网络安全协议及分析
网管安全SNMPv3

密码与网络安全系　刘虹

2025年春季学期

课程体系

第一章 概述

第二章 链路层扩展L2TP

第三章 IP层安全IPSec

第四章 传输层安全SSL和TLS

第五章 会话安全SSH

第六章 代理安全Socks

第七章 网管安全SNMPv3

第八章 认证协议Kerberos

第九章 应用安全

本章学习目标

- SNMPv3的基本概念
- SNMPv3的体系结构
- SNMPv3的消息及消息处理模型

提纲

SNMP概述

- 简单网络管理协议（Simple Network Management Protocol，SNMP）是TCP/IP架构下的网络管理标准：
  - 包括至少一个网络管理站、多个被管理节点、管理信息和用于在SNMP实体之间传递管理信息的通信协议。
- SNMP通信协议工作于应用层，它可以在不同的传输层协议上工作
  - UDP、网间分组交换协议（Internetwork Packet Exchange，IPX)等。
- SNMP不应只被看做一个通信协议，它是一个有关网络管理体系结构的整体规范，包括以下要素：
  - 规范语言、MIB定义、协议定义以及安全与管理

SNMP概述

- SNMP的前身是简单网关监控协议（Simple Gateway Monitoring Protocol，SGMP)
- SNMPv1的访问控制基于共同体名（Community Name），实质上是一个明文口令。
- SNMPv2延续了VI所确定的管理框架，将规范语言升级为SMIv2。
- SNMPv3协议可看作一个安全规范，它定义一种标准化的SNMP框架结构，为两种SNMPv1与SNMPv2消息提供各种安全功能

SNMP概述

- SNMPv3提供数据完整性保护和数据源发认证功能，并把该类安全服务作为其首要目标。
- 此外，它还提供机密性和有限的传输流机密性保护，并且能够防止重放攻击。它把安全服务分为三个级别：
  - 不认证不加密（NoAuthNOPriv，用1表示）；
  - 认证不加密（authNoPriv，用2表示）；
  - 认证且加密（authPriv，用3表示）。

提纲

一、SNMP概述

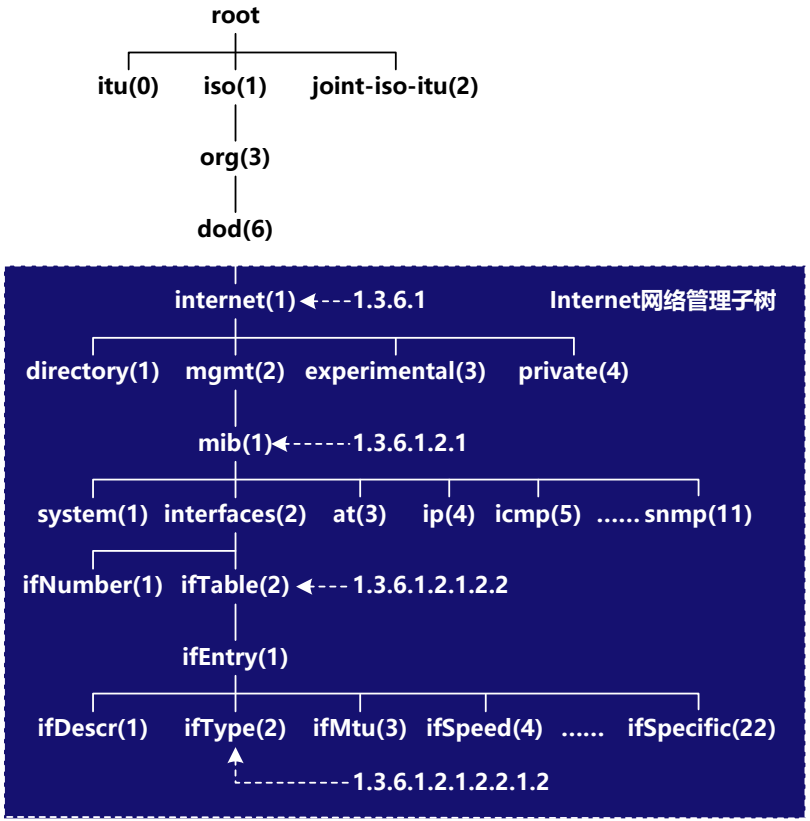
二、SNMP体系简介

三、SNMPv3体系结构

四、 SNMPv3消息及消息处理模型

二 SNMP体系

- 管理信息库（Management Information Base，MIB）
  - 对象
    - 所有对象和实例都应被赋予唯一的名字，即对象标识符OID。
    - 比如，设备的物理接口表是一个对象，其中第一个接口就是一个实例。
    - 管理信息库使用一棵命名树有效确保了OID的唯一性



