思科教育城域网解决方案

思科教育城域网解决方案

什么是教育城域网?

随着教育信息化在全国逐渐普及，学校相继建立了自己的校园网络，形成了层次分明功能完善的纵向网络体系，但是在学校之间的网络建设则相对滞后，在教育系统内部出现了众多的信息孤岛。这样的局面，我们如何避免？在校园网络解决方案日益趋同的背景下，我们如何来获得更多更新的内容，如何来引入更有价值的应用？

为了解决上述问题，教育城域网应运而生。教育城域网是将本地区的教育机构、研究机构全部通过网络互联，使教育资源整合、开放、共享，达到整体信息化的集成运用的宽带网络，最终形成的一个区域性的互联、互动、信息交换、资源共享和远程教育的基础架构。

通常，教育城域网以当地教委信息中心作为网络中心和资源中心，各学校和科研机构作为分中心和资源提供节点，覆盖全地区各级教育行政机构，同时网内共享管理平台，实现接入学校办公管理、教学管理和通讯管理的自动化，从而提高办学效率和质量。

如何建设教育城域网?

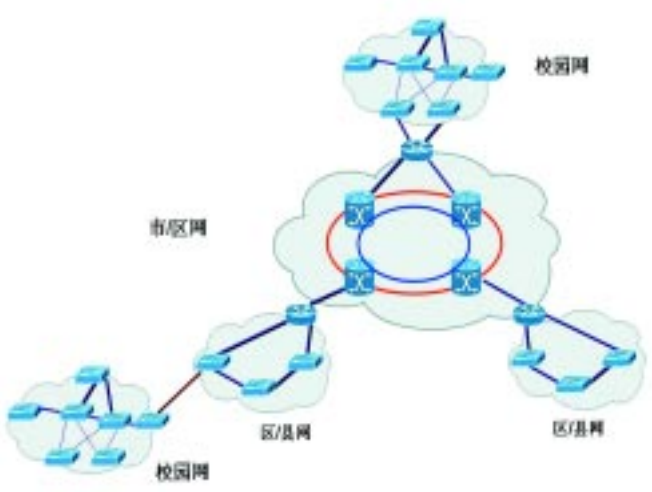
与普通校园网不同，教育城域网发挥骨干网的作用，承载信息与整合资源，将全市各地区分散的局域网从物理上联系起来。因此，建设教育城域网要遵循一般网络建设的原则，即：首先，要面向应用，注重实效，采用先进成熟的网络技术、方法和设备；其次，系统必须能够可靠运行，关键设备应有冗余，还要具有良好的网络管理、网络监控、故障分析和处理能力，以及高度的保密机制、灵活方便的权限设定和控制机制；再次，系统建设所选择的产品应具有良 好的互操作性和可执行性，并且符合相关的国际标准和工业标准；最后，一个系统应当在投资保护及长远性方面作适当考虑。

对于教育城域网的建设可以参照常规网络规划的步骤分为三个部分进行：

- 网络连接技术选择
- 应用设计及资源建设策略
- 安全网络结构设计

对于网络来说，选择何种技术直接决定了网络的基本性能和业务种类，因此，正确地选择连网技术是我们必须首要考虑的。

图 1



选择何种技术?

在网络连接技术方面技术繁多，但对于要求千兆以上的骨干网络一般采用高可靠的光纤技术，通常我们可以租用或另外铺设光纤线路作为教育城域网络和接入现有互联网络CERNET/ChinaNet/服务提供商，利用 VPN 技术，形成虚拟专用教育城域网这两种方案。

具体到光纤线路，通常有三种光纤传输技术供我们选择：

- SDH（Synchronous Digital Hierarchy，同步数字序列 ）
- RPR（Resilient Packet Transport，弹性分组环）
- Gigabit Ethernet/ 10Gigabit Ethernet（千兆以太网 / 万兆以太网）

SDH 同步数字序列

SDH是一套可进行同步信息传输、复用、分插和交叉连接的标准化数字信号的结构等级，而SDH网络则是由一些基本网络单元(NE)组成的，在传输介质上（如光纤、微波等）进行同步信息传输、复用、分插、和交叉连接的传送网络，它具有全球统一的网络节点接口（NNI）。SDH采用一套标准化的信息结构等级，称之为同步传送模块STM-N，同时，SDH具备灵活的复用于映射结构，允许将不同级别的信号经处理后放入不同的虚容器（VC-n）中，因而具有广泛的适应性。

SDH在组网时采用了大量的软件功能进行网络管理、控制及配置，具有很强的可扩充性和可维护性，尤其是在环形网、网状网等网络中应用时，可进行灵活的组网与业务调度，可实现高可靠的网络自愈。

