运营商级 SD-WAN 组网 NTP 时钟同步方案

赵乾艮，王羽，汤凌，颜永明
（中国电信股份有限公司上海分公司，上海 200085）

摘　要：SD-WAN 发展势头迅猛，电信运营商与互联网企业都在不断扩大布局。作为形态多样化的技术，SD-WAN 中并未对时钟同步做出明确规范。分析了时钟同步对 SD-WAN 技术实现和业务运行的重要性。简述了在 SD-WAN 被广泛采用的互联网公共 NTP 服务时钟同步方案的利弊，由此展开讨论在不同场景可实现的自建 NTP 服务时钟同步方案，并设计了基于自建 NTP 服务利用管理隧道加密传输 NTP 同步数据的时钟同步方法，使 SD-WAN 平台和设备在时间同步时获得更高的安全性与稳定性。

关键词：SD-WAN；时钟同步；IPSec 隧道；DTLS 隧道
中图分类号：TP393.2
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2022092

Carrier-grade NTP clock synchronization scheme of SD-WAN network

ZHAO Qiangen, WANG Yu, TANG Ling, YAN Yongming
Shanghai Branch of China Telecom Co., Ltd., Shanghai 200085, China

Abstract: SD-WAN is developing rapidly, and telecom operators and Internet companies are constantly expanding their layout. As a technology with diverse forms, SD-WAN has not made a clear specification for clock synchronization. The importance of clock synchronization to SD-WAN technology implementation and business running was analyzed. The advantages and disadvantages of the clock synchronization scheme of Internet public NTP service widely used in SD-WAN realizations were sketched. Thus the clock synchronization scheme of self-built NTP service in different scenarios was discussed. Furthermore, a clock synchronization method using management tunnel to transmit encrypted NTP synchronization data was designed, which made SD-WAN platform and devices obtain higher security and stability in time synchronization.

Key words: SD-WAN, time synchronization, IPSec tunnel, DTLS tunnel

0　引言

软件定义广域网（software defined wide area network，SD-WAN）作为软件定义网络（software defined network，SDN）技术在广域网中的应用，越来越受到广大企业用户的青睐，它在兼具企业用户对网络可靠性与安全性刚需的同时，又为企业用户提供了成本低、网络灵活变更的新选择。

收稿日期：2021−07−13；修回日期：2022−04−06

SD-WAN 是包括完整运营生命周期的网络产品。在业务功能实现、平台运营维护、用户体验感知等场景都需要整个网络维系同步的时间。时间的不匹配可能带来业务的紊乱和用户感知的下降。对互联网厂商，由于自身没有基础资源（包括时钟源资源），他们设计的方案都需要依赖互联网。电信运营商如果有效利用自身基础资源，就可以为用户提供更安全、更稳定的时间同步方案。

1 时钟同步对 SD-WAN 的重要性

1.1 技术实现的必要性

SD-WAN 的转发平面以加密隧道作为网络组成的主体。对 SD-WAN 行业中主流厂商进行了研究，其普遍采用了 IPSec（internet protocol security）或以 IPSec 为基础组成的隧道。IPSec 通过 IKE（internet key exchange）确定加密算法及密钥维护 IP 数据包收发两端之间的共享状态，为 IP 数据包提供机密性、数据完整性、访问控制和数据源身份验证。IPSec 支持使用电子证书、公钥和预共享密钥 3 种身份认证方式。在采用电子证书的情况下，证书在生成时都带有效期。如果 IPSec 任意一端的时间偏移超出了证书的有效期（过早或过晚），则证书将会失效，隧道无法建立。

1.2 业务运行的必要性

SD-WAN 控制平台具有用户友好的界面，并且可根据需求开发各种可交互性模块，包括实时展示、资源管理、命令下发等功能。但这些功能都基于最基本的数据采集，业务运行的必要性体现在以下两个方面。