二 SNMP体系

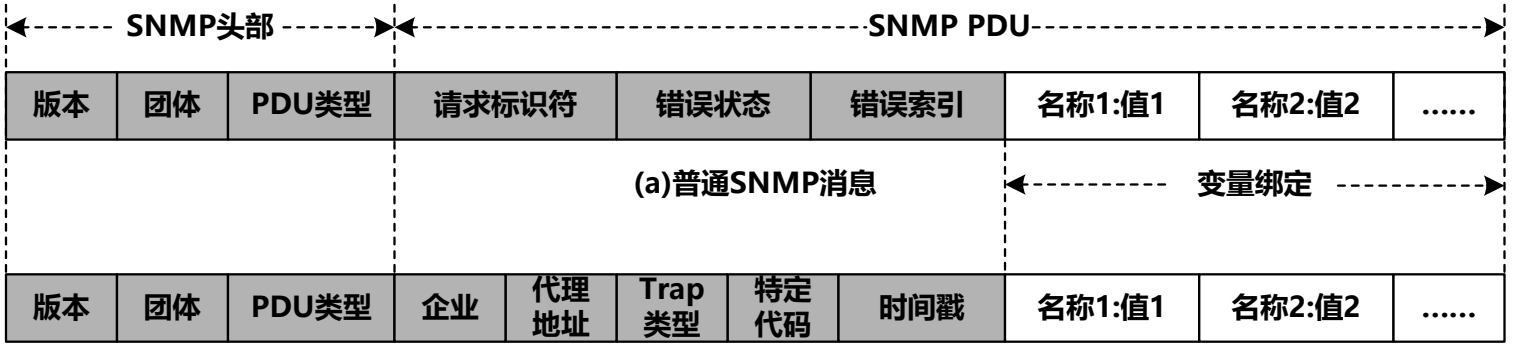
- 管理信息库（Management Information Base，MIB)
  - 实例：实例是对象的具体化
    - "sysObjectID.0"就是sysObjectID对象的一个实例

