配置关键点:

1. Switch1是支持本地时钟作为主时钟的交换机。
2. 在配置带验证功能的NTP连接时，设置的对应体或服务器后面一定要绑定已经配置好的密钥，否则发出的报文不会携带验证信息。

3. 当交换机接收到带有验证信息的NTP报文时：

- 1) 如果本地启动了NTP验证功能，则对报文进行正常的验证操作；
- 2) 如果本地没有启动NTP验证功能，则系统默认该报文通过验证并进行下一步处理。

4. 当交换机接收到没有验证信息的NTP报文时：

- 1) 如果本地启动了NTP验证功能，则该报文不能通过验证，将被视为非法报文而丢弃；
- 2) 如果本地没有启动NTP验证功能，则不会对该报文进行任何验证处理。

5. S5600作NTP服务器之前，必须先和别的NTP Server同步。