第一，用户侧设备时间与平台侧时间不匹配会体现在用户展示界面上。如果两者时间有漂移，那么流量显示就会出现漂移，如果两者的步进有快慢区别，那么统计周期的长度也会出现错误使流量大小失真，从而使用户在流量分析时接收错误信息，对以此错误作为基础进行的组网扩展规划产生误判，影响用户的业务使用。

第二，运营商作为负责运营维护的一方，需要日常巡检，遇到故障需要及时判断故障找到问题。如果用户侧设备时间与平台侧时间不匹配，会对维护人员的问题定位和事件分析形成干扰。

2 SD-WAN 时钟同步现有方案

SD-WAN 行业中主流厂商全都使用了互联网公共 NTP（network time protocol）服务，且为扁平化排布，即平台控制器和网管网元、POP（point of presence）点网元、用户侧 CPE（customer premises equipment）网关设备单独向互联网公共 NTP 服务器同步，SD-WAN 互联网公共 NTP 服务时钟同步方案如图 1 所示。

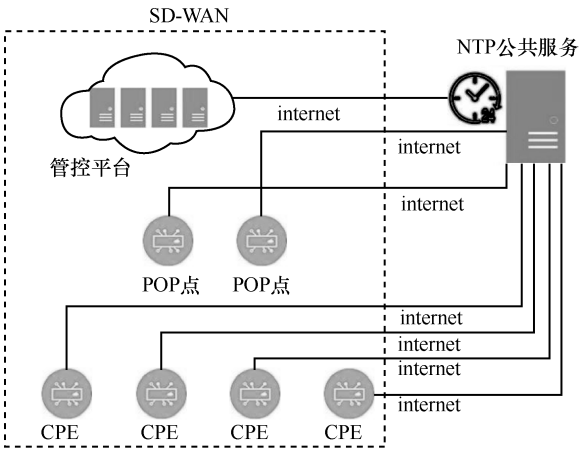

图 1 SD-WAN 互联网公共 NTP 服务时钟同步方案

2.1 厂商普遍采纳的原因

NTP 通过私有网络或公共互联网将计时信息从主服务器传送到辅助时间服务器和客户机。NTP 同步一般的设计思路是封闭系统中采用系统自建主服务器，而在连接互联网的系统中，客户机直接向公共 NTP 服务器发起同步请求。作为 SDN 在广域网的应用，SD-WAN 网络 underlay 层面更多依托于互联网，厂商方案依赖互联网公共 NTP 服务，平台自身不用提供时钟服务，在功能实现上更便捷。更重要的是，方案厂商都是互联网企业，不具备基础时钟源资源，无法依靠自身

提供标准源时间，只能将互联网上可以获取的资源整合利用，这一点是互联网厂商的天然短板。并且厂商对外服务通常只需保障业务的实现，维护职责归属用户，厂商的设计容易忽略对安全防护要求的考量。

2.2　现有方案缺点

SD-WAN 互联网公共 NTP 服务时钟同步方案虽然体现便捷的特点，但该方案存在 3 个方面隐患。

第一，面向公网同步意味着将 NTP 端口暴露在公网上。NTP 软件本身存在漏洞被利用的风险，为防止该风险需要投入对软件的更新补丁的持续关注。

第二，NTP 公共服务需要为互联网全网用户提供服务，关闭了 authentication 功能以保证服务兼容性，用户侧减少了一种身份校验的安全保障方法。

第三，依赖于第三方公共服务，对于一个独立系统而言相当于引入了新的不确定因素，虽然可以配置不同的 NTP 公共服务器作为主备提高容灾性，但由第三方维护的可靠性无法掌握，不确定可靠性的容灾也无法保证。

3　平台自建 NTP 服务时钟同步方案设计

为了应对使用公共 NTP 服务带来的可靠性不确定问题，本文在 SD-WAN 平台中搭建平台自用的 NTP 主服务器。NTP 同步可多级分层，分层结构跟随 SD-WAN。方案分为扁平化同步方案与分级同步方案，分场景适应 SD-WAN 组网中的点对点组网和 POP 点组网两种方式。

