

NewLync 2.0

安全白皮书

文档版本：01

发布日期：2025-05-15



版权所有©上海迅时通信设备有限公司 2025。保留一切权利

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

网址: <http://www.newrocktech.com>

文档中心: <https://www.newrocktech.com.cn/DocumentCenter>

电话: 021-61202700

传真: 021-61202704

目 录

目 录	I
关于本文档.....	1
1 安全功能概述	2
1.1 TLS 加密	2
1.1.1 TLS 1.2 和 TLS 1.3 的差异	2
1.1.2 TLS 1.2 与 TLS 1.3 的兼容与互补性	6
1.1.3 TLS 加密流程	7
1.1.4 TLS 握手流程	8
1.1.5 NewLync 2.0 中的应用	10
1.2 SIP 消息完整性检测 (SIP Message Integrity Check)	12
1.2.1 功能概述	13
1.2.2 计算方法示例.....	13
1.2.3 NewLync 2.0 中的应用	14
1.3 IMS-AKA 鉴权认证 (IMS-AKA Authentication)	14
1.3.1 鉴权认证原理.....	14
1.3.2 NewLync 2.0 中的应用	15
1.4 端到端加密	16
1.4.1 加密原理	16
1.4.2 NewLync 2.0 中的应用	16
1.5 媒体流加密 (SRTP)	17
1.5.1 加密原理	17
1.5.2 NewLync 2.0 中的应用	18
1.6 量子加密通信.....	19

1.6.1 加密原理	20
1.6.2 量子密钥分发 (QKD)：与传统加密的对比	21
1.6.3 NewLync 2.0 中的应用	21
1.7 国密加密	22
1.7.1 加密协议简介	22
1.7.2 SM2、SM3、SM4 协议：如何增强本地加密安全	23
1.7.3 TLS v1.3 与国密加密结合：确保国内加密通信的合规性和安全性	24
1.7.4 NewLync 2.0 中的应用	24
1.8 系统备份与恢复功能 (System Backup and Recovery)	26
1.8.1 数据库恢复	26
1.8.2 录音文件恢复	27
1.8.3 配置文件恢复	27
1.9 访问控制与系统安全	28
1.9.1 用户权限管理	28
1.9.2 身份验证	28
1.9.3 访问权限	29
1.9.4 限制注册新账号	29
1.9.5 限制境外 IP 登录	29
1.9.6 系统状态监控	29
1.9.7 故障告警	29
1.9.8 软件更新	30
1.9.9 安全日志	30
1.9.10 防暴力破解与密码保护策略	30
1.9.11 限制非法登录 IP	31
2 安全功能清单	32

关于本文档

本文档是 NewLync 2.0 平台的安全白皮书，旨在详细介绍 NewLync 2.0 融合通信平台的安全架构与防护措施。文档涵盖了平台在数据传输、用户认证、权限管理、加密技术等方面的安全功能，旨在帮助用户和管理员了解如何通过多层次的安全机制保护系统的机密性、完整性和可用性。

本文档是 NewLync 2.0 系列文档的一部分，NewLync 2.0 系列文档包含：

名称	内容
NewLync 2.0 配置与操作手册	帮助高效管理和维护 NewLync 2.0，确保系统安全、稳定运行。内容涵盖系统概述、安装部署、基础配置、运维管理和故障排查等方面
NewLync 2.0 运维平台使用指南	内容涵盖系统设置、用户管理、录音存储、数据备份、安全设置等各个方面，帮助管理员根据实际需求进行灵活的运维操作
NewLync Teams 协作办公 平台_PC 端&移动端_操作、 管理和维护指南	内容涵盖 NewLync 协作办公平台在 PC 端和移动端的操作、管理和维护方法
NewLync 2.0 高可用白皮书	内容涵盖 NewLync 2.0 系统的高可用架构设计、部署方案及核心功能

1 安全功能概述

1.1 TLS 加密

在 NewLync 2.0 中，TLS 协议是保护平台内所有通信的核心技术，广泛应用于语音、视频、即时消息等数据的传输加密。TLS 的主要功能是保证数据的机密性、完整性，TLS 不仅对信令数据进行加密，还通过的身份认证机制保护通信双方的合法性。

- 语音通信：保护呼叫信令过程（如呼叫发起、修改和终止）的加密，防止在语音会话中的数据遭到恶意篡改或窃听，每次语音通话的管理信令都受到 TLS 协议的保护。
- 视频通信：保护视频会议的控制信令数据，控制信令包括视频通话的启动、暂停、结束等操作，确保视频流中的指令不被篡改或中途截取。
- 即时消息传输：对即时消息数据进行加密，确保信息在传输过程中不被第三方读取或篡改。

1.1.1 TLS 1.2 和 TLS 1.3 的差异

TLS 1.2

TLS 1.2（传输层安全协议版本 1.2）是 TLS 协议的第一个主流版本，于 2008 年发布。

TLS 1.2 是对 TLS 1.1 的增强，广泛应用于现代互联网通信中，提供了端到端的加密保护、身份验证、数据完整性校验等安全机制。

关键特性

- 加密支持：TLS 1.2 支持多种加密算法，允许客户端和服务端选择最合适的加密套件来保护数据传输。采用对称及非对称加密来加密数据，确保通信内容不被第三方窃取。
- 身份验证：采用认证证书来验证通信双方的身份，确保客户端和服务端是合法的。
- 消息完整性：使用设备的 MAC 地址来验证数据的完整性。每个数据块附加一个 MAC 值，接收方用来检查数据是否被篡改。若传输中的数据发生篡改，MAC 校验会失败，接收方会拒绝接收该数据。
- 密钥交换与算法：TLS 1.2 支持多种密钥交换协议，包括 RSA、Diffie-Hellman 和 ECDHE。
- 算法灵活：TLS 1.2 提供了较大的灵活性，客户端和服务端可以协商使用的加密算法和哈希算法，从而满足不同的安全要求。
- 支持 ECC，提供更高效的加密方案，适合低功耗设备及高并发环境。

TLS 1.2 的局限性

- 握手过程复杂：TLS 1.2 的握手过程比较复杂，需要多次往返（RTT）来协商加密算法、密钥交换等，导致连接建立的时间较长，特别是在高延迟环境中。
- 支持弱加密算法：虽然 TLS 1.2 较为安全，但仍支持一些过时和不安全的算法（如 RC4 和 SHA-1），这些算法在现代网络环境中存在已知漏洞。