例如，在interface组中包含

- 用于描述物理接口总数的“ifNumber”
- 用于描述每个接口的“ifTable“，其下为”ifEntry”。

二 SNMPv1消息的基本结构

- SNMPv1消息包括：
  - SNMP头部
  - 协议数据单元（Protocol Data Unit，PDU）



(b)Trap消息

提纲

一、SNMP概述

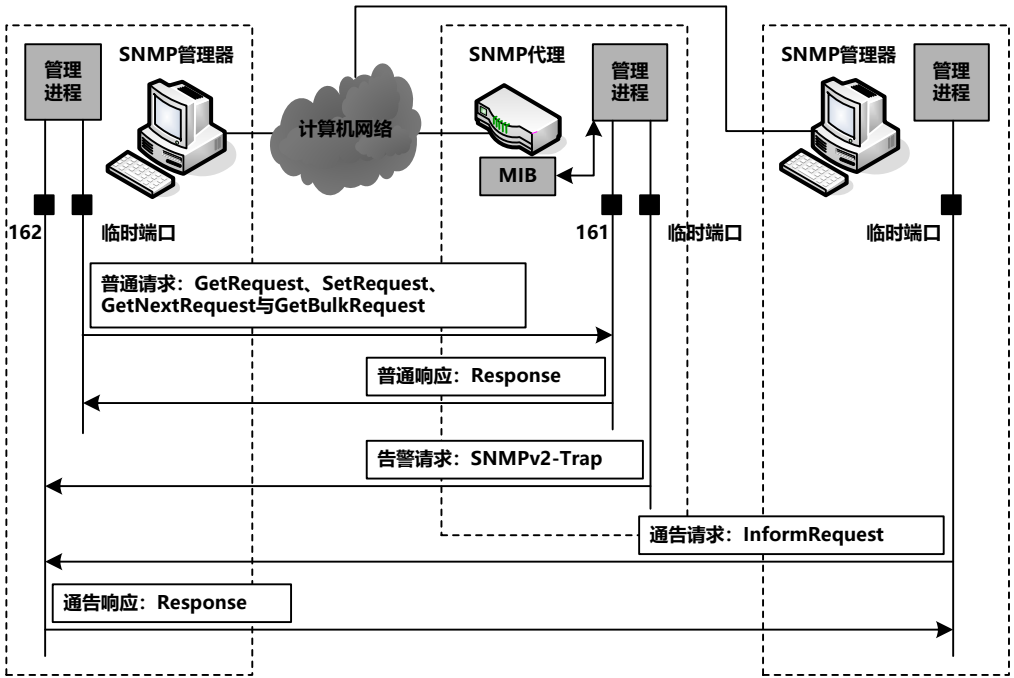
二、SNMP体系简介

三、SNMPv3体系结构

四、 SNMPv3消息及消息处理模型

三 SNMPv3体系结构

- SNMPv3没定义新的网管操作、消息类型与PDU结构，主要改进在于安全性
  - 定义一种标准化的SNMP框架结构
  - 为两种SNMPv1与SNMPv2消息提供各种安全功能



三 SNMPv3的网管操作

- **普通操作：**
  - **由SNMP管理器向代理发送，需要SNMP代理返回响应的网管操作**
- **通告操作：**
  - **SNMP管理器向其它管理器发送，需要SNMP管理器返回响应网管操作**
- **告警操作：**
  - **由SNMP代理主动向管理器发送，不需要SNMP管理器返回响应的网管操作**

三 SNMPv3的安全机制

- 数据认证
  - 防止SNMP消息在传输过程中被篡改，或SNMP消息来自伪造的SNMP实体
- 数据加密
  - 防止SNMP消息在传输过程中被窃听

SNMPv3体系结构

- SNMPv3实体的主要类型
  - 管理器（Manager）：
    - 请求发送与响应接收
  - 代理（Agent）：
    - 请求接收与响应发送
  - 代理服务器（Proxy）：
    - 请求与响应转发

三 SNMPv3体系结构

- SNMP引擎与SNMP实体是一对一的关系，它包括消息发送与接收以及认证与加密功能，同时能够提供对被管对象的访问控制。
- 每个SNMP引擎都有一个ID（snmpEngineID），处于同一管理域的每个引擎ID应该不同。
  - 调度程序
  - 消息处理模块
  - 安全模块
  - 访问控制模块

三 SNMPv3体系结构

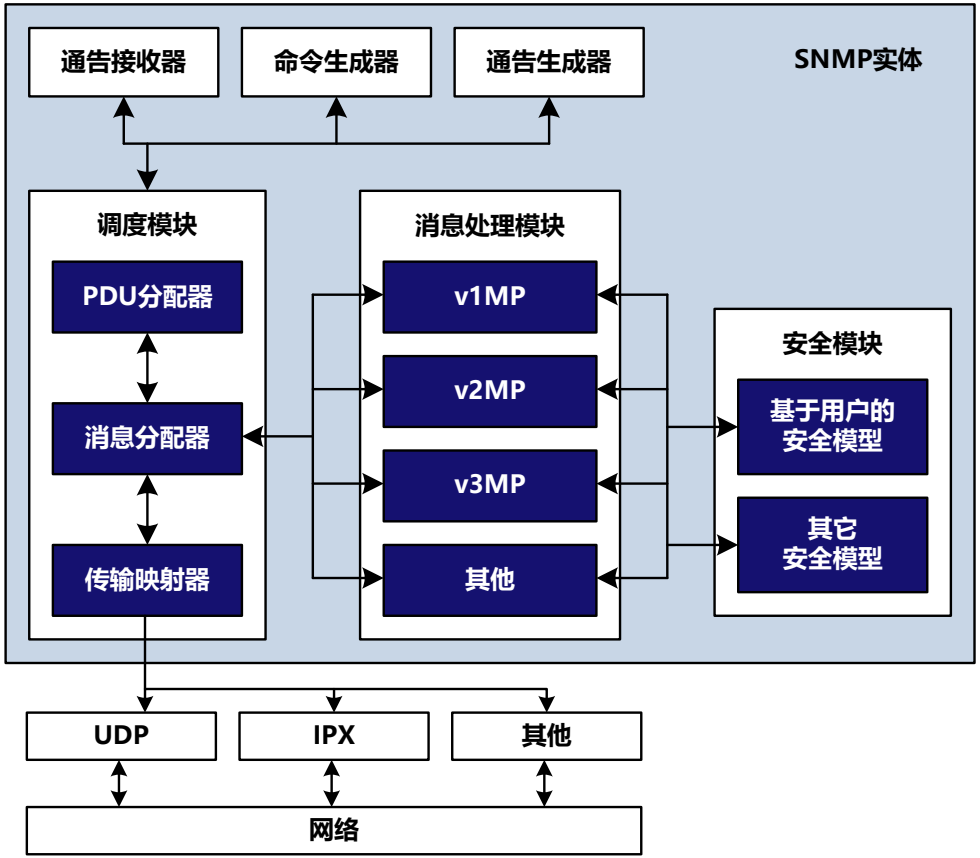
- 调度程序（Dispatcher Model）：
  - 负责SNMP消息的发送与接收
- 消息处理模块（Message Processor Model）：
  - 负责SNMP消息的分析与处理
- 安全模块（Security Model）：
  - 负责SNMP消息的认证与加密
- 访问控制模块（Access Control Model）：
  - 负责MIB中对象的访问控制