3.1　扁平化方案

在扁平化方案中，平台控制器和网管网元、POP 点网元、用户侧 CPE 网关设备都向自建 NTP 服务器发起同步请求，适用于所有用户组网场景，SD-WAN 平台自建 NTP 服务扁平化时钟同步方案如图 2 所示。

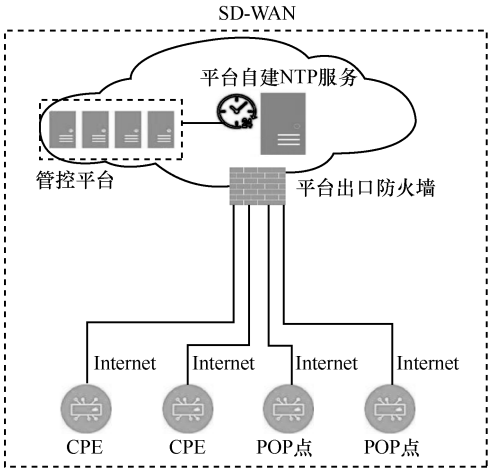

图 2　SD-WAN 平台自建 NTP 服务扁平化时钟同步方案

扁平化同步方案由平台承担全部 NTP 同步请求，对平台 NTP 服务的压力较大。若平台宕机或失联，分点将失去时钟同步源。平台对外提供 NTP 服务，运营商需要在平台侧对所有 CPE 和 POP 做地址白名单，复杂度与 CPE 设备数量成正比。扁平化同步方案最大的优点在于应用面广，所有组网方式如全互联、部分互联的直连方式，以及 hub-spoke 组网方式与 POP 点组网方式，都可以采用该方案。

3.2　分级方案一——hub-spoke 分级

在 hub-spoke 方案中，用户分点 CPE 向总头 CPE 同步，总头再向平台同步，总头同时扮演服务器（server）和客户端（client）的角色，如图 3 所示。

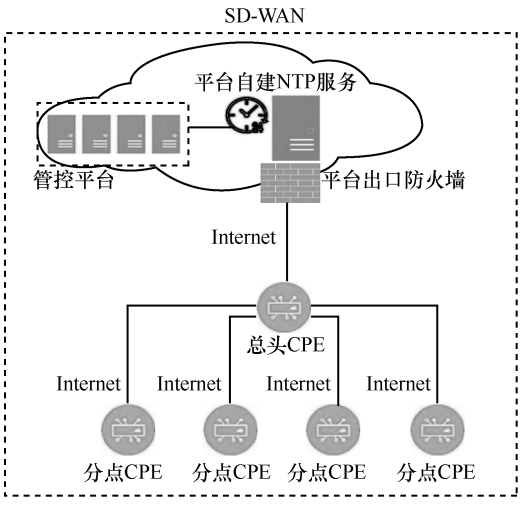

图 3　SD-WAN 平台自建 NTP 服务 hub-spoke 分级时钟同步方案

该方案适用于分点数量较多且地理位置密集的连锁商店等商业模式场景，用户建立 hub-spoke 模式组网的情况。hub-spoke 分级同步方案将数量庞大的用户 NTP 同步请求分散到用户各自的总头设备上，对平台 NTP 服务的压力较小。分点与总头保持同步，即使平台出现故障失联，也能保证用户封闭网络内的时间高度一致性。运营商只需要在平台侧对总头 CPE 设备做地址白名单，复杂度较小。

3.3 分级方案二——POP 点分级

在 POP 点方案中，用户点 CPE 向 POP 点同步，POP 点各自向平台同步，SD-WAN 平台自建 NTP 服务 POP 点分级时钟同步方案如图 4 所示。