在广域线路业务中应用较早的DDN技术是SDH技术的延伸和细化，可以提供比SDH更为低速的带宽（如64K，128K等）。实际上，SDH是DDN的骨干核心网络。随着宽带业务的普及，SDH才由后台走到前台。由于DDN业务开展的相对较早，网络覆盖范围很大，几乎到了无所不在的程度。也正是因为DDN业务地域广和带宽选择灵活等特点，DDN广域线路仍会在很长一段时间发挥作用。

SDH/DDN 的主要特点

- 由于采用了同步复用方式和灵活的复用映射结构，使低阶信号和高阶信号的复用 / 解复用一次到位，简化了处理过程和电路单元，省去了大量的有关电路单元，从而改善了网络的业务透明性。
- SDH 网可容纳各种数字业务信号，因此具有完全的前向兼容性和后向兼容性。
- 由于具有全球统一的网络节点接口，并对各网络单元的光接口有严格的规范要求，从而使得任何网络单元在光路上得以互通，体现了横向兼容性。
- 帧结构中安排了丰富的开销比特，使网络的运行、管理、维护与指配能力大大加强，通过软件下载的方式，可实现对各网络单元的分布式管理，同时也便于新功能和新特性的及时开发与升级，促进了先进的网络管理系统和智能化设备的发展。
- 虽然在理想情况下，网络中各网元都由统一的高精度基准钟定时，但实际网络中各网元可能分属不同的运营者，在一定范围内是能够同步工作的（同步岛），若超出这一范围，则有可能出现一些定时偏差。SDH采用了先进的指针调整技术，使来自于不同业务提供者的信息净负荷可以在不同的同步岛之间进行传送，并有能力承受一定的定时基准丢失。
- SDH引入了“虚容器”的概念，所谓虚容器（VC）是一种支持通道层连接的信息结构，当将各种业务信号经处理装入虚容器以后，系统只需处理各种虚容器即可达到目的，而不管具体的信息结构如何，因此具有很好的信息透明性，同时也减少了管理实体的数量。
- 采用先进的分插复用器（ADM）、数字交叉连接（DXC）等设备，使组网能力和自愈能力大大加强，同时也降低了网络的维护管理费用。
- 产品标准成熟完善，兼容性好，国际通用。

SDH/DDN 接入

所谓SDH接入是指将面对用户的各支路物理接口的用户信息映射到标准的2.048Mbit/s信号帧中，再对应每个 2.048Mbit/s 信号帧配置一个 VC-12，利用 SDH 技术将 VC-12 复接进 STM-1。

SDH 接入非常类似于 DDN，提供的数字电路为全透明的半永久性连接。所谓透明传输是指经过传输通道后数据比特流没有发生任何协议上和顺序上的变化。这样，在SDH网上即可传输两端认可的任何通信协议、各种通信业务，并且由于没有发生任何数据包顺序上的变化，在接收端路由器上可以省去数据包排序功能，从而提高数据处理能力。半永久性连接指电路一旦由网管生成后，用户两端之间的连接便是固定不变的，直到用户提出业务变更时网管才进行相关数据变动。

利用 SDH 组网的安全性和可靠性很高，由于 SDH 的传输中继采用光纤，自身又为点对点的通信方式，通信的安全性很好。另外安全性很好也指网络各节点间一般都通过自愈环互联，当前路由发生故障时，网络节点会自动倒换到另外一条迂回路由以保证通信正常。

SDH 只提供底层端到端的数字传输通道，而没有任何拥塞控制机制，也就是说在任何时候不会减小用户可用带宽，从而真正保证了用户的可用带宽。

图 2
教育城域网 SDH 应用设计

SDH 骨干网的建设:在教育城域网中，建议采用 Cisco ONS 15454 系列多业务光传输平台作为 SDH 骨干网的核心设备。该系列产品可以快速、经济地将当前限制诸多的时分复用（TDM）传输网转变为未来灵活方便的数据密集型信息高速公路。通过在单一硬件平台上提供集成的数据传输方式、强大的多业务支持能力以及完善的带宽管理功能。

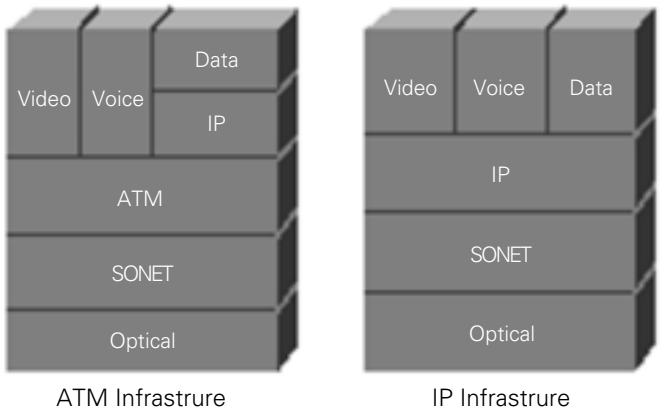
Cisco ONS 15454可以大大降低网络设备需求和服务提供成本，在为服务供应商提供无以伦比的光传输能力和无限的带宽扩展能力的同时，最大限度地保护现有的网络投资。这样，整个教育城域网的骨干网就形成了以ONS为中心的基于SDH的骨干网络。

