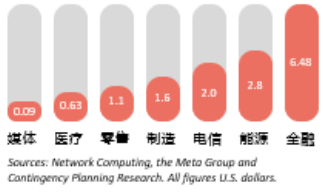
网络管理协议介绍

- 随着人工智能、大数据、云计算等新技术快速发展，未来各行业将面临数字化转型，企业业务随着数字化转型也变得丰富多样，使网络管理成为网络管理员面临的最具挑战的问题之一。我们无法仅依赖人手工来完成整个的网络管理的工作，迫切的需要一种自动化和智能化的工具协助我们管理网络中的设备和资源。
- 本次课程，将简要介绍网络管理的发展历程及网络管理的相关概念，同时会着重介绍网络管理中使用到的不同的协议以及它们的使用场景。最后，简要介绍网络管理的典型应用案例。

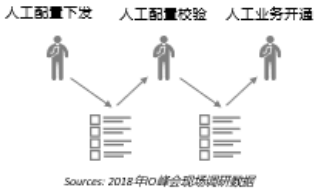
- 随着互联网产业的飞速发展，网络面临巨大变革，多业务融合成为未来网络的主流趋势。网络的融合需要管理的融合，统一网管能实现多业务、多设备的统一集中管理。

传统网络管理面临的挑战

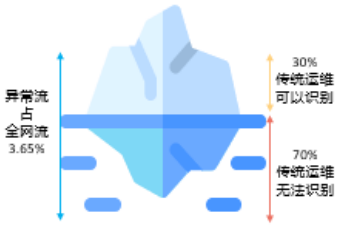
网络规模大、业务开通慢、排障效率低



故障损失
每小时停机损失百万美元



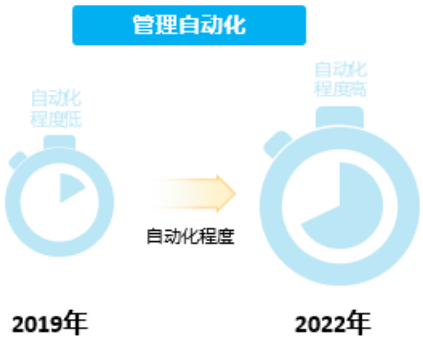
业务开通慢
>70%的网络通过CLI方式管理网络



故障定位难
一个故障定位平均耗时76min

- 人工智能、大数据、云计算等新技术正在快速发展，未来十年各行业将面临数字化转型，企业业务随着数字化转型也变得丰富多样。因此，数字化带来网络模型的变化，传统的网络管理模式已经不能适应数字化业务带来的新需求。传统网络的建设、管理和运维手段已无法满足数字化带来的新的网络需求。

网络管理的发展趋势



通过在线的网规、部署、优化和巡检工具，实现本地网络免管理，可以有效降低OPEX。

网络故障提前预警，故障解决更快，降低业务损失，潜在故障识别率大幅提升。

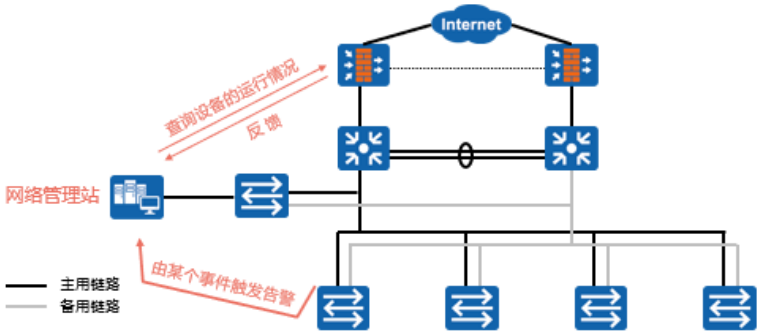
- OPEX（Operating Expense，运营支出）：指企业运行付出的各种支出成本，包括维护费用、营销费用、人工成本以

及折旧。

- 根据行业知名分析机构在 2019 年 4 月发布的关于 AI 和自动化提高网络可靠性的报告中指出，到 2022 年，将会有 65%的企业在园区网络部署网络自动化技术，而今天这个比例只有 17%。
- 管理自动化：正如家用洗衣机一样，从手动到半自动，到今天的全自动甚至是智能洗衣，让人人都能操作一个复杂的机器完成复杂的任务。对于网络管理也是如此，从基于命名行的逐台设备的配置与管理，到基于图形化界面的管理控制系统，到今天基于业务语言对网络进行自动化配置。从网络管理的视角，企业网络管理将几乎 1/3 的时间花费在网络的规划、部署上。未来网络自动化有两个层面：
- 全生命周期的自动化：包括自动化工具是否能从网络的规划、部署、策略发放、网络状态监测和维护以及管理的全生命周期，均实现自动化。
- 整网自动化：包括企业的 LAN、WLAN、以及 WAN 网络是否能够进行集中式地管理和策略配置，是否能从全局视角定义基于用户身份和应用类型的业务策略。
- 运维智能化：智能化是网络管理运维的更高级别能力。以前，网络运维工作很简单，主要关注网络和设备的 KPI 指标，无法感知用户体验和业务质量。而今天，网络连接的质量直接影响到了业务的质量，从而影响了企业的运作效率。甚至在部分工业和生产场景，因不同业务的需要，网络质量有了差异化的要求，每终端的带宽、时延、丢包、无线漫游的切换时间仅依托以网元为中心的运维系统是无法完成如此复杂的工作。这就像医生为了检测病人，需要采用更为先进的机器。

什么是网络管理?

