网络安全协议及分析
IP层安全IPSec

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

- IPSec的概述
- ISAKMP协议流程
- 地址驱动的网络安全管控结构

提纲

一、IPSec协议概述

二、ISAKMP协议

三、地址驱动的网络安全管控结构

IPSec协议

- 交换协议：
  - 互联网安全关联与密钥管理协议（Internet Security Association and Key Management Protocol，lSAKMP）
  - 互联网密钥交换（Internet Key Exchange，IKE）
- 数据封装协议：
  - 数据封装处理协议的认证首部（Authentication Header，AH）
  - 封装安全载荷（Encapsulating Security Payload，ESP）

IPSec协议

- IP层的安全风险
  - **IP可能遭受欺骗攻击**：IP地址是发送方和接收方的标识，但攻击者可以轻易构造一个包含虚假源地址的数据报（IP Datagram）。
  - **IP层是点到点通信**：IP数据报在从源端被发送到目的端的过程中可能被多个路由器转发。

If you reveal your secrets to the wind,.

You should not blame the wind for revealing them to trees.

IPSec协议历史和现状

- The Architecture and Implementation of Network Layer Security in UNIX
- 三个版本
  - IPSecv1对应RFC 1825-1829
  - 旧IPSec：IPsecv2对应RFC 2401-2411
  - 新IPSec：IPsecv3对应RFC 4301-4309

The Architecture and Implementation of Network-Layer Security Under Unix

John Ioannidis
Columbia University
New York, NY 10027
ji@cs.columbia.edu

Matt Blaze
AT&T Bell Laboratories
Holmdel, NJ 07733
mab@research.att.com

ABSTRACT

swIPe is a network-layer security protocol for the IP protocol suite. This paper presents the architecture, design philosophy, and performance of an implementation of swIPe under several variants of Unix. swIPe provides authentication, integrity, and confidentiality of IP datagrams, and is completely compatible with the existing IP infrastructure. To maintain this compatibility, swIPe is implemented using an encapsulation protocol. Mechanism (the details of the protocol) is decoupled from policy (what and when to protect) and key management. swIPe under Unix is implemented using a virtual network interface. The parts of the implementation that process incoming and outgoing packets are entirely in the kernel; parameter setting and exception handling, however, are managed by user-level processes. The performance of swIPe on modern workstations is primarily limited only by the speed of the underlying authentication and encryption algorithms; the mechanism overhead is negligible in our prototype.

1. Introduction

Traditionally, system security has been addressed in an *ad-hoc* fashion and at a fairly high level, usually in the applications themselves. As applications become more distributed in nature and are relying more and more on the integrity of information received from their peers, it becomes attractive to consider common, general solutions to replace *ad-hoc*, application-specific security mechanisms. Most system-level security work has focused on the operating system and on arbitrating access to resources on a particular machine. Relatively little attention has been paid to securing communications in any consistent way. In modern distributed systems, however, which are characterized by a large number of single-user or single-purpose machines, the network itself is emerging as the best candidate for concentrating security efforts.

The explosively increasing size of the Internet, with its concomitant security problems, coupled with the wide range of services and applications that it supports, make IP-based networks a good choice for understanding and exploring network security issues. The rising mobility of users, the advent of wireless networking services, and the increasingly critical dependence of financial and commercial services on the Internet infrastructure, call for the adoption of authentication, integrity, and privacy features as *sine qua non* features of the network.

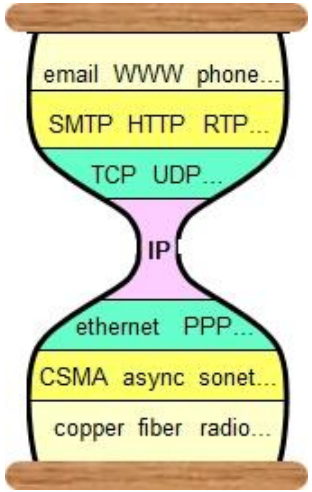
There have been a number of efforts aimed at providing security services at some layer in the network hierarchy [4,8,12,16]. However, no existing protocol is completely satisfactory for large-scale Internet-based deployment. Existing network-layer security protocols such as SP3 and NLSP

IPSec协议提供的安全服务

- 身份认证
- 机密性
- 完整性
- 通信流机密性保护
- 协议的互操作性

IPSec协议的优势和劣势

- 优势：
  - IPsec在通用性
  - 部署灵活性
  - 安全策略统一性
- 劣势：
  - 使用简便性
  - 通信效率
  - 应用开发支持



IPSec的组成

- IP通信过程分成协商和数据交互两个阶段
  - 在协商阶段，通信双方互相认证对方的身份，并根据安全策略协商使用的加密、认证算法，生成共享的会话密钥；
  - 在数据交互阶段，通信双方利用协商好的算法和密钥对数据进行安全处理以实现IPsec的各种安全功能。
- 相关协议
  - 互联网密钥交换协议（Internet Key Exchange，IKE），对应IPsec的协商阶段。
  - 认证首部AH和封装安全载荷（Encapsulating Security Protocol，ESP），对应IPsec的数据交互阶段。

IPSec的组成

标准组成

- IPsec体系结构描述IPsec标准中的基本概念、安全需求以及IPsec的应用模式等内容。
- ESP协议规定ESP的语法、语义和时序。
- AH协议规定AH的语法、语义和时序。
- 加密算法描述各种加密算法如何应用于ESP。
- 认证算法描述各种认证算法如何应用于AH和ESP。
- 组合算法描述如何将加密和认证算法组合以提供服务。
- IKE规定协商协议的语法、语义和时序。

安全策略

- 安全策略定义了系统中哪些行为是允许的，哪些是不允许的。

- 按授权的性质不同，安全策略包括基于规则的策略和基于身份的策略。
  - **基于规则的安全策略**是根据系统的一般属性建立的一组规则，授权通常依赖于信息与资源的敏感属性，它们通常是强制性的。
  - **基于身份的策略**是建立在特定的个别属性之上的授权准则，其目的是过滤对特定数据或资源的访问和使用。

