网络运维管理

第4讲：NTP服务实现

河南中医药大学信息技术学院
许成刚

一、谈谈时间同步的重要性

1. 谈谈时间同步的重要性

- 在一个大的系统中，时间同步（一致）的重要性。

1. 谈谈时间同步的重要性

计算机中的时间

计算机时间包括硬件时间和系统时间。

硬件时间

- 计算机主板上的RTC（实时时钟）以振荡器为时钟源，通过振荡器产生脉冲信号的振荡频率计时。由CMOS电池为RTC和CMOS供电，RTC计时并将时间存储到CMOS。

系统时间

- 计算机运行时CPU内核振荡器产生高频脉冲信号，为系统时钟提供了一个精确的脉冲信号周期时间（如：时钟频率为1GHz，周期为1ns）。系统时钟也基于对CPU的振荡器产生脉冲信号的频率进行系统计时。
- 计算机启动时通过BIOS程序从CMOS读取硬件时间，根据系统时区确定系统时间。

1. 谈谈时间同步的重要性

- 为什么会出现不同步？
  - 随着计算机网络的迅猛发展，网络中的设备种类和业务类型越来越多，服务器的数量也与日俱增。传统上，各种服务器、网络设备使用的时间都是由设备内部时钟来提供的。
  - 在网络中，由于不同设备本地时钟频率、运行环境的不同，进行过时钟校准的设备运行一段时间后会出现时间不一致。
  - 由于服务器、网络设备本身的时钟误差是不可避免的，尽管这种误差每天不大，但经过一段时间的累积就会出现大的时间差，从而导致网络中各服务器、网络设备的时间不一致。而这种不一致，将会对网络服务产生较大影响。

1. 谈谈时间同步的重要性

- “不同步”带来的问题
  - 案例1：医院的医生工作站开具处方，并保存在服务器中。若服务器时间不正确，则无法进行正常的处方回溯；
  - 案例2：安全设备的时间策略，例如防火墙。因为时间的不一致，无法正常实现安全策略。
  - 案例3：服务器系统监控，因为时间的不统一，就无法判定出业务（或故障）具体发生时间。
  - 案例4：研究生考试，不同考场的时间若不同步，影响考试的公平性。

1. 谈谈时间同步的重要性

- 随着网络拓扑的日益复杂，整个网络内设备的时钟同步将变得十分重要。如果依靠管理员手工修改系统时钟，不仅工作量巨大，而且时钟的准确性也无法得到保证。
  - 需要解决两个问题
    - 标准的时间源
    - 网络内的时间同步方式

二、谈谈标准的时间源

2.谈谈标准的时间源

- 时间如何确定？
  - “天”是怎么来的？
    - 观察太阳。由于地球的自转，人们可以看到日出日落，所以就把这一周期现象定义为“天”。进而有了时、分、秒
  - 世界时
    - 确定了天文规律，人们开始制造钟表，把时间表示出来。所以，在1927年，人们以基于天文现象和钟表计时，确立了第一套时间标准，也就是世界时（Universal Time，简称 UT），并被广泛用于全球标准时间。

2.谈谈标准的时间源

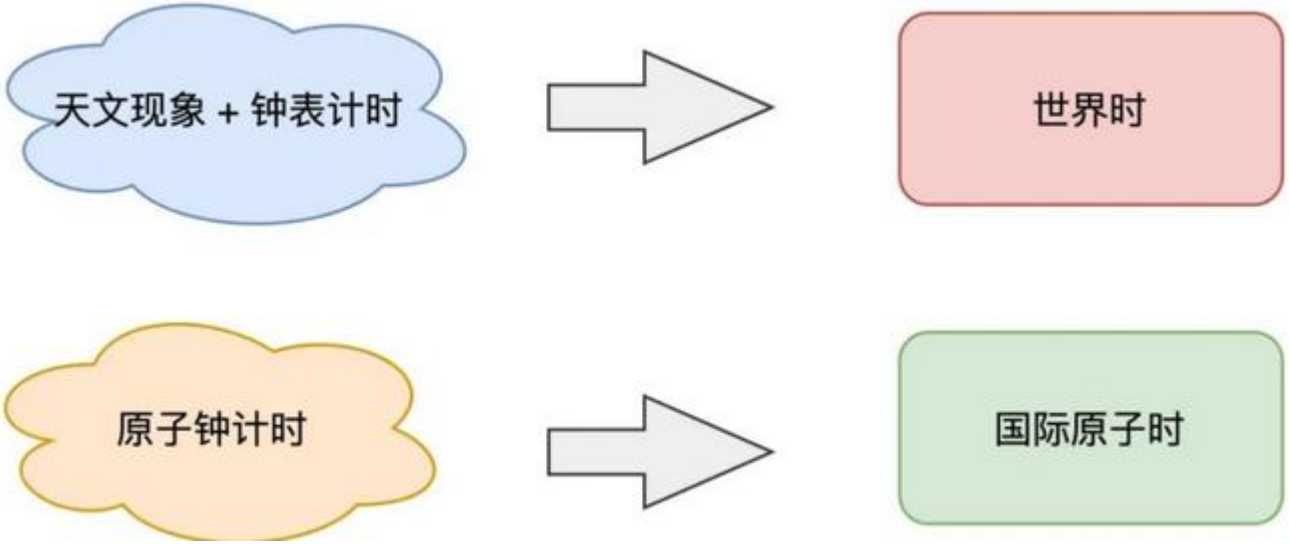
- 时间如何确定？
  - 国际原子时
    - 通过天文观测的世界时的不精准性，地球自转在减慢；
    - 从微观层面探索“秒”的定义！希望每一秒是固定的！
    - 人们发现，原子内的电子发生跃迁时，原子会吸收或放出一定能量的电磁波，这类电磁波就是一种周期运动，我们也可以把它看成原子内部的振荡。基于这个原理，科学家们开始不断地试验、研究，终于发现铯原子内部的振荡周期比其它原子都要更短、更稳定，而且，这个过程基本不受环境因素的干扰。

2.谈谈标准的时间源

- 时间如何确定？
  - 国际原子时
    - 科学家们就以之前定义的"秒"为基础，去测量一秒内这个铯原子内部电子周期运动的次数，测量出来的结果为9192631770 次。
    - 基于此，科学家们决定抛弃原来基于天文测量的秒，重新定义"秒"的时长，就是这个高度稳定的运动周期。
    - 因此，在1967年国际度量衡大会决定采用，以铯原子跃迁 9192631770 个周期所持续的时间长度定义为1秒，而基于这个铯原子振荡制造出来的时钟，被称为原子钟。
    - 有了原子钟，人们基于原子钟又确立了一套新的时间标准，叫做国际原子时（International Atomic Time，简称 TAI）。