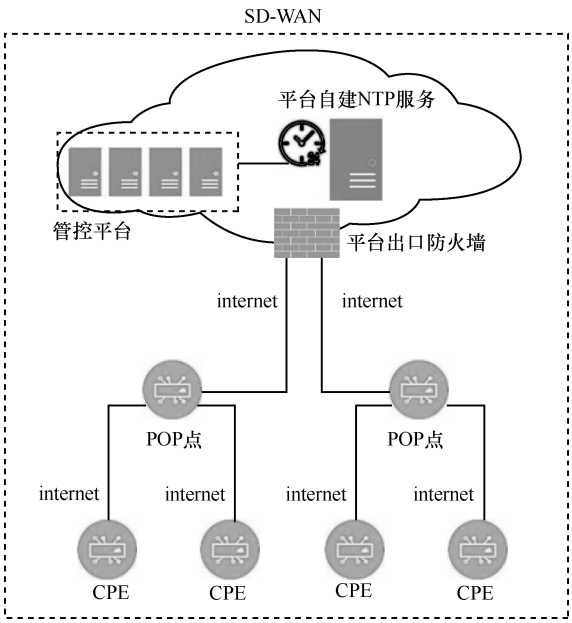

图 4 SD-WAN 平台自建 NTP 服务 POP 点分级时钟同步方案

该方案适用于用户分点分布区域分散，距离跨度较大的全国生产/办公模式场景，用户采用 POP 点组网的情况。POP 点分级同步方案将数量庞大的用户 NTP 同步请求分散到 POP 点上，对平台 NTP 服务的压力较小。运营商需要在平台侧与 POP 点处做地址白名单，复杂度与 CPE 数量成正比。并且 POP 点均部署在天翼云上，白名单有数量限制，这将成为该方案实施的瓶颈。

3 种平台自建 NTP 服务方案比较见表 1。

平台自建 NTP 服务可以规避第三方公共服务带来的不确定性，也可以通过主备方案增加容灾可靠性。同时只有系统内的设备需要同步，主服务端可以启用 authentication 功能获得同步过程的排他性。但用户侧设备向平台同步的需求决定了 NTP 主服务器监听端口暴露在互联网上，这将使主服务器在保持了公共方案的服务漏洞隐患外，还会引入暴露面安全防护要求，为应对此问题进行的地址白名单的防护工作会有很大难度。

4 基于平台自建 NTP 服务利用管理隧道加密传输 NTP 数据的时钟同步方案

为解决平台自建 NTP 服务时钟同步方案暴露面的问题，在平台自建 NTP 服务的基础上，设计利用 SD-WAN 平台与 CPE 设备间的管理隧道加密传输 NTP 数据。SD-WAN 的组成架构中用户侧 CPE 之间建立传输信道使用业务隧道，而平台管控侧向用户侧 CPE 进行配置下发、用户侧 CPE 向平台管控侧上报统计数据时使用的是管理隧道。因不需要向业务隧道一样参与流量转发，管理隧道采用的隧道技术与业务隧道不尽相同，SD-WAN 行业主流厂商采用的管理隧道有 IPSec、SSL/TLS 和 DTLS 等。可以利用已建立的平台与用户侧 CPE 的管理隧道，将 NTP 同步信息在该隧道中传输，而平台仍然维护自建的具有高可用

表 1 3 种平台自建 NTP 服务时钟同步方案比较

方案	适用场景	平台 NTP 服务压力	用户网内一致性	白名单复杂度
扁平化同步	所有场景	大	弱	大
hub-spoke 分级同步	hub-spoke 场景	小	强	小
POP 点分级同步	POP 点场景	小	弱	大