为保证骨干网络的可靠性，我们建议所有设备都采用双连。每个中心节点连到另外两个相邻节点ONS 15454上，这样确保网络的冗余可靠性。

区域级网络：在具备了以ONS 15454为骨干网络设备的同时，我们建议采用Cisco GSR、OSR7600或Catalyst6500园区骨干网交换式路由器作为教育城域网的区域级设备。GSR、OSR7600或Catalyst6500上使用Packet Over Sonet/SDH模块（POSIP）通过SDH线路或使用千兆以太网模块通过1000Mbps以太网线路连至ONS。OSR7600或Catalyst6500上百兆/千兆/万兆以太网端口可用于连接接入级网络或连接局域网内的其它设备。

OSR7600或Catalyst6500系列园区网交换式路由器提供线速、无阻塞IP、IPX和多层交换的功能，并提供高级的服务质量（QOS）。OSR7600或Catalyst6500为第2/3层交换提供720Gbps交换式结构，总吞吐量为每秒四百万个数据包，因在每个线卡上都使用了高速应用专用集成电路（ASIC）技术，确保他们执行真正的第三层交换。它还有希望取消居于中间的ADM。IP交换速度的提高、其经济性以及基于语音和视频产品的发展使这种配置早已成为现实。

图3



Cisco公司的Packet over SONET/SDH将IP层直接放在SONET/SDH层之上，并且在提供服务保证的同时避免了管理SONET之上及ATM之上的IP所需的间接费用（见上图）。Cisco公司的POS能够更好地适应迅速发展的网络通信流量、提供第一个创建基于IP的多服务网络的可靠方法，这已被GTE Internetworking、Qwest、Sprint、UUNET、中国电信、网通等国内外领先的服务供应商所采用。

内嵌RPR的MSTP

什么是内嵌RPR的MSTP？

在现有的光传送网中，除了承载着大量的TDM业务以外，实际上还有不少数据通信业务，如POS接口、帧中继和ATM协议。由于以SDH为基础的传输体系是首先为TDM业务为服务对象的，缺乏对数据业务的有效处理，如突发性能管理、多点到多点业务的连接等，所以电信运营商一直致力于在充分利用现有传输资源的基础上，寻找一个更为有效的传送数据业务的方式。

随着 Ethernet Over SDH（EoS）技术出现，衍生出了我们称之为 MSTP 的产品（在国际电信行业中大家称其为 MSPP）。GFP、VCAT 和 LCAS 等技术在一层（Layer 1）的处理上解决数据传送的标准化和带宽调整。但是，也出现了一种看法，认为 GFP、VCAT/LCAS 是 MSTP 的技术精华和全部。但从数据网络的技术特征和数据业务的实际应用看问题，在带宽资源的充分利用上，我们会有另外的认识。目前，弹性分组环 RPR 和针对数据特性的 QoS 技术在 MSTP 的推广应用就是为了更有效地在以 SDH 为技术核心的光传送网络中，很好地提供数据业务。

关于 GFP，VCAT 和 LCAS

采用传统的 EoS 技术实现以太网的连接，往往可能存在下面一些缺陷：

- “电路模式”只能提供点对点的以太网端口的连接；
- “电路模式”的一层（Layer 1）EoS 技术无法提供多个业务的统计复用；
- 一旦将某个以太网端口“静态”地分配到某个电路中（也就是说将其映射到 SDH 的某个虚容器中），它将独占该带宽，不可能有“突发”流量；
- 使用 SDH 保护机制会使得系统资源占用增加一倍；
- SDH 的虚容器不能提供足够细化的传输带宽，通常只能是 2M（VC-12）、50M（VC-3）、155M（VC-4），或它们的倍数（VC 的连续级联，如 VC-4-4C、VC-4-16C）；
- 当需要更改电路带宽时，必须在网管系统中做重新配置。

虚连接（VCAT）和链路容量调整技术（LCAS）可以较好解决上面提到的最后两个问题。GFP 封装技术主要是解决不同厂商的 MSTP 产品之间以太网业务互通问题。由此可以看见，还需要其它的技术来解决数据业务的统计复用、多点到多点连接、允许过量使用电路（突发业务）、不需预留传输带宽的情况下完成业务的自愈保护等等。

完成点对点以太网端口的透明传输连接不是 MSTP 技术和产品的最终目的，这应该只是 MSTP 的应用之一。尤其是在城域网应用环境下，在尽量靠近最终用户的设备上提供统计复用功能可以为运营商节省设备开支，提高系统的资源利用率。