TLS 1.3

TLS 1.3 是 TLS 协议的最新版本，于 2018 年发布。相较于 TLS 1.2，TLS 1.3 经过了简化和优化，显著提高了安全性和性能，解决了 TLS 1.2 中存在的一些问题，成为现代网络通信的首选加密协议。

关键特性

一、 简化握手过程

- TLS 1.3 大大简化了握手过程，减少了握手所需的往返次数（RTT），使得连接建立速度更快。相比 TLS 1.2 的两轮握手，TLS 1.3 仅需要一次往返。
- 引入 0-RTT 数据传输：允许客户端在握手过程中立即发送数据，从而减少连接建立的延迟。

二、 加强的加密算法

- TLS 1.3 移除了许多不再安全的算法，仅支持 AES-GCM、ChaCha20 等现代、强加密算法。
- 所有加密算法都采用 AEAD（Authenticated Encryption with Associated Data）模式，确保加密和完整性校验合并为一个步骤，从而减少潜在的攻击面。

三、 前向保密性（PFS）

- 在 TLS 1.3 中，前向保密性（PFS）是强制性的，即使密钥被泄露，过去的通信数据也无法被解密。

四、 安全性增强

- 移除了 TLS 1.2 中的一些易受攻击的功能，例如客户端身份验证（在 TLS 1.3 中已不再支持）和不安全的加密算法。

- TLS 1.3 通过更简单的协议结构、加密算法选择以及更强的身份验证机制，显著提高了抵御各种攻击的能力。

五、 新的密钥交换机制

- TLS 1.3 强制使用 ECDHE（椭圆曲线 Diffie-Hellman Ephemeral）密钥交换协议，确保每次会话使用不同的密钥，避免了 TLS 1.2 中长时间使用相同密钥带来的安全问题。
- TLS 1.3 的密钥交换过程进一步优化，减少了暴露密钥的风险，使得攻击者更难在传输过程中窃取密钥。

六、 会话恢复

- TLS 1.3 引入了会话恢复机制，支持会话票据（Session Tickets），让客户端能够缓存会话信息，避免每次连接时都要进行完整的握手，减少了会话建立所需的时间，特别是在高延迟的网络环境中，可以显著提高性能。

TLS 1.3 的局限性

向后兼容性问题：虽然 TLS 1.3 在安全性和性能上都有大幅改进，但由于它去除了许多 TLS 1.2 支持的功能（如不安全的加密算法），它与老旧的 TLS 客户端和服务端不完全兼容。因此，升级到 TLS 1.3 可能需要一些配置上的调整或重新部署。

TLS 1.2 与 TLS 1.3 的对比分析

特性	TLS 1.2	TLS 1.3
握手过程	复杂，需要多次往返（2-3 RTT）	简化，减少为 1 RTT，支持 0-RTT 数据传输
加密算法	支持多种算法，包括过时算法（如 RC4、SHA-1）	只支持现代加密算法（AES-GCM、ChaCha20）
前向保密性	可选（依赖于协议配置）	强制前向保密性

密钥交换协议	支持 RSA、Diffie-Hellman (DH)、ECDHE 等	强制使用 ECDHE 密钥交换协议
加密模式	AEAD (非强制性)	默认使用 AEAD 模式 (确保加密和完整性校验)
降级攻击防护	较弱, 可能存在降级攻击风险	防止降级攻击, 禁止使用弱协议和算法
协议兼容性	与旧版 TLS 兼容	与 TLS 1.2 及以下版本不完全兼容
性能	较慢, 因握手复杂度和加密算法选择而受影响	更快, 优化了握手过程, 减少延迟

1.1.2 TLS 1.2 与 TLS 1.3 的兼容与互补性

NewLync 2.0 支持 TLS 1.2 和 TLS 1.3 两个版本, 实现了这两个协议版本的兼容性和互补性。为平台提供了更强的灵活性和安全保障。

一、 向后兼容性 (Backward Compatibility)

TLS 1.2 是一个成熟且广泛使用的协议, 许多现有的客户端和服务端仍然依赖于 TLS 1.2。因此, 在尚未支持 TLS 1.3 的环境中, TLS 1.2 可以确保 NewLync 2.0 与这些设备和应用程序兼容。

TLS 1.3 的引入, 虽然增加了安全性和性能, 但与 TLS 1.2 相比有一些不兼容的变化 (如去除某些算法和功能), 可能会导致与老旧设备或系统的兼容问题。因此, NewLync 2.0 保留对 TLS 1.2 的支持, 确保在过渡到 TLS 1.3 时, 能够无缝地与旧版客户端进行通信。

二、 安全性与性能的互补

TLS 1.3 引入了多项优化, 例如简化的握手过程、强制前向保密性、加密算法的强化等, 提升了 NewLync 2.0 在安全性和性能上的表现。TLS 1.3 的 0-RTT 数据传输可以大幅度减少连接建立时的延迟, 使得实时通信 (如语音、视频通话) 更加流畅和高效。

TLS 1.2 虽然在性能上略显不足，但其加密算法和协议灵活性依旧使其成为很多现有系统的首选。对于一些不要求极低延迟的场景，TLS 1.2 仍然可以提供强大的加密保护。

三、 高兼容性

NewLync 2.0 可以根据客户端和服务器的能力选择合适的 TLS 版本。若客户端和服务端都支持 TLS 1.3，那么会使用 TLS 1.3 提供的增强安全性和性能；如果某些客户端或设备不支持 TLS 1.3，那么系统会自动回退到 TLS 1.2 以保证兼容性。

1.1.3 TLS 加密流程

TLS 协议基于公钥基础设施（PKI）和对称加密技术，在两端之间建立起一个加密的安全通道。TLS 的工作流程包括了以下几个方面：

一、 数据加密：

- 对称加密：TLS 协议使用对称加密算法（如 AES）来加密会话数据。对称加密的优势在于加密和解密操作速度较快，但需要在客户端和服务端之间共享密钥。每个 TLS 会话都会生成一个 会话密钥，用于加密数据传输内容。
- 非对称加密：在 TLS 握手阶段，非对称加密（如 RSA）用于密钥交换和身份验证。非对称加密确保在通信双方没有事先共享密钥的情况下，能够安全地交换密钥。