的 NTP 主服务器，基于自建 NTP 服务 SD-WAN 管理隧道加密传输 NTP 数据的时钟同步方案如图 5 所示。

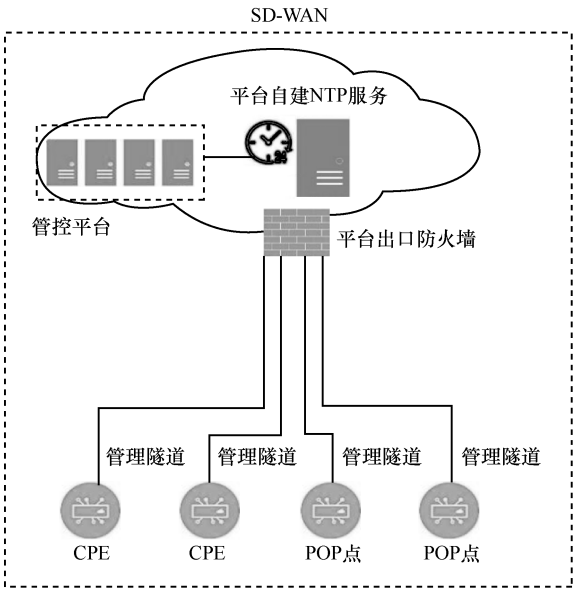

图 5　基于自建 NTP 服务 SD-WAN 管理隧道加密传输 NTP 数据的时钟同步方案

方案兼具了自建 NTP 主服务器的可靠性与容灾性，规避第三方公共服务带来的不确定性，同时启用 authentication 功能获得同步过程的排他性。设备与平台同步，即使与外部时钟失联，平台作为一个整体在内部仍然是同步的。方案采取隧道传输能避免将提供 NTP 同步服务的端口暴露在互联网，规避暴露面安全防护要求，同步过程加密封装，进一步提升了其安全性。

采用管理隧道而非业务隧道出于三方面考虑：平台与 CPE 之间不存在业务隧道，采用业务隧道只能使组网中的 CPE 获得时间统一而与平台隔离，只有管理隧道可以建立平台与 CPE 的联系；采用管理隧道不会挤占业务隧道的带宽导致业务有效带宽降低；SD-WAN 的一大特点是组网灵活，用户可以通过下发配置随时变更组网情况，这将造成终端的 NTP 角色和配置相应变化，对讲求稳定的时间同步而言管理隧道更有利。

5　管理隧道内 NTP 时钟同步实现验证

主流厂商 SD-WAN 平台使用的管理隧道有 IPSec、SSL/TLS 和 DTLS，其中 SSL 隧道是 TCP 隧道，IPSec、DTLS 隧道是 UDP 隧道。NTP 传送 UDP 报文，更适合通过 UDP 隧道进行传递。本文通过部署虚拟环境对 IPSec 与 DTLS 两种适合 NTP 报文传输的 UDP 隧道进行实现，并验证时间同步。

5.1　IPSec 方式

IPSec 作为管理隧道仅需传递平台与设备之间的交互信息，不需要与业务隧道一样，将 CPE 作为站点隐藏子网，因此采用传输模式用 ESP 加密，采用 strongswan 作为 IPSec 的实现，配置为传输模式，采用 PSK 预配置密钥方式建立加密隧道，两端地址分别为 192.168.26.30、192.168.26.31。将两台虚拟服务器的 NTP 服务开启，其中 192.168.26.30 配置为 NTP 客户端，192.168.26.31 作为 NTP 服务器。开启 NTP authentication。服务开启后，NTP 客户端成功向 NTP 服务器同步时间，NTP 同步成功如图 6 所示。

```
[root@localhost ~]# chronyc ntpdata

Remote address  : 192.168.26.31 (C0A81A1F)
Remote port     : 123
Local address   : 192.168.26.30 (C0A81A1E)
Leap status     : Normal
Version         : 4
Mode            : Server
Stratum         : 2
Poll interval   : 6 (64 seconds)
Precision       : -25 (0.000000030 seconds)
Root delay      : 0.038986 seconds
Root dispersion : 0.002930 seconds
Reference ID    : 727607A1 ()
Reference time  : Wed Apr 21 03:12:57 2021
Offset          : -0.001060157 seconds
Peer delay      : 0.000941984 seconds
Peer dispersion : 0.000002442 seconds
Response time   : 0.000248942 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : No
Authenticated   : Yes
TX timestamping : Daemon
RX timestamping : Kernel
Total TX        : 4
Total RX        : 4
Total valid RX  : 4
```