以太网业务结构类型

为了更好理解上面提出的观点，我们下面分析一下以太网业务类型。我们根据用户的各种应用环境，大致可以将以太网业务结构分成两大类：

- 专有业务网：在一个网络中为一个用户提供点对点或多个节点上的互连。不同的用户各自占用独立的网络带宽。业务的带宽通常由 SDH 的虚容器大小来决定，如 2M（VC-12）或 155M（VC-4）等等。
- 共享容量网：在一个网络中为多个用户提供点对点、多点对多点的业务互连。通常是在一个 SDH 的虚容器或某一个 GE 的 trunking 中有多个用户存在。

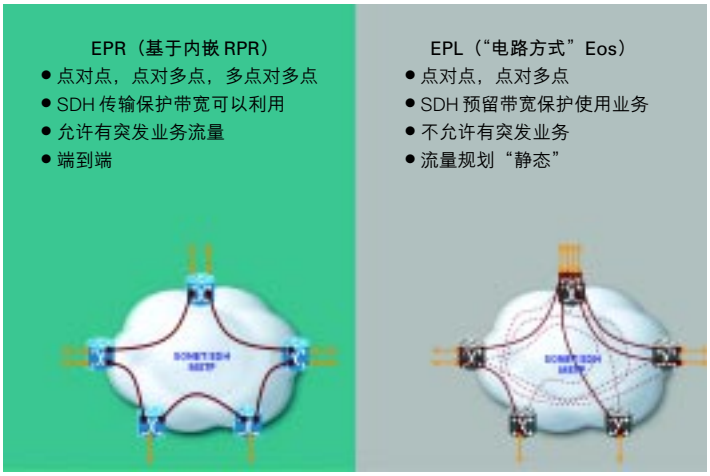
“专有业务网”非常 TDM 电路的业务模型方式，非常适合需要独占带宽、极高安全性能的高端用户。而大多数的驻地用户或流量不均匀的业务都可以采用“共享容量网”方式，最大限度地提供网络的资源利用率，这时候，通常需要将 MSTP 网络和二 / 三层数据网络或 MPLS 网络配合在一起来实现。MSTP 主要实现以太网的统计复用和传输连接；二 / 三层数据网络或 MPLS 网络来完成终结、转发业务功能。

单就 MSTP 系统来看，我们可以将以太网在 SDH 网络中细分为两类：

- 以太网专线业务（EPL-Ethernet Private Line）：客户端的以太网直接映射到 SDH 的某些虚容器中，MSTP 设备不对以太网中的数据流做任何进一步的识别或处理。
- 以太网私有网业务（ERP - Ethernet Private Ring）：在 MSTP 网络中利用 SDH 的某个独立的带宽（虚容器）来完成多个节点上以太网的互连，构成一个独立的 LAN。

下图给出了两种类型的业务模型的示例和主要区别。

图 4
EPL vs. EPR



以太网私有网业务（EPR）的实现

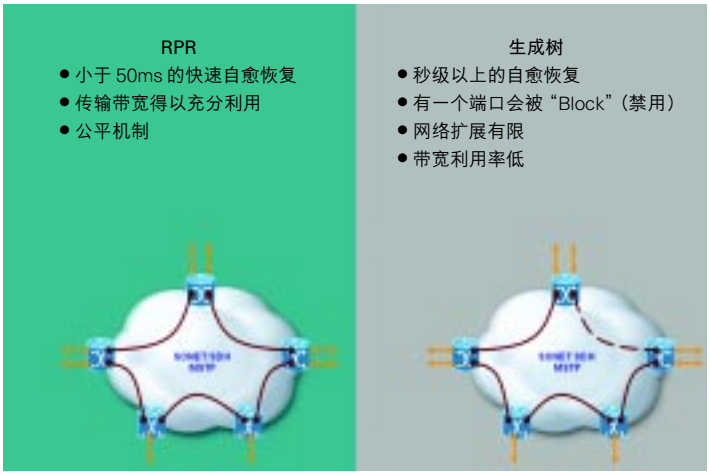
对电信运营商而言，由于市场竞争加剧，传统的点对点TDM电路租线的利润在不断下降。EPR以太网业务模式通过多点对多点的连接方式和对突发流量的处理，可以为运营商带来更多的增值服务。为了实现以太网私有网业务EPR，目前通常在MSTP设备中是采用基于STP（生成树）或RSTP（快速生成树）的“共享以太环网”技术。但是，更为先进的是象思科公司采用的内嵌式RPR技术。