安全策略

安全策略的表示与管理

- 策略是通过自然语言表达的，而机器只能识别形式语言。通常不存在一个映射方式，将自然语言表达式无损地映射到形式语言表达式中。

- 安全策略通常以**安全策略库**（Security Policy Database，SPD）的形式表现出来，库中的每条记录对应一个安全策略。
- IPsec系统所使用的SPD一般保存在一个策略服务器中。
  - 该服务器为域中的所有节点（主机和路由器）维护策略库。
  - 各节点可将策略库拷贝到本地，也可使用轻目录访问协议（Lightweight Directory Access Protocol，LDAP）动态获取策略。

安全策略

- 安全策略的要素
  - IPsec本身没有为策略定义标准，只规定了两个策略组件：
    - 安全策略库（Security Policy Database，SPD）
    - 安全关联库（Security Association Database，SAD）

- 策略描述：即对“谁"实施“何种"安全保护
  - 对通信特性的描述
  - 对保护方法的描述

安全策略

- 对通信特性的描述：**选择符**
  - 目的IP地址：单个IP地址、地址列表、地址范围或通配（掩码）地址。
  - 源IP地址：单个IP地址、地址列表、地址范围或通配（掩码）地址。
  - 名字：DNS名、X.500区分名或者在IPsec DOI中定义的其他名字类型。
  - 传输层协议：TCP或UDP。
  - 源和目标端口：TCP或UDP端口号，可为单个端口、端口列表或通配端口。
  - 数据敏感等级：通信数据的保密等级，可分为普通、秘密、机密、绝密。

安全策略

- 对保护方法的描述
  - 对于进入或外出的每一份数据报，都可能有三种处理方式：丢弃、绕过或应用IPsec。
  - 若应用IPsec，策略要包含使用的安全协议（AH或ESP）、模式、算法等，这些参数以**安全关联（security association，SA）**的形式存储在关联数据库中。

安全策略

- 安全关联（Security Association，SA）
  - 安全关联用于实现安全策略，是安全策略的具体化和实例化，它详细定义了如何对一个具体的数据报进行处理。
  - 对于安全策略库SPD中的一条记录，如果策略的要求是应用IPsec进行保护，它必定要指向一个或多个安全关联SA。

安全策略

- 安全关联（Security Association，SA）
  - 安全关联是两个IPsec实体（主机、路由器）间的一个单工“连接"，决定保护什么、如何保护以及谁来保护通信数据。
  - 它规定了用来保护数据报安全的安全协议、密码算法、密钥以及密钥的生存期等。SA是单向的，要么对数据报进行“进入（接收到的）”保护，要么对数据报进行“外出（发送出去的）"保护。
  - 每个SA用一个三元组<安全参数索引、目的IP地址、安全协议>来标识

安全策略

- 安全关联库SAD
  - SAD为进入和外出数据报维持一个活动的SA列表，其中的记录是无序的。
  - 外出SA用来保障外出数据报的安全，进入SA用来处理进入的数据报。
- 安全关联的字段
  - 目的IP地址
  - 序号计数器
  - 抗重放窗口
  - 安全关联的生存期
  - 路径最大传输单元（Maximum Transmission Unit，MTU）
  - IPsec协议
  - 序号计数器溢出标志
  - 密码算法及密钥
  - IPsec协议模式（传输、隧道）

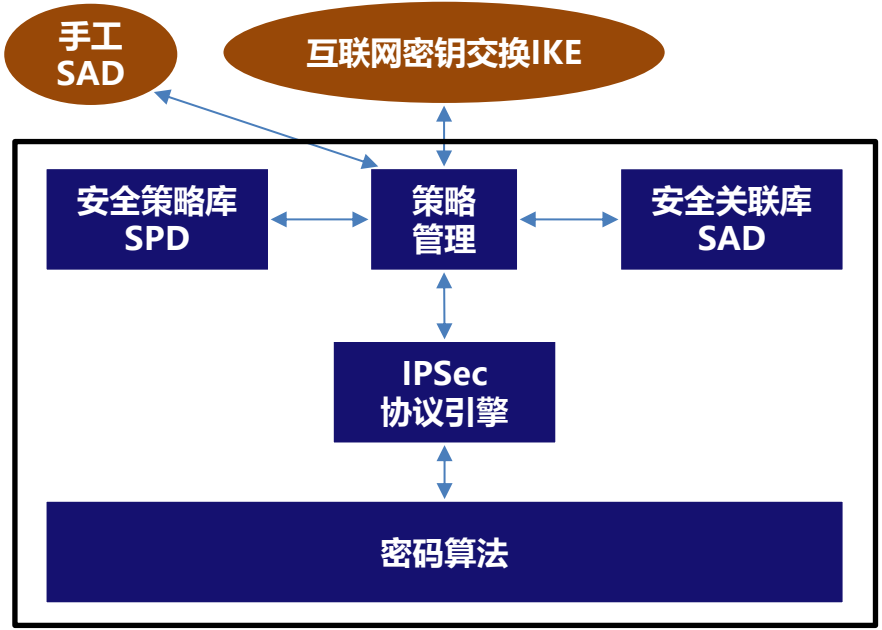
安全策略

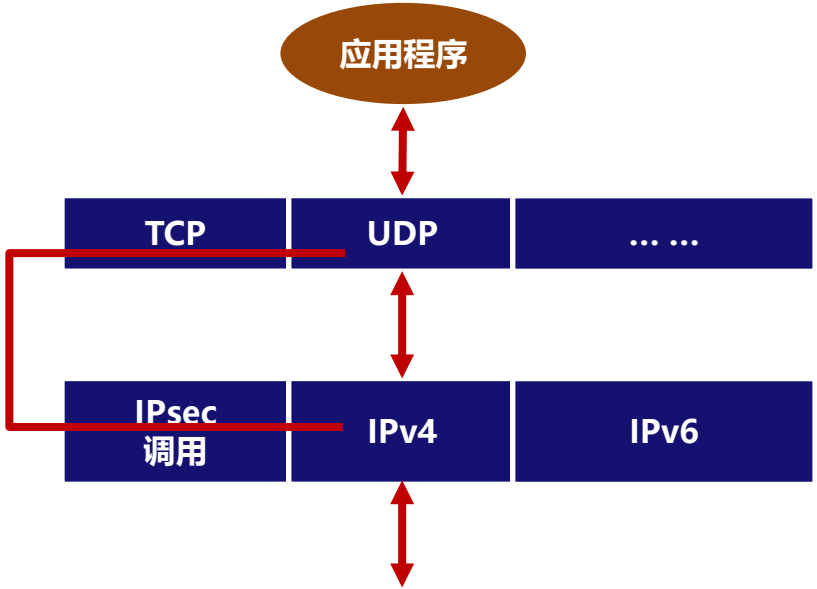
- IPsec协议模式：
  - 传输：提供对高层协议数据的保护
  - 隧道：提供对IP数据报的保护

