第 8 篇 开放应用体系架构

第 25 章 OAA

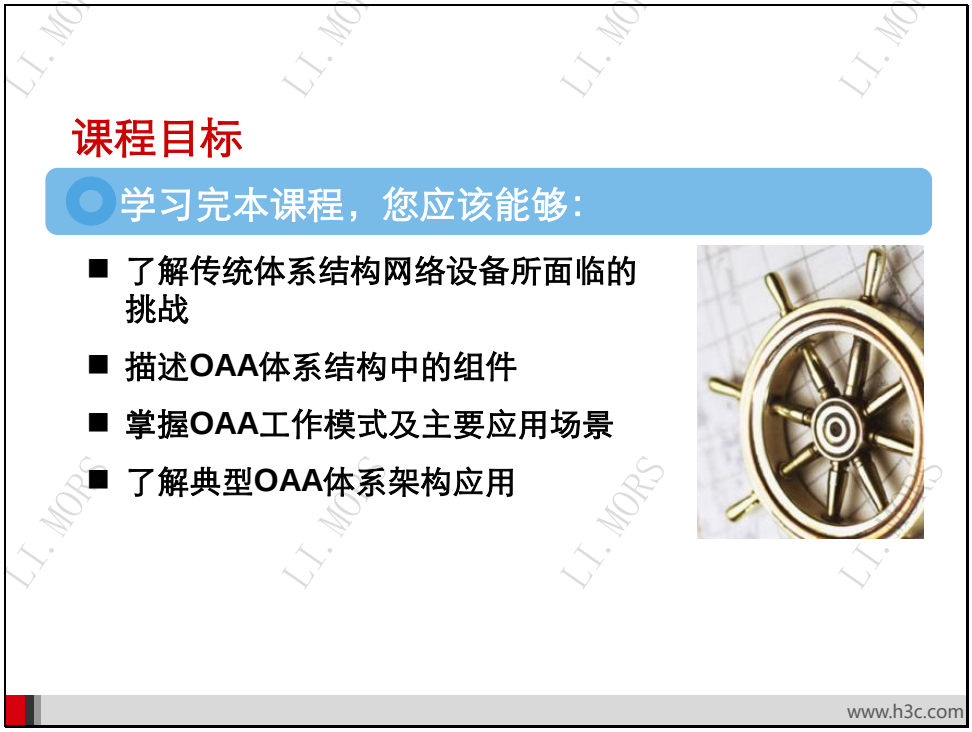
第25章 *开放应用体系架构

随着各种业务不断地融入传统数据通讯网络，以及对网络安全性、可管理性要求的不断提高，用户需要网络设备在转发数据包之外提供更多、更复杂、更灵活的服务。例如，用户需要网络设备能够接入电话和传真、统计和计费，防范网络攻击、防病毒，流量监控和调整等等。这一切都对网络设备提出了更高的要求。

传统网络中，上述功能由专用设备来独立完成。但出于降低网络建设、管理、维护成本的考虑，用户往往希望能够在一台网络设备上完成多种功能。另外，还有很多用户对网络服务有个性化的需求，而往往一家独立的技术厂商很难同时提供客户所要求的所有需求和服务。

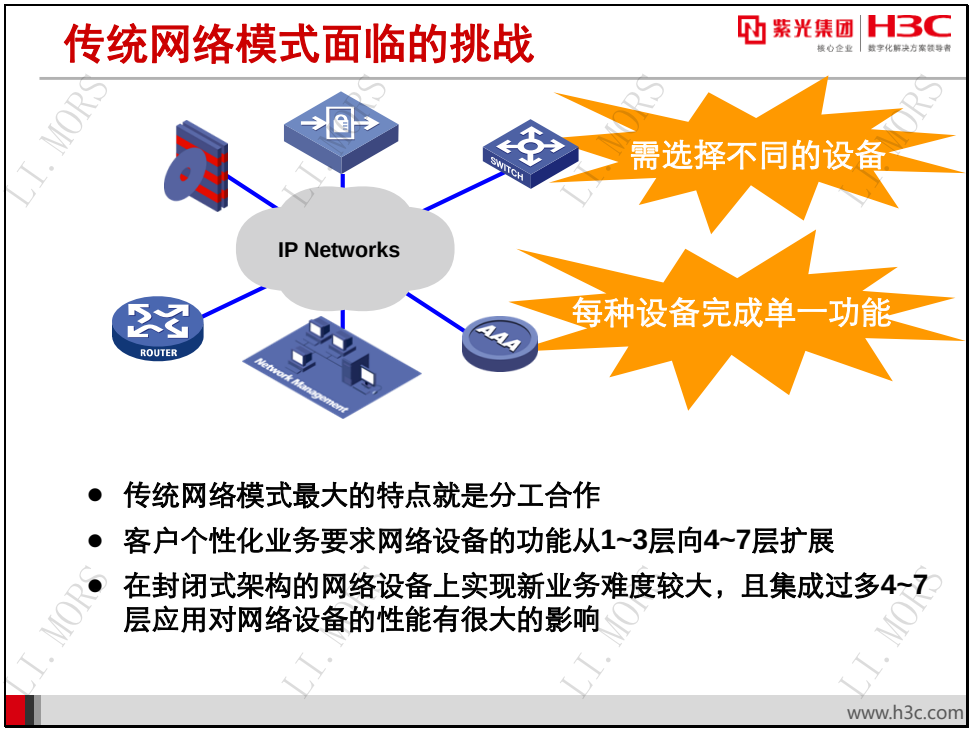
面对这样的情况，H3C 提出了一个开放的软硬件体系架构——OAA（Open Application Architecture，开放应用体系架构）。OAA 允许对传统的路由交换设备进行二次开发，满足客户的多样化需求；允许众多厂商生产的设备和软件无缝集成在一起，像一台设备那样工作。