三 SNMPv3应用

- **命令生成器**：用于SNMP管理器，生成SNMPv1与SNMPv2普通请求，接收SNMPv1与SNMPv2响应
- **命令接收器**：用于SNMP代理，接收SNMPv1与SNMPv2普通请求，生成SNMPv1与SNMPv2响应
- **通告生成器**：用于SNMP管理器或SNMP代理，为代理生成SNMPv1与SNMPv2告警请求与SNMPv2通告请求，接收SNMPv2通告响应
- **通告接收器**：用于SNMP管理器，接收SNMPv1与SNMPv2告警请求与SNMPv2通告请求，生成SNMPv2通告响应
- **代理转发器**：用于SNMP代理或代理服务器，转发接收的SNMP命令与响应

三 SNMPv3应用

- 管理站的应用
  - 通告接收器
  - 命令生成器
  - 通告生成器
- 只要具备前两个应用就是一个管理站，但是管理站可能也包含通知发起器应用。



三

SNMPv3的服务接口

- 应用程序与SNMP引擎的分配器模块之间，以及SNMP引擎中的不同模块之间，通过**服务接口（Service Interfere）**进行通信
- 服务接口由多个事先定义好的**原语**组成。每个原语包括固定的语法格式与数据元素，用于应用程序与不同模块之间实现某种功能

三 SNMPv3协议的主要原语

- 调度程序的原语

原语名	用途说明
sendPdu	生成来自应用程序的请求PDU
returnResponsePdu	生成来自应用程序的响应PDU
processPdu	处理来自远程实体的请求PDU
processResponsePdu	处理来自远程实体的响应PDU
registerContextEngineID	为应用程序注册处理的PDU
unregisterContextEngineID	为应用程序解除注册处理的PDU

三 SNMPv3协议的主要原语

- 消息处理模块与访问控制模块的原语

原语名	用途说明
prepareOutgoingMessage	为分配器模块准备发送的请求
prepareResponseMessage	为分配器模块准备发送的响应
prepareDataElements	从分配器模块接收消息中提取数据
isAccessAllowed	判断对管理对象访问操作是否合法