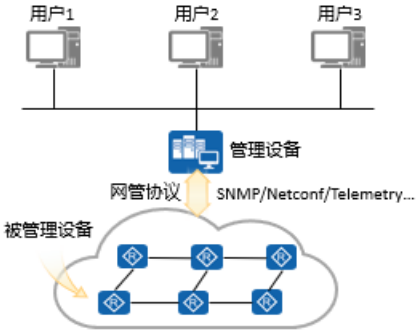
- 网络管理，简单地说是对网络的管理，是一个网络的基本诉求。当前，用户能够通过各种协议、工具、应用或设备来实现对网络的管理，其管理对象包括网络中的硬件及软件。
- 网络管理的目标是实现对网络软硬件的监控、测试、配置、分析、评价及控制等，确保网络运行正常。

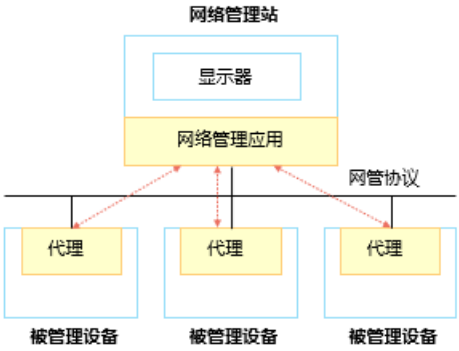


网络管理的典型架构

通常情况下，网络管理系统具有相同的基本体系结构。该体系结构包含两个关键元素：

- 管理设备，也被称为网络管理站。
- 被管理设备，也被称为代理设备。





网络管理的四大模型

OSI 网络管理模型由四个主要的模型组成:

- 组织结构模型(Organization Model)：描述网络管理系统组件的功能和基础架构。
- 信息模型(Information Model)：描述被管理对象及其关系的信息库。
- 通信模型(Communication Model)：描述管理者与被管理

者之间交换信息的方式。

- 功能模型(Functional Model)：包括配置管理、性能管理、故障管理、安全管理和计费管理五个功能区域。

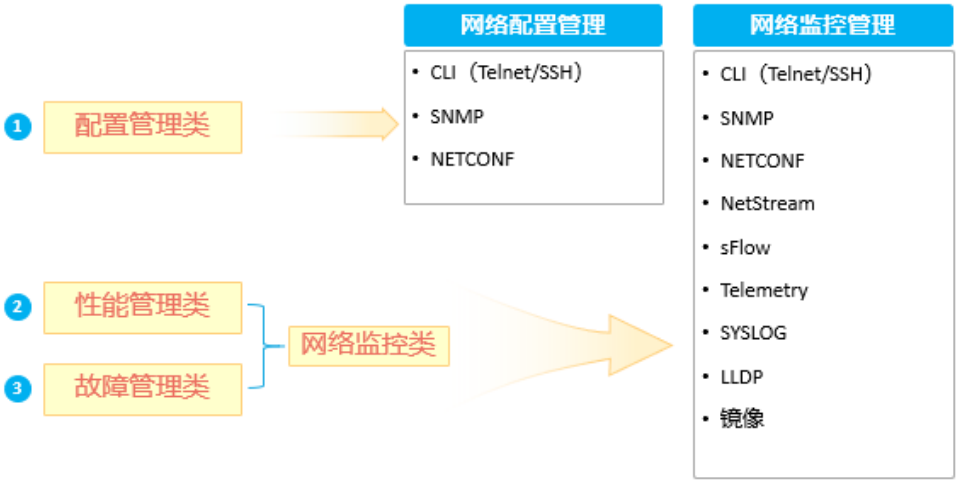
- 组织结构模型定义管理者，代理和被管理对象。 它描述了网络管理系统的组件，组件的功能和基础架构。
- 信息模型与信息结构和存储有关。 它指定用于描述被管理对象及其关系的信息库。 管理信息结构（SMI）定义了存储在管理信息库（MIB）中的管理信息的语法和语义。 代理进程和管理器进程都使用 MIB 进行管理信息交换和存储。
- 通信模型处理代理与管理者之间以及管理者之间交换信息的方式。 通信模型中包含三个关键元素：传输协议，应用程序协议和要传达的实际消息。
- 功能模型包括网络管理的五个功能区域：配置管理、性能管理、故障管理、安全管理和计费管理。

- OSI 定义网络管理的五大功能模型。
- 配置管理（Configuration Management）：
- 配置管理涉及初始化网络，提供网络资源和服务以及监

视和控制网络。 更具体地说，配置管理的职责包括在网络运行期间设置，维护，添加和更新组件之间的关系以及组件的状态。

- 配置管理包括设备配置和网络配置。设备配置可以在本地或远程执行。 自动化的网络配置，例如动态主机配置协议（DHCP）和域名服务（DNS）在网络管理中发挥关键作用。
- 性能管理（Performance Management）：
- 性能管理与评估和报告被管理网络对象的行为和有效性有关。 网络监视系统可以测量和显示网络状态，例如收集有关流量，网络可用性，响应时间和吞吐量的统计信息。
- 故障管理（Fault Management）：
- 故障管理涉及检测，隔离和纠正可能导致OSI网络故障的异常操作。 故障管理的主要目标是确保网络始终可用，并在发生故障时尽快将其修复。
- 安全管理（Security Management）：
- 安全管理可以保护网络和系统免受未经授权的访问和安全攻击。 安全管理机制包括身份验证，加密和授权。 安全管理还涉及加密密钥以及其他与安全相关的信息的生成，分发和存储。 安全管理可以包括提供实时事件监视和事件日志的安全系统，例如防火墙和入侵检测系统。
- 计费管理（Accounting Management）：
- 计费管理可以计量被管理对象的使用费用，并确定这种使用的成本。 该度量可能包括消耗的资源，用于收集会计数据的设施以及为客户使用的服务设置计费参数，维护用于计费目的的数据库，以及准备资源使用情况和计费报告。

网络管理概览

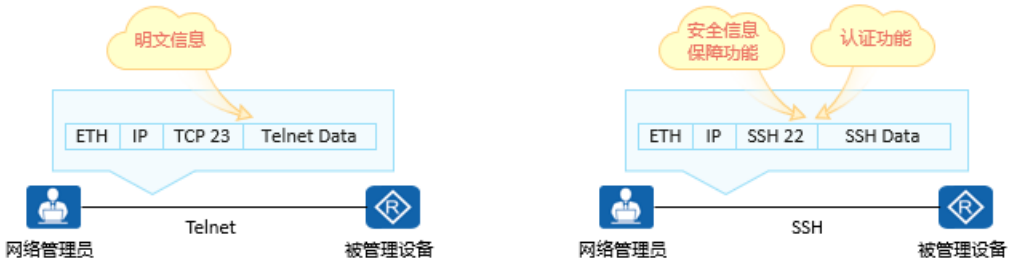


- CLI（Command-Line Interface，命令行界面）既可以支持网络配置管理，也可以支持网络监控管理。
- SNMP（Simple Network Management Protocol，简单网络管理协议）的 Set 功能可以支持网络配置管理，Trap 功能可以支持网络监控管理。
- NETCONF（Network Configuration Protocol，网络配置协议）的 Edit 功能可以支持网路配置管理，Get 功能可以支持网络监控管理。