25.1 本章目标



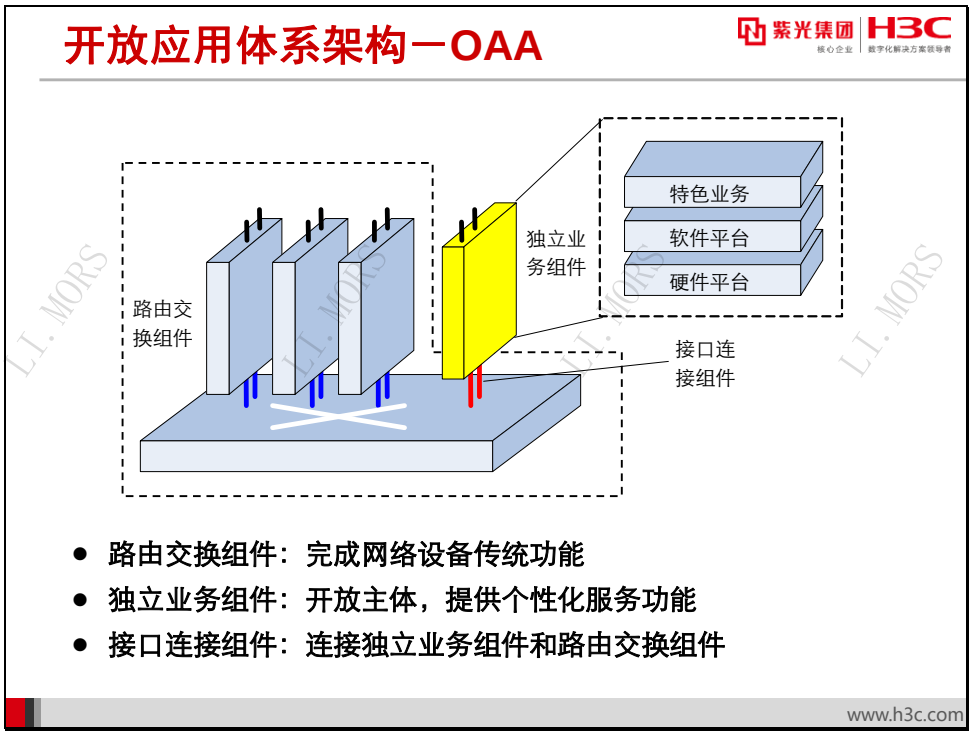
25.2 OAA概述

25.2.1 OAA 架构简介



传统网络模式最大的特点就是分工合作，客户根据需求选择不同的网络设备，然后将它们通过 IP 网络连接而成。比如选择路由器完成基本路由、连接异构网络功能；交换机可以提供高密度、高速主机接入；语音服务器、AAA 服务器提供语音管理、认证计费等功能；防火墙提供基本安全功能；网管系统提供集中化设备监控、管理功能。

如果客户有新的需求，比如在连接广域网的路由器上实现应用加速，在网管平台集成网络流量分析，在防火墙上新增网络杀毒应用，往往很难实现。一方面因为部分网络设备是为 1~3 层功能、性能而设计的，而应用加速、网络流量分析、网络杀毒则要求网络设备具备深度的 4~7 层分析处理能力，而即使原有网络设备实现了这些 4~7 层功能，也会占用网络设备过多资源，从而影响网络设备的 1~3 层功能和性能；另一方面因为这些网络设备往往架构封闭，新增功能只能由厂商开发、编译、加载，客户要求的新功能也不是厂商的专长，开发的新功能往往不能完全符合客户业务需求。

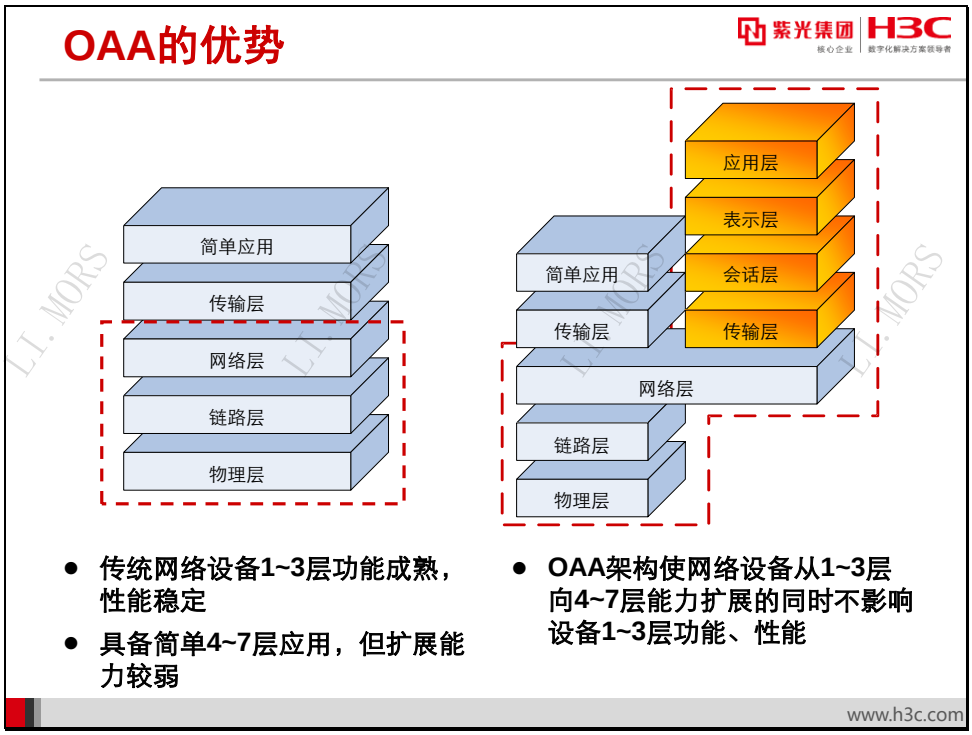


针对这种情况，H3C 及时地提出 OAA 开放应用体系架构，该架构的特点在于不影响网络设备固有 1~3 层功能、性能的同时，提供开放接口实现深度 4~7 层扩展。

OAA 架构主要分为 3 个组成部分：

- **路由交换组件：**路由交换组件是网络设备主体部分，这部分有着完整的路由器或交换机的功能，也是用户管理控制的核心。
- **独立业务组件：**独立业务组件是 OAA 架构的核心部分，是可以开放给第三方合作开发的主体，主要用来提供各种独特的业务服务功能。
- **接口连接组件：**接口连接组件是网络设备和独立业务组件的连接器件，它使各组件形成一个统一的产品。

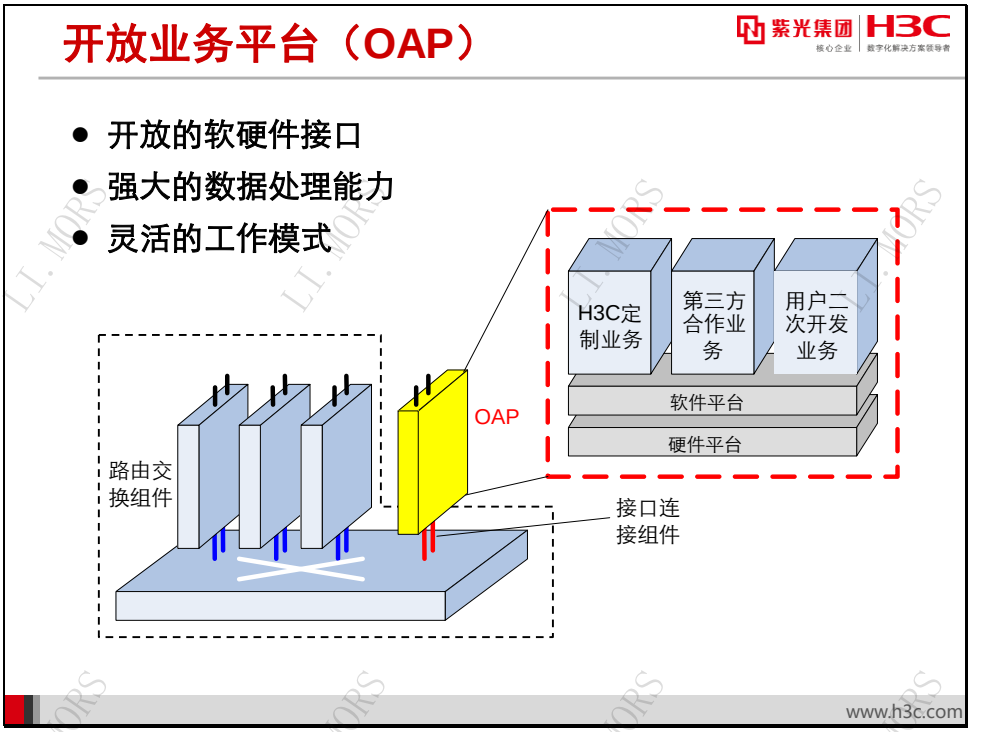
独立业务组件可以分为硬件平台、软件平台和特色业务 3 个平面，每个层面都是开放、标准的规范接口，可以进行灵活的二次开发。比如擅长硬件开发的第三方可以根据 OAA 规范开发独立业务组件的硬件平台部分，擅长软件平台开发的第三方可以在标准 OAA 硬件平台上开发软件平台，擅长业务集成开发的第三方以在 OAA 标准软件平台上开发特色业务。