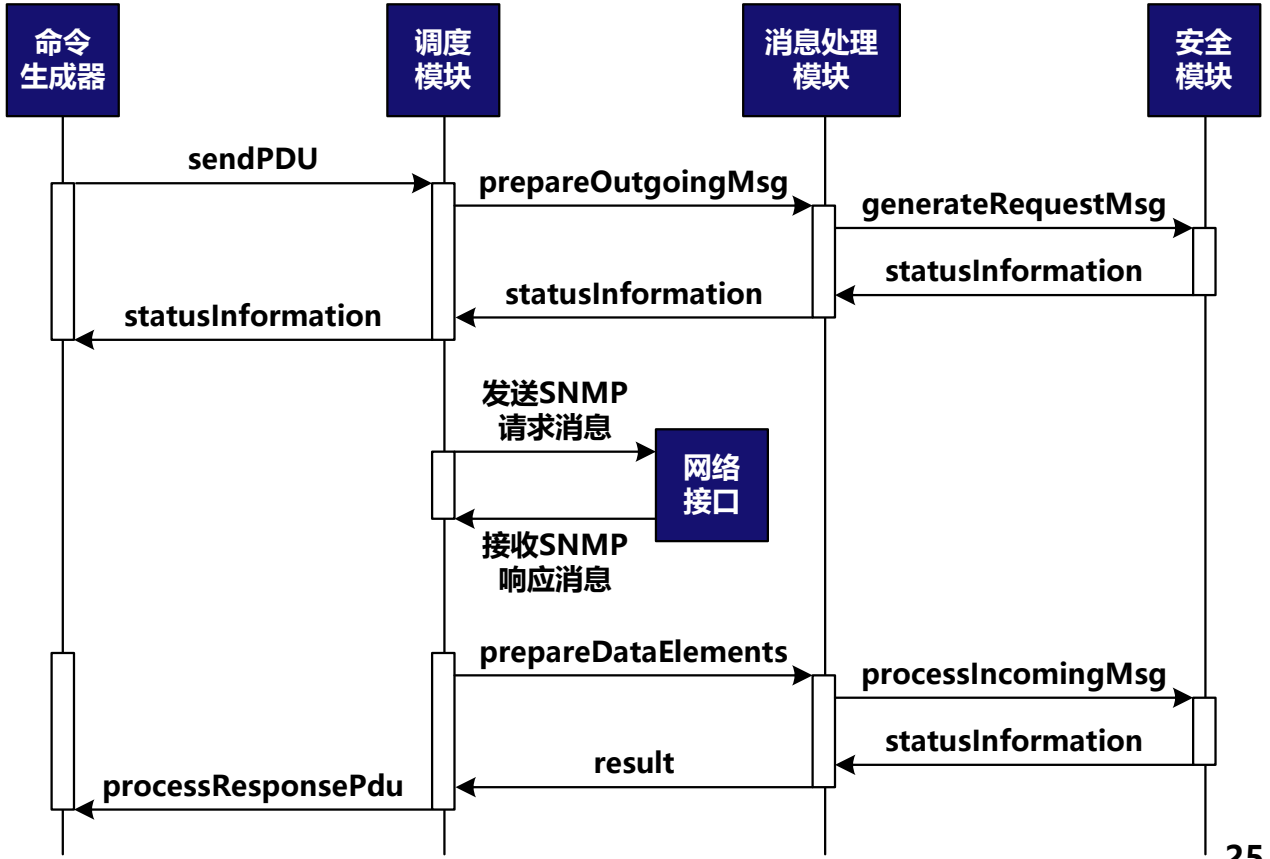
三 SNMPv3协议的主要原语

- 安全模块的原语

原语名	用途说明
generateRequestMsg	为消息处理模块准备发送的请求
generateResponseMsg	为消息处理模块准备发送的响应
processIncomingMsg	处理消息处理模块的接收消息
authenticateIncomingMsg	使用认证算法认证发送消息
authenticateOutgoingMsg	使用认证算法认证接收消息
encryptData	使用加密算法加密数据
decryptData	使用解密算法解密数据