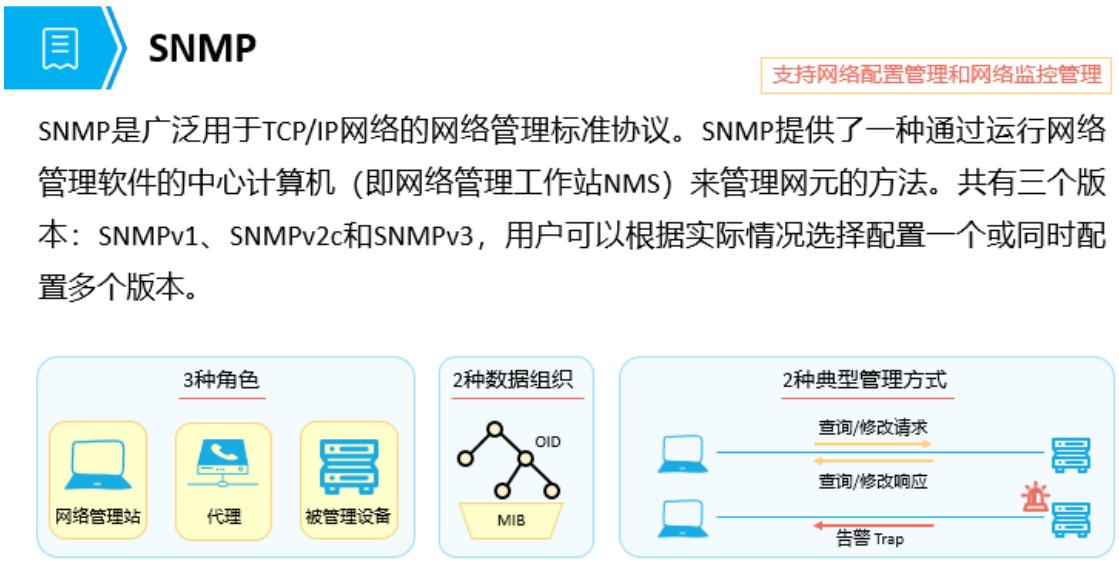
CLI（Telnet/SSH）

支持网络配置管理和网络监控管理

CLI是在图形用户界面得到普及之前使用最为广泛的用户界面，它通常不支持鼠标，用户通过键盘输入指令，设备接收到指令后，予以执行。



- 网络管理员可以采用 CLI 对设备进行配置和网络监控，操作简单便捷，一旦进行大规模部署，就必须借助于自动化工具来进行批量配置。
- Telnet 是电信（Telecommunications）和网络（Networks）的联合缩写。
- Telnet 使用专用的 TCP 端口号 23，它不是一种安全通信协议，通过网络/互联网传输明文格式的数据，包括密码。
- Telnet 中没有使用任何验证策略及数据加密方法。
- SSH（Secure Shell，安全外壳）
- SSH 使用专用的 TCP 端口号 22，它是一种非常安全的协议，通过网络/互联网传输加密格式的数据，一旦经过加密就极难解压和读取该数据。
- SSH 还使用公钥用于对访问者的用户身份验证，这种方式提供了更高的安全性。
- Telnet 和 SSH 是两种远程管理设备的方式，其中 SSH 连接方式较 Telnet 更为安全，因此目前网络都会要求部署 SSH。



- 网络管理站（Network Management Station，NMS）向被管理设备发送各种查询报文，以及接收被管理设备发送的

告警。

- 被管理设备（Devices）

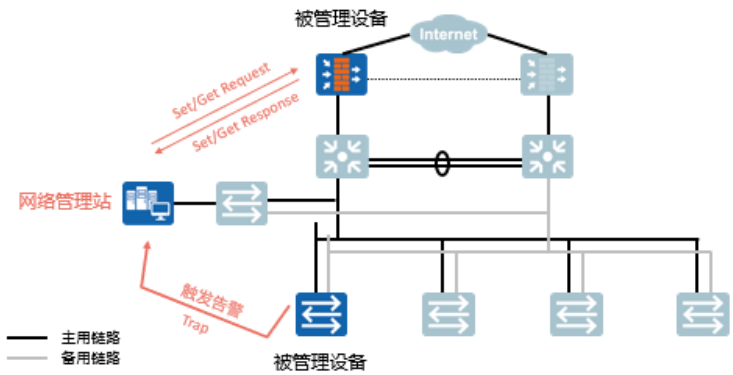
也就是网络中的各种接受网管的设备。

- 代理（Agent）

驻留在被管理设备上的一个进程。Agent 的作用如下：

- 接收、解析来自网管站的查询报文。
- 根据报文类型对管理变量进行 Read 或 Write 操作，并生成响应报文，返回给网管站。
- 根据各协议模块对告警触发条件的定义，当发生某个事件（如端口 UP/DOWN，STP 拓扑变更、OSPF 邻居关系 DOWN 掉等）的时候，主动触发一个告警，向网管站报告该事件。
- MIB（Management Information Base ）是一个数据库，指明了被管理设备所维护的变量（即能够被 Agent 查询和设置的信息）。MIB 在数据库中定义了被管理设备的一系列属性：对象的名称、对象的状态、对象的访问权限和对象的数据类型等。
- OID（Object IDentifier）：MIB 是以树状结构进行存储的，树的节点表示管理对象 Object，对象可以用从根 Root 开始的一条路径来唯一的识别，这就是 OID 也即对象标示符