OAA 架构优势在于全面的 1~7 层解决方案定制能力，使得网络设备的扩展能力大增。

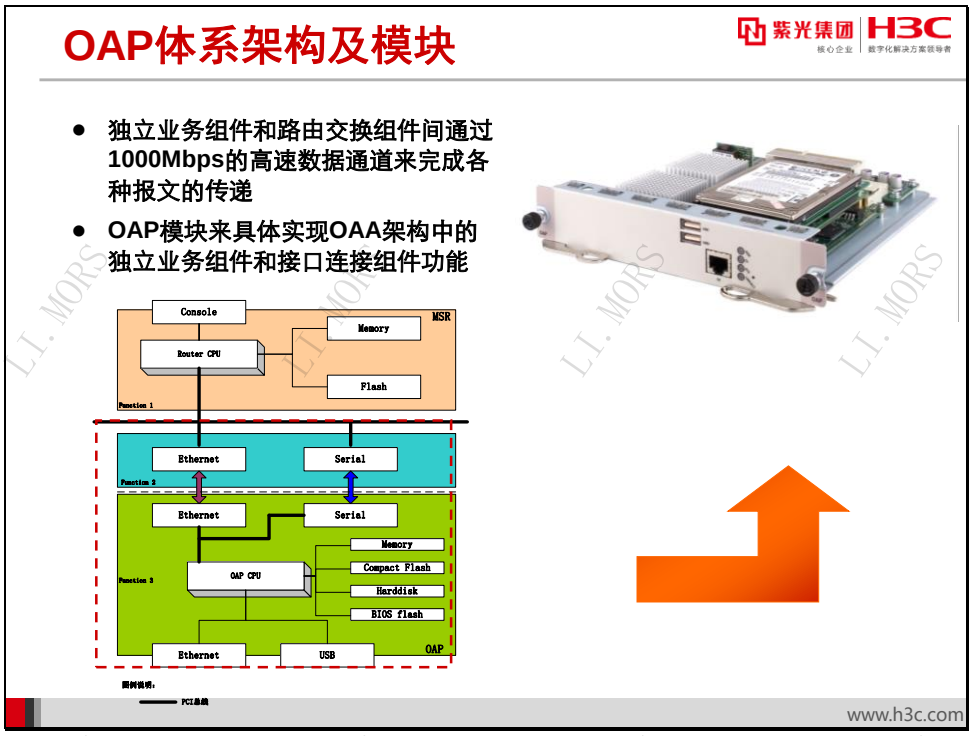
传统网络设备的优势在于丰富的 1~3 层特性，附带一定的 4 层特性和简单的应用，但是 4 层以上特性扩展能力相对较弱。基于 OAA 架构的网络设备在 1~3 层功能特性和性能上与传统网络设备相当，同时通过开放的独立业务组件而实现深度 4~7 层扩展。这种开放式的架构不但使网络设备厂商可以更加方便的集成更多高层特性，也有利于和第三方深度合作，共同开发符合市场需求的特性；甚至用户也可以根据自身需要而在 OAA 平台上进行灵活的二次开发。

25.2.2 开放业务平台（OAP）



开放应用平台 OAP（Open Application Platform）是 H3C 根据 OAA 架构规范而实现的具体产品平台。OAP 实现了 OAA 架构中的独立业务组件功能，包括硬件平台、软件平台和特色业务。OAP 平台具有开放的软硬件接口、强大的数据处理能力以及灵活的工作模式等特点。

通过 OAP 这个开放业务平台，H3C 可以向客户提供特定的业务功能；也可以和第三方合作进行开发共同对客户提供完整的业务；当然，用户也可以根据需要在软件平台上进行二次业务开发。所有的这一切都不影响传统路由交换组件的自身功能。



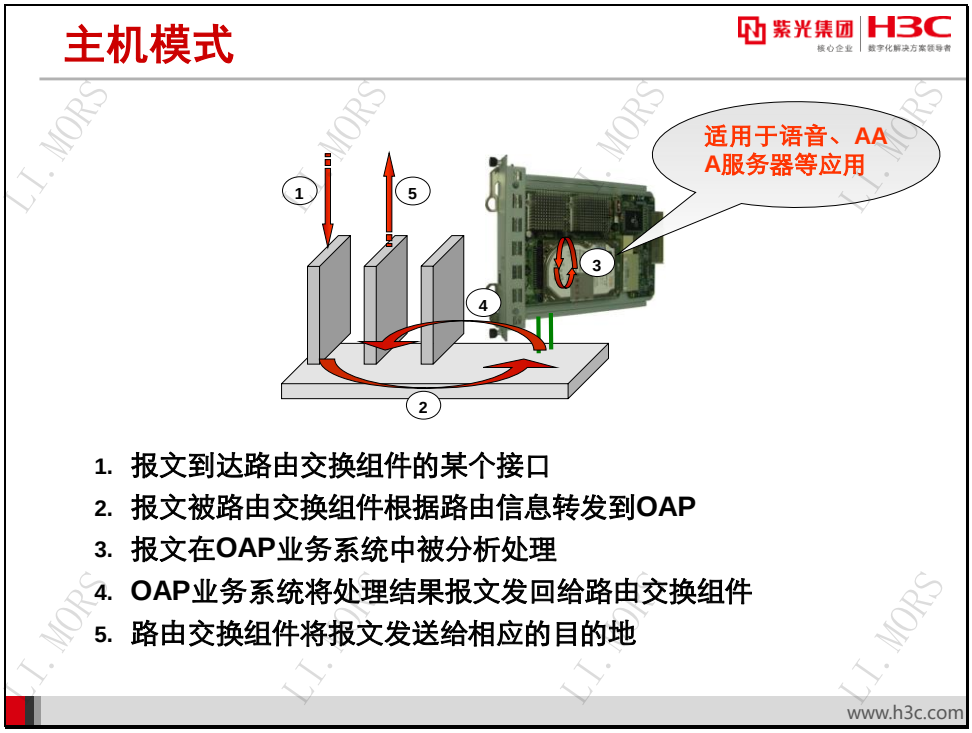
上图是 OAP 架构示意图。在图中，功能模块 1 是路由交换组件，完成传统路由交换功能。一台支持 OAP 功能的网络设备就是功能模块 1；功能模块 2 是接口连接组件，包括一个数据通道（以太接口）和一个控制通道（串行接口），其中数据通道的速率可达 1000Mbps；功能模块 3 是独立业务组件，它既提供了连接路由器的高速以太网口和串口，也对外提供了一个独立的以太网口来扩展业务连接。为了能够实现独立的业务功能，独立业务组件（功能模块 3）内置有 BIOS、CPU、内存、硬盘等硬件。