2.谈谈标准的时间源

- 两套时间标准存在的问题
  - 这就出现两套时间标准



2.谈谈标准的时间源

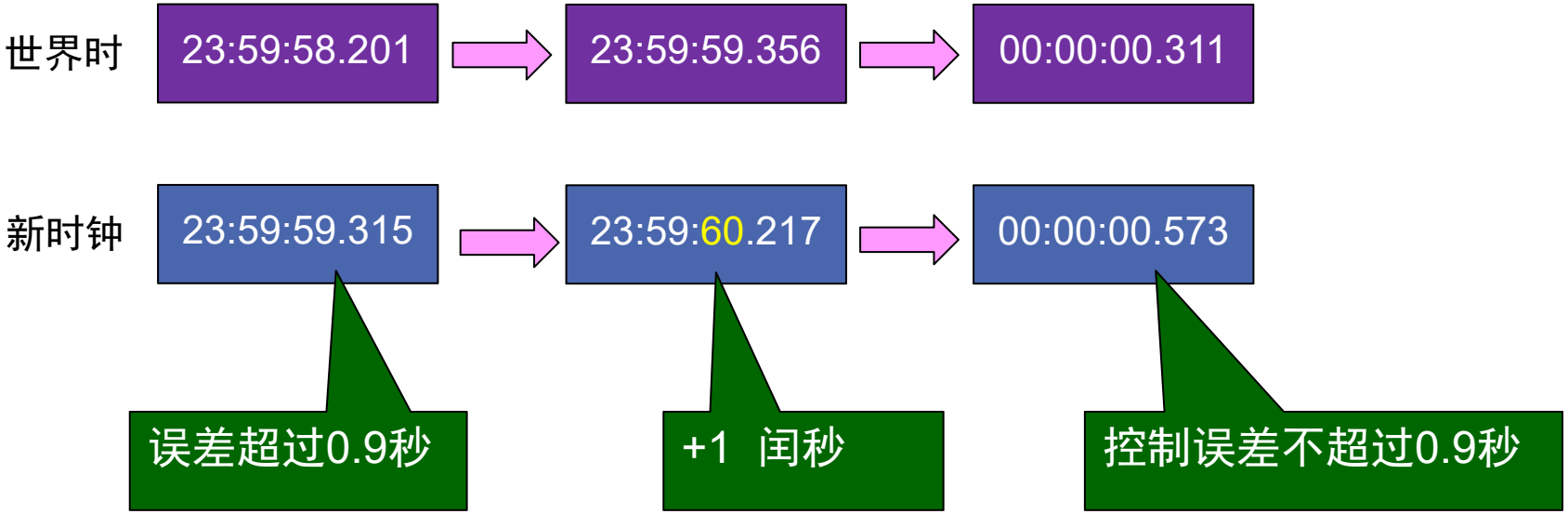
- 两套时间标准存在的问题
  - 假设我们以国际原子时为时间标准，那会发生什么现象呢？因为原子时非常稳定，但世界时随着地球自转变慢，会越来越慢，就会发生这种现象，原子时走得快，世界时走得慢，时间越久，两者差距越来越大，一般来说一至二年会差大约1秒时间。
  - 基于天文测算的世界时，已经指导我们人类生活了上千年，人类早已习惯了这种时间标准，直接被原子时取代，肯定是不能接受的。但我们又需要原子时这种高度稳定的计时标准，来发展科学研究，两者发生矛盾，这怎么办？

2.谈谈标准的时间源

- 一个互相兼容的解决方案！
  - 我们可以再建立一套新的时间标准，这套时间以原子时为基准，开始计时，走的每一秒都是稳定、精确的。同时，为了兼顾基于天文测量的世界时，人类会持续观测这个新时钟与世界时的差距。如果发现两者相差过大时，我们就人为地调整一下这个时钟（加一秒或减一秒），让两者相差不超过 0.9 秒，而加的这一秒，科学家把它定义为闰秒。
  - 例如：若地球自转变慢，原子时误差将超过+0.9秒时，便人为地加进1秒，反之则要扣去1秒钟。
  - 国际上规定，这种闰秒由国际时间局根据实际情况来随时处理，但加减必须在特定的时刻进行:12月31日或6月30日最后一分钟的最后一秒之后。

2.谈谈标准的时间源

- 一个互相兼容的解决方案！
  - 举例：闰秒的应用



2.谈谈标准的时间源

- UTC (Universal Time Coordinated) 协调世界时
  - 这个兼容性方案的好处在于，新时钟的每一秒的计时依旧是精确的，而且还兼顾了日常生活使用的世界时，一举两得。由于这个时钟是基于原子时 + 世界时协调得出的，所以科学家们把它定义为协调世界时（Coordinated Universal Time，简称 UTC）。
  - 有了这个研究成果，有技术能力的国家都纷纷制造自己的原子钟，然后计算协调世界时。中国会在自己算出的世界协调时的基础上，再加8个小时（中国在东八区），最终得出来的时间，就是北京时间。至此，全新的世界标准时间确立了，这套时间标准于1972年正式确定，一致沿用至今。

2.谈谈标准的时间源

- 协调世界时——闰秒
  - 2015年，全球进行闰秒调整。当时，国际标准时UTC在闰秒调整前后的时间标记为：2015年06月30日的23时59分59秒、2015年06月30日23时59分60秒、2015年07月01日00时00分00秒。
  - 由于我国位于东八区（UTC+8），闰秒调整出现在北京时间2015年07月01日上午，当时北京时间的闰秒调整顺序为：2015年07月01日07时59分59秒、2015年07月01日07时59分60秒、2015年07月01日08时00分00秒。

2015年1月，中科院国家授时中心宣布，我国将在北京时间2015年7月1日的7时59分59秒和全球同步进行闰秒调整，届时会出现07:59:60的特殊现象

三、网络内的时间同步方式

3.网络内的时间同步方式

- 有了标准时间，如何进行同步？
  - 通常，国家授时中心产生时间后会通过一系列方式，例如无线电波、网络、电话等，把这个时间广播出去，这个过程，就叫做授时。
  - 一般无线电波的传播速度更快、传播误差小，所以授时中心会通过这种方式，把时间发送给全国各地的时间服务器。
  - 时间服务器有了准确的时间后，再通过其它方式（例如网络）广播到下一层的终端用户使用。

3.网络内的时间同步方式

- 计算机网络内如何同步这个标准时间？
  - 最简单的方式就是：客户端向时间服务器端请求获取标准时间，服务端响应时间数据，客户端修改本机时间即可。
  - 问题：但事情没这么简单，因为数据在网络传输过程中，也是需要时间的，这个时间也会影响到时间的准确性。这怎么办呢？。
  - 使用NTP！
    - 当计算机在做时间校准时，也需要把网络延迟计算进去，最后修正这个同步过来的时间，降低误差。这个服务就是 NTP（Network Time Protocol），它可以保证每台机器的时间与时间服务器保持同步。