SNMP的应用场景



在网络管理站中配置SNMP管理程序，在被管理设备端启用Agent代理程序，同时在组网中配置SNMP协议。

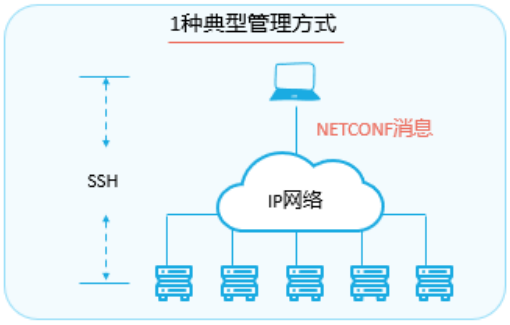
通过SNMP协议：

- 网络管理站可以通过Agent获取或变更设备的信息，实现远程监控和管理。
- Agent可以及时地向网络管理站报告设备的状态。

NETCONF

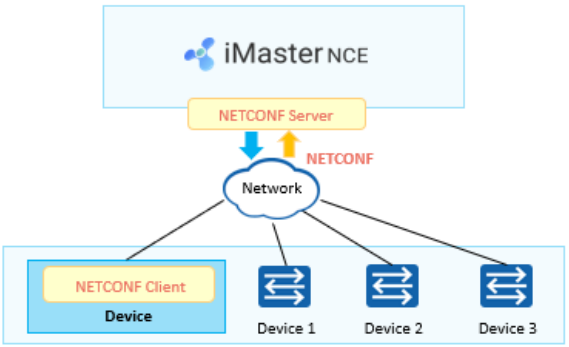
支持网络配置管理和网络监控管理

NETCONF是一种基于XML的网络配置协议，它存在的目的在于用可编程的方式实现网络配置的自动化，从而简化、加速网络服务地部署。



- NETCONF 使用 SSH 实现安全传输，使用 RPC(Remote Procedure Call)远程调用的机制实现客户端和服务端的通信。
- NETCONF 消息以 XML 格式呈现。

NETCONF的应用场景



NETCONF的优势：

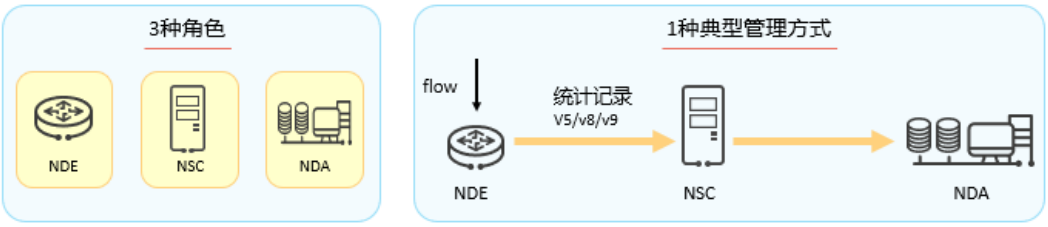
- 可扩展性强，数据结构化、协议标准化。
- 采用分层框架，丰富的协议操作。
- 支持多个配置库，实现事务机制验证回滚。
- 能够分别获取配置数据和状态数据，并且可以跨设备的比较。
- 支持网络级的业务配置能力，支持网络级配置事务。
- 支持配置备份和恢复。

- NETCONF 提供一套管理网络设备的机制。用户可以使用这套机制增加、修改、删除、备份、恢复、锁定、解锁网络设备的配置，同时还具备事务和会话操作功能，从而来获取网络设备的配置和状态信息。

NetStream

支持网络监控管理

- NetStream技术是一种基于网络流信息的统计技术，可以对网络中的业务流量情况进行统计和分析。在网络的接入层、汇聚层、核心层上，都可以通过部署NetStream。
- NetStream支持IP报文（UDP、TCP、ICMP报文）和MPLS报文的统计。

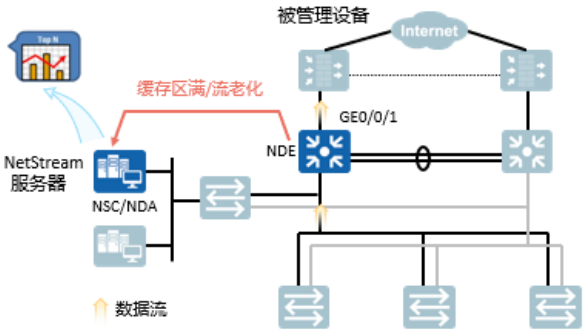


- 一个典型的 NetStream 系统由网络流数据输出器（NetStream Data Exporter, NDE）、网络流数据收集器（NetStream Collector, NSC）和网络流数据分析器（NetStream Data Analyzer, NDA）三部分组成。
- NDE：负责对网络流进行分析处理，提取符合条件的流进行统计，并将统计信息输出给 NDA（NetStream Data Analyzer）设备。 输出前也可对数据进行一些处理， 比如聚合。配置了 NetStream 功能的设备在 NetStream 系统中担当 NDE 角色。
- NSC：通常为运行于 Unix 或者 Windows 上的一个应用程序，负责解析来自 NDE 的报文，把统计数据收集到数据库中，可供 NDA 进行解析。 NSC 可以采集多个 NDE 设备输出的数据，对数据进行进一步的过滤和聚合。
- NDA：是一个网络流量分析工具，它从 NSC 中提取统计数据，进行进一步的加工处理，生成报表，为各种业务提供依据（比如流量计费、网络规划，攻击监测）。通常， NDA 具有图形化用户界面，使用户可以方便地获取、显示和分析收集到的数据。
- NetStream 流输出方式：
- 原始流输出方式：在流老化时间超时后，每条流的统计

信息都要输出到 NSC。原始流输出方式的优点是：NSC 可以得到每条流的详细统计信息。

- 聚合流输出方式：聚合流输出方式是指设备对与聚合关键项完全相同的原始流统计信息进行汇总，从而得到对应的聚合流统计信息。通过对原始流进行聚合后输出，可以明显减少网络带宽。