独立业务组件和路由交换组件间通过 1000Mbps 的高速数据通道来完成各种报文的传递。另外，通过独立的管理通道，用户可以登录到独立业务系统而进行各种配置和管理。同时，由于两个系统之间是由通道连接的一种松耦合关系，所以彼此之间独立性很强。路由交换组件专注于完成路由交换功能，就像传统的网络转发设备一样；而独立业务组件则专注于自己独特的业务功能。

H3C 开发了 OAP 模块来具体实现 OAA 架构中的独立业务组件和接口连接组件功能。从外观上看，OAP 模块与普通模块类似；使用时，和其它模块一样，插入到路由器的扩展槽中。

25.3 OAA工作模式

25.3.1 主机模式

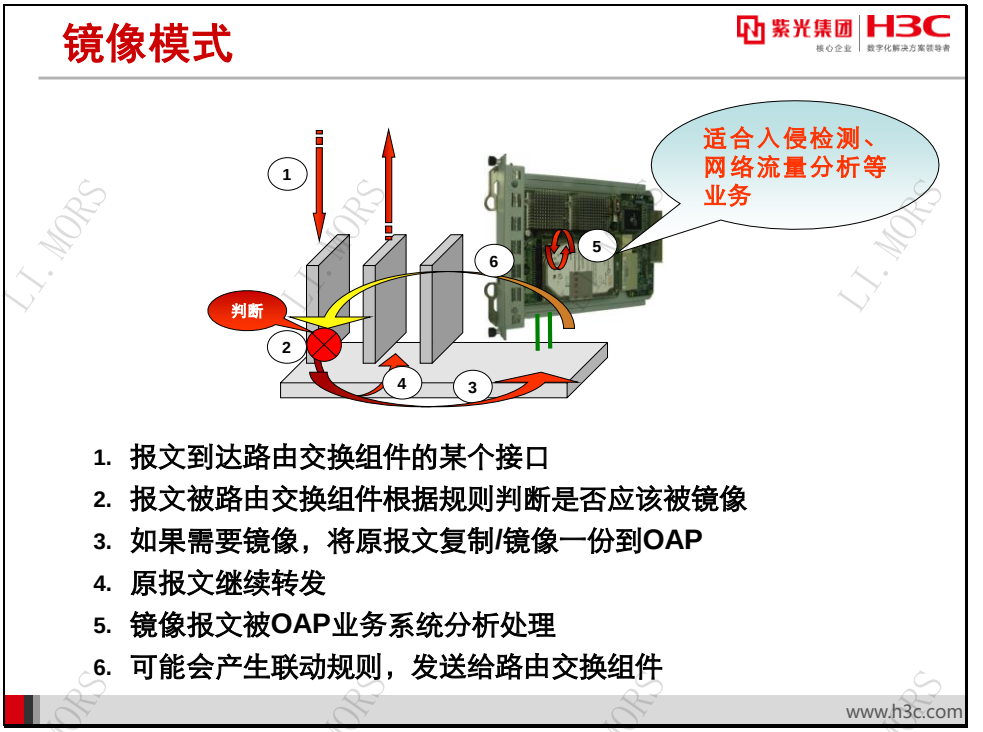


OAP 可以被二次开发为各种不同的业务系统，可以满足各种业务特性需求。根据路由交换组件和独立业务组件之间的数据交互方式的不同，OAP 提供了 4 种工作模式：主机模式、镜像模式、重定向模式和透明模式（也称为桥接模式）。

在主机模式下，独立业务系统像网络上的一台主机一样工作，拥有自己的 IP 地址，作为网络末梢存在。IP 报文是通过路由交换组件连接独立业务组件的高速数据通道转发，路由交换部件相当于独立业务系统的网关。路由交换部件收到数据报文后，如果判断出数据需要送给 OAP 模块处理（目的 IP 地址为 OAP 模块地址），则将此数据转发给 OAP 模块，OAP 模块处理完成后，将回应的报文返回路由交换组件，由路由交换部件将报文发送给相应的目的地。这种工件模式下，路由交换部件和独立业务组件间的耦合是最松的。

主机模式适合语音服务器、AAA 服务器等应用。例如，当 OAP 模块上集成了 AAA 服务器应用，则当认证请求报文到达网络设备后，网络设备根据路由信息将认证请求报文转发给 OAP 模块；OAP 模块上的 AAA 服务器根据认证请求报文中携带的用户信息判断认证是否通过，通过则返回正确授权报文，不通过则返回认证拒绝报文。不管是授权报文还是拒绝报文都转交给网络设备，网络设备收到报文后根据路由/转发信息选择正确的出接口转发报文。

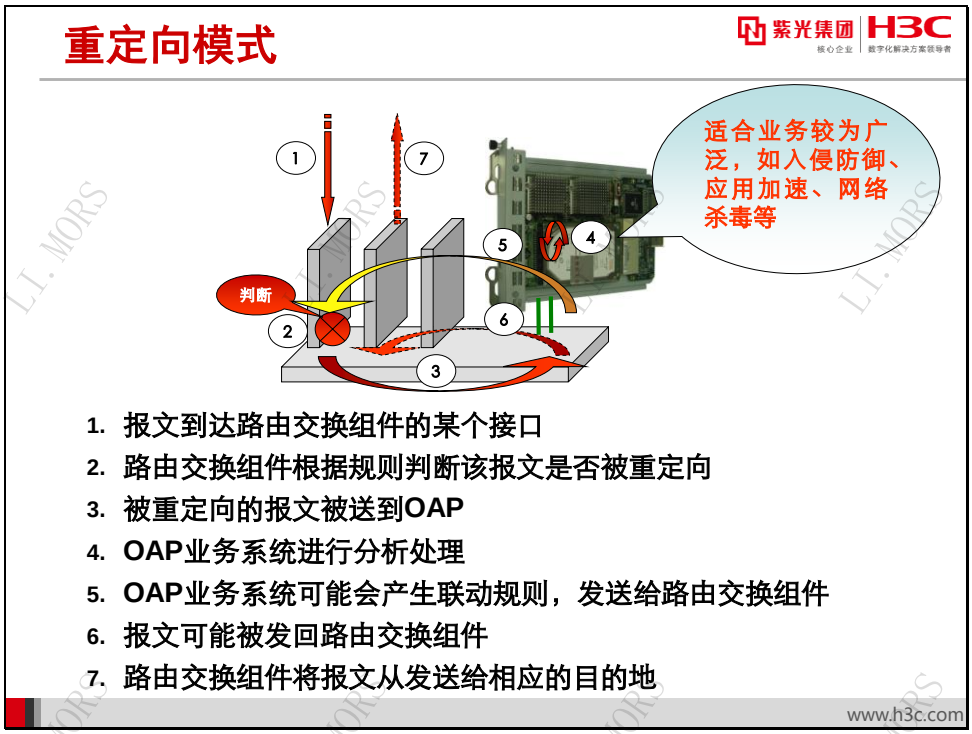
25.3.2 镜像模式



镜像模式下，路由交换部件根据要求，把特定的报文复制一份给独立业务组件，原始报文继续完成正常的转发。而独立业务组件收到这个报文以后进行分析和处理，然后将报文丢弃。当然路由交换组件和独立业务组件也可以进行联动，独立业务组件分析完镜像报文后可以下发联动规则要求路由交换组件对相应业务流进行限速、阻断等特殊处理。这种模式下，镜像报文也是通过路由交换组件连接独立业务组件的高速数据通道转发。