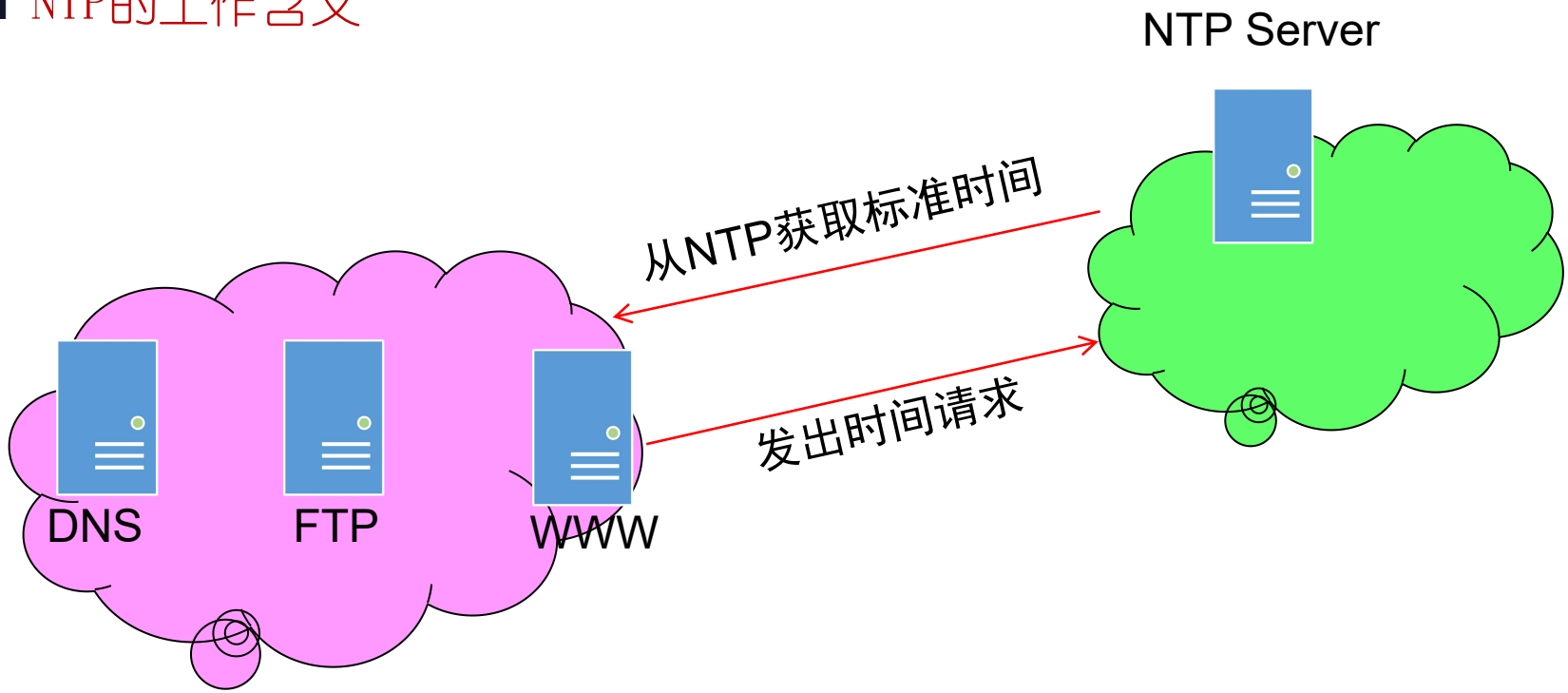
四、认识NTP

4.认识NTP

- 网络时间协议NTP (Network Time Protocol)
  - 是TCP/IP协议族里面的一个应用层协议。
  - NTP用于在一系列分布式时间服务器与客户端之间同步时钟。NTP的实现基于IP和UDP。
  - NTP报文通过UDP传输，端口号是123。

4.认识NTP

- NTP的工作含义



4.认识NTP

- NTP的主要应用场景
  - 网络管理：对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
  - 计费系统：要求所有设备的时钟保持一致。
  - 多个系统协同处理同一个复杂事件：为保证正确的执行顺序，多个系统必须参考同一时钟。
  - 备份服务器和客户机之间进行增量备份：要求备份服务器和所有客户机之间的时钟同步。
  - 系统时间：某些应用程序需要知道用户登录系统的时间以及文件修改的时间。

4.认识NTP —— NTP的版本

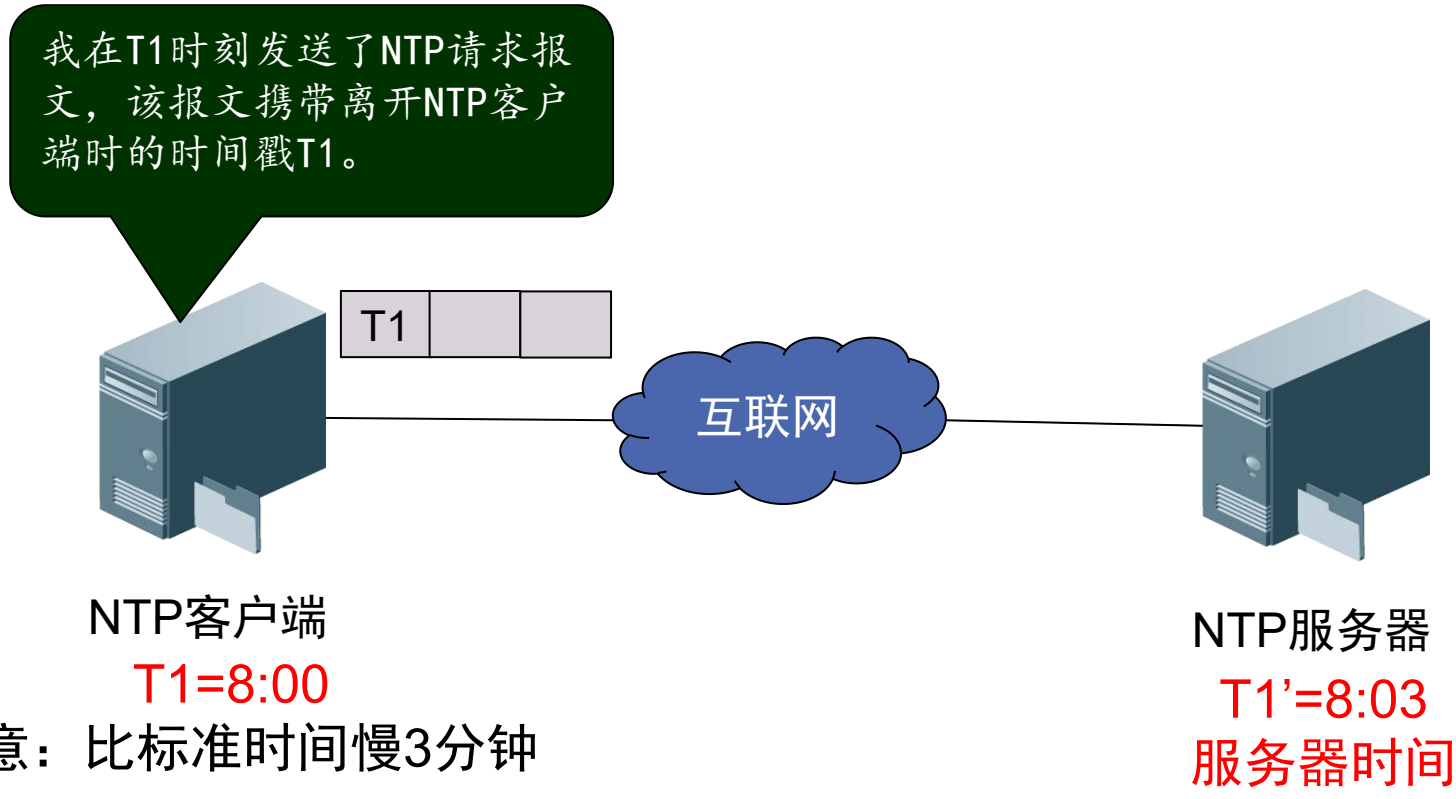
版本	时间	协议号	描述
NTPv1	1988年6月	RFC 1059	NTPv1首次提出了完整的NTP规则以及算法，但是NTPv1不支持认证和控制消息。
NTPv2	1989年9月	RFC 1119	NTPv2在NTPv1的基础上支持认证和控制消息。
NTPv3	1992年3月	RFC 1305	NTPv3正式引入了校正原则，并改进了时钟选择和时钟过滤算法。NTPv3目前应用较为广泛。
NTPv4	2010年6月	RFC 5905	•NTPv3仅支持IPv4网络，但是随着IPv6的发展和对网络安全性的要求不断提高，NTPv4产生。NTPv4是对NTPv3的扩展，并兼容NTPv3。 NTPv4同时支持IPv4和IPv6网络。 •NTPv4提供了一套完整的加密认证体系，安全性上相对NTPv3有了很大的提高。