安全策略

IPSec协议流程

- IPsec协议流程就是依托安全策略对IP数据报进行安全处理和验证的过程





安全策略

- IPSec协议流程：丢弃、应用IPsec、绕过IPsec
  - 外出处理
    - 丢弃数据报。
    - 绕过IPsec给数据报添加IP头，然后发送。
    - 应用IPsec查询SAD，确定是否存在有效的SA。
  - 进入处理
    - 在收到一个数据报后，首先查询SAD。如得到有效的SA，则查询为该数据报提供的安全保护是否与策略要求的相符。

提纲

一、IPSec协议概述

二、ISAKMP协议

三、ISAKMP协议报文及载荷

二 ISAKMP协议通用框架

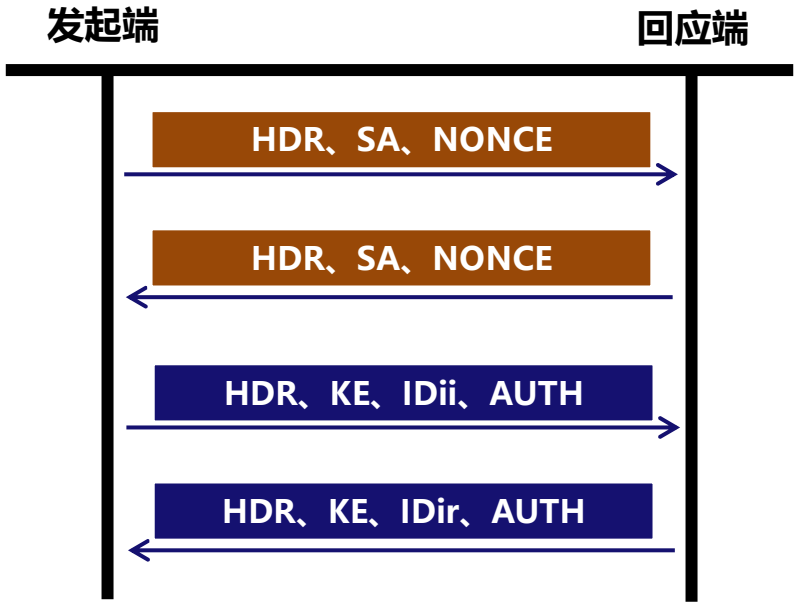
- 互联网安全关联与密钥管理协议（Internet Security Association and Key Management Protocol，ISAKMP)
  - 一种应用层协议，基于UDP，利用端口500
  - IPsec协商的目标：通信对等端身份认证、协商SA及生成共享的会话密钥。
    - 1）定义了通信对等端身份认证、安全关联的创建和管理以及密钥生成技术；
    - 2）定义了建立、协商、更改和删除SA的步骤及报文格式；
    - 3）定义了密钥交换和认证载荷。
- ISAKMP的协商过程包括两个阶段
  - 第一阶段协商获取ISAKMP SA，用以保护第二阶段的协商过程
  - 第二阶段协商获取安全协议SA，用于保护通信数据。

二 ISAKMP协议

- 协商与交换
  - 基本交换
  - 身份保护交换
  - 只有认证的交换
  - 野蛮交换
  - 通知交换
- 报文信息
  - HDR表示报文首部、SA表示安全关联、NONCE表示随机数、IDii表示发起端身份；IDir表示接收方身份；AUTH表示认证信息。