二、 数据完整性校验：

- TLS 协议通过设备的 MAC 地址对数据进行完整性校验。每一段传输的数据都会附带一个 MAC 值。接收方通过验证 MAC 值，确保数据未被篡改或损坏。如果数据在传输过程中发生篡改，接收方将立即发现并拒绝传输数据。

三、 身份验证：

- 数字证书：在 TLS 握手阶段，客户端和服务端通过交换数字证书来验证彼此的身

份。证书由受信任的证书颁发机构（CA）签发，确保通信双方的身份是合法的。

TLS 通过公钥和私钥的配对验证通信的合法性，防止攻击或身份伪造。

- 公钥基础设施（PKI）：TLS 依赖 PKI 系统来管理数字证书和密钥，通过公钥和私钥对的配合，验证通信双方的身份。

1.1.4 TLS 握手流程

TLS 握手是建立加密连接的初步过程，它确保双方能够安全地交换密钥和验证身份。握手阶段主要包括以下几个步骤：

一、 客户端 Hello

- 客户端发起连接请求：在 TLS 握手的开始阶段，客户端向服务器发送一个“Hello”消息。
- 协商加密算法：客户端在“Hello”消息中包含它支持的加密套件、哈希算法、以及支持的 TLS 版本（如 TLS 1.2 或 TLS 1.3），帮助服务器选择合适的加密算法。
- 生成客户端随机数：客户端生成一个随机数并将其发送给服务器，这个随机数在后续的加密和密钥生成过程中用于增强加密强度。

在此阶段，客户端提出其支持的加密算法、TLS 版本等参数，服务器会选择一种协议进行后续通信。

二、 服务器 Hello

- 服务器回应：服务器收到客户端的“Hello”消息后，会根据客户端的建议选择一个合适的加密算法和 TLS 版本，生成一个“Hello”消息并返回。
- 服务器证书：服务器将自己的数字证书发送给客户端，以证明自己的身份，客户端会使用证书中的公钥验证服务器身份。

- 生成服务器随机数：服务器会生成一个随机数，该随机数也会在后续的密钥交换中起到关键作用。
- 加密算法选择：服务器通过选定的加密算法和加密套件来保证数据传输的安全。

三、 密钥交换 (Key Exchange)

- 密钥交换协议：客户端和服务端使用密钥交换协议来生成会话密钥。密钥交换协议确保即使通信内容被窃听，也无法泄露密钥。
- 生成会话密钥：客户端和服务端通过交换随机数、密钥交换参数及证书等信息，最终协商并生成一个共享的会话密钥。这个会话密钥用于后续的对称加密数据传输。
- 证书验证：客户端验证服务器证书的合法性，以防止攻击。如果证书无效或与服务器身份不符，客户端将终止连接。

四、 客户端密钥交换 (Client Key Exchange)

- 客户端发送密钥交换信息：客户端会发送用于后续加密的密钥信息。该信息是加密的，只有服务器可以解密。
- 生成主密钥：客户端和服务端通过密钥交换协议生成一个主密钥。这个密钥用于生成最终的会话密钥。

五、 服务器完成 (Server Finished)

- 加密连接确认：服务器通过加密后的消息告诉客户端，它已经完成密钥交换并且已准备好开始安全通信。此时服务器会向客户端发送一条“Finished”消息，表示握手过程的结束。

六、 客户端完成 (Client Finished)

- 客户端确认：客户端收到服务器的“Finished”消息后，也会发送一条加密的“Finished”消息，确认它已经完成了密钥交换。客户端和服务器的加密密钥（会话密钥）现在已经建立，并且所有后续的通信都将使用该密钥进行对称加密。

七、 建立加密连接

- 一旦握手过程完成，客户端和服务端便能够通过会话密钥进行加密通信。所有后续数据的传输都使用这个共享的会话密钥进行对称加密。

1.1.5 NewLync 2.0 中的应用

在 NewLync 2.0 中，TLS 协议被集成到整个系统架构中，以保证平台的通信数据得到有效保护，具体应用包括：

一、 SIP 信令加密

- NewLync 2.0 使用 TLS 协议 对所有 SIP 信令进行加密，确保语音、视频和即时消息的信令数据传输的机密性和完整性。保护信令数据，使其在传输过程中不被窃取或篡改。
- 在握手阶段，系统通过 TLS 证书验证通信双方的身份，防止伪造服务器或客户端身份，保障通信的真实性。

二、 TLS 1.3 协议的应用

- NewLync 2.0 支持 TLS 1.3 协议，大幅减少了握手延迟和加密过程的复杂度，优化了大规模并发连接的性能。通过 TLS 1.3 的引入，平台能够在保持强大安全性保障的同时，显著提高了连接速度。
- TLS 1.3 协议的简化和优化降低了与传统 TLS 1.2 协议相比的延迟，并通过更强的

加密算法提升了数据保护能力。

三、 会话密钥管理

- 每次 TLS 连接时，NewLync 2.0 会生成新的 会话密钥，该密钥用于对称加密传输中的所有数据。每次会话结束后，系统会丢弃该密钥，并为下一次会话生成新的密钥，避免长期使用相同密钥而带来的风险。

四、 证书管理与身份验证

- NewLync 2.0 使用 TLS 协议 对每次连接进行身份验证。通过认证证书，客户端和服务端确认彼此的合法身份，防止攻击和伪造身份。

五、 数据完整性校验

- TLS 通过设备的 MAC 地址对传输数据进行完整性校验。每次传输的数据段都附带有一个设备的 MAC 值，接收方通过该值校验数据是否在传输过程中遭到篡改。若数据发生变动，TLS 会阻止该数据继续传输，确保传输内容的完整性。

保护机制

一、 语音通信的加密保护

- 呼叫信令的加密：当用户发起、接收、修改或终止语音通话时，相关的 SIP 信令数据会通过 TLS 协议 进行加密。通过加密这些信令数据，NewLync 2.0 可以有效防止中途的篡改或窃听。
- 身份验证：TLS 协议通过证书验证通信双方的身份，确保只有合法用户能够发起或接收语音通话。避免了攻击和伪造身份的风险。
- 密钥交换与保护：TLS 协议在握手阶段通过安全的密钥交换机制，确保双方在没有事先共享密钥的情况下，能够安全地交换用于加密的密钥。