NetStream的应用场景



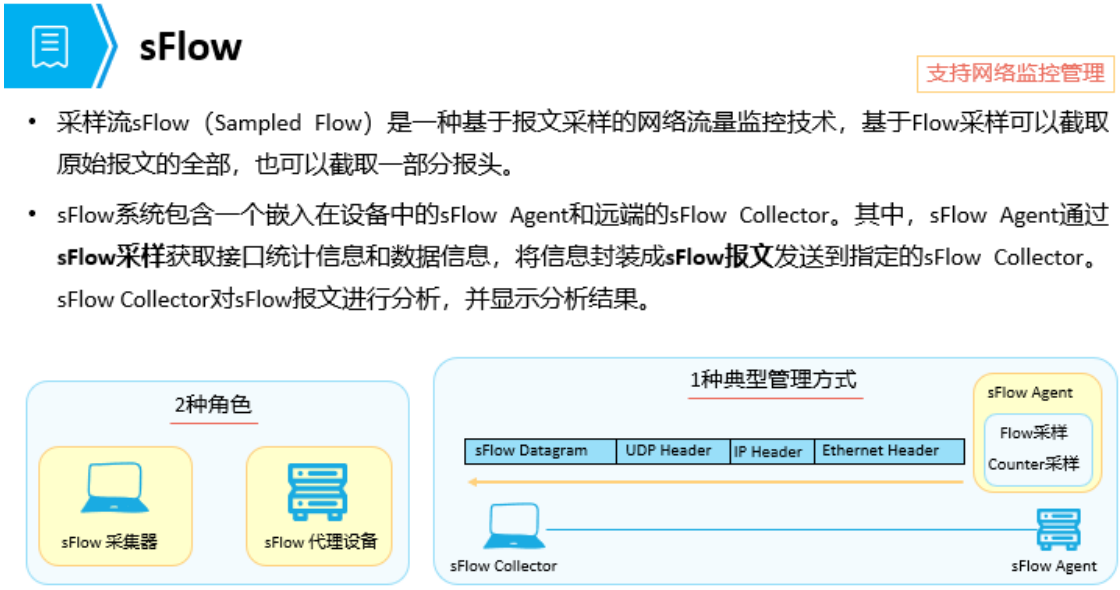
NetStream工作过程：

- 配置了NetStream功能的设备（即NDE）把采集到的关于流的详细统计信息定期发送给NSC。
- 信息由NSC初步处理后发送给NDA。
- NDA对数据进行分析，以用于计费、网络规划等应用。

- 在实际的应用中，NSC 和 NDA 一般集成在一台 NetStream 服务器上。NDE 通过 NetStream 采样获取 GE0/0/1 接口出方向流量信息，并按照一定条件建立 NetStream 流，当 NetStream 缓存区已满或者 NetStream 流达到老化时间，NDE 会将统计的信息封装成 NetStream 报文发送到 NetStream 服务器。NetStream 服务器对 NetStream 报文进行分析处理，并显示分析结果。
- 传统的流量统计的实现方法和局限性：
- 基于 IP 报文计数：统计的信息简单，无法针对多种信息进行统计。
- 使用 ACL：要求 ACL 的容量很大，对于 ACL 规则以外的流没有办法统计。
- SNMP 协议：功能不强。要不断的通过轮询向网管查询，

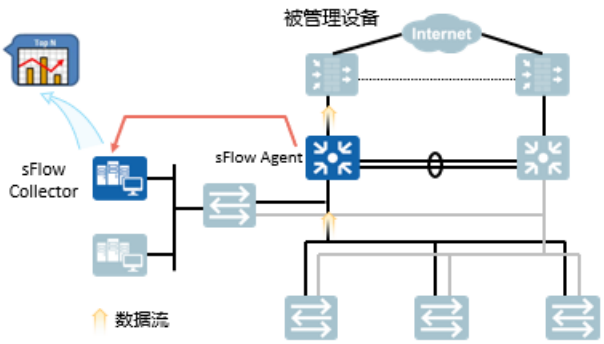
浪费 CPU 和网络资源。

- 端口镜像：成本高，同时消耗设备的一个接口，对于无法镜像的端口无能为力。
- 物理层复制：成本高，同时还需要购买专用的硬件设备。



- Flow 采样是 sFlow Agent 设备在指定接口上按照特定的采样方向和采样比对报文进行采样分析，用于获取报文数据内容的相关信息。该采样方式主要是关注流量的细节，这样就可以监控和分析网络上的流行为。
- Flow 采样可以截取原始报文的全部，也可以截取一部分报头。
- Counter 采样是 sFlow Agent 设备周期性的获取接口上的流量统计信息，Counter 采样支持获取的采样信息。与 Flow 采样相比，Counter 采样只关注接口上流量的数量，而不关注流量的详细信息。

sFlow的应用场景



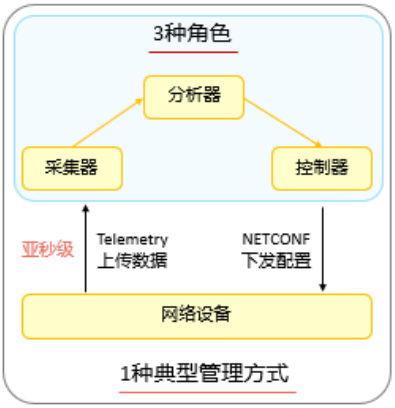
企业网用户对于接口的流量情况、整体设备运行情况有明确的需求。企业用户更需要一种以设备接口为基本采样单元的流量监控技术来实时监控流量状况，及时发现异常流量以及攻击流量的源头，从而保证企业网络的正常稳定运行。sFlow关注的是接口的流量情况、转发情况以及设备整体运行状况，适合于网络异常监控以及网络异常定位，特别适合于企业网用户。

- 如图所示，只需要在支持 sFlow Agent 的设备上进行部署，远端连接一个 sFlow Collector，就可以对流量进行基于接口的搜集和详细的分析。
- 使用 NetStream 也可以对网络流量进行统计分析， 而 NetStream 是一种基于网络流信息的统计技术，网络设备自身需要对网络流进行初步的统计分析，并把统计信息储存在缓存区，当缓存区满或者流统计信息老化后输出统计信息。 与 NetStream 相比， sFlow 不需要缓存区，网络设备仅进行报文的采样工作，网络流的统计分析工作由远端的采集器完成。
- sFlow 与 NetStream 比较具有以下优势：
- 节省资源、降低成本：由于不需要缓存区，对网络设备的资源占用少，实现成本低。
- 采集器灵活、随需的部署：由于网络流的分析和统计工作由采集器完成，采集器可以灵活的配置网络流特征进行统计分析，实现灵活、随需的部署。

