

网络设备时间同步管理

1. NTP概述

1.1. 协议规范

1.2. 角色/功能/专业术语

1.2.1. NTP服务器

1.2.2. NTP客户端

1.2.3. 层数 (stratum)

1.2.4. 硬件时钟

1.2.5. 主动对等体

1.2.6. 被动对等体

1.2.7. 广播服务器

1.2.8. 广播客户端

1.3. NTP安全机制

2. 网络设备部署NTP服务器/客户端

2.1. 调整网络设备时间、日期、时区

2.2. 将IOSV路由器配置为NTP服务器

2.3. 为NTP同步添加身份验证(MD5)

2.3.1. 服务器端配置

2.3.2. 客户端端配置

1. NTP概述

NTP (Network Time Protocol, 网络时间协议) 是一种用于网络设备时间同步化的应用层协议。它可以使网络设备对其服务器或时钟源做同步化, 提供高精度度的时间校正 (LAN上与标准时间差小于1毫秒, WAN上几十毫秒), 且可使用加密确认的方式来防止攻击。NTP基于UDP传输协议实现, 使用的UDP端口为123。思科产品支持NTP的客户端与服务器功能, 即设备既可以从时间服务器上同步时间, 也能够作为时间服务器对其他设备进行时间同步。在作为服务器工作时设备仅支持单播Server模式, 还支持对等体模式和广播模式。

1.1. 协议规范

RFC 1305: Network Time Protocol (Version 3)

RFC 5905: Network Time Protocol (Version 4)

1.2. 角色/功能/专业术语

1.2.1. NTP服务器

设备将本地时钟作为参考时钟源，为网络中的其它设备提供时间同步服务。

1.2.2. NTP客户端

设备作为NTP客户端从网络中的NTP服务器同步时间。

1.2.3. 层数 (stratum)

NTP使用“层数 (stratum)”的概念来描述设备距离权威时钟源的“跳数 (hops)”。一个层数为1的时间服务器应当有个直连的原子钟或电波钟；层数为2的时间服务器就从层数为1的服务器获取时间；层数为3的服务器就从层数为2的获取时间.....如此递推。因此时钟层数数值更低的时钟源即被认为拥有更高的时钟精度。16跳不可达。

1.2.4. 硬件时钟

硬件时钟根据设备上的石英晶体振荡器频率工作，由设备的电池为其供电，设备关机后硬件时钟依然运行。在设备启动运行后，会从硬件时钟读取时间信息，作为设备的软件时间。

1.2.5. 主动对等体

定期向被动对等体发送同步报文，报文中的Mode字段设置为1。不考虑它的对等体是否可达以及对等体的层数。运行在这一模式下的主机可以向对方提供同步信息，也可以依照对方的时间信息同步本地时钟。

1.2.6. 被动对等体

接收到主动对等体报文并做出响应，报文中的Mode字段设置为2。运行在被动对等体模式的主机可以向对方提供同步信息，也可以依照对方的时间信息同步本地时钟。

1.2.7. 广播服务器

在广播模式下，服务器周期性向广播地址255.255.255.255发送时钟同步报文，报文中的Mode字段设置为5。不管它的对等体是否可达或层数为多少。运行在广播模式的主机通常是网络内运行高速广播介质的时间服务器，向所有对等体提供同步信息，但不会修改本设备的时钟。

1.2.8. 广播客户端

客户端侦听来自服务器的时钟同步报文。当接收到第一个时钟同步报文，客户端与服务器交互Mode字段为3（客户端模式）和4（服务器模式）的NTP报文，即客户端先启用一个短暂的服务/客户端模式与远程服务器交换消息，以获得客户端与服务器间的网络延迟。之后恢复广播模式，继续侦听时钟同步报文的到来，根据到来的时钟同步报文对本地时钟再次进行同步。