二、 视频通信的加密保护

- 视频信令加密：视频通话中的控制信令（如视频通话的发起、暂停、结束等）会通过 TLS 协议 进行加密，防止信令数据在传输过程中被第三方截获或篡改。
- 前向保密性（PFS）：通过 TLS 1.3 协议的前向保密性，确保每次视频通话都使用独立的加密密钥，即使密钥被泄露，也无法解密历史的视频通信数据。
- 身份验证：视频会议中，通过 TLS 证书 的验证机制，确保参与者身份的合法性，防止未经授权的用户参与视频会议。

三、 即时消息的加密保护

- 消息数据的加密：即时消息的内容会通过 TLS 协议 进行加密，确保消息内容在传输过程中不会被窃取或篡改。每次发送的消息都会使用 TLS 加密，从而保障消息的机密性。
- 身份验证：TLS 协议不仅加密数据，还确保消息的发送者身份真实可靠。通过数字证书验证，确保消息发送方是经过身份认证的合法用户。
- 防止信息篡改：通过验证设备的 MAC 地址等技术，TLS 协议确保消息在传输过程中不被恶意篡改，保证信息完整性。

1.2 SIP 消息完整性检测 (SIP Message Integrity Check)

SIP 消息完整性检测通过在信令中增加自定义 Header 并使用加密算法生成认证码，确保信令在传输过程中不被篡改或伪造。在 NewLync 2.0 中，所有 SIP 信令（如呼叫发起、修改、终止等）都进行完整性检测，防止恶意篡改，保障通信安全。

1.2.1 功能概述

SIP (Session Initiation Protocol) 是用于管理和控制语音通信、视频会议和即时消息等多媒体通信会话的协议。通过在呼叫信令 SIP 消息中增加自定义 Header，用于 SIP 呼叫信令消息的完整性校验。要求发起呼叫方即初始发送 SIP INVITE 消息的 UE 在信令中增加自定义 Header，服务端对收到的 SIP INVITE 消息进行完整性校验，校验失败，则禁止呼叫。

常见的 SIP 信令传输场景包括：

- 呼叫发起：用户通过 SIP 发起通话时，平台将使用 SIP 信令传输通话的请求信息，包括通话目标、参数以及授权信息。任何对信令数据的篡改都可能导致呼叫建立失败或非法呼叫。
- 呼叫修改：在通话过程中，SIP 信令用于对通话进行修改（如音频质量调整、视频启用/禁用等）。篡改或伪造这些信令可能会导致通话参数不一致，进而影响通话质量。
- 呼叫终止：当通话结束时，SIP 信令用于通知双方关闭会话。如果攻击者篡改了这些信令数据，可能会导致通话未能正确断开或存在会话残留，影响用户体验。

NewLync 2.0 采用 SIP 消息完整性检测 来防止这些潜在的安全威胁，确保所有 SIP 信令在传输过程中不被恶意篡改和伪造。

1.2.2 计算方法示例

SIP 自定义 Header：

X-Sec-Identity: xxxxxxxxxxxxxxxxx

X-Sec-Identity 计算方法示例：

alg=hmac-sha-1-96 或国密 sm3;

X-Sec-Identity: sm3(R-URI:xxx|From:xxx|To: xxx|Call-ID:xxxx|Contact:xxxx|rand|key)

1.2.3 NewLync 2.0 中的应用

在 NewLync 2.0 中，SIP 消息完整性检测 被应用于平台的 所有 SIP 信令，以确保信令数据在传输过程中不被篡改及伪造。

- 保护音视频通信的合规性：在 NewLync 2.0 中，所有的 SIP 信令（如呼叫发起、修改、终止请求等）都经过 消息认证码的完整性检测。确保信令数据的完整性和真实性，防止恶意篡改。
- 防攻击：NewLync 2.0 通过 SIP 消息完整性检测防止攻击。即使攻击者拦截到 SIP 信令数据，消息的完整性校验会失败，篡改的消息将无法通过认证并被拒绝。

1.3 IMS-AKA 鉴权认证 (IMS-AKA Authentication)

在 NewLync 2.0 中，IMS-AKA 协议被应用于固话通信领域，所有连接平台的设备，包括智能手机、视频会议终端等，都需要通过 IMS-AKA 协议进行身份认证。IMS-AKA 协议支持大规模设备和用户的高效认证，确保每个设备和用户都能快速、安全地接入平台，适用于高并发的场景，防止非法设备侵入系统。

1.3.1 鉴权认证原理

IMS-AKA 协议利用密钥协商机制来进行设备和用户的身份验证，确保信令传输的机密性和完整性。具体的加密原理如下：

一、 密钥认证：

- 在 IMS-AKA 协议中，设备身份验证依赖于存储的共享密钥。该密钥由网络运营商

为每个用户和设备分配，设备本身作为安全硬件存储该密钥。设备在进行身份验证时，会使用该密钥与服务器进行安全的加密和解密过程。

二、 密钥协商机制：

- 在 IMS-AKA 协议的身份验证过程中，IMS-AKA 采用挑战/响应机制（Challenge-Response Mechanism）来完成密钥的交换和身份验证。
- 生成随机数（Challenge）：当设备或用户尝试连接时，平台生成一个随机数并发送给设备。
- 响应（Response）：设备使用存储的密钥对随机数进行加密，生成响应消息。响应中包含了加密的随机数，以及从设备密钥生成的认证信息。
- 平台验证：平台通过相同的算法对响应进行解密和验证，确保发送方的身份合法性。如果响应验证成功，设备或用户身份验证通过，平台允许其接入。

1.3.2 NewLync 2.0 中的应用

在 NewLync 2.0 中，将 IMS-AKA 鉴权认证应用到固话通信领域，每个接入系统的设备（如智能手机、视频会议终端、音频设备等）都需要通过 IMS-AKA 协议进行身份认证。

- NewLync 2.0 使用 IMS-AKA 协议对所有连接设备进行身份验证。每个设备在接入平台之前，都会与平台进行密钥协商，通过存储的密钥验证设备的身份。只有认证通过的设备才被允许接入平台，参与语音和视频通信。
- NewLync 2.0 支持大规模设备和用户的认证。在高并发场景下，IMS-AKA 协议能够高效地进行设备和用户认证，确保每个设备和用户都能够快速、安全地接入平台。

1.4 端到端加密

端到端加密（End-to-End Encryption, E2EE）是确保通信内容在传输过程中的机密性和完整性的重要技术。端到端加密的核心思想是：数据从发送端加密后，只有接收端能够解密，任何第三方，都无法访问或篡改传输的数据。端到端加密技术广泛应用于语音通话、视频会议、即时消息和文件传输等多种通信场景，保证通信的隐私和安全。