RPR 技术提供了：

- 类似 SDH 的 50ms 快速业务自愈能力。
- 双向传输数据业务提高带宽利用率。
- 网络上业务多点与多点的互连。
- QoS 管理功能

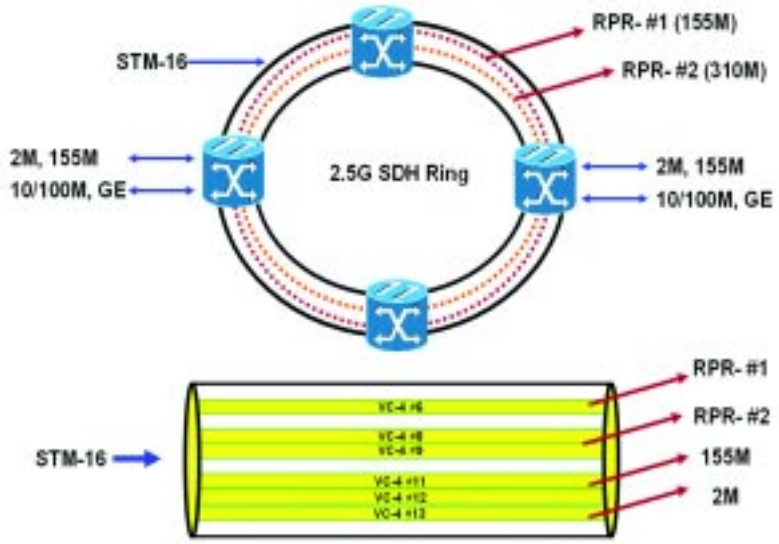
这些功能都是生成树无法实现的，也就是说“共享以太环网”技术无法和RPR比拟。下面有图示做一个比较：

图 5
在 MSTP 上采用
RPR vs 生成树



在MSTP系统设备中采用RPR技术被称为“内嵌式RPR”。简单说就是划分SDH的部分带宽构成RPR逻辑虚拟环。如下图，在一个2.5G的SDH环中可以指配定义一个155M的RPR环路（RPR - #1）和一个310M的RPR环路（RPR - #2），其中，RPR-#1环使用一个VC-4资源和另一个RPR-#2环使用了另外2个VC-4资源。

图6
RPR over SDH

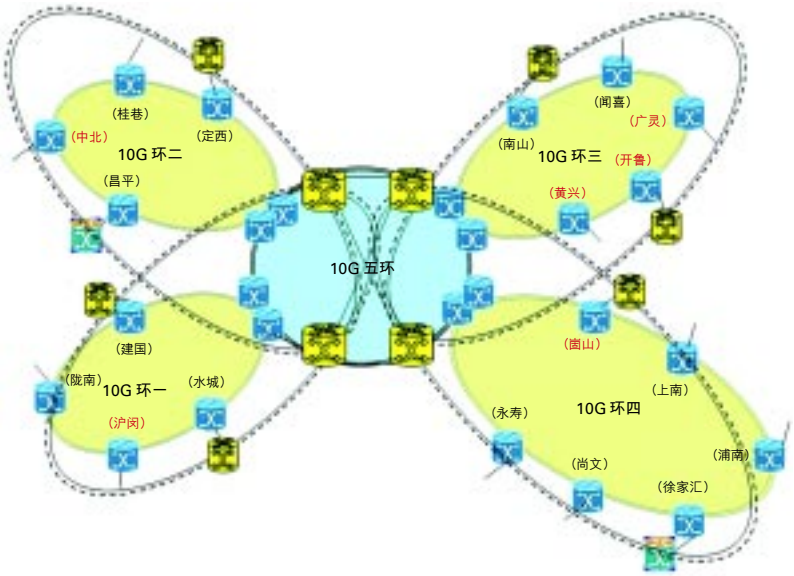


SDH的其它资源带宽还可以继续用于传统的TDM业务传输。MSTP节点上的数据业务可以以10/100M或GE端口方式接入RPR环。目前已商用化的思科公司MSTP产品还能基于以太网物理端口、VLAN、IP DSCP等特性进行数据业务的分类，同时配合响应的策略(Policing)和队列(Queue)机制完成业务全面的QoS管理。这样一来，我们还可以在一个RPR环通过VLAN或QinQ等标签技术把若干不同类型的业务进行分类处理。

因此，采用内嵌式RPR的MSTP技术可以为运营商带来全新的业务模式:

- 在光传送网络中直接提供独享带宽的多点连接方式的VPN业务。VPN适合对安全性和带宽有很高要求的业务。业务的网络拓朴结构可以是点对多点汇聚或多点对多点；
- 提供高品质的视频组播。利用内嵌式RPR环上提供的组播/广播功能，大大节省光传送网络的传输带宽；
- 结合二层交换技术和QoS管理特性，在RPR环上接入多种类型的业务，如Internet业务、IP-VPN等。利用光传输网络的覆盖面，把内嵌式RPR的MSTP技术作为“精品数据网”（即所谓的高性能要求的IP网络）的汇聚和接入手段之一。