Telemetry

支持网络监控管理

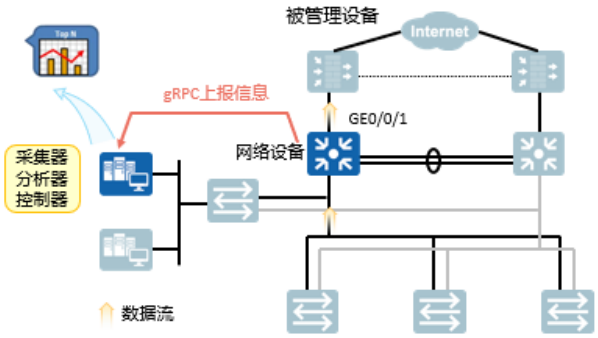
- Telemetry，也称为Network Telemetry，即网络遥测技术。主要用于监控网络，包括报文检查和分析，安全侵入和攻击检测，智能收集数据，应用的性能管理等。
- Telemetry优势：
  - 支持多种实现方式，满足用户的不同需求。
  - 采集数据的精度高，且类型十分丰富，充分反映网络状况。
  - 一次订阅，持续上报。
  - 故障定位更快速、精准。



- 随着网络的普及和新技术的涌现，网络规模日益增大，部署的复杂度逐步提升，用户对业务的质量要求也不断提高。为了满足用户需求，网络运维务必更加精细化、智能化。当今网络的运维面临着如下挑战：
- 超大规模：管理的设备数目众多，监控的信息数量非常庞大。
- 快速定位：在复杂的网络中，能够快速地定位故障，达到秒级、甚至亚秒级的故障定位速。
- 精细监控：监控的数据类型更多，且监控粒度更细，以便完整、准确地反应网络状况，据此预估可能发生的故障，并为网络优化提供有力的数据依据。网络运维不仅需要监控接口上的流量统计信息、每条流上的丢包情况、 CPU 和内存占用情况，还需要监控每条流的时延抖动、每个报文在传输路径上的时延、每台设备上的缓冲区占用情况等。
- 采集器、分析器和控制器都位于网管侧。
- 采集器用于接收和存储网络设备上报的监控数据。
- 分析器用于分析采集器接收到的监控数据，并对数据进行处理，例如以图形化界面的形式展现给用户。
- 控制器通过 NETCONF 等方式向设备下发配置，实现对

网络设备的管理。控制器可以根据分析器提供的分析数据，为网络设备下发配置，对网络设备的转发行为进行调整；也可以控制网络设备对哪些数据进行采样和上报 。

Telemetry的应用场景



基于gRPC的Telemetry技术可以采集设备的接口流量统计、CPU、告警等数据，然后经过Protocol Buffer编码，实时上报给采集器进行接收和存储。

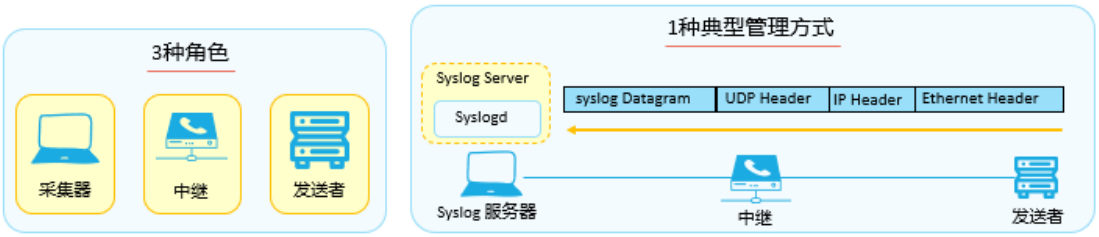
	Telemetry	SNMP Get	SNMP Trap	CLI	SYSLOG
工作模式	推模式	拉模式	推模式	拉模式	推模式
精度	亚秒级	分钟级	秒级	分钟级	秒级

- gRPC（Google Remote Procedure Call， Google 远程过程调用）是 Google 发布的基于 HTTP 2.0 传输层协议承载的高性能开源软件框架，提供了支持多种编程语言的、 对网络设备进行配置和管理的方法。
- 传统的网络监控手段（SNMP、CLI、日志）已无法满足网络需要：
- SNMP 和 CLI 主要采用“拉模式”获取数据，即发送请求来获取设备上的数据，限制了可以监控的网络设备数量，且无法快速获取数据。
- SNMP Trap 和日志虽然采用“推模式”获取数据，即设备主动将数据上报给监控设备，但仅上报事件和告警，监控的数据内容极其有限，无法准确地反映网络状况。
- Telemetry 是一项监控设备性能和故障的远程数据采集技术。它采用“推模式”及时获取丰富的监控数据，可以实现网络故障的快速定位，从而解决上述网络运维问题。

Syslog

支持网络监控管理

- Syslog是一种工业标准的协议，可用来记录设备的日志。在UNIX系统，路由器、交换机等网络设备中，系统日志（System Log）记录系统中任何时间发生的大小事件。管理者可以通过查看系统记录，随时掌握系统状况。
- Syslog协议提供了一种通过IP网络传送事件消息的机制，它允许主机将事件消息通过IP网络传输到接收消息的主机上，这些主机通常称为syslog server。