1.4.1 加密原理

端到端加密的基本原理是通过对称加密和非对称加密技术，在数据传输的两端（发送方和接收方）加密和解密消息。

- 对称加密：在对称加密中，发送方和接收方使用相同的密钥来加密和解密数据。
系统在会话建立时动态生成一个会话密钥，该密钥用于加密整个会话的数据流。
通过对称加密算法，通信双方确保数据的加密性和机密性。
- 非对称加密：非对称加密在端到端加密的密钥交换阶段使用。发送方使用接收方的公钥加密数据，接收方则使用其私钥解密数据。
- 密钥交换：为了确保端到端加密的安全性，通信双方在开始会话时通过安全的密钥交换协议协商出一个共享的会话密钥。
- 会话独立性：每次会话的密钥都是动态生成的，因此，即使某次会话的密钥被泄露，历史通信数据也无法被解密。

1.4.2 NewLync 2.0 中的应用

- 语音和视频加密: NewLync 2.0 在所有的语音、视频通信、即时消息和文件共享内容中实现端到端加密，确保通话内容只能由通话的发起方和接收方访问。
- 即时消息传输：即时消息的内容，如文本、图片、文件等，经过端到端加密，只

有发件人和收件人能够访问和读取消息，避免中途被拦截或篡改。

1.5 媒体流加密（SRTP）

媒体流加密用于保护语音、视频及其他多媒体数据流，防止在传输过程中被截取或篡改。

没有加密的媒体流可能在公共网络上传输时被窃取或篡改，影响数据的机密性和完整性。

在 NewLync 2.0 中，SRTP 协议应用于语音通信和视频通信中的媒体流加密，在实时通话或会议时，SRTP 能够有效保护用户的通话内容，防止通信中的音视频数据被窃取或篡改。

1.5.1 加密原理

SRTP 协议采用对称加密和消息认证技术，保护传输的音频和视频数据流机密性、完整性和认证性。

一、 对称加密：

- 在 SRTP 中，使用对称加密算法来加密音频和视频流数据。发送方和接收方在会话开始时通过密钥协商生成一个共享的会话密钥，然后使用该密钥进行数据加密和解密。对称加密是非常高效的方式，因为加密和解密操作使用相同的密钥，且加密算法计算较为快速，适合实时应用场景。

二、 消息认证：

- SRTP 使用设备的 MAC 地址来确保数据在传输过程中的完整性。每个数据包都附加一个 MAC 值。接收方在解密数据后，使用相同的密钥对数据进行认证，确保数据没有在传输中遭到篡改。

三、 密钥管理：

- 在 SRTP 中，密钥管理通过动态会话密钥的生成和更新来保证通信的安全。每次

会话开始时，双方通过安全的密钥交换协议协商出一个新的会话密钥，确保每次通信使用独立的加密密钥，增加会话的安全性和前向保密性。

四、 抗重复攻击：

- SRTP 通过引入 序列号 和 时间戳 机制，防止重复攻击。每个数据包都有唯一的序列号和时间戳，接收方可以验证收到的每个数据包是否是有效的。如果收到的包与先前的包重复，系统将拒绝该数据包。

五、 媒体流加密：

媒体流加密是 SRTP 协议的核心功能，它通过加密传输中的音频和视频数据，保证通话或会议的内容不被窃听或篡改。具体的加密方式包括：

- 实时加密：音频和视频流在传输的每一帧数据上都进行加密，每次数据传输都通过强加密算法对媒体流进行加密，保证数据在整个会话过程中的机密性。
- 独立加密：每个会话都有独立的会话密钥，确保每个数据包都是独立加密的，即使攻击者获得了某次会议的密钥，也无法解密其他会议的数据。
- 实时解密：接收方在接收到加密的媒体数据后，使用相同的会话密钥进行解密操作，恢复原始的音视频数据并进行实时播放，确保通信双方的实时互动不受影响。
- 数据完整性：SRTP 通过对每一数据包的 MAC 校验，确保数据在传输过程中未被篡改。即使数据包在传输过程中被中途截取，篡改后的数据包会被自动丢弃。

1.5.2 NewLync 2.0 中的应用

在 NewLync 2.0 中，SRTP 协议是保护平台内音视频通话的核心技术。所有语音和视频数据流都通过 SRTP 进行加密，从而确保通信的机密性和完整性。

具体应用如下：

一、 语音通话的媒体流加密：

- NewLync 2.0 在语音通话中采用 SRTP 协议 来加密所有音频流。每次通话开始时，系统为语音数据生成独立的会话密钥，通过对每一语音包进行加密，确保通话内容在传输过程中不会被第三方监听或篡改。

二、 视频会议的媒体流加密：

- SRTP 同样用于加密视频会议中的音视频数据。无论是视频流、音频流，还是控制信令数据，都通过加密保护。NewLync 2.0 的视频会议系统能够为每个参与者的音视频流提供独立的加密会话，保障每个用户的隐私。

三、 数据流完整性校验：

- 在 NewLync 2.0 的所有音视频会话中，SRTP 协议对传输的数据进行完整性校验，确保数据未被篡改。任何不一致的数据包都会被自动拒绝，从而保护通话过程中的信息安全。

四、 防止未授权访问：

- SRTP 在会话建立时，采用 TLS 协议进行身份验证，确保只有合法设备和用户能够加密和解密媒体流，防止伪造设备或恶意用户接入平台进行非法监听。

五、 支持高并发：

- NewLync 2.0 在大规模用户接入时，依然能够高效地为每个会话提供 SRTP 加密。

1.6 量子加密通信

在 NewLync 2.0 中，量子加密技术得到了实际应用。平台利用量子密钥分发（QKD）技术确保每次通信会话中的密钥交换安全，并结合传统加密算法为数据传输提供多层次保护。

1.6.1 加密原理

量子加密技术的加密原理基于量子力学的核心定律，量子叠加、量子纠缠和量子不确定性原理。传统的加密算法依赖于数学难题（如大数分解、离散对数问题），而量子计算机能够利用其强大的计算能力突破这些算法。因此，量子加密采用量子态来加密信息，从根本上避免了量子计算机破解的风险。

量子加密技术中，量子密钥分发（QKD）是确保密钥安全分发的核心技术。QKD 通过量子比特（qubits）来生成共享密钥，不仅保障密钥传输的机密性，还能确保密钥的来源合法性。以下是量子加密的基本原理：