五、NTP的工作原理

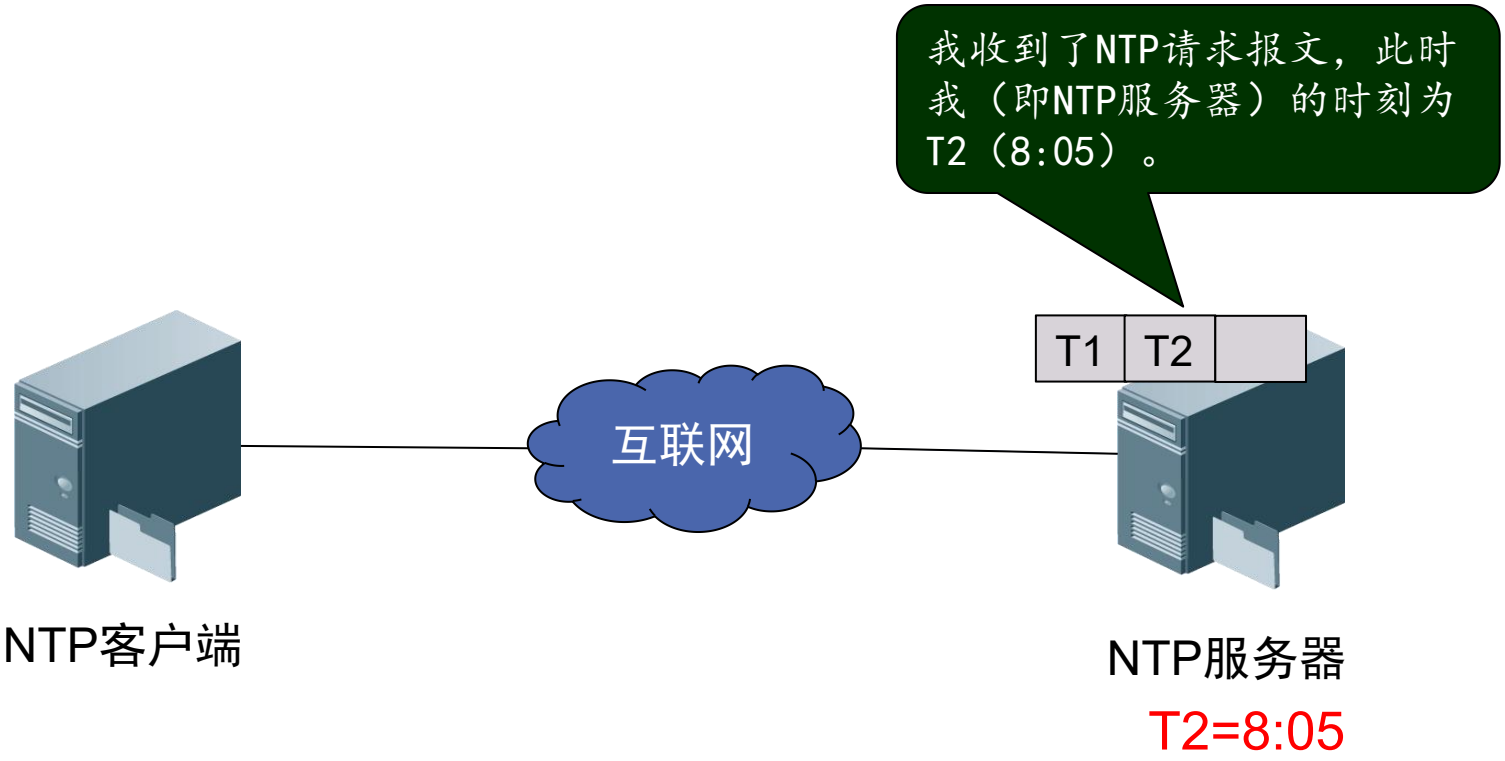
5. NTP的工作原理

- NTP客户端和NTP服务器相连，它们都有自己独立的系统时钟，现在通过NTP实现系统时钟自动同步
- NTP客户端的时钟设定为Ta，NTP服务器的时钟设定为Tb。假设Ta比Tb慢3分钟

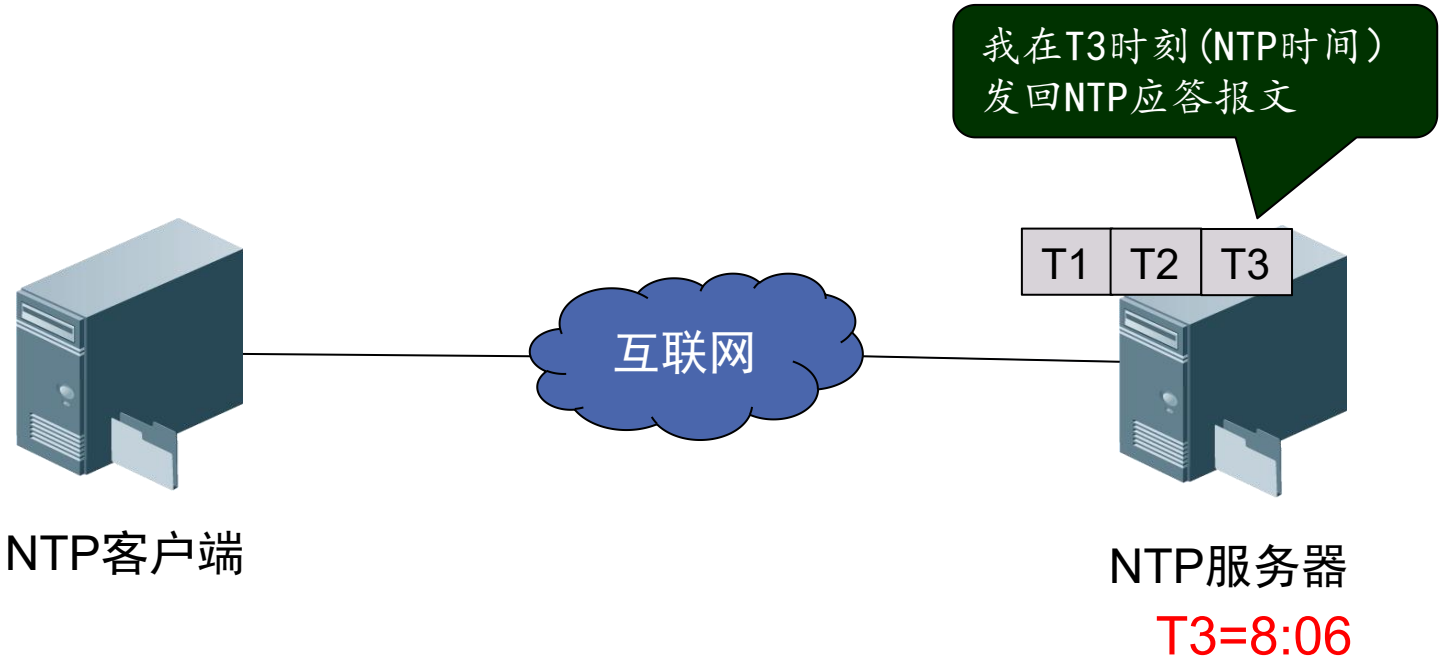
① NTP客户端在T1时刻（客户端的时间，假设8:00）发送一个NTP请求报文给NTP服务器，该请求报文携带离开NTP客户端时的时间戳T1。