图 7
RPR Over SDH
应用



10GE ——万兆以太网

万兆以太网技术以简单的以太网技术为基础，为网络主干提供 10Gbps 的带宽。与其它速率相当的网络技术相比，万兆以太网的搭建成本较低，实施技术相对简单，是在传统以太网基础上的拓展。

1999 年底 IEEE 成立了 802.3ae 工作组开始万兆以太网技术的研究。2002 年 6 月 802.3ae 10GE 标准正式发布。图为 IEEE 802.3ae 万兆以太网技术标准的体系结构。

图 8

在物理层，802.3ae大体分为两种类型，一种为与传统以太网连接速率为10Gbps的“LAN PHY”，另一种为连接SDH/SONET速率为9.58464Gbps的“WAN PHY”。每种PHY分别可使用10GBase-S（850nm短波）、10GBase-L（1310nm长波）、10GBase-E（1550nm长波）三种规格，最大传输距离分别为300m、10km、40km，其中LAN PHY还包括一种可以使用DWDM波分复用技术的“10GBASE-LX4”规格。WAN PHY与SONET OC-192帧结构的融合，可与OC-192电路、SONET/SDH设备一起运行，保护传统基础投资，使运营商能够在不同地区通过城域网提供端到端以太网。

802.3ae目前支持9um单模、50um多模和62.5um多模三种光纤，而对电接口的支持规范10GBASE-CX4目前正在讨论之中，尚未形成标准。

接口类型	应用范围	传送距离	波长	线缆类型
10GBase-LX4	局域网	300 米	1310nm	多模光纤
		10 公里	WWDM	单模光纤
10GBase-SR	局域网	300 米	850nm	多模光纤
10GBase-LR	局域网	10 公里	1310nm	单模光纤
10GBase-ER	局域网	40 公里	1550nm	单模光纤
10GBase-SW	广域网	300 米	850nm	多模光纤
10GBase-LW	广域网	10 公里	1310nm	单模光纤
10GBase-EW	广域网	40 公里	1550nm	单模光纤
10GBase-CX4	局域网	15 米	–	4 根 Twinax 线缆
10GBase-T	局域网	25-100 米	–	双绞铜线

在数据链路层，与传统的以太网相同的是，802.3ae继承了802.3以太网的帧格式和最大/最小帧长度，支持多层星型连接、点到点连接及其组合，充分兼容已有应用，不影响上层应用，进而降低了升级风险。与传统的以太网不同的是，802.3ae仅仅支持全双工方式，而不支持单工和半双工方式，不采用CSMA/CD机制；802.3ae不支持自协商，可简化故障定位，并提供广域网物理层接口。

由于万兆以太网的帧格式和帧尺寸大小等都与所有以太网技术相同，不需要对网络做任何改变，利用交换机或路由器可以与现有低速的以太网用户和设备连接起来，对于千兆以太网相对于其它高速网络技术在经济性和管理性能方面都是较好的选择。凭借强大的伸缩性，万兆以太网已经成为以太网家族的第四个成员。

在城域网应用中，有很多新的应用需求不断出现，包括视频和音频。以前人们认为这些对时延要求高的应用只有在ATM这样的网络上才能实现，然而现在一些新技术（交换技术、视频压缩技术，如MPEG－2）、新协议（RTP、RTCP、RSVP等）和新标准（如802.1Q、802.1p等）的出现使得在城域网骨干—万兆位以太网也可以极好地支持视频和音频等多媒体数据应用。

万兆以太网的设计非常灵活，几乎对网络结构没有限制，可以是交换式、共享式的或基于路由器的。现在正在应用的网络互连技术，例如，特定IP交换技术和第三层交换技术，都与万兆以太网完全兼容。万千兆以太网可以通过价格便宜的交换机或路由器来实现。

万兆以太网的技术优点主要包括：

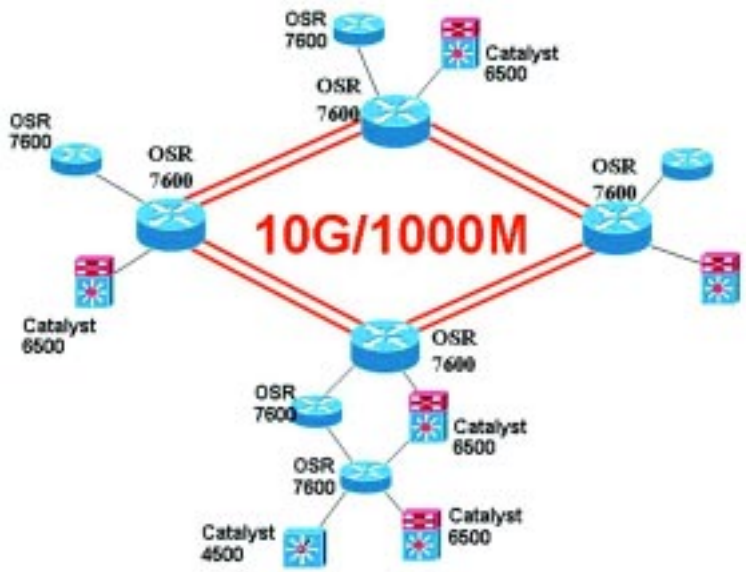
- 实现技术简单，保留了以太网的帧格式、管理工具等。
- 便于升级，无需引入新的技术即可平滑地过渡到万兆以太网，无论现有是传统以太网、快速以太网或是千兆以太网。
- 网络投资得到保护，无需对用户进行额外培训。
- 具有有良好的互操作性和向后兼容性。
- 端口价格相对较低。
- 提供10倍于千兆以太网的传输速度。