图 6　NTP 同步成功

链路抓包，使用解密文件将加密部分解密，可以看到 ESP 载荷部分由 ESP 头、ESP 校验位和一个被加密的 UDP 包组成，且目标端口为 123，表明上层协议为 NTP。

5.2 DTLS 方式

DTLS 被设计为尽可能类似 TLS，既可以最小化新的安全性发明，又可以最大限度地提高代码量和基础设施重用。采用 openconnect 作为 DTLS 的实现，两端地址分别为 192.168.26.32、192.168.26.33，openconnect 建立 TLS 隧道以进行身份认证和维持连接状态并作为备用隧道，认证完成后建立 DTLS 隧道用于数据传输。将两台虚拟服务器的 NTP 服务开启，其中，192.168.26.33 的配置为 NTP 客户端，192.168.26.32 作为 NTP 服务器，openconnect 的客户端登录后会被分配到 192.168.100.0/24 内地址（本例中为 192.168.100.149），流量都经过隧道。同时开启 NTP authentication。由于 openconnect 服务器的 192.168.26.32 被用作隧道出口，将 LAN 侧 192.168.100.1 作为 NTP 服务器地址，NTP 服务开启后，NTP 客户端成功向 NTP 服务器同步时间，NTP 同步成功如图 7 所示。

```
[root@localhost ~]# chronyc ntpdata

Remote address  : 192.168.100.1 (C0A8C801)
Remote port     : 123
Local address   : 192.168.100.149 (C0A86495)
Leap status     : Normal
Version         : 4
Mode            : Server
Stratum         : 10
Poll interval   : 6 (64 seconds)
Precision       : -25 (0.000000030 seconds)
Root delay      : 0.000000 seconds
Root dispersion : 0.000000 seconds
Reference ID    : 7F7F0101 ()
Reference time  : Tue May 04 16:35:42 2021
Offset          : +0.073474906 seconds
Peer delay      : 0.147764236 seconds
Peer dispersion : 0.000295678 seconds
Response time   : 0.000044922 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : No
Authenticated   : Yes
TX timestamping : Daemon
RX timestamping : Kernel
Total TX        : 4
Total RX        : 4
Total valid RX  : 4
[root@localhost ~]#
```

图 7 NTP 同步成功

链路抓包后，可以看到筛选的 DTLSv1.2 报文，源目地址分别为两侧服务器地址，服务器侧端口为预设的 11443 端口，用户侧信息被加密外界无法查看。

实验验证了可以通过 IPSec 与 DTLS 隧道传送 NTP 同步数据使 NTP 客户端向服务端同步成功。

5.3 与互联网公共 NTP 服务时钟同步方案对比

SD-WAN 管理隧道内 NTP 时钟同步方案相比较于互联网公共 NTP 服务时钟同步方案由于建立了隧道，在原始报文外层嵌套了新的报头，提升了开销。互联网公共 NTP 服务时钟同步报文为 90 byte。IPSec 管理隧道方案报文需要 150 byte，而 DTLS 管理隧道方案报文则需要 180 byte。

提升开销换来的是规避第三方公共服务的不确定性，获得 authentication 功能，解决了电信作为运营商面临暴露面安全防护要求，加密封装进一步提升了安全性。

试验验证的 IPSec 与 DTLS 两种隧道覆盖了厂商使用的 UDP 隧道，而 DTLS 与作为 TCP 隧道的 TLS 同源，在开发上有许多可重复利用的部分，并且不少开源库（如 openssl、gnutls 等）已提供对 DTLS 的支持，对采用 SSL 作为管理隧道的厂商来说，向 DTLS 过渡十分便捷。运用基于改进无证书公钥密码的轻量级 DTLS 协议，还能避免证书管理的复杂性并降低额外的网络开销。