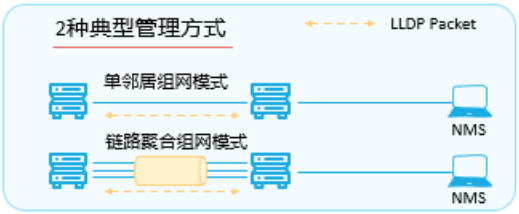


- 该协议从最初的加州大学伯克利分校软件中心整理，后来由于其操作管理的实用性迅速成为很多网络设备操作管理协议的一部分。现在已经有相应的 RFC3164,RFC3195 进行通用的定义。前者定义的是使用 UDP 形式传输，后者定义的是使用 TCP 形式传输。
- 几乎所有的网络设备都可以通过 syslog protocol 将日志信息以 UDP 方式传送到远端服务器，远端接收日志服务器必须通过 syslogd 来监听 UDP Port 514，并且根据 syslog.conf 中的配置来处理本机和接收访问系统的日志信息，把指定的事件写入特定档案中，供后台数据库管理和响应之用。
- 角色分类
- 发送者 sender：产生 syslog message 的网元；
- 中继 relay：能接收到后进行转发 syslog message 的网元或其他设备；
- 收集者 collector：接收了不再转发 syslog message 的 syslog server；

其他 - LLDP

支持网络监控管理

LLDP（Link Layer Discovery Protocol）是IEEE 802.1ab中定义的链路层发现协议，可以将本端设备的管理地址、设备标识、接口标识等信息组织起来，并发布给自己的邻居设备，邻居设备收到这些信息后将其以标准的管理信息库MIB（Management Information Base）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

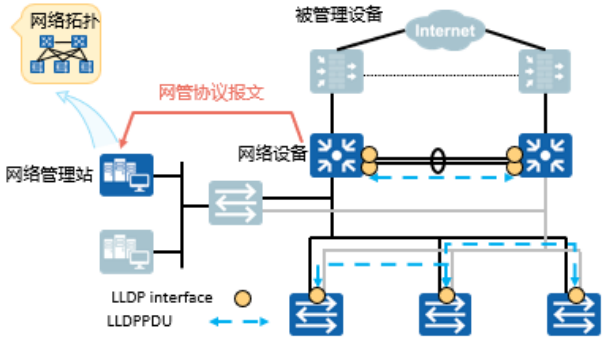


- LLDP 是一种邻近发现协议。它为以太网网络设备，如交换机、路由器和无线局域网接入点定义了一种标准的方法，使其可以向网络中其他节点公告自身的存在，并保存各个邻近设备的发现信息。例如设备配置和设备识别等详细信息都可以用该协议进行公告。
- LLDP 信息是定期传输的，并且只在一定的期限内保留。IEEE 已经定义了一个建议的传输频率，即每 30 秒传输一次。LLDP 设备在收到邻近网络设备发出的 LLDP 信息后，将把 LLDP 信息存储在一个 IEEE 定义的简单网络管理协议（SNMP）管理信息库（MIB）中，并且在一定的时限内保持有效。定义该时限的 LLDP“生存时间”（TTL）值就包含在所收到的数据包内。
- 该协议使网络管理系统能够精确地发现和模拟物理网络拓扑结构。由于 LLDP 设备发送和接收公告，这些设备将会把自己发现的邻近设备信息存储下来。公告数据，如邻近设备的管理地址、设备类型和端口号，都有助于确定邻近设备到底属于什么类型，以及它们通过哪些端口实现互联。
- 单邻居组网模式：
- 单邻居组网模式是指交换机设备的接口之间直接相连，

而且接口只有一个邻居设备的情况。

- 链路聚合组网模式：
- 链路聚合组网模式是指交换机设备的接口之间存在链路聚合，接口之间是直接相连，链路聚合之间的每个接口只有一个邻居设备。

LLDP的应用场景



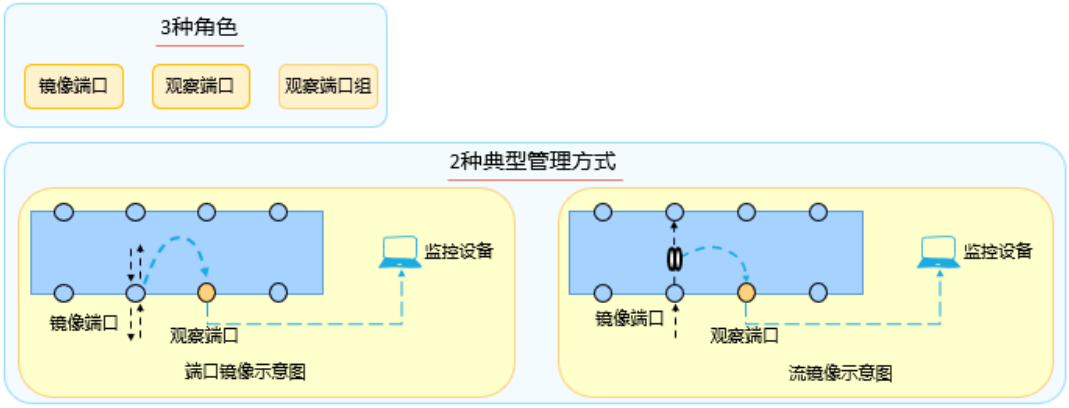
- 如右图所示，交换机之间直接或者通过Eth-Trunk相连，网络管理站与交换机之间路由可达且网管协议配置已经完成。
- 通过LLDP协议机制，发现网络中链路层邻居信息，同时通过网络管理协议上报给网络管理站，从而图形化展示网络拓扑结构。

- Eth-Trunk 以太网链路聚合，简称链路聚合，它通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽的目的。

其他－镜像

支持网络监控管理

镜像是指将镜像端口（源端口）的报文复制到观察端口（目的端口）。

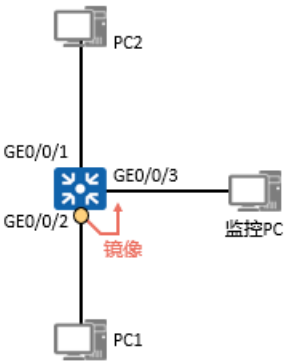


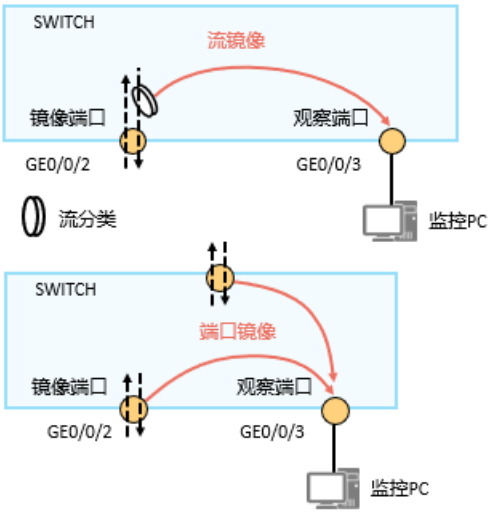
- 在网络维护的过程中会遇到需要对报文进行获取和分析

的情况，比如怀疑有攻击报文，此时需要在不影响报文转发的情况下，对报文进行获取和分析。镜像可以在不影响报文正常处理流程的情况下，将镜像端口的报文复制一份到观察端口，用户利用数据监控设备来分析复制到观察端口的报文，进行网络监控和故障排除。