对于城域网来说，要求能够支持宽带、窄带、实时、非实时业务等多种业务。但目前的TDM资源调度困难，难以综合宽带、窄带业务，对于具有突发特征的非实时业务而言，TDM方案并不理想。相比之下，IP技术在支持实时业务取得了长足的进展，目前正逐步进入商业运营如IP电话、基于IP网络的可视化通讯等。对于非实时业务，IP技术已经能够全面支持。应用决定网络的发展，城域网的未来必将是以IP网络为主体。万兆以太网由于与传统以太网一脉相承，能够完全融入现有IP网络，形成全面IP化的万兆以太网，顺应网络发展的趋势，充分保护客户的投资。

教育城域网万兆骨干网应用设计

在教育城域网的万兆骨干网的建设中我们建议采用Cisco OSR7600系列路由器平台来完成万兆骨干网络的高速连接和路由计算。该系列产品集成全新新路由转发引擎的高性能的720Gbps交换矩阵，可提供每插槽40Gbps的全双工容量。同时该系列路由器能支持非常丰富的接口模块，对诸如第三代的高性能千兆位和万兆位以太网接口、所有的LAN、WAN接口模块以及广泛采用的FlexWAN和光服务模块等众多服务模块都能很好兼容，为教育城域网的接入提供了灵活的手段，扩展了其作为核心网络节点的功能，大大提高了嵌入式网络服务的能力。

图9



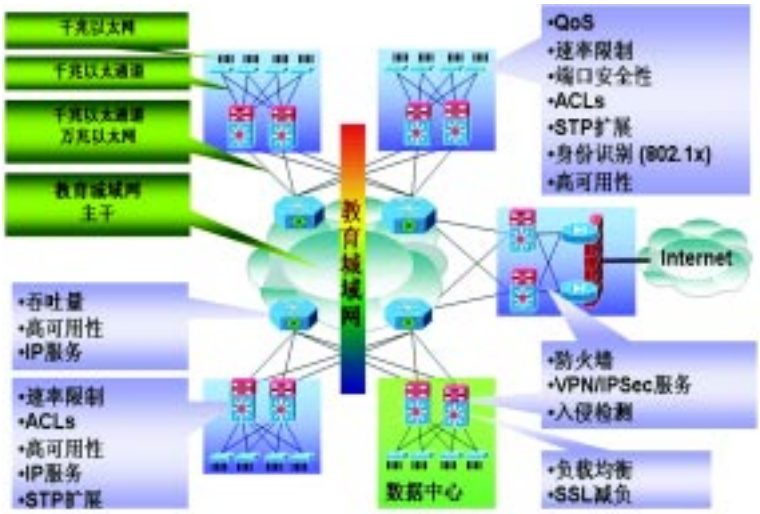
教育城域网的建设

作为网络传输技术的现实载体，网络设备支撑整个网络的运转，如何选择网络设备自然是重中之重。

对于教育城域网的建设我们需要考虑以下问题：

- 如何保证网络的可靠性；
- 如何在网络中嵌入安全；
- 如何确保网络、应用的高性能；
- 如何进行控制和管理；
- 如何扩展。

图 10
教育城域网功能设计模型



如何保证网络的可靠性

一般来说，网络的可靠性是为了避免单点故障的出现。主要体现在两个方面：一方面在于网络拓扑的设计，尽量使网络上不存在单点故障；另一方面，网络设备必须支持插卡、接口、电源等部件的冗余与热插拔能力以及支持例如 VRRP/HSRP 等冗余协议。在教域城域网的建设中，我们主要考虑骨干网络的可靠性。但是网络的可靠性并不是单一设备可靠性的简单叠加，它主要包括：