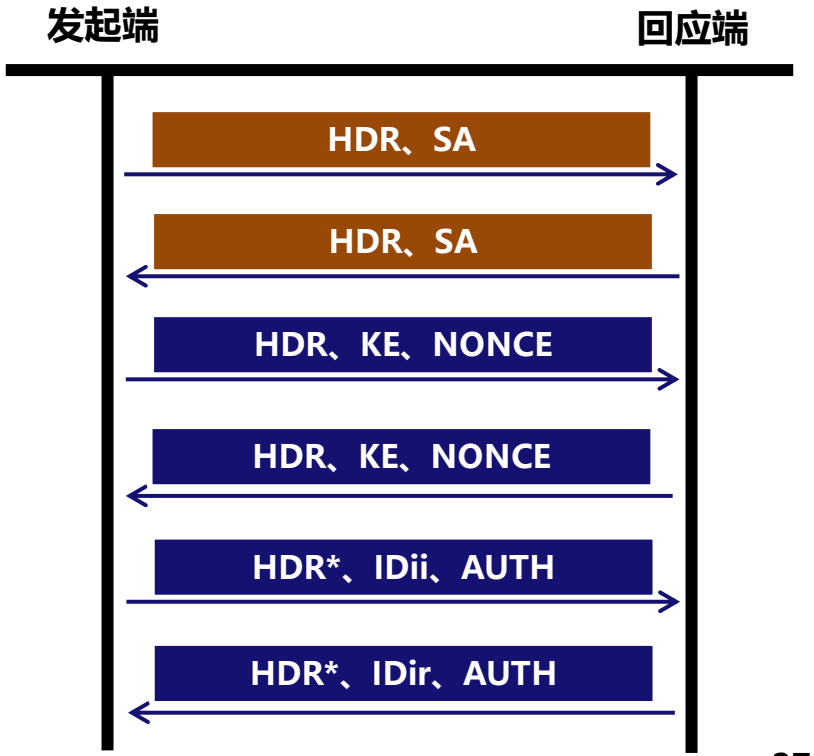
二 协商与交换

- 基本交换
  - 开始ISAKMP协商
  - 协定基本SA
  - 回应端生成密钥，验证发起端身份
  - 发起端验证回应端身份，生成密钥



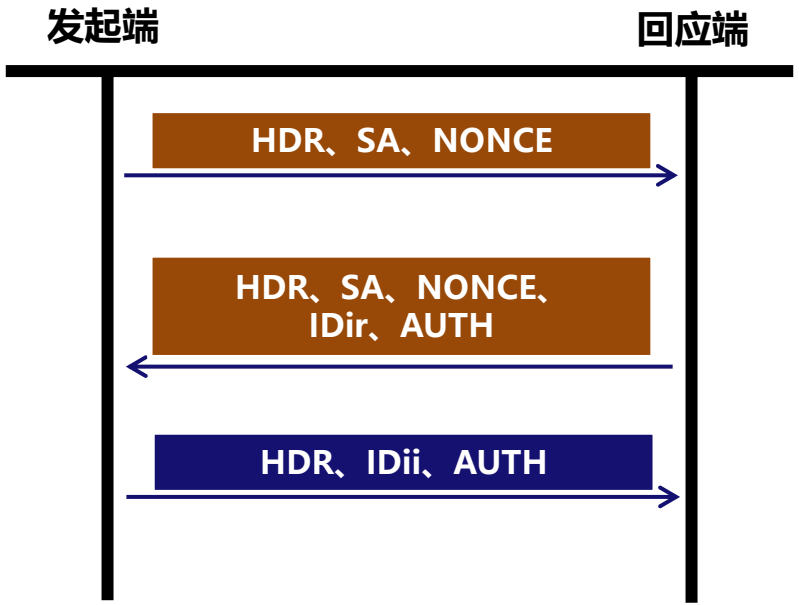
二 协商与交换

- 身份保护交换
  - 开始ISAKMP协商
  - 协定基本SA
  - 回应端生成密钥
  - 发起端生成密钥
  - 回应端验证发起端身份
  - 发起端验证回应端身份



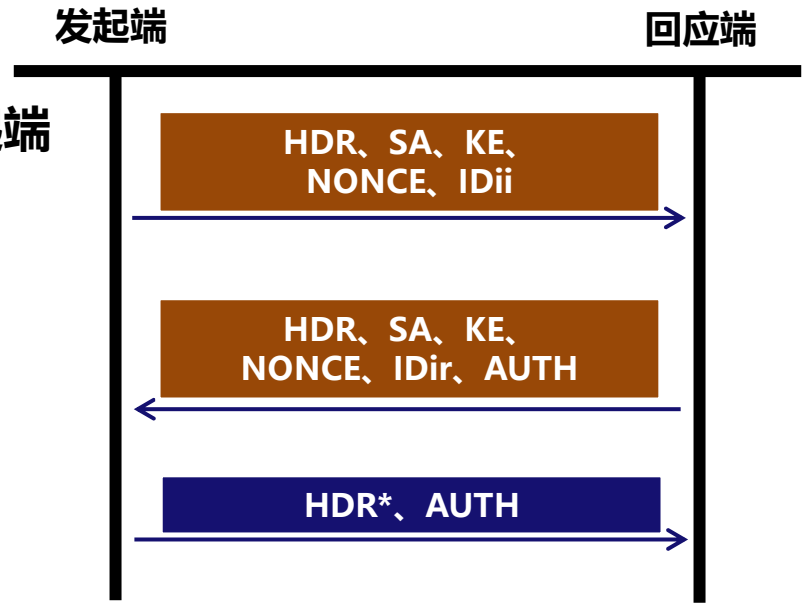
二 协商与交换

- 只有认证的交换
  - 开始ISAKMP协商
  - 协定基本SA，发起端认证回应端身份
  - 回应端认证发起端身份



二 协商与交换

- 野蛮交换
  - 开始ISAKMP协商，回应端生成密钥
  - 协定基本SA，发起端生成密钥；发起端认证回应端身份
  - 回应端认证发起端身份



二 协商与交换

- 通知交换
  - "N/D"表示通知/删除
  - 单向通知机制
    - 如果某一方发现有差错发生，需使用这种交换通告对等端；
    - 用于SA管理，例如当通知对等端删除某个SA时，需利用这种交换。