一、 量子不可克隆性：

- 量子加密依赖于 量子不可克隆定理，即量子态不能被精确复制。攻击者无法复制或窃取量子密钥的状态。如果试图窃听，量子态将发生变化，通信双方可以通过量子测量检测到这一变化，从而识别出窃听者的存在。

二、 量子纠缠：

- 量子纠缠是量子力学中的一种现象，其中两个量子系统可以在空间上分离，但他们的状态依然相互关联。通过纠缠的量子比特，通信双方可以在量子信道中安全地交换信息，而不用担心被窃取。即使攻击者能够截获部分量子比特，也无法破解加密内容。

三、 量子密钥分发（QKD）：

- QKD 技术通过量子叠加和量子纠缠原理，在通信双方之间传递加密密钥。量子密钥通过不确定性原理确保不可窃取，即使是通过量子计算机进行攻击，密钥的安全性依然得到保障。

1.6.2 量子密钥分发（QKD）：与传统加密的对比

传统加密技术依赖于复杂的数学问题（如大数分解或离散对数）来保障通信数据的安全性，而量子计算机的出现使得传统的 RSA 和 ECC 等加密算法面临被破解的风险。量子计算可以通过 Shor 算法 高效破解传统加密，从而威胁到所有依赖于大数分解和离散对数的加密方法。

与传统加密方法不同，量子密钥分发（QKD） 利用 量子力学的原理（如量子不可克隆性）确保通信的安全性。

加密类型	基本原理	安全性	可能的破解方式	优势
传统加密	基于经典数学难题，采用 RSA 或 ECC 算法	依赖于计算的复杂性，量子计算机通过 Shor 算法可破解	量子计算机利用 Shor 算法在短时间内破解	简单且已广泛应用，但未来可能不再安全
量子加密	基于量子力学原理，采用量子密钥分发（QKD）技术	量子抗性，即使在量子计算机的攻击下也能保证安全	量子态干扰使得窃听行为可以被实时检测	提供量子抗性，确保长远的安全性

1.6.3 NewLync 2.0 中的应用

在 NewLync 2.0 中，量子密钥分发（QKD）和量子加密技术被集成到平台的通信架构中，确保平台能够有效抵御量子计算攻击，保障语音通话、视频会议、即时消息等通信内容的机密性和完整性。具体应用如下：

一、 量子密钥分发保障通信安全：

- NewLync 2.0 采用量子密钥分发技术（QKD）来生成共享的密钥。每次通信会话开始时，平台通过量子信道安全地交换密钥，确保密钥的机密性。通过量子不可克隆性原理，任何窃听行为都会干扰量子态，通信双方能够实时检测窃听并中止

通信，确保密钥交换的安全。

二、量子加密技术确保数据传输的安全：

- NewLync 2.0 在数据传输过程中，利用量子加密技术对语音、视频、即时消息等通信内容进行加密。

三、量子与传统加密技术结合：

- 为了进一步加强加密保护，NewLync 2.0 在量子密钥分发（QKD）技术的基础上结合了传统的加密算法，为数据传输提供多层次的加密保护。传统加密为数据提供实时加密，而量子加密则保护密钥交换过程的安全性，从而提升平台的整体安全性。

1.7 国密加密

国密加密（中国国家密码算法）是由中国政府制定的一系列密码算法标准，旨在提升国内信息安全技术的自主可控性和可信度。国密加密标准包括多个密码算法，如 SM2（公钥加密算法）、SM3（哈希算法）和 SM4（对称加密算法）。这些标准广泛应用于国内的各类网络安全、金融、政府和军事实践中，确保信息传输和数据存储的安全性。

1.7.1 加密协议简介

SM2、SM3 和 SM4 是中国国家密码管理局（SCA）发布的三种密码算法，分别用于公钥加密、哈希运算和对称加密。在 NewLync 2.0 中，平台结合这三种算法为用户提供全方位的通信安全保护。

一、SM2（公钥加密算法）：

- SM2 是中国的椭圆曲线公钥加密算法，广泛应用于数字签名、密钥交换和公钥加密。与 RSA 等传统公钥加密算法相比，SM2 能够在相同的安全级别下提供更短的

密钥长度，减少了计算资源的消耗，因此特别适用于低功耗设备和高并发环境。

- SM2 在 NewLync 2.0 中应用于身份认证、数据加密和数字签名验证，通过与 SM3 哈希算法和 SM4 对称加密算法结合，提供强有力的数据安全保障。

二、 SM3（哈希算法）：

- SM3 是中国的哈希算法，用于生成数据的摘要。其主要应用在数字签名、完整性校验和消息认证等场景中。SM3 与传统哈希算法相比，具有更高的安全性。
- 在 NewLync 2.0 中，SM3 用于加密数据的完整性校验，确保在数据传输过程中，信息未被篡改，防止恶意攻击者修改通信内容。

三、 SM4（对称加密算法）：

- SM4 是中国的对称加密算法，广泛应用于数据加密和密钥保护。与传统的对称加密算法相比，SM4 的设计更适应国内网络安全要求，并提供与 AES 相当的加密强度。
- 在 NewLync 2.0 中，SM4 算法用于对敏感数据（如语音、视频、即时消息等）进行加密，确保通信内容的机密性，防止数据在传输过程中被第三方窃取或篡改。

1.7.2 SM2、SM3、SM4 协议：如何增强本地加密安全

- SM2 的应用为 NewLync 2.0 提供了强大的身份验证能力。无论是在用户身份验证还是设备认证过程中，SM2 通过椭圆曲线算法为密钥交换和数字签名提供高效的加密支持。
- SM3 增强了数据完整性保护。SM3 的哈希算法生成的数据摘要，在确保消息传输不被篡改的同时，也提高了数据认证的精度。无论是数据传输中的语音、视频还是即时消息，SM3 确保了每条数据的完整性和真实性，防止遭到攻击。

- SM4 则是保护传输数据的加密核心。在传输过程中的每一条消息、每一个数据包都使用 SM4 进行加密，确保数据在传输过程中的机密性和安全性。使用 SM4 加密数据流的好处是其计算效率高，能够应对高并发的网络环境，适用于大规模并发的视频会议和语音通话。