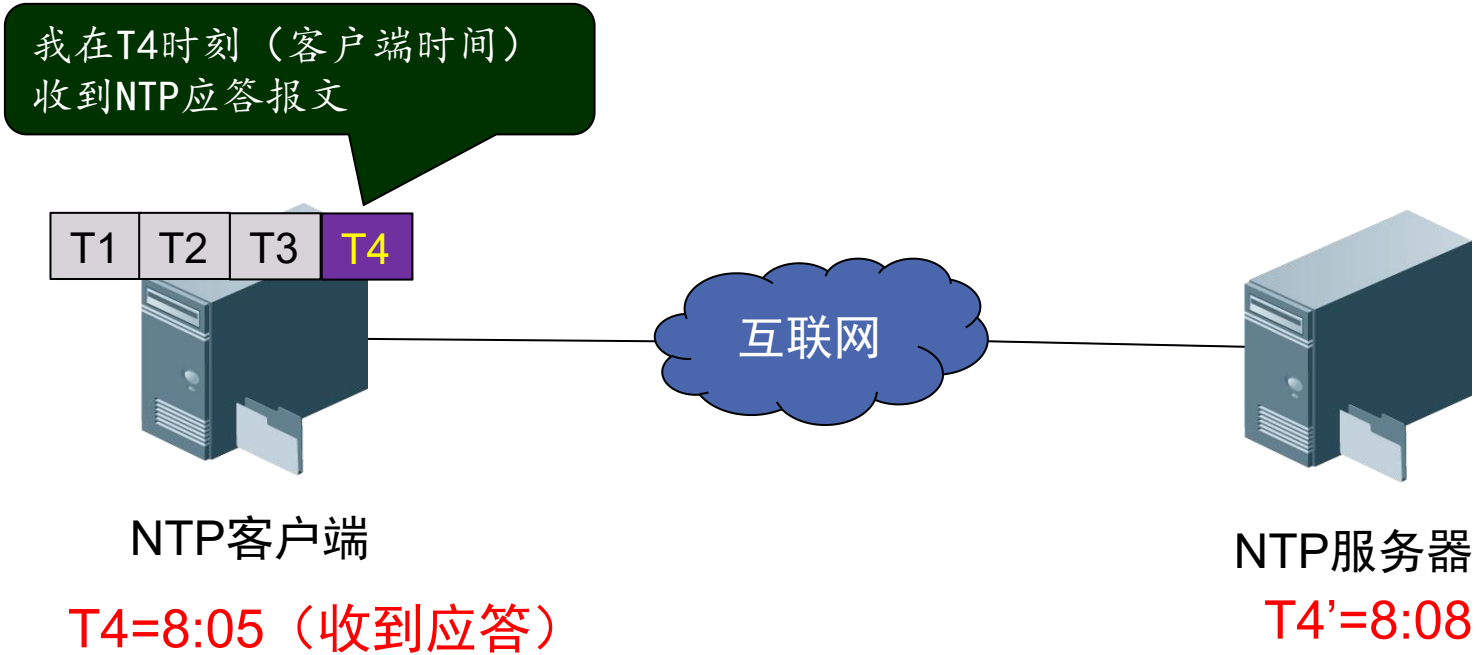
② NTP请求报文到达NTP服务器，此时NTP服务器的时刻为T2（服务器的时间，假设8:05）。



③ NTP服务器处理之后，于T3时刻（服务器的时间，假设8:06）发出NTP应答报文。该应答报文中携带离开NTP客户端时的时间戳T1、到达NTP服务器时的时间戳T2、离开NTP服务器时的时间戳T3



④ NTP客户端在T4时刻（客户端的时间，假设8:05）接收到该应答报文。

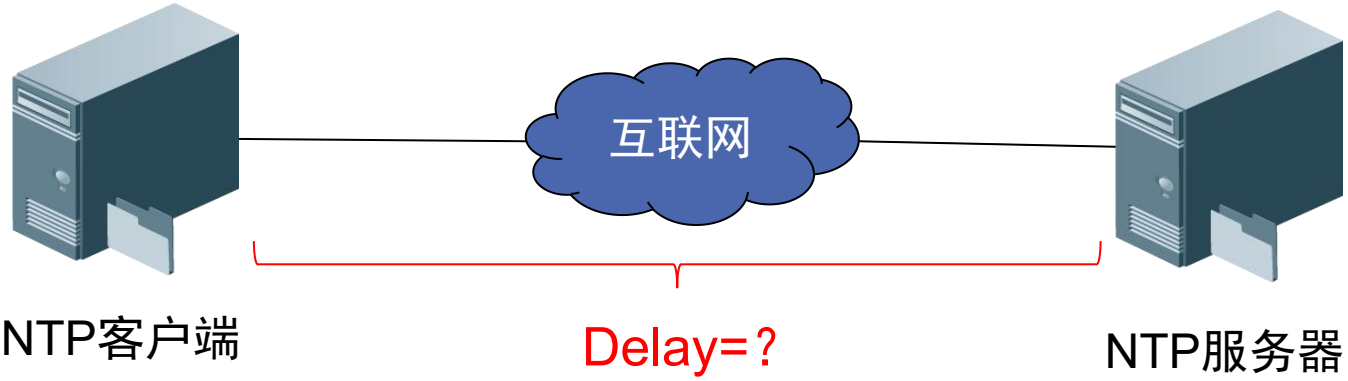


求：NTP报文从NTP客户端发送到NTP服务器所需要的平均时间Delay。

客：T1=8:00（发出请求）
服：T2=8:05（收到请求）
服：T3=8:06（发出应答）
客：T4=8:05（收到应答）

Delay = [(T4 - T1) - (T3 – T2)] / 2

代入T1～T4的假设值，得出Delay=2



求：设NTP客户端与NTP服务器之间的时间差为Offset。

以T4时刻为例，在这个时刻点（即NTP服务器发送过来的报文被客户端收到时），服务器的时刻已经为T3 + Delay。那么时间差Offset可由以下公式获得：

T4 + Offset = T3 + Delay

Offset = T3 + Delay-T4

=8:06+2-8:05=3

NTP客户端根据Offset来调整自己的时钟，实现与NTP服务器的时钟同步

NTP客户：Ta+Offset

例如此处：Ta+3

Delay = [(T4 - T1) - (T3 – T2)] / 2=2

T4 + Offset = T3 + Delay

Offset = T3 + Delay-T4=3

假设客户端比标准时间快3分钟

例如T1=8:00，T2=7:59，T3=8:00，T4=8:05

Ta'=Ta+（-3）
相当于客户端将自身时间减慢3分钟，变为标准时间

Delay = [(T4 - T1) - (T3 – T2)] / 2=2

T4 + Offset = T3 + Delay

Offset = T3 + Delay-T4= - 3

NTP客户端　　NTP服务器

注意：比标准时间快3分钟

六、 公共的NTP服务器

6. 公共的NTP服务器

- 中国科学院国家授时中心： http://www.ntsc.ac.cn/
  - NTP服务器
    - ntp.ntsc.ac.cn

6. 公共的NTP服务器

- 中国公共NTP服务器： https://www.pool.ntp.org/zone/cn
  - NTP服务器
    - 0.cn.pool.ntp.org
    - 1.cn.pool.ntp.org
    - 2.cn.pool.ntp.org
    - 3.cn.pool.ntp.org