镜像模式适用于网络流量分析、入侵检测 IDS 等应用。比如，网络流量分析应用中，数据包进入网络设备接口处理后被镜像到 OAP 模块，同时源报文被正常转发。OAP 中的网络流量分析功能对镜像报文进行分析，如果发现报文中有占用大量带宽的 BT 应用数据流，那么网络分析应用程序会针对该镜像报文所代表的数据流生成限速联动规则，并下发给网络设备，网络设备应用该联动规则就可以对 BT 流进行限速。

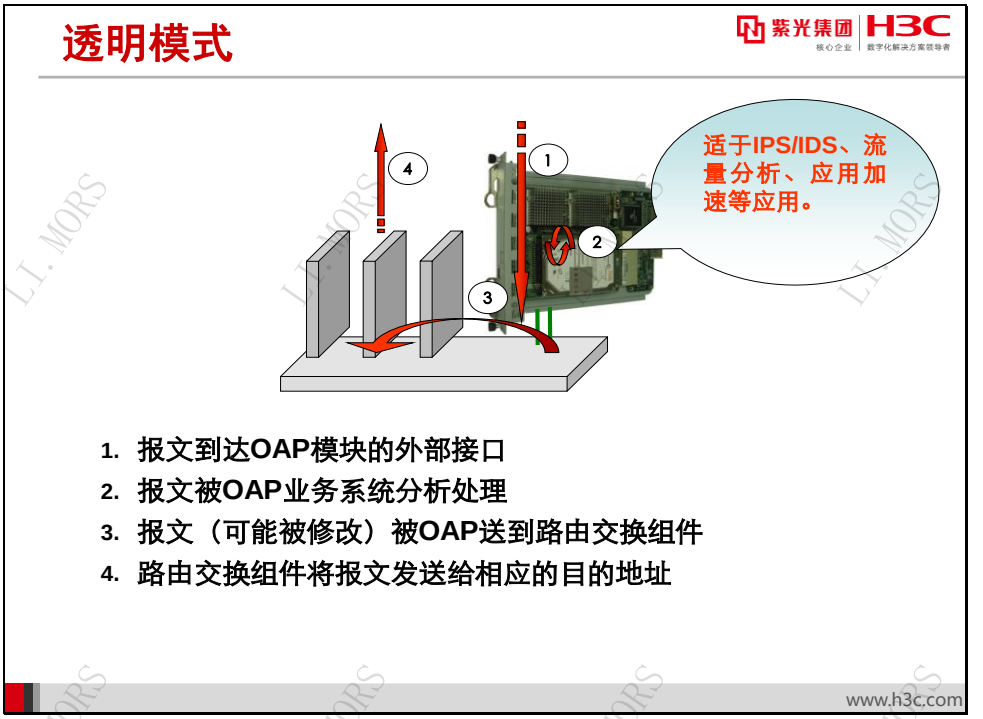
25.3.3 重定向模式



在重定向工作模式下，数据包到达网络设备接口后根据规则判断是否被重定向，如果符合重定向规则那么将该报文重定向 OAP 模块中。OAP 模块中的业务系统对重定向报文进行分析处理，然后根据处理结果判断是否生成联动规则并发送给网络设备。根据不同业务的需求，重定向报文也有可能被返回给网络设备，网络设备对返回报文进行正常转发。

重定向模式所适用的业务比较广泛，如入侵防御、应用加速、网络杀毒等。比如在网络杀毒应用中，携带病毒的 HTTP 报文到达网络设备后，根据配置的规则判断应被重定向到 OAP 模块中，模块中的杀毒应用程序发现病毒并将病毒查杀，再下发联动规则要求网络设备过滤该 HTTP 站点。同时，OAP 模块上杀毒应用程序生成一个 HTTP 页面返回给网络设备，表示用户访问的网页有病毒。网络设备再将此 HTTP 页面发送给访问用户，以通知用户。

25.3.4 透明模式



透明模式下，独立业务组件像二层网桥设备一样工作，不需要配置 IP 地址。外来的数据流从 OAP 模块上的外部以太网接口流入，穿过独立业务组件，经过内部高速数据通道到达路由交换组件。在路由交换组件看来，外部数据直接到达了连接部件上的高速以太网口，内嵌的独立业务系统似乎根本不存在一样。实际上，当数据流通过独立业务系统的时候，独立业务系统会做相关的记录分析，必要的时候，业务系统还会对报文会做一定的修改以完成相关的功能。

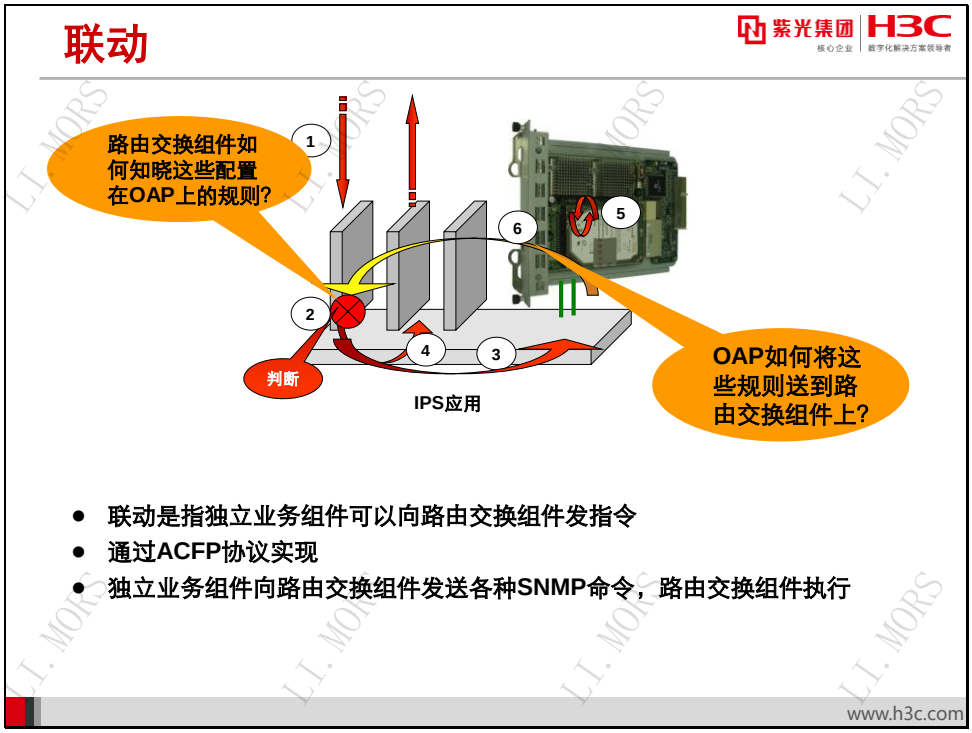
这种模式下，路由交换组件和独立业务系统之间的耦合也是比较松的。

这种工作模式适用于 IPS/IDS、流量分析、应用加速等。

在 IPS/IDS 应用中，报文抵达 OAP 外部接口后，IPS/IDS 应用程序对该报文进行分析处理，如果检测出来是攻击报文，则将该报文丢弃，并生成对应防火墙规则过滤该数据流；如果是正常报文则允许其通过。