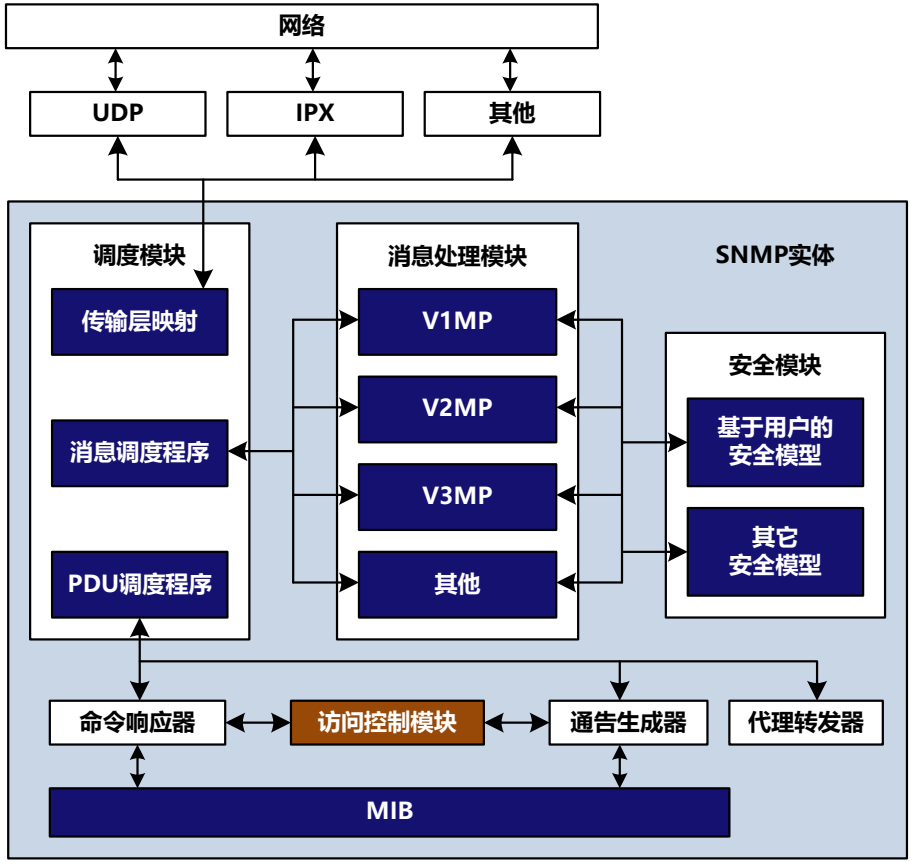
三 SNMPv3协议

- 管理站组件交互



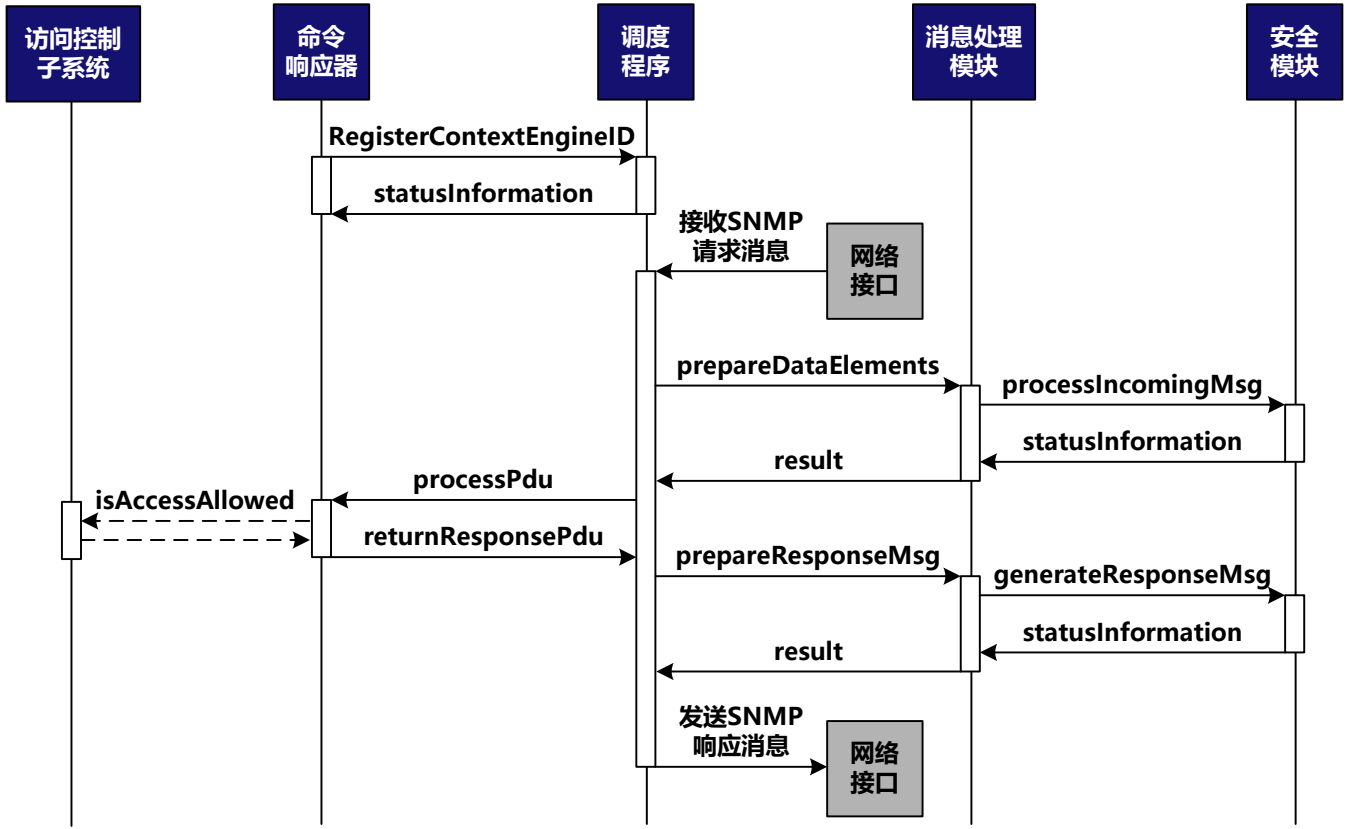
SNMPv3协议

- SNMP代理（Agent)
  - 增加访问控制模块
    - 由于被管节点需要对管理站身份进行认证并赋予其相应的读写权限



三 SNMPv3协议

- 代理组件交互



提纲

一、SNMP概述

二、SNMP体系简介

三、SNMPv3体系结构

四、 SNMPv3消息及消息处理模型

四 消息格式

- 消息：版本、首部、安全参数、ScopedPDU数据

首部：消息ID、最大长度、标志、安全模型

加密的PDU：二进制串

明文ScopedPDU：contextEngineID、contextName、数据

PDU：请求ID、错误状态、错误索引、VBL

VBL：变量1、变量1值、…、变量n、变量n值

四 ScopedPDU

- SNMPv3定义了8种ScopedPDU：
  - 读类：读管理信息，包括GetRequest-PDU、GetNextRequest-PDU以及CetBulkRequest-PDU；
  - 写类：更改管理信息，即SetRequest-PDU；
  - 响应类：对请求的响应，包括Response-PDU和Report-PDU
  - 通知类：通知操作，包括SNMPv2-Trap-PDU和InformRequest-PDU；
  - 内部类：用于SNMP引擎之间的通信，即Report-PDU。

四 ScopedPDU

- GetRequest-PDU
  - 请求读取对象值时，发送方使用GetRequest-PDU。
  - 接收方会处理其VBL中包含的所有对象。如果在本地MIB中找到这个对象，会读取相应的值以构造响应信息，否则值字段应被设置为空。