6. 公共的NTP服务器

- 阿里云公共NTP
  - NTP服务器
    - ntp.aliyun.com
    - ntp1.aliyun.com
    - ntp2.aliyun.com
    - ntp3.aliyun.com
    - ntp4.aliyun.com
    - ntp5.aliyun.com
    - ntp6.aliyun.com
    - ntp7.aliyun.com

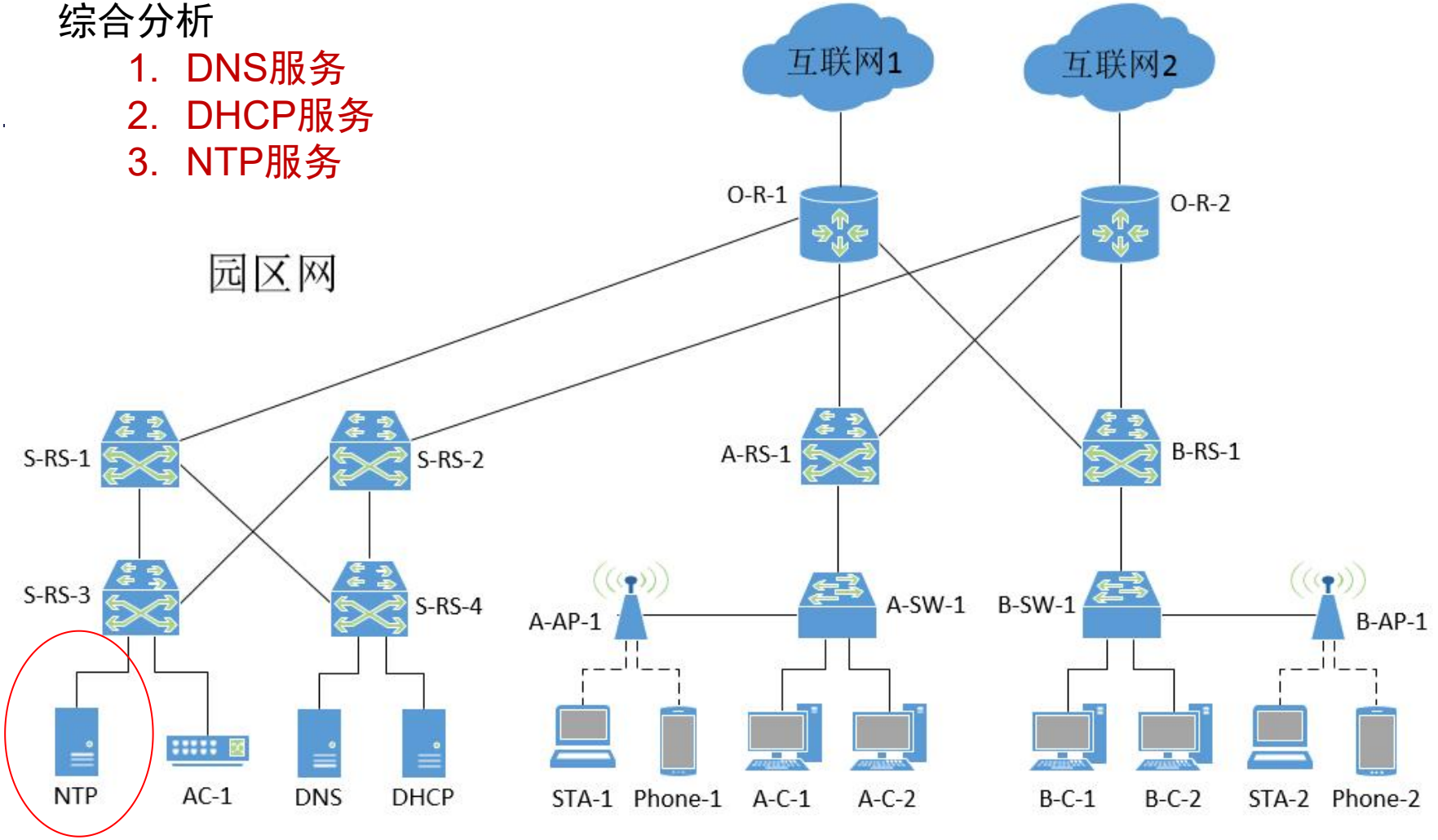
6. 公共的NTP服务器

- 腾讯公共NTP
- https://cloud.tencent.com/document/product/213/30392
  - NTP服务器：
    - ntp.aliyun.com
    - ntp1.aliyun.com
    - ntp2.aliyun.com
    - ntp3.aliyun.com
    - ntp4.aliyun.com
    - ntp5.aliyun.com
    - ntp6.aliyun.com
    - ntp7.aliyun.com