25.4 联动及管理

25.4.1 联动

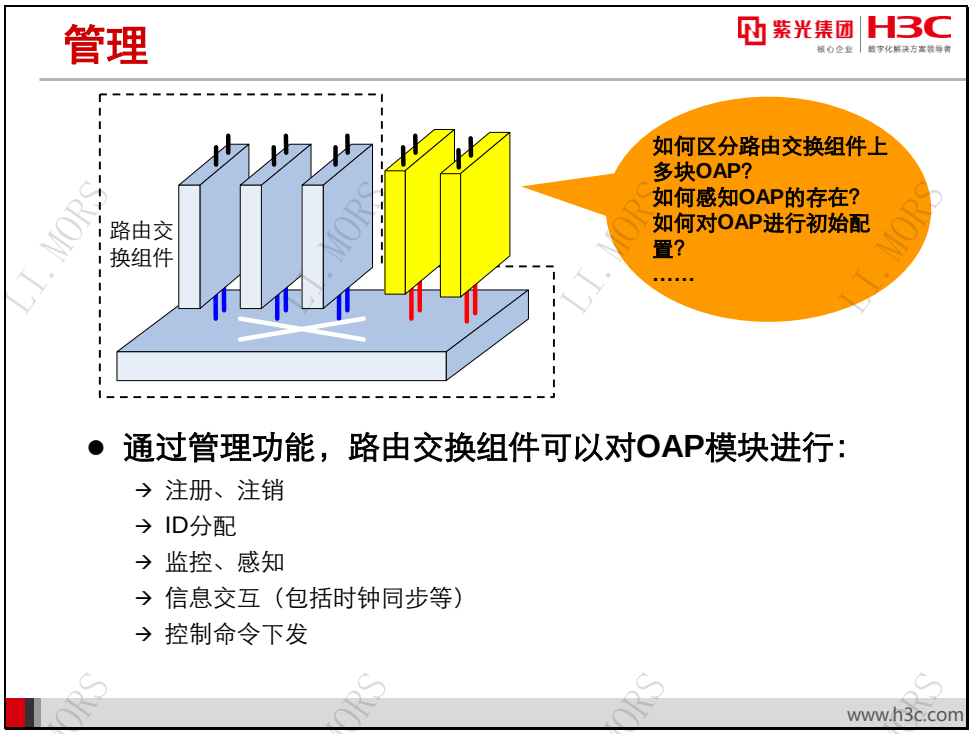


OAA 体系结构中，路由交换组件与独立业务组件是两个独立的主体，这两个主体协作完成具体业务。为达到这种目的，两者之间有时需要互通一些信息，这种信息交互就是联动。简单而言，就是指独立业务组件可以向路由交换组件发指令，改变路由交换组件的动作。

联动功能主要是通过 ACFP（Application Control Forwarding Protocol，应用控制转发协议）来实现的。ACFP 是基于 SNMP 协议而开发的管理协议。ACFP 协议的运行过程与网管软件运行有些类似。独立业务组件就像网管系统一样，向路由交换组件发送各种 SNMP 命令；而路由交换组件上支持 SNMP Agent 功能，可以执行下发的这些命令。

为了支持联动功能，要求路由交换组件支持相关 MIB。

25.4.2 管理

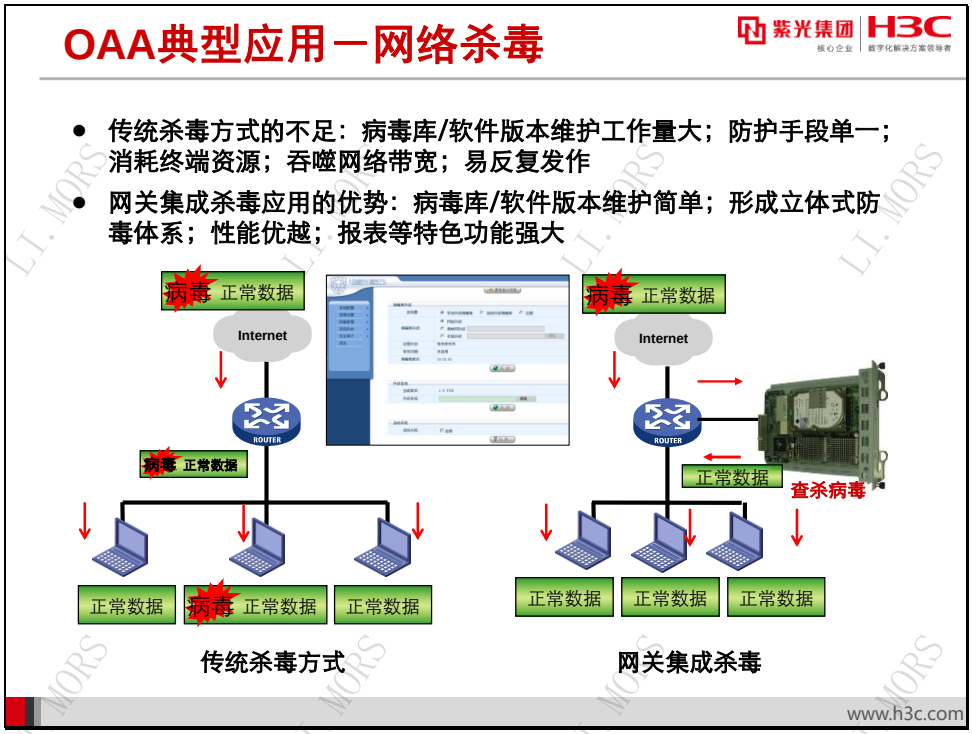


除了联动外，路由交换组件和独立业务组件间还需要互相监控、互相感知，有时还需要路由交换组件向独立业务组件发送一些指令，指示独立业务组件进行相应操作。这种路由交换组件监控、指挥独立业务组件的行为就是管理。

路由交换组件对独立业务组件的管理是通过 ACSEI 协议来完成的。通过 ACSEI 协议，路由交换部件可以区分不同插槽上的多个 OAP 模块，监控、记录各个 OAP 模块的运行状态。路由交换组件与 OAP 模块间还通过 ACSEI 协议来完成互相监测、信息交互、时钟同步等功能；路由交换组件还可以对 OAP 模块下发如业务系统关闭、重新启动等命令。