提纲

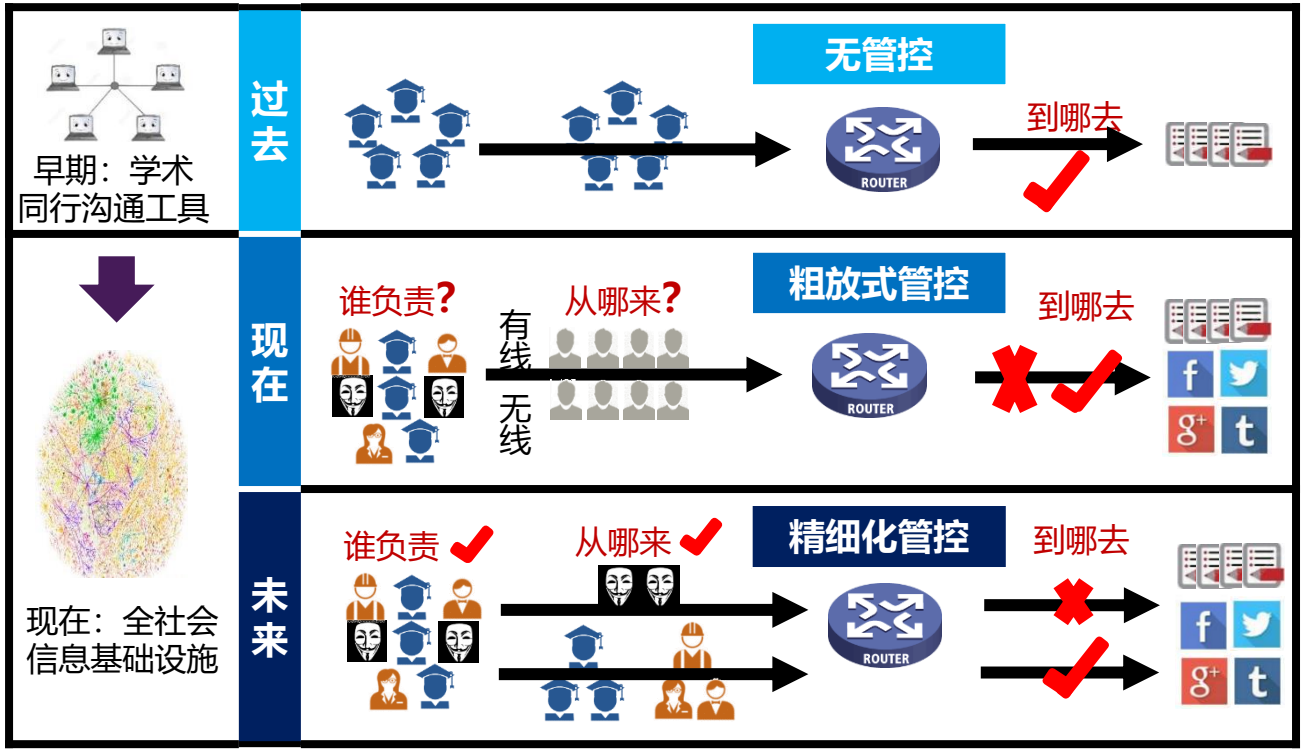
一、IPSec协议概述

二、ISAKMP协议

三、地址驱动的网络安全管控结构

三 IPv6安全管控现状

- 体系结构缺乏安全可信基础，不能适应环境的巨变



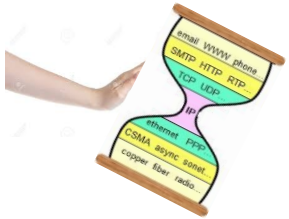
三 研究现状

提升互联网安全可信两个思路

“有病治病”
可信基础缺失，
仅能打补丁式解决安全漏洞

“增强体质”
体系结构
解决安全可信主要根源

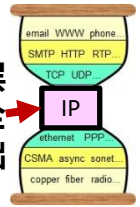
推倒重来



重新设计：NDN、XIA
缺点：代价高、难部署

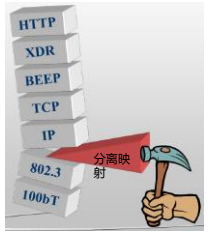
平滑革新

IP核心层
提升安全
可信基础



探索开放互通
与安全管控的
最大公约数