1.7.3 TLS v1.3 与国密加密结合：确保国内加密通信的合规性和安全性

TLS v1.3 协议与国密加密协议的结合，在 NewLync 2.0 中提供了双重加密的保护机制，确保了国内通信的安全性和合规性：

- TLS v1.3 是当前最为先进的加密传输协议，它不仅优化了加密性能，还增强了抗攻击能力。相比旧版的 TLS 协议，TLS v1.3 减少了握手过程中的往返延迟（RTT），提升了通信效率。同时，TLS v1.3 删除了不再安全的加密算法，强化了协议的安全性。
- 在 NewLync 2.0 中，TLS v1.3 协议配合国密加密算法（如 SM2、SM3 和 SM4）共同工作，确保了通信数据的机密性、完整性。通过 SM2 实现的数字证书和公钥交换，SM3 提供的哈希算法保障了数据完整性，SM4 对称加密算法则确保了数据的传输过程不被篡改或窃听。
- 结合 TLS v1.3 和国密加密，NewLync 2.0 满足了中国的网络安全法和行业标准，为国内用户提供了更高的加密保护和合法性，确保了平台的合规性。

1.7.4 NewLync 2.0 中的应用

NewLync 2.0 将国密加密算法（SM2、SM3、SM4）与 TLS v1.3 协议结合，确保平台在通信过程中符合国内的安全标准。具体应用如下：

一、 通信加密：

- NewLync 2.0 为所有的语音通话、视频会议、即时消息等通信提供了全面的加密保护。通过 SM4 加密数据内容、SM2 公钥加密身份信息，结合 SM3 哈希校验机制，平台保障了数据传输的机密性和完整性。

二、 身份认证：

- 在 NewLync 2.0 中，用户和设备在连接平台时，首先会通过 SM2 公钥加密算法进行身份认证。数字证书验证和 SM2 协议确保了通信双方的合法性，防止恶意攻击者伪造身份。

三、 会话加密：

- 每次会话的密钥交换都通过 TLS v1.3 协议完成，确保通信过程中会话密钥的安全交换。加密通信内容时，使用 SM4 算法加密数据流，同时 SM3 校验算法确保数据的完整性和可靠性。

四、 合规性保障：

- NewLync 2.0 使用国密加密标准符合中国网络安全法和相关行业标准，为国内用户提供了合法合规的加密服务。通过结合 TLS v1.3 协议与国密加密算法，平台在保障数据安全的同时，满足了法律法规的要求。

五、 防止未经授权的访问：

- 通过 SM2 公钥加密和 TLS v1.3 协议的结合，NewLync 2.0 确保了平台上所有设备和用户在接入时都经过严格身份验证，防止未经授权的访问。

1.8 系统备份与恢复功能 (System Backup and Recovery)

系统备份与恢复功能是确保平台在面临硬件故障、系统崩溃或数据丢失等灾难性事件时，能够迅速恢复关键业务和服务的关键技术。该功能的核心目标是保障数据的安全性和确保系统的持续运行，减少因故障带来的数据损失和服务中断。

通过定期备份，平台能够确保即使在遇到不可预测的系统故障时，能够迅速恢复数据，并最大限度地减少业务停机时间，保证业务连续性。备份机制为数据的恢复提供了多层保护，保障了数据完整性，确保了平台的正常运行。

在 NewLync 2.0 中，系统备份与恢复功能被设计为关键的灾难恢复和业务连续性保障工具。该功能涵盖了数据库、用户数据、录音文件和配置文件等方面。平台通过以下几项技术来实现备份和恢复：

1.8.1 数据库恢复

数据库是平台中最核心的数据存储部分，包含了所有的用户数据、应用配置、业务记录等重要信息。为了防止数据库在系统崩溃或其他故障时的损坏，NewLync 2.0 实现了数据库备份机制，确保所有关键数据可以在故障后快速恢复。

- 数据库备份方案：NewLync 2.0 平台定期执行备份，保证数据始终处于安全备份状态。
- 自动化备份任务：平台会定期（如每日凌晨三点）自动进行备份操作，确保在系统遭遇灾难时能够迅速恢复数据，减少人为错误导致的数据丢失风险。
- 恢复过程：在系统发生故障时，管理员可以通过平台提供的恢复功能从备份中恢复数据库文件。系统将自动恢复用户数据、录音文件和配置文件等，确保恢复后的数据完整性和一致性。

- 数据一致性和完整性校验：为了确保恢复过程中的数据一致性，平台在恢复数据时会执行一致性检查，确保恢复后的数据库与备份时的一致。

1.8.2 录音文件恢复

在 NewLync 2.0 中，所有 语音通话 和 视频会议 的录音文件也会进行定期备份。这样，即使系统发生故障或数据丢失，管理员也能够快速恢复这些重要数据。

- 定期备份录音数据：所有的会议录音、语音通话录音和视频会议文件都会根据设置的备份频率进行备份。
- 录音恢复机制：一旦系统发生故障，管理员可以通过恢复备份的方式迅速恢复所有录音数据。
- 保障会议内容完整性：确保会议录音文件在恢复后内容不丢失或损坏。

1.8.3 配置文件恢复

配置文件恢复 是平台恢复操作中的另一个重要功能。配置文件包含了平台的系统设置、用户权限配置、服务配置等内容，确保系统能够在不同环境下正常运行。

- 系统设置恢复：恢复过程中，平台会自动恢复包括 服务端配置、网络配置 和 安全策略设置 等配置文件。
- 用户权限与角色恢复：所有用户的角色配置和权限设置都会被备份。恢复过程将会重新加载这些权限和角色配置，确保数据恢复后，平台的访问控制不被中断，防止出现用户权限泄露或错误分配的情况。
- 服务恢复与配置：系统恢复不仅仅是恢复用户数据，还会恢复 服务配置。例如，平台在运行时的 负载均衡配置 和 连接管理设置 等内容，都能够通过恢复操作快速恢复，确保平台运行时能够继续为用户提供稳定的服务。

1.9 访问控制与系统安全

在 NewLync 2.0 平台中，账号管理 功能覆盖了整个系统的用户管理需求，确保平台内的所有用户只能访问其权限范围内的资源。通过访问控制、角色管理和账户审计，平台为管理员提供精细化的用户账户管理功能，以提升系统的安全性和合规性。

1.9.1 用户权限管理

在 NewLync 2.0 中，用户权限管理 是确保平台安全的重要组成部分。管理员可以根据用户的职责、岗位要求以及安全策略分配不同的权限，以确保每个用户的访问权限得到合理划分。通过角色划分，确保只有特定角色的用户能够访问系统中的敏感信息，防止未经授权的用户访问、修改或泄露敏感数据。