通过路由交换组件和独立业务组件之间的管理通道，已经登录到路由交换组件上的用户，可以向独立业务组件发起连接，登录到独立业务组件的控制台上。

25.5 OAA典型应用

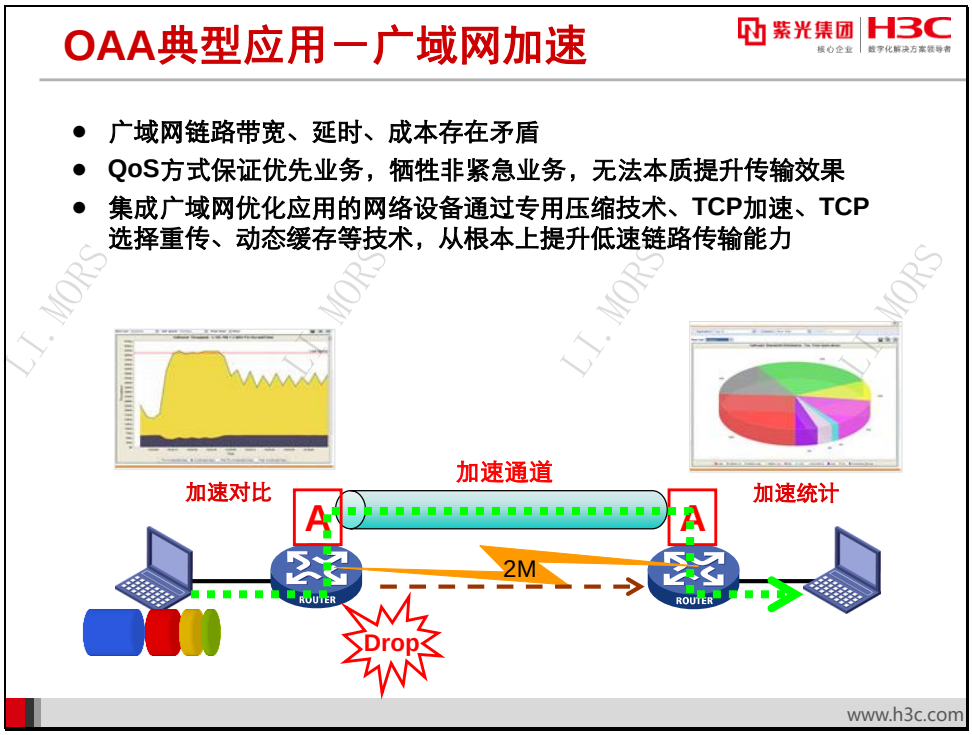


计算机进入互联网时代后，病毒也借助网络大规模传播，传播速度快、扩散范围广。

传统杀毒方式都是将杀毒软件部署在内部网络主机上。这种杀毒方式下，各个主机各自为战。因此，病毒会在一段时间内在网络中肆虐，网络带宽会受到病毒吞噬，部分网络设备甚至会遭受到病毒攻击而无法正常工作。另外，传统网络设备只能通过基于访问控制列表（ACL）的防火墙来进行被动防御，无法进行深度杀毒。

通过在 OAP 模块上进行二次开发，可以将杀毒产品厂家成熟的杀毒引擎移植到 OAP 模块上，使网络设备具备了对 HTTP、FTP、SMTP、POP 等数据流杀毒的能力，从而能够将大部分病毒截杀在用户网络入口，减少了病毒冲击内部网络的几率。通过将网关集成杀毒与单机杀毒部署相结合，在网络中能够形成立体防毒体系，从而大幅度提高网络的健壮性。

同时，根据现实需求，OAP 模块还可以集成病毒库自动更新、Web 网管、实时生成报表等功能。

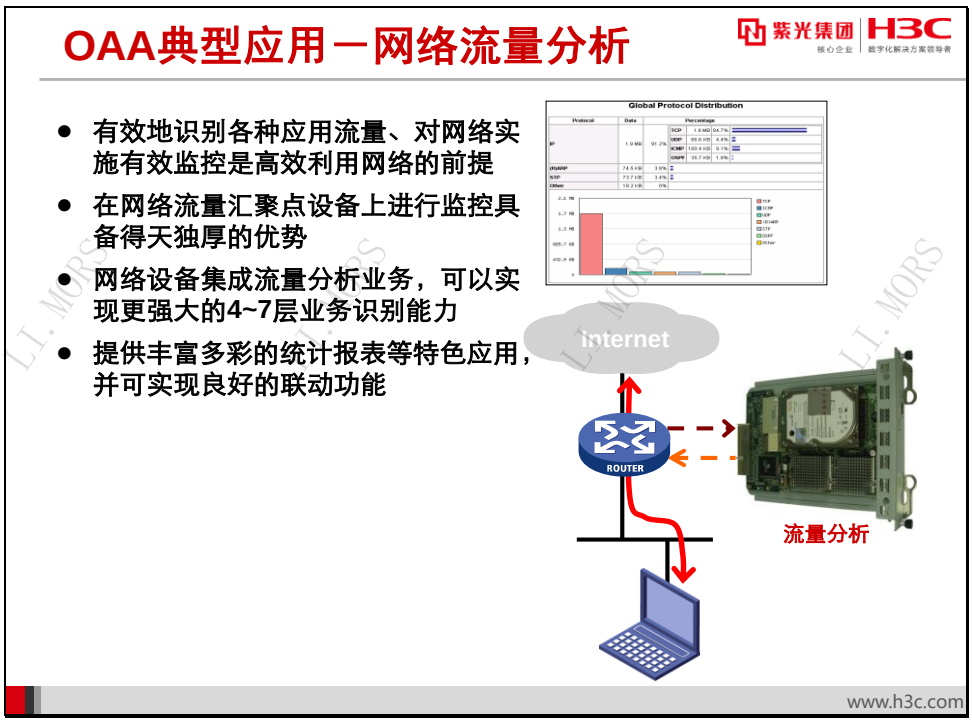


广域网性能优化和应用加速方案是 OAA 的另一种典型应用。

在广域网建设上，链路高带宽/低延时和建设成本一直存在不可调和的矛盾。要增大带宽、降低延时，必然要追加投资。另外，在广域网传输过程中，时延较大一直是突出的问题。

另外，随着企业网络规模不断壮大，通过广域网传输的数据越来越多，广域网带宽逐渐成为企业业务的瓶颈。在传统的广域网优化解决方案中，使用 QoS 来保证优先业务，从而导致非关键业务得不到传输质量保证。