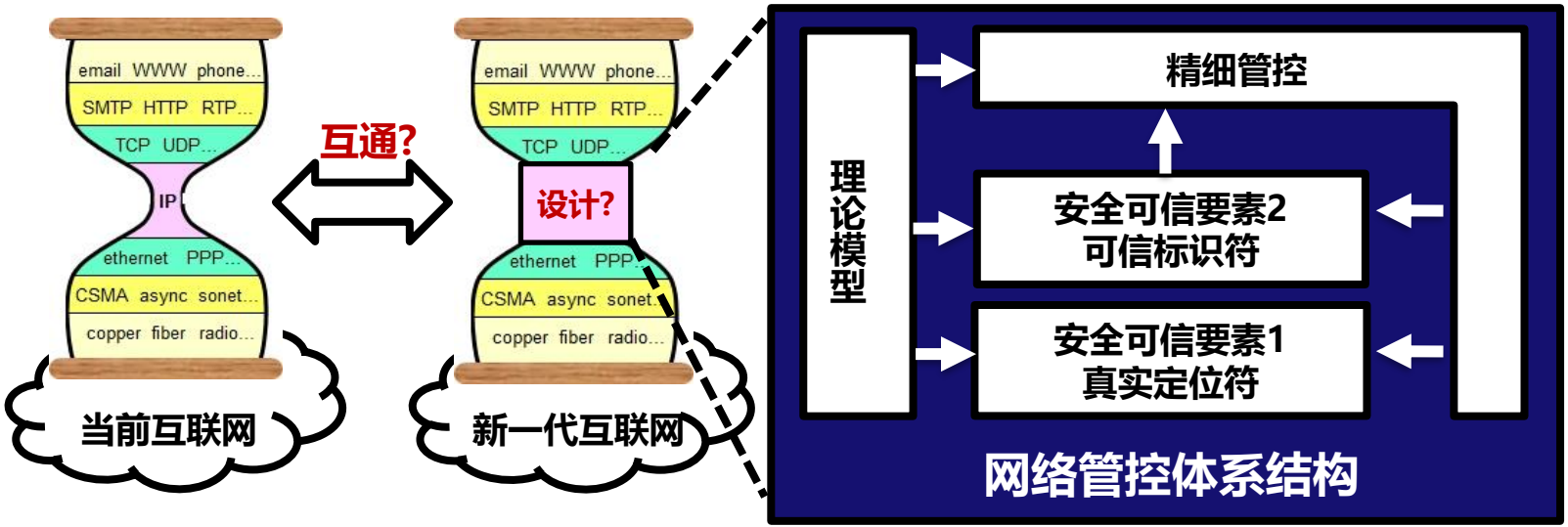
割裂封闭



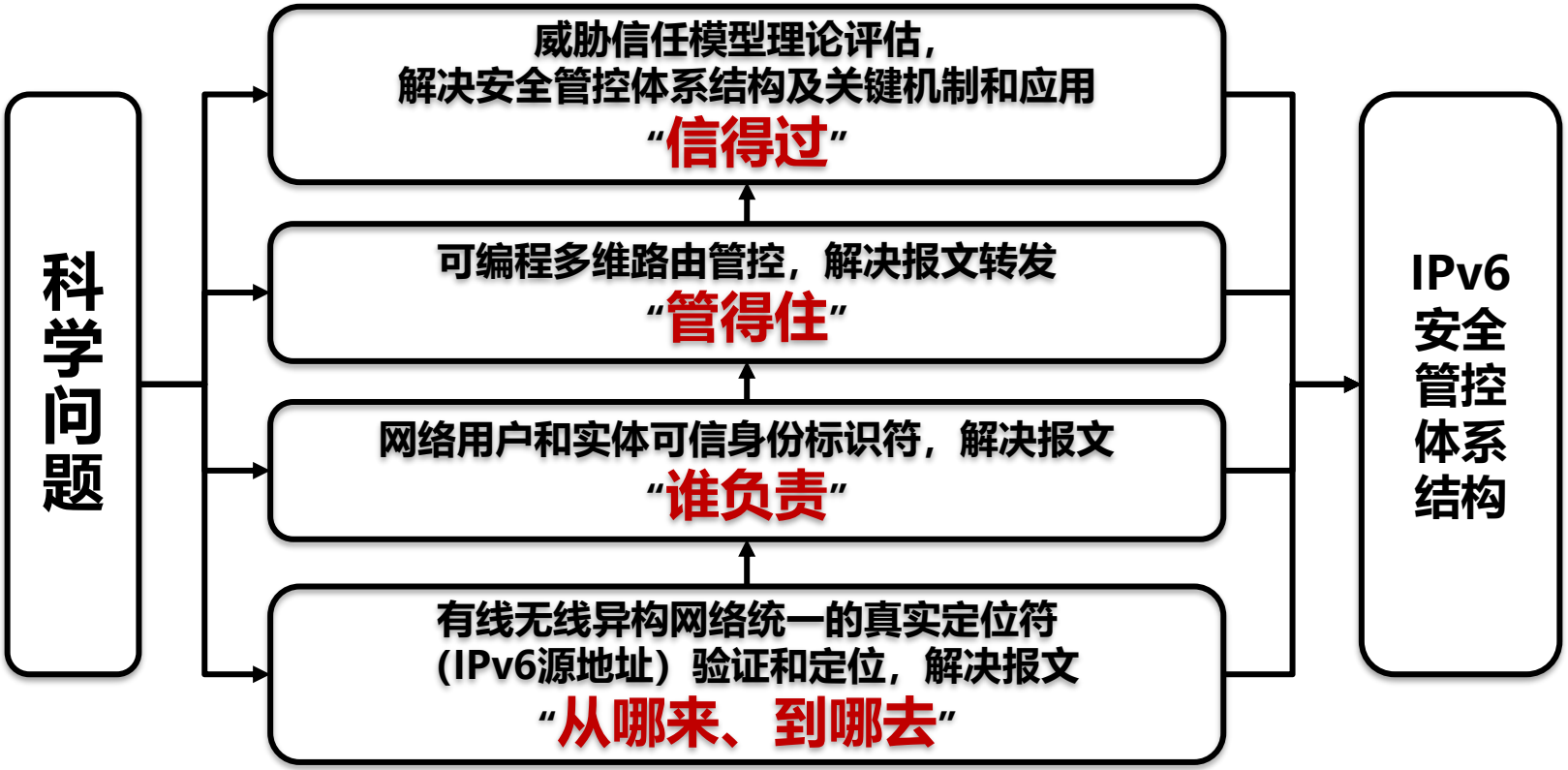
分离映射：LISP、MF
缺点：破坏互通，
较适于专网

三 科学问题

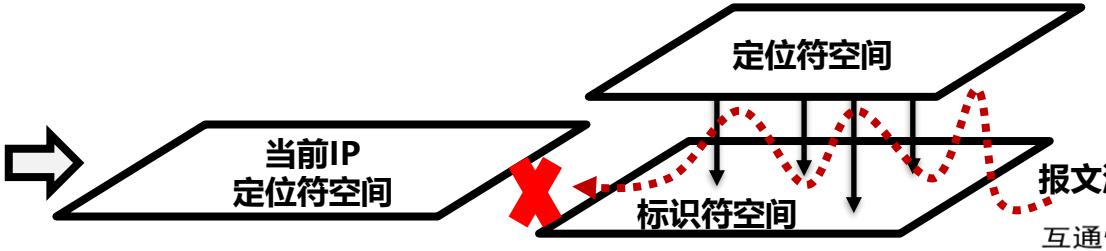
- 科学问题：如何保持互联网体系结构基本模型不变，解决**可信基础要素缺失**，构建网络安全管控体系结构
- 难点：既**安全管控**，又保证**开放互通**



三 重点内容


科学问题
威胁信任模型理论评估，
解决安全管控体系结构及关键机制和应用
“信得过”
可编程多维路由管控，解决报文转发
“管得住”
网络用户和实体可信身份标识符，解决报文
“谁负责”
有线无线异构网络统一的真实定位符
(IPv6源地址）验证和定位，解决报文
“从哪来、到哪去”
IPv6安全管控体系结构