- 权限分配与管理：管理员根据平台的不同需求，将每个用户分配到相应的用户组中。每个用户组对应不同的访问权限，确保最小权限原则，即用户只能访问其工作所需的资源。
- 角色与权限：例如，平台管理员可以拥有全权访问所有功能的权限，而普通用户仅能访问自己的数据或业务功能。

1.9.2 身份验证

身份验证是保障 NewLync 2.0 平台安全性的基础机制之一。平台提供多种身份验证方式，包括 用户名/密码 和短信验证，以确保用户的身份真实性，防止未授权用户访问企业内部信息。

- 用户名和密码验证：每个用户在平台登录时需要输入正确的用户名和密码。密码设置采用高强度的加密算法，保障传输过程中的安全性。
- 短信验证：为了进一步提高安全性，在用户输入正确密码后，系统会要求用户提

供第二层验证（手机验证码）。防止单一密码被窃取后的账户风险。

1.9.3 访问权限

访问权限是确保用户权限分配合理的核心机制。根据企业的实际需求，管理员可以创建用户组，并为每个用户组内成员配置不同的访问权限，确保其仅能访问与其职责相关的资源。

1.9.4 限制注册新账号

通过控制用户注册的权限，可以有效管理系统用户数量。启用时，任何符合条件的用户都可以进行注册；禁用时，只有管理员手动添加用户或已有用户可以继续使用现有账号。

1.9.5 限制境外 IP 登录

- 启用：允许来自境外的 IP 地址登录平台。适用于需要为全球用户提供服务的系统，但可能会增加被攻击的风险。
- 禁用：限制只有国内 IP 地址可以登录，防止境外 IP 的潜在安全风险，减少非法访问的机会。此选项可提高系统的安全性，适用于防止跨国攻击和数据泄漏。

1.9.6 系统状态监控

- 监控设备和系统状态：实时监控所有关键设备和系统组件的状态，包括服务器、网络设备、数据库等。通过定期检查系统性能、资源使用率和健康状况，确保系统在最佳状态下运行。
- 及时发现安全问题：系统会自动检测和识别潜在的安全威胁和异常行为，如未经授权的访问、资源过载或异常数据流，及时报警并记录日志，帮助管理员快速定位问题并采取应对措施。

1.9.7 故障告警

- 出现故障时及时告警：一旦系统或设备出现故障，系统会自动生成告警并通过邮

件及平台通知等方式告知管理员。此机制可以确保管理员在最短时间内获知故障信息，采取紧急措施避免进一步损害。

- 保证系统恢复：通过故障告警系统，可以快速响应和恢复服务。告警信息中将包含详细的故障类型，帮助技术人员精准定位故障源，并确保系统快速恢复正常运行，最大程度降低停机时间和业务中断风险。

1.9.8 软件更新

- 定期更新系统和安全补丁：确保系统保持最新的版本，以修复已知漏洞和增强系统的安全性。定期检查并安装操作系统和应用程序的安全补丁，防止系统暴露于已知的安全威胁之下。
- 更新日志和版本控制：记录每次更新的内容和修复的漏洞，便于管理员追踪和验证更新是否正常应用。

1.9.9 安全日志

- 安全日志：系统自动记录所有用户操作日志。
- 管理员日志：专门记录管理员和高级别用户的敏感操作，如修改系统设置、用户权限变更、访问核心数据等。日志包含操作时间、操作人员、操作内容等信息。

1.9.10 防暴力破解与密码保护策略

- 密码锁定策略：配置密码保护策略，当用户连续输入错误密码多次时，自动锁定该账号一段时间或要求进行进一步身份验证。
- 强密码要求：要求用户设置强密码（包括大小写字母、数字和特殊字符的组合），并定期更换密码。

1.9.11 限制非法登录 IP

- 限制非法登录 IP：配置系统只允许来自合法 IP 地址范围的访问请求，所有不在允许范围内的 IP 地址将被拒绝访问。
- IP 黑名单与白名单：设置白名单和黑名单机制，支持管理员根据需要手动添加或删除 IP 地址。
- 动态 IP 检测：频繁失败的登录尝试将自动触发警报并限制登录。

2 安全功能清单

序号	功能名称	功能描述	子功能名称	子功能描述
1	呼叫与会议权限	管理呼叫权限，防止非法干扰	呼叫权限	管理国内外长途、紧急电话等权限
2	数据备份与恢复	支持定期备份数据库和录音文件	/	/
3	安全日志	记录操作日志，确保可追溯性	管理员日志	跟踪管理员操作情况
			用户日志	记录所有用户操作日志
4	防暴力破解	防止暴力破解攻击	密码保护	配置频繁登录密码锁定策略，防止暴力破解
			短信验证	增加额外短信验证，确保账户安全
			限制非法登录 IP	配置非法登录 IP 范围，防止非法访问，频繁登录失败的 IP 将加入黑名单
5	账号及权限管理	管理用户账户，精细化权限分配	用户权限	根据角色设定可访问内容
			访问控制	控制员工添加好友、群组及通过 WEB 入会
6	设备管理	管理终端设备	设备控制	限制账户接入的设备数量
			新设备二次验证	新设备登录时需二次验证
			设备锁定	锁定已登录设备
7	加密	保证数据传输安全	国密加密	支持国密 SM2、SM3、SM4 的 TLS v1.3 加密通信
			TLS 加密	应用于语音、视频、即时消息等数据的传输加密
			量子加密	使用量子密钥分发技术（QKD）提供量子安全防护
			端到端加密	用于确保前后端数据传输的安全性
			IMS-AKA 鉴权认证	用于确保信令传输的机密性和完整性
			SIP 消息完整性检测	防止非法篡改 SIP 消息
			SIP 信令加密	加密 SIP 信令，防止信号被篡改
			媒体流加密	加密媒体流，防止数据泄露
			配置文件加密	加密配置文件，防止被篡改

8	账号设置	配置账号创建和登录 验证设置	允许注册账号	启用或禁用用户注册新账号
			限制境外 IP 登陆	控制是否允许境外 IP 地址登录
9	软件更新	保持系统和客户端软件最新	系统更新	定期更新系统和安全补丁
10	状态监控	管理设备状态、查看 告警信息	系统状态监控	支持监控设备和系统状态
			故障告警	出现故障时及时发送告警通知