1.3. NTP安全机制

为防止对时间服务器的恶意破坏，提高时间同步的安全性，NTP提供了安全认证和访问控制功能。

- NTP使用了认证(Authentication)机制，检查时间同步信息是否是真正来自所宣称的服务器并检查信息的返回路径，以提供对抗干扰的保护机制。
- NTP客户端和服务端配置相同的密钥。发送请求报文和响应报文时，设备根据指定的密钥和NTP报文内容采用MD5算法计算出报文的哈希值填充到报文的认证信息。接收设备根据认证信息判断是否报文发送端是否可信的设备或者报文是否被篡改。

2. 网络设备部署NTP服务器/客户端

2.1. 调整网络设备时间、日期、时区

要配置 Cisco 网络设备的时间、日期和时区，你可以按照以下步骤进行：

- 1. **进入特权模式：**通过输入 enable 命令并提供特权级别密码，进入特权模式。
- 2. **进入全局配置模式：**输入 configure terminal 命令，进入全局配置模式。
- 3. **设置时区：**使用 clock timezone 命令来设置时区。例如，如果你在东部时间（EST）区域，可以输入：

▼ Plain Text |

```
1 NTP-SERVER(config)#clock timezone EST -5
```

这将把时区设置为东部标准时间，偏移量为 -5 小时。

- 4. **设置夏令时（可选）：**如果你所在的地区使用夏令时，你可以使用 clock summer-time 命令来配置夏令时。例如：

▼ Plain Text |

```
1 NTP-SERVER(config)#clock summer-time EDT recurring
```

这将配置夏令时，EDT 代表东部夏令时，recurring 表示夏令时是递归的，也就是每年都会生效。

- 5. **手动设置时间和日期：**输入 end 退出全局配置模式，再使用 clock set 命令来手动设置时间和日期。例如：

▼ Plain Text |

```
1 NTP-SERVER#clock set 14:30:00 June 6 2024
```

这将设置时间为下午 2 点 30 分，日期为 2024 年 6 月 6 日。

- 6. **确认设置：**在全局配置模式输入 show clock 命令来确认时间和日期设置是否正确。

▼ Plain Text |

```
1 NTP-SERVER#show clock
2 09:30:21.439 EDT Thu Jun 6 2024
```

记住，在配置时区和夏令时时，确保选择正确的选项以匹配你所在的地理位置和当地的规则。

2.2. 将IOSV路由器配置为NTP服务器

要将 Cisco IOSV 路由器配置为 NTP（Network Time Protocol）服务器，你可以按照以下步骤进行：

1. **进入特权模式**：通过输入 `enable` 命令并提供特权级别密码，进入特权模式。
2. **进入全局配置模式**：输入 `configure terminal` 命令，进入全局配置模式。
3. **配置路由器的时钟源**：在 NTP 服务器上，你需要设置路由器的时钟源。通常，你可以选择使用外部 NTP 服务器或者使用本地的时钟作为时钟源。如果你选择使用外部 NTP 服务器，你可以跳过这一步。如果你想使用本地时钟作为时钟源，可以执行以下命令：

```
1 NTP-SERVER(config)#clock timezone [时区] [偏移量]
```

例如：

```
1 NTP-SERVER(config)#clock timezone EST -5
```

这将把时区设置为东部标准时间，偏移量为 -5 小时。

4. **配置 NTP 服务器**：使用 `ntp master` 命令将路由器配置为 NTP 主服务器。你可以指定你希望的 NTP 级别。例如：

```

1  NTP-SERVER(config)#ntp master 1
2
3
4  NTP-SERVER(config)#do show ntp associations
5
6  address          ref clock      st   when   poll reach  delay  offset  di
sp
7  *~127.127.1.1    .LOCL.          0    9     16   377   0.000   0.000
0.261
8  * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configure
d
9
10
11 NTP-SERVER(config)#do show ntp status
12 Clock is unsynchronized, stratum 1, reference is .LOCL.
13 nominal freq is 1000.0003 Hz, actual freq is 1000.0003 Hz, precision is 2*
*15
14 ntp uptime is 37500 (1/100 of seconds), resolution is 1000
15 reference time is EA0C38DC.ED5D8696 (09:32:12.927 EDT Thu Jun 6 2024)
16 clock offset is 0.0000 msec, root delay is 0.00 msec
17 root dispersion is 0.48 msec, peer dispersion is 0.26 msec
18 loopfilter state is 'FREQ' (Drift being measured), drift is 0.000000000 s/
s
19 system poll interval is 16, last update was 13 sec ago.