  - 当所有的对象都处理完成后，接收方通过Response-PDU返回应答，其“消息ID”和“请求ID"字段值与请求消息相同，“错误状态"和“错误索引"字段根据对变量的处理结果设置。

ScopedPDU

- GetNextRequest-PDU
  - GetNextRequest-PDU既可以读取单个对象，也可以读取表格。

- GetBulkRequest-PDU
  - GetBulkRequest-PDU的处理方式与GetNextRequest-PDU类似，但它为SNMP通信双方提供了批量交互数据的能力，从而提高了通信效率。

四 ScopedPDU

- **SetRequest-PDU**
  - SetRequest-PDU用于更改管理对象的值。
  - 在收到该请求后，回应方会对PDU进行两步检查：第一步检查OID的合法性，第二步修改对象值。

- **InformRequest-PDU**
  - InformRequest-PDU用于一个管理站向另一个管理站发送通知消息或者请求其控制的管理信息。
  - 回应方收到InformRequest-PDU后，应返回Response-PDU应答。在不发生差错的情祝下，应答与请求的内容相同。

四 ScopedPDU

- Response-PDU
  - Response-PDU用于对上述5类PDU的响应。
- SNMPv2-Trap-PDU
  - 被管节点通过SNMPv2-Trap-PDU向管理站报告某个事件发生或某个条件具备。它的VBL设置与InformRequest-PDU类似，但它不需要应答。
- Report-PDU
  - 不是用于管理站和被管节点之间交互管理信息，而是用于错误通告。
  - 这种错误通告并不是像发送Trap信息那样通告设备的异常情况，而是表示协议操作过程中所发生的错误。

办公地点：理科大楼B1209

联系方式：17621203829

邮箱：liuhongler@foxmail.com