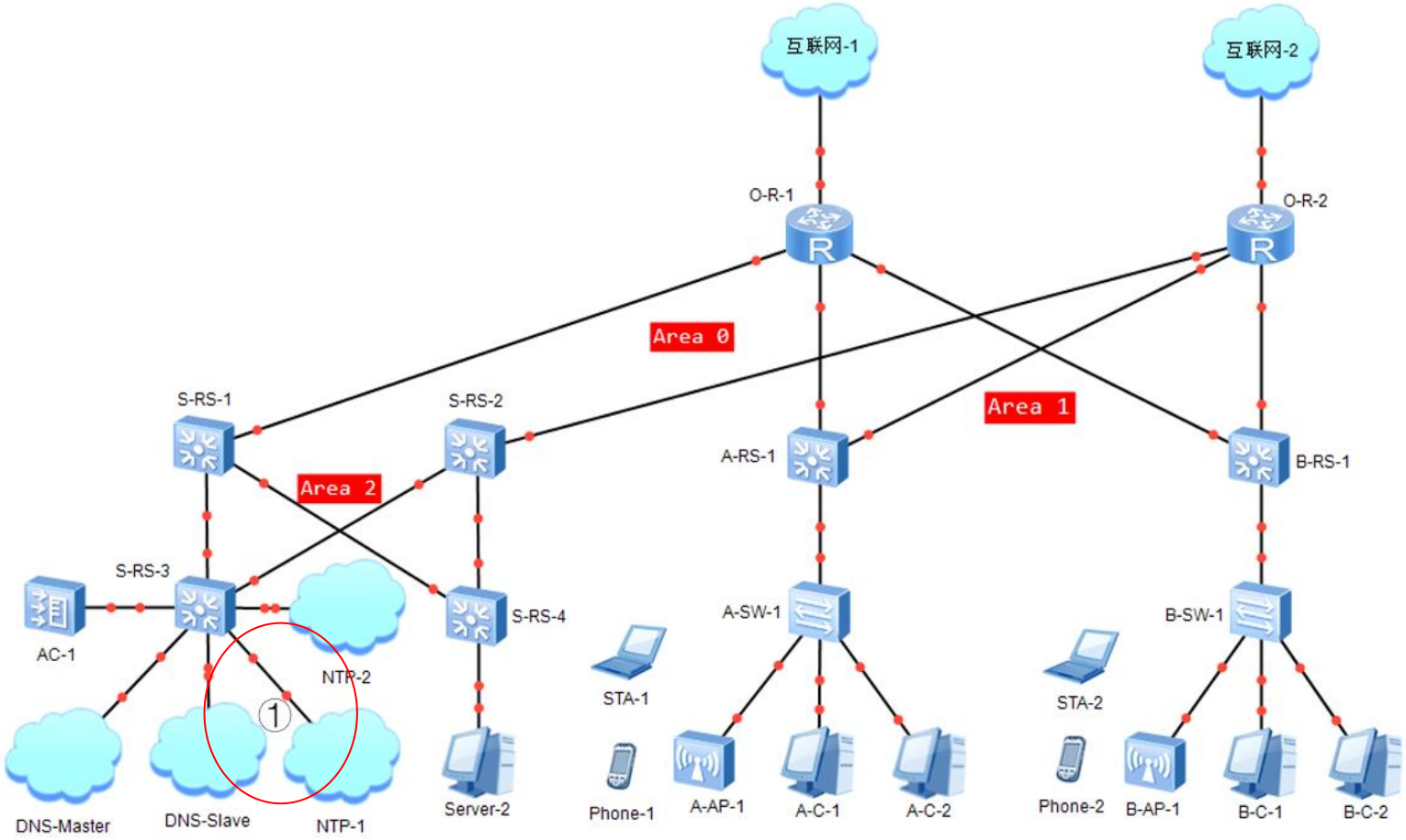
七、 抓包分析NTP报文

综合分析

1. DNS服务
2. DHCP服务
3. NTP服务

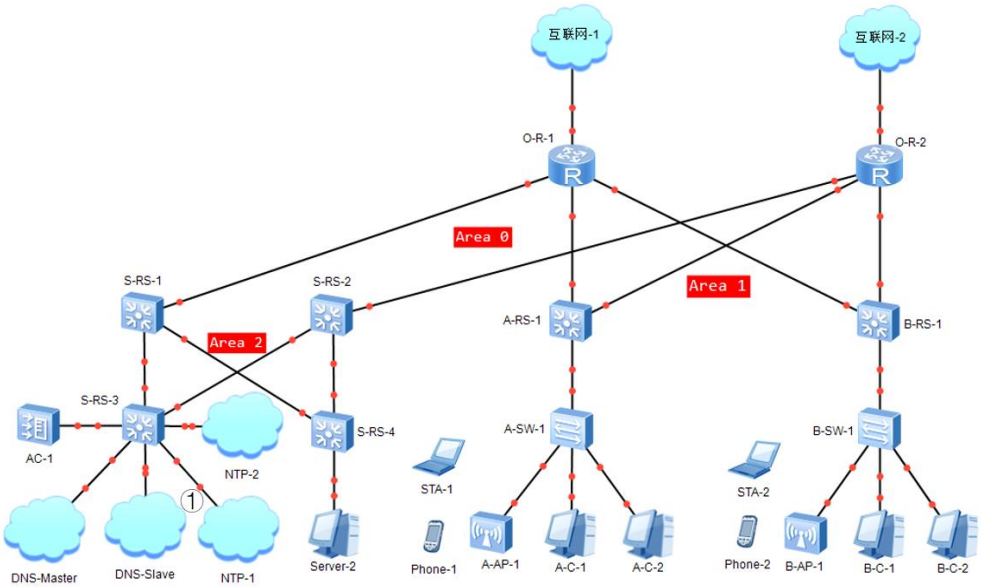


➢ 设置抓包点


互联网-1
互联网-2
O-R-1
O-R-2
Area 0
Area 1
Area 2
S-RS-1
S-RS-2
S-RS-3
S-RS-4
A-RS-1
B-RS-1
AC-1
NTP-2
NTP-1
DNS-Master
DNS-Slave
①
Server-2
STA-1
Phone-1
A-SW-1
A-AP-1
A-C-1
A-C-2
STA-2
Phone-2
B-SW-1
B-AP-1
B-C-1
B-C-2

➢ 设置抓包点

- 园区网内部的DNS服务器和网络设备自动向园区网内的NTP服务器发出时间同步请求，并获取时间同步；而园区网内的NTP服务器除了要响应园区网内部其他设备发来的时间同步请求之外，其自身还要和互联网上的公共NTP服务器之间进行时间同步操作。



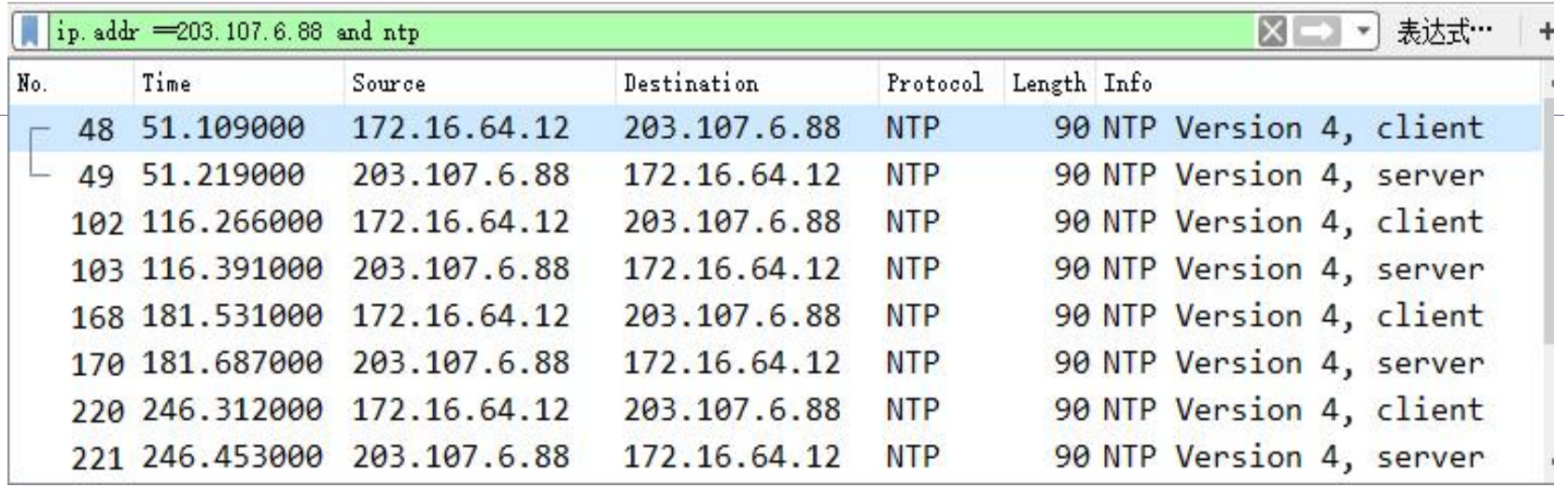
- 因此，在Cloud设备NTP-1的Ethernet 0/0/1接口处启动抓包程序，既可抓取NTP-1和园区网内的其他服务器以及网络设备之间的NTP报文，也可以抓取NTP-1和其chrony配置文件中设置的公共NTP服务器（即ntp.aliyun.com）之间的NTP报文。