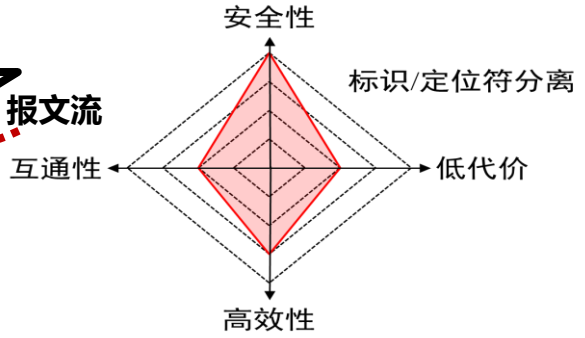
三 技术路线选择

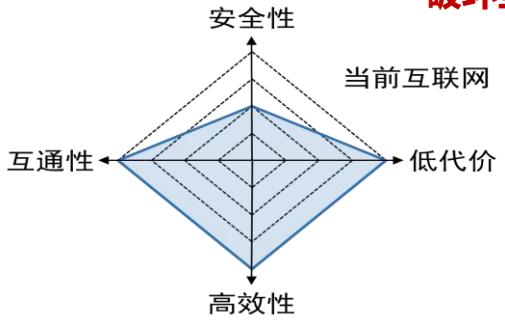


破坏互通

割裂封闭

重新设计标识符空间
分离/映射/封装/解封装

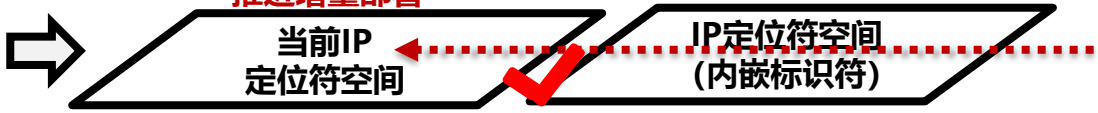




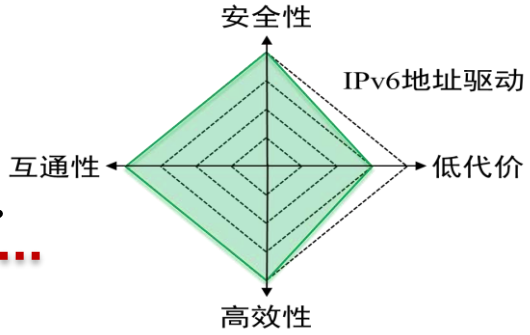
平滑革新

遵循标准地址格式语法
增加管控标识符的语义

通过国际标准
推进增量部署



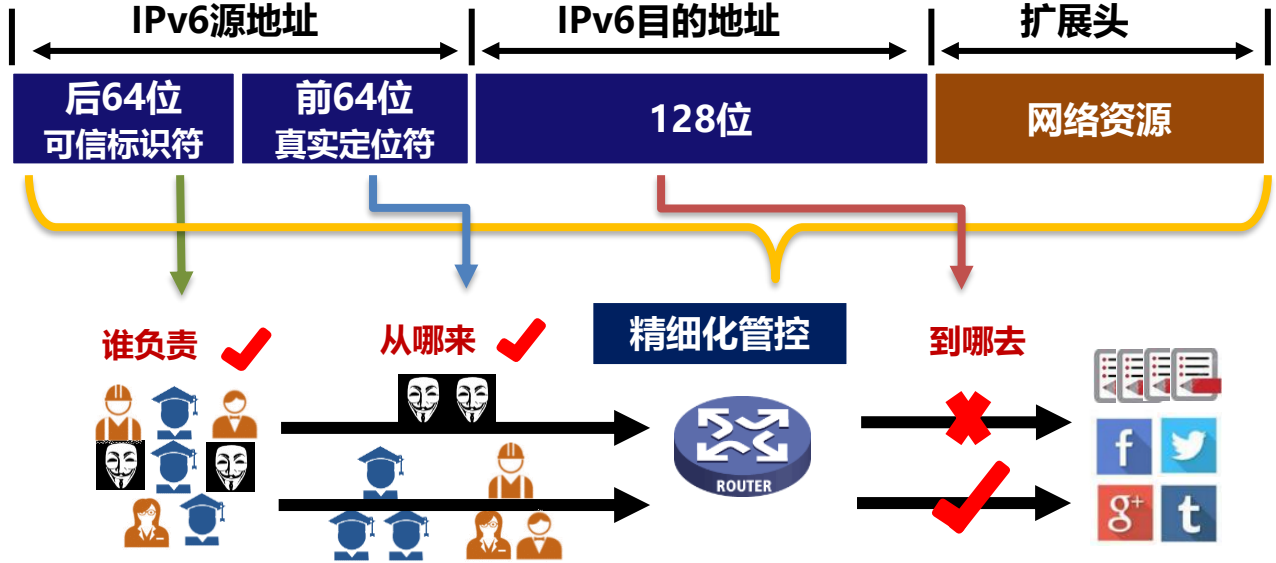
保持互通



三 技术路线核心思想：IPv6地址驱动

技术机遇：全球唯一、空间巨大的IPv6地址（定位符），可成为信任锚点

- IPv6源地址真实 管控基础（从哪来）
- 嵌入地址的身份可信管控 核心（谁负责）
- 基于地址的多维路由管控 手段（管得住）



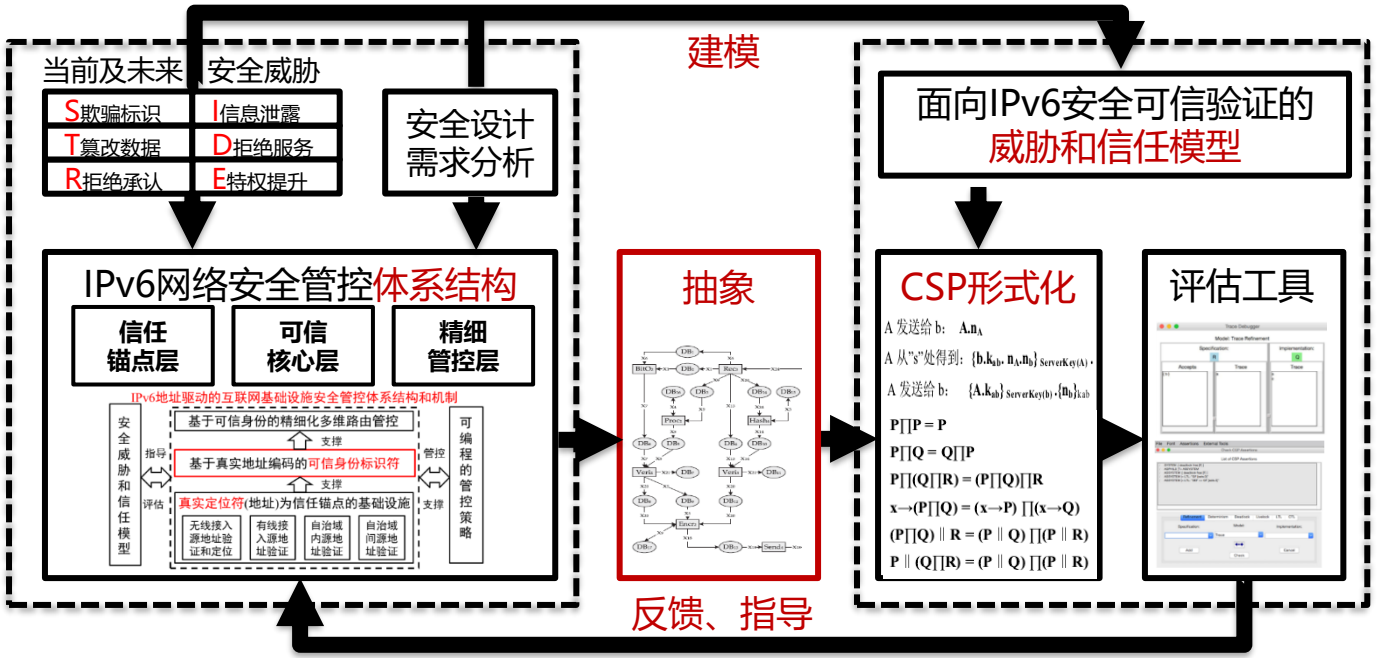