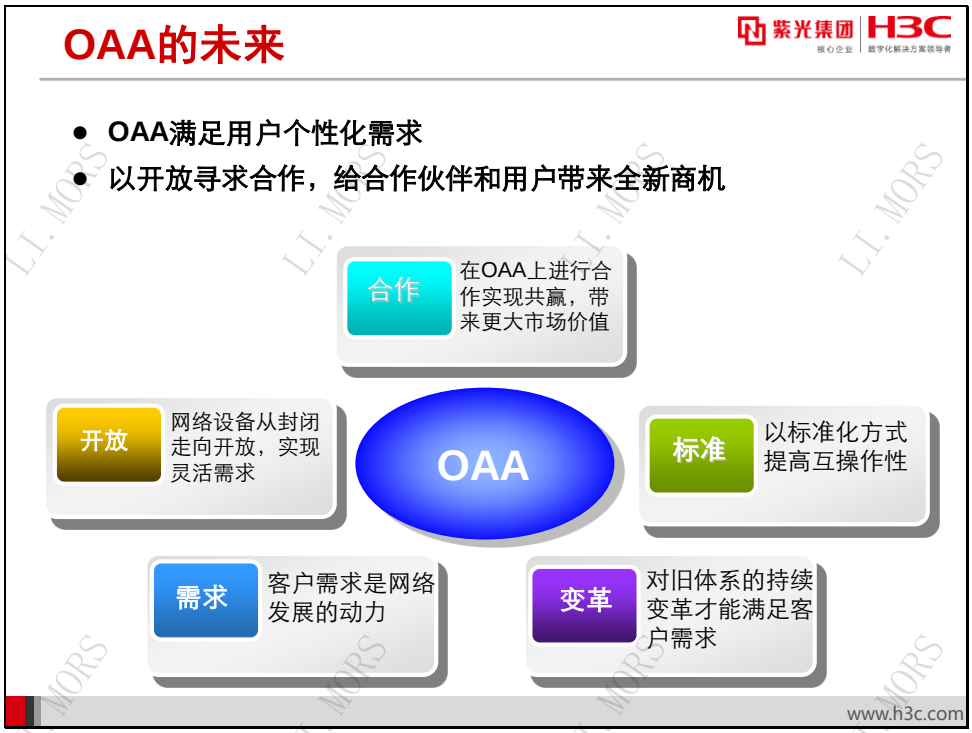
OAA 广域网优化方案则从应用加速的角度上，致力于在低速链路提高数据传输能力。通过在连接广域网的网络设备上部署 OAP 模块，从而在两端网络设备的 OAP 加速模块之间建立加速通道。当广域网数据流到达网络设备后，网络设备将数据流重定向到 OAP 模块中，OAP 模块可以通过深度应用识别采用最合适的压缩算法提升传输效率。此外，OAP 模块还可以通过 TCP 加速、TCP 选择重传、HTTP/FTP 缓存等技术大幅度提高低速链路上的传输性能。



目前，在 IP 网络上运行的应用种类非常丰富，网络也是四通八达。因此，流量监控技术有两大技术难题，一是如何深度识别各种应用，二是如何进行灵活有效地实时监控网络各处流量。

网络设备是各种网络流量的必经之路，在网络设备上进行应用流量深度监控具备得天独厚的优势。OAA 网络流量分析应用具备强大的 4~7 层业务识别能力和链路质量检测功能，能够自定义流量监控、攻击报警、恶意流量报警，另外还有丰富多彩的统计报表功能。由于通过 OAP 模块实现流量监控，所以网络设备的其余功能如数据转发不会受到任何影响。

25.6 OAA的未来

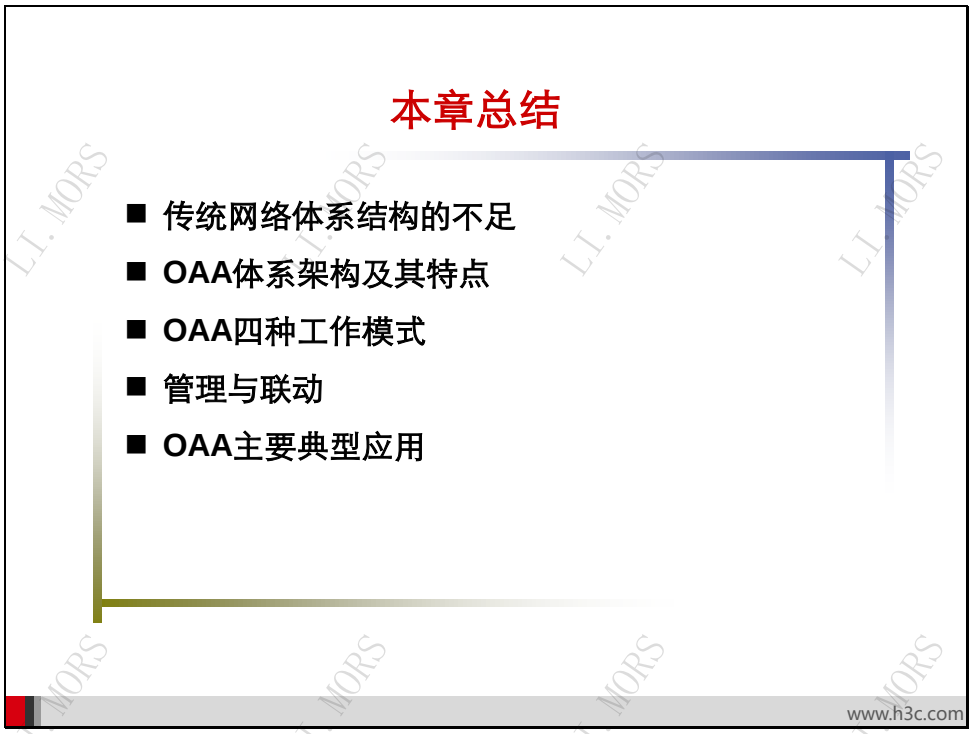


用户需求推动网络发展。用户日益复杂的个性化需求使得传统网络设备封闭的体系架构越来越捉襟见肘。要满足用户需求，必须要对原有的体系、解决方案进行变革。OAA 体系架构以其优秀的兼容性和扩展性，必定会引领网络设备体系架构的变革。

OAA 架构以标准化的形式对外开放，一方面以标准化提高互操作性，另外通过开放以实现更灵活的需求。OAA 架构以开放寻合作，目标是与合作伙伴、用户实现共赢，共同开拓市场，带来更大的市场价值。

封闭的终将过去，开放才能引领未来。

25.7 本章总结


本章总结
传统网络体系结构的不足
OAA体系架构及其特点
OAA四种工作模式
管理与联动
OAA主要典型应用
www.h3c.com

25.8 习题和解答

25.8.1 习题

1. OAA 主要包括三个组件，包括路由交换组件、独立业务组件和（　　）。
2. 下列哪种模式下，独立业务组件就像网络上的一台主机，拥有自己的 IP 地址，作为网络末梢存在？（　）

   A. 主机模式　　B. 重定向模式

   C. 镜像模式　　D. 透明模式
3. 下列哪种模式中独立业务组件没有 IP 地址，并且一定要有外在的以太网口？（　）

   A. 主机模式　　B. 重定向模式

   C. 镜像模式　　D. 透明模式
4. 下列关于 OAA 组件之间的联动描述，哪些是正确的？（　）

   A. 联动功能主要是通过 SNMP 协议实现的。

   B. 独立业务组件仿照网管系统的功能，向路由交换组件发送各种 SNMP 命令。

   C. 路由交换组件仿照网管系统的功能，向独立业务组件发送各种 SNMP 命令。

   D. 联动功能主要是通过 TR069 协议实现的。
5. 路由交换组件对 OAP 模块的管理是通过什么协议完成的？（　）

   A. ACFP 协议　　B. ACSEI 协议

   C. TR069 协议　　D. SNMP 协议

25.8.2 习题答案

1. 接口连接组件　　2. A　　3. D　　4. AB　　5. B