- 基本概念：
- 镜像端口是被监控的端口，从镜像端口流经的所有报文或匹配流分类规则的报文将被复制到观察端口。
- 观察端口是连接监控设备的端口，用于输出从镜像端口复制过来的报文。
- 观察端口组是连接多个监控设备的一组端口。观察端口组中的多个成员端口分别连接多个监控设备，当使用观察端口组镜像报文时，镜像到观察端口组的报文将被复制到所有的成员端口。
- 端口镜像：是指设备复制一份从镜像端口流经的报文，并将此报文传送到指定的观察端口进行分析和监控
- 流镜像：是将镜像端口上特定业务流的报文复制到观察端口进行分析和监控。在流镜像中，镜像端口应用了包含流镜像行为的流策略。如果从镜像端口流经的报文匹配流分类规则，则将被复制到观察端口。

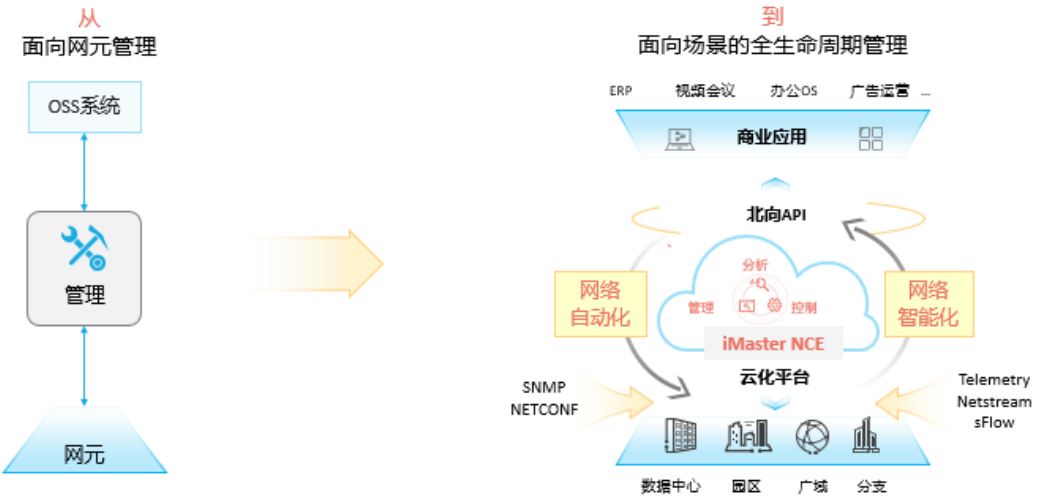
镜像的应用场景





- 在某些场景中，我们可能需要监控交换机特定端口的入站或出站报文，或者需要针对特定的流量进行分析，例如上图中，GE0/0/2 口上承载了许多流量，基于某种需求，我需要对接口的收发报文进行分析从而进行网络的故障定位。那么我可以在交换机的 GE0/0/3 口接一个 PC，在 PC 上安装协议分析软件，然后部署端口镜像，将 GE0/0/2 的入、出站流量镜像到 GE0/0/3 口上来，接下来我只要在 PC 上通过协议分析软件查看报文即可。
- 注意到，如果没有端口镜像技术，除非数据包的目的地是监控 PC（所连接的端口），否则报文是不会发向该端口的。因此事实上端口镜像就是将某个特定端口的流量拷贝到某个监控端口。

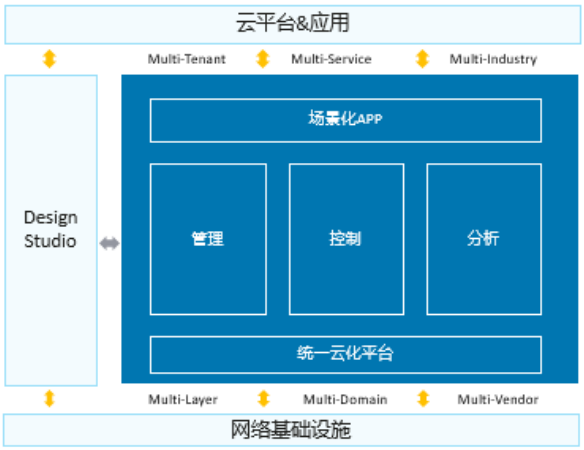
网络管理典型应用场景



- 随着网络的快速发展，数字化转型日益凸显，网络管理逐步从面向网元管理的方式转到面向场景的自动化。
- 网络管控系统是自治网络的演进方向，包含了控制器、分析器和管理器。
- SNMP 和 NETCONF 一般用于配置下发，Telemetry、Netstream 和 sFlow 一般用于数据上报。

什么是iMaster NCE?

iMaster NCE产品架构和客户价值



网络自动化
意图驱动，基于模型
跨域、跨层、跨厂家

网络智能化
基于大数据和AI的预测性维护

敏捷的系统集成
可编程的Design studio
开放的REST API

基于云的弹性扩展
可部署于公有云&私有云
弹性扩展 &高可靠

思考题：

1. （多选题）网络管理体系结构包含的两个关键元素是什么（　）

A. 管理设备　　B. 被管理设备
C. 代理　　D. 网管协议

2. （多选题）网络管理的基本功能，以下描述正确的是（　）

A. 配置管理　　B. 性能管理　　C. 故障管理
D. 安全管理　　E. 计费管理

答案：

- AB
- ABCDE