IPv6安全管控体系结构和模型

平滑革新

保持互联网体系结构基本模型的基础上，提升安全可信基础要素，达到兼顾开放互通与安全管控

理论支撑

利用抽象建模、通信顺序进程CSP语言等形式化方法，理论验证指导体系结构的安全可信



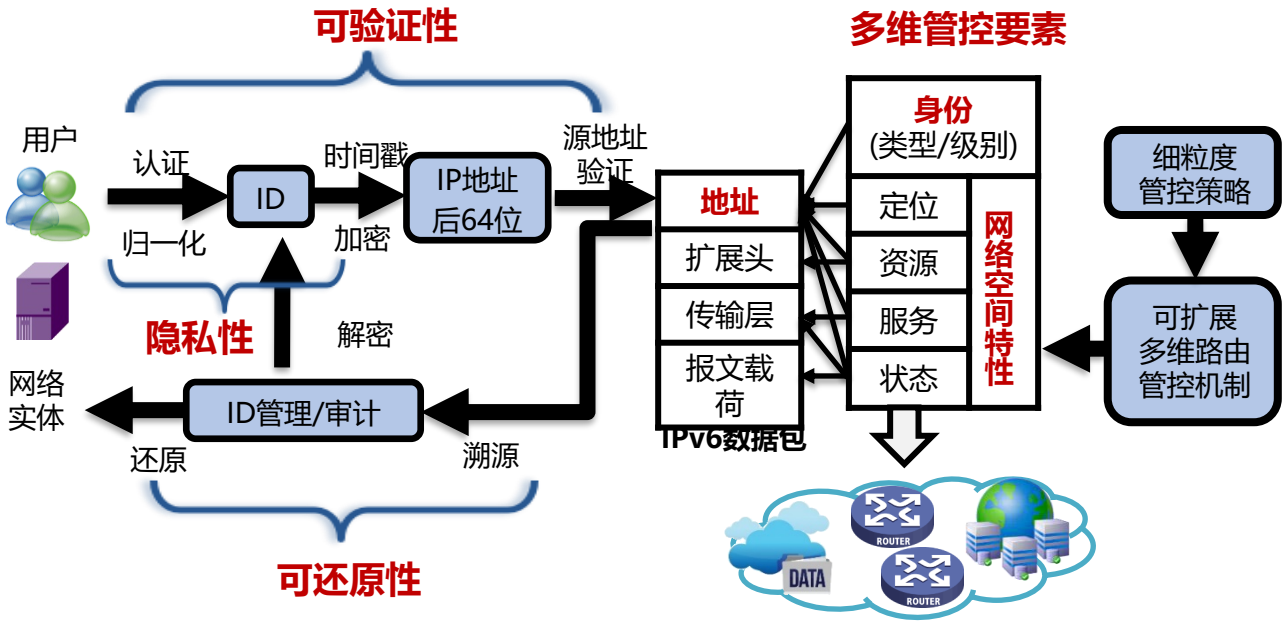
三 可信身份标识符和多维路由管控机制

地址语义创新

兼容IPv6地址格式语法，加密生成身份标识符语义，兼顾身份可验证性、隐私性和可还原性

路由与管控有机结合

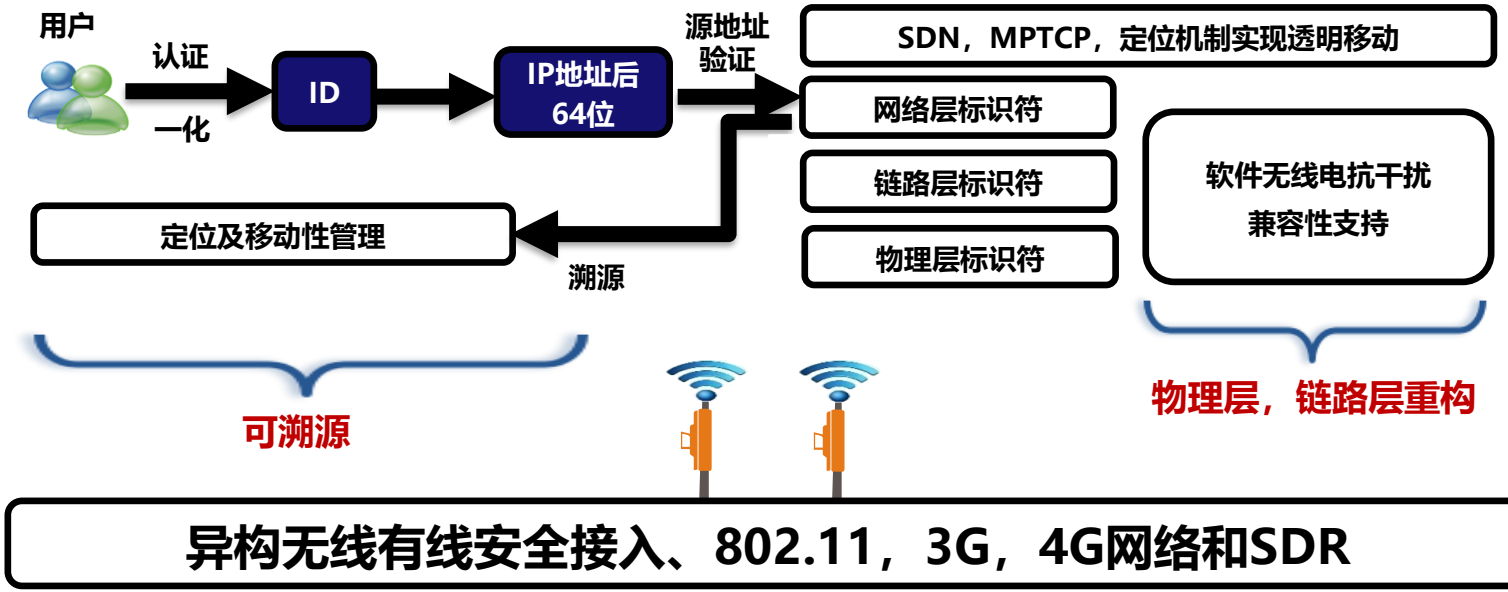
路由策略内嵌报文携带的可信身份等多维管控要素，变粗放管控为精细路由管控



三 有线无线一体化安全接入

跨层协作式的无线异构接入安全可信

- 信息域安全扩展到物理域：IPv6真实地址与无线L2和L1特征结合
- 变被动为主动：IPv6溯源与异构网络无线定位相结合



办公地点：理科大楼B1715

联系方式：17621203829

邮箱：liuhongler@foxmail.com