6 结束语

本文通过分析 NTP 时钟同步在不同 SD-WAN 的应用场景，说明了时钟同步对 SD-WAN 技术实现和业务运行的重要性。受制于厂商作为互联网企业的角色定位，在各 SD-WAN 实践中广泛采用的第三方公共服务时钟同步方式，在安全性上存在提升空间。依托于电信基础资源搭建 SD-WAN 管理平台的优势，在不同场景下可实现多种组网方式的自建 NTP 服务时钟同步方案，进一步衍生一种基于自建 NTP 服务利用 IPSec 与 DTLS 两种管理隧道

加密传输 NTP 同步数据的时钟同步方法并进行了实现验证，可以使 SD-WAN 平台和设备在同步时获得更高的安全性与稳定性。未来电信将视管理隧道内 NTP 时钟同步的方案为推荐的 NTP 同步方案，力争为用户提供运营商独有高安全高可用的 SD-WAN 业务。

参考文献：

[1] RFC. Internet key exchange protocol version 2 (IKEv2)[R]. 2010.

[2] RFC. IP encapsulating security payload (ESP)[R].1998.

[3] 牛路宏, 陈晓苏. IKE 协议认证机制及其实现分析[J]. 通信技术, 2002, 35(10): 82-83, 89.
NIU L H, CHEN X S. Analysis of identify mechanism and its implementation of IKE[J]. Communications Technology, 2002, 35(10): 82-83, 89.

[4] RFC. Network time protocol version 4: protocol and algorithms specification[R]. 2010.

[5] 宋妍, 朱爽. 基于 NTP 的网络时间服务系统的研究[J]. 计算机工程与应用, 2003, 39(36): 147-149,152.
SONG Y, ZHU S. A network time service system based on NTP[J]. Computer Engineering and Applications, 2003, 39(36): 147-149, 152.

[6] 牛佳, 颜永明, 林志华. SD-WAN 隧道技术与组网模式[J]. 电信科学, 2021, 37(1): 137-146.
NIU J, YAN Y M, LIN Z H. SD-WAN tunnel technology and network construction[J]. Telecommunications Science, 2021, 37(1): 137-146.

[7] 柴瑶琳, 穆琋博, 马军锋. SD-WAN 关键技术[J]. 中兴通讯技术, 2019, 25(2): 15-19.
CHAI Y L, MU Y B, MA J F. Key technology in SD-WAN[J]. ZTE Technology Journal, 2019, 25(2): 15-19.

[8] RFC. Datagram transport layer security version 1.2[R]. 2012.

[9] 许国栋, 刘光杰, 乔森, 等. 基于改进无证书公钥密码的轻量级 DTLS 协议设计[J]. 南京信息工程大学学报(自然科学版), 2021, 13(5): 628-634.
XU G D, LIU G J, QIAO S, et al. Lightweight DTLS protocol design based on improved certificateless public key cryptography[J]. Journal of Nanjing University of Information Science & Technology (Natural Science Edition), 2021, 13(5): 628-634.

[作者简介]

赵乾艮（1991− ），男，中国电信股份有限公司上海分公司工程师，主要研究方向为网络安全、SDN 等。

王羽（1980− ），男，中国电信股份有限公司上海分公司助理工程师，主要研究方向为数据网络、SDN 等。

汤凌（1986− ），男，中国电信股份有限公司上海分公司助理工程师，主要研究方向为数据网络、SDN 等。

颜永明（1978− ），男，中国电信股份有限公司上海分公司信息网络部综合运营监控中心经理、正高级工程师，主要研究方向为数据网络、云组网等。