```

这将配置路由器为 NTP 主服务器，并指定级别为 1。

5. **配置 NTP 客户端**（可选）：如果你的网络中有其他设备需要同步时间，你可以将它们配置为 NTP 客户端，以便从路由器同步时间。在客户端设备上，你可以使用以下命令：

```

1  ntp server [路由器的IP地址]

```

这将把路由器配置为客户端设备的时间源。

例如：

```

1  NTP-CLIENT(config)#ntp server 192.168.10.200 source gigabitEthernet 0/0
2
3

```

6. **确认设置：**输入 `end` 退出全局配置模式，并使用 `show ntp status` 命令来确认 NTP 服务器的状态和配置是否正确。

记得在设置 NTP 服务器时，确保路由器的时间是准确的，以便提供准确的时间同步服务。

2.3. 为NTP同步添加身份验证(MD5)

2.3.1. 服务器端配置

1. 首先，进入全局配置模式，以便进行配置更改。在终端输入以下命令：

```
1 NTP-SERVER> enable
2 NTP-SERVER# configure terminal
```

2. 启用 NTP 身份验证以增强安全性。输入以下命令：

```
1 NTP-SERVER(config)# ntp authenticate
```

3. 配置 NTP 身份验证密钥。这个密钥将用于 MD5 身份验证。输入以下命令：

```
1 NTP-SERVER(config)# ntp authentication-key 1 md5 Skills39
```

这里，1 是密钥号，"Skills39" 是你选择的 MD5 密码。

4. 将刚刚配置的密钥标记为受信任的密钥，以确保 NTP 会话的安全性。输入以下命令：

```
1 NTP-SERVER(config)# ntp trusted-key 1
```

5. 最后，配置设备为 NTP 服务器。这会使设备提供时间同步服务给网络中的其他设备。你可以使用 `ntp master` 命令，也可以指定级别。例如，输入以下命令：

```
1 SW1(config)# ntp master
```

或者，如果你想指定级别：

```
1 SW1(config)# ntp master 1
```

2.3.2. 客户端配置

1. 与服务器端一样，首先进入全局配置模式。在终端输入以下命令：

```
1 NTP-CLIENT> enable
2 NTP-CLIENT# configure terminal
```

2. 启用 NTP 身份验证以增强安全性。输入以下命令：

```
1 NTP-CLIENT(config)# ntp authenticate
```

3. 配置 NTP 身份验证密钥。输入以下命令：

```
1 NTP-CLIENT(config)# ntp authentication-key 1 md5 Skills39
```

4. 将刚刚配置的密钥标记为受信任的密钥。输入以下命令：

```
1 NTP-CLIENT(config)# ntp trusted-key 1
```

5. 配置 NTP 服务器。指定服务器的 IP 地址和之前配置的密钥号。输入以下命令：

```
1 NTP-CLIENT(config)# ntp server [服务器地址] key 1
```

这里，[服务器地址] 是 NTP 服务器的 IP 地址。

6. 配置完成后，退出配置模式。输入以下命令：

```
1 NTP-CLIENT(config)# end
```

7. 最后，确认配置是否正确。在命令提示符下输入以下命令：

▼ Plain Text |

```
1 NTP-CLIENT# show ntp associations
```

这样你就完成了服务器和客户端的 NTP 配置，并且添加了 MD5 身份验证。确保在客户端配置中正确指定了 NTP 服务器的地址和密钥号，以确保 NTP 通信受到身份验证的保护。