➢ NTP报文列表

ip.addr ==203.107.6.88 and ntp　　表达式…

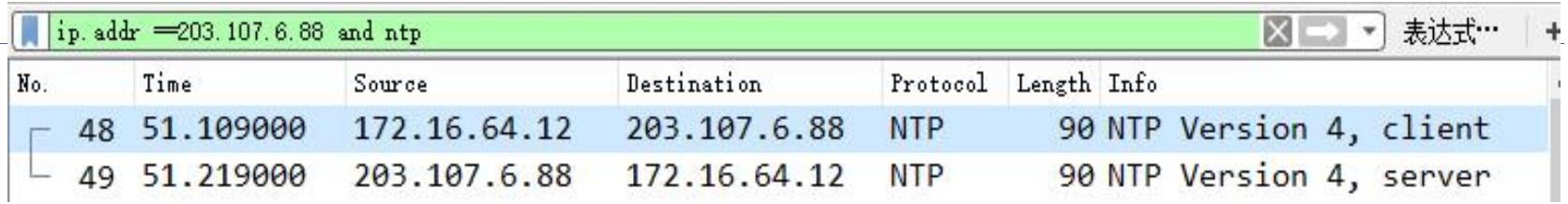
No.	Time	Source	Destination	Protocol	Length	Info
48	51.109000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
49	51.219000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server
102	116.266000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
103	116.391000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server
168	181.531000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
170	181.687000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server
220	246.312000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
221	246.453000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server

园区网内部的NTP服务器NTP-1（172.16.64.12）与公共NTP服务器（203.107.6.88）之间的时间同步报文

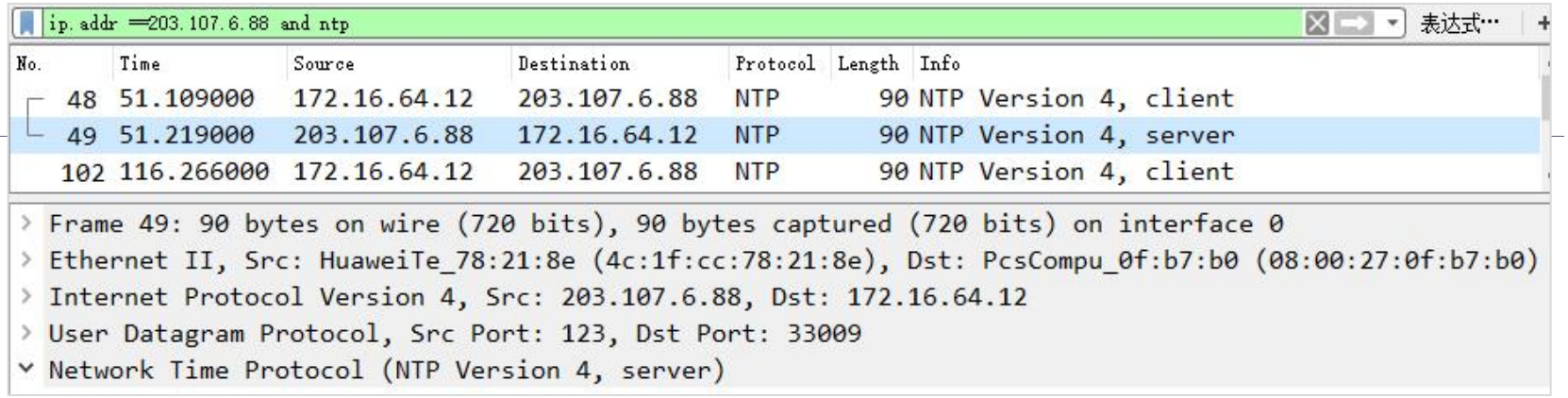


No.	Time	Source	Destination	Protocol	Length	Info
48	51.109000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
49	51.219000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server
102	116.266000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
103	116.391000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server
168	181.531000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
170	181.687000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server
220	246.312000	172.16.64.12	203.107.6.88	NTP	90	NTP Version 4, client
221	246.453000	203.107.6.88	172.16.64.12	NTP	90	NTP Version 4, server

- 此处的NTP时间同步方式是Client/Server方式，其中，NTP-1属于NTP客户端（client），而互联网上的公共NTP服务器（203.107.6.88）则作为NTP服务器端（server），向NTP-1提供时间同步服务；
- 通过48、102、168和220号报文的“Time”字段的值可知，默认情况下，NTP客户端（此处为NTP-1）大约每64秒与其上级NTP服务器（此处是公共NTP服务器203.107.6.88）进行一次时间同步。



- 以49号报文为例，分析NTP报文的内容。
- 这是从互联网上的公共NTP服务器（203.107.6.88）发往NTP-1（172.16.64.12）的NTP响应报文，即NTP服务器端发往NTP客户端的报文。



- 分析报文首部基本信息

序号	名称	内容 / 值	备注
数据链路层首部	源MAC地址	4c-1f-cc-78-21-8e	S-RS-3的MAC地址，即NTP-1所在网络的默认网关的MAC地址
	目的MAC地址	08:00:27:0f:b7:b0	NTP-1的MAC地址
网络层首部	源IP地址	203.107.6.88	阿里云公共NTP服务器IP地址
	目的IP地址	172.16.64.12	NTP-1的IP地址
运输层首部	运输层协议	UDP	User Datagram Protocol-
	源端口	123	NTP服务器端
	目的端口	33009	NTP客户端

➢ 分析报文NTP内容

```
Network Time Protocol (NTP Version 4, server)
  Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server
  Peer Clock Stratum: secondary reference (2)
  Peer Polling Interval: 6 (64 sec)
  Peer Clock Precision: 0.000000 sec
  Root Delay: 0.011871337890625 seconds
  Root Dispersion: 0.000579833984375 seconds
  Reference ID: 10.137.38.86
  Reference Timestamp: Mar 14, 2021 09:27:47.952487823 UTC
  Origin Timestamp: Apr  5, 2007 10:22:48.440507649 UTC
  Receive Timestamp: Mar 14, 2021 09:28:41.284131190 UTC
  Transmit Timestamp: Mar 14, 2021 09:28:41.284145160 UTC
```

➢ 分析报文NTP内容

序号	名称	内容 / 值	备注
1	Leap Indicator	no warning	无闰秒提示
2	Version number	NTP Version 4	当前版本是NTPv4
3	Mode	Server	以服务器模式工作
4	Peer Clock Stratum	Secondary reference (2)	对等时钟的层数为第2级
5	Peer poll Interval	6 (64 sconds)	对等轮询间隔时间为64秒
6	Peer Clock Precision	0.000000 seconds	对等时钟精度
7	Root Delay	0.01187133789… seconds	到主参考时钟的总往返延迟时间
8	Root Dispersion	0.00057983398… seconds	本地时钟相对于主参考时钟的最大误差
9	Reference ID	10.137.38.86	参考时钟的ID
10	Reference Timestamp	Mar 14, 2021 09:27:47.952487823 UTC	本地时钟最近一次同步的时间
11	Origin Timestamp	Apr 5, 2007 10:22:48.440507649 UTC	NTP报文离开源端（即NTP-1）的时间
12	Receive Timestamp	Mar 14, 2021 09:28:41.284131190 UTC	本端（即公共NTP）收到NTP报文时间
13	Transmit Timestamp	Mar 14, 2021 09:28:41.284145160 UTC	本端（即公共NTP）应答报文发出时间

Thanks.