- 设备级可靠性
- 链路级可靠性
- 软件级或系统级可靠性

设备级可靠性

设备级的高可靠性设计是网络核心设备选型时最关键因素。此时我们往往只考虑设备硬件的冗余，忽略了运行和存储于硬件上的软件、网络信息和管理信息。

一般情况下，设备级的可靠性主要包括：

- 物理冗余：提供双电源、双引擎、双交换矩阵和双时钟，甚至双核心设备。
- 逻辑冗余：利用 Ethernet Channel、FastEthernet Channel 和 Gigabit Ethernet Channel 技术为设备间链路提供负载的分担和链路的冗余；利用 VRRP/HSRP 技术为第三层路由提供冗余，并利用所形成的虚拟路由器实现路由器之间的负载分担和冗余操作。
- 独立的可重置模块：模块的重置只局限于模块自身，并不会导致其它模块或整机的重置。
- 路由处理器冗余（RPR+）：路由处理器冗余 +，RPR+ 特性是 RPR 特性的增强。当主处理引擎与备用处理引擎发生切换时，它可以避免板卡的复位和重加载。与 RPR 相比，RPR+ 准许切换时不对接口卡进行重置，进一步加快了 RSP 切换的速度。RPR+ 保持第 2 块引擎处于“暖启动”状态，保持路由、QoS、ACL 信息同步更新，从而实现主备引擎之间 0.06~3 秒的快速切换，灾备时间减少 50%。
- 无停顿转发（Nonstop Forwarding，NSF）和状态切换（Stateful Switchover，SSO）功能：用于维护路由器中两个交换引擎之间路由状态信息，使主备引擎可以在不中断网络运行或丢弃包的情况下进行切换；在切换期间，Cisco SSO 提供零中断第 2 层连接，而 Cisco NSF 转发第 3 层数据包时保证不丢失分组，或丢失量最小。分组连续转发可以重新建立对等关系，而无需在整个网络中再次收敛路由协议。
- 不间断系统运行的软件升级（ISSU）：升级系统的软件或软件模块不会中断或影响系统的操作。

链路级可靠性

网络链路级可靠性可以分为 2 层路由链路和 3 层路由链路两个方面：

- 更快的链路灾备
  - 快速生成树：为了解决了物理线路中断所造成的网络终端，我们往往会设置备份的物理线路，但是它们往往会形成环路，回路会产生无休止的数据路径，导致网络服务的中断以及额外的系统管理费用。IEEE802.1D生成树协议通过从网格化物理拓扑结构而构建一个无环路逻辑转发拓扑结构，提供了冗余连接，消除了数据流量环路的威胁。原始生成树协议 IEEE 802.1D 通常在50秒内就可以恢复一个链接故障[融合时间=(2xForward_Delay)+Max_Age]。当设计此协议时，这种停机还是可接受的，但是当前的关键任务应用（如语音和视频）却要求更快速的网络融合。为加速网络融合并解决与生成树和虚拟LAN（VLAN）交互相关的地址可扩展性限制的问题，IEEE 委员会开发了两种新标准：在 IEEE 802.1w 中定义的快速生成树协议（RSTP）和在IEEE 802.1s 中定义的多生成树协议（MST）。如果使用适当的话，RSTP 能将在连接故障和恢复时所需的重新配置和恢复服务时间，减少到低于秒的量级，并保持同基于 STP 设备的兼容性。RSTP 可以保证在一个桥接 / 交换、桥接端口或 LAN 发生故障之后，其连接性的快速恢复。一个新的根端口可以快速转换至传送端口状态。在LAN中桥接与转换之间明确的应答，允许指定端口快速转换至传送端口状态，此时，桥接端口可被配置在桥接 / 交换重新初始化时直接转换为传送端口状态。当特定的桥接端口连接于 LAN 边缘的一个 LAN 段时，这一点将十分有用，例如在该 LAN 段没有其它的桥接或交换可用的情况时。

  - PortFast：生成树协议会运行在交换机的所有端口上，但接入层交换机的许多端口连接着工作站或服务器，这些点到点连接是不会出现环路的。PortFast 技术将这类端口从 STP 的计算中排除出去。当主机连接到交换机时，启动 PortFast 的端口将直接成为转发状态，避免了 STP 计算造成用户在最初一段时间不能使用网络的情况，将工作站或服务器连接上网的时间减至最短。针对 Access 端口跳过 listening-learning 阶段。

  - UplinkFast：当接入层交换机有两条链路连接汇聚层设备时，如果出现环路肯定会有一条链路在 STP 计算时被阻断掉。在主链路断掉时，被生成树阻断的端口需要重新进行计算，在经过 50 秒后被打开参与用户数据的转发。在访问层交换机上启动UplinkFast功能后，如果交换机在直连的主链路上检测到失效，那么交换机会立即将被阻断的备份端口打开转发数据，通常情况下只需要 2 到 4 秒钟的时间。这样就可以通过 UplinkFast 提高交换网络的收敛速度。

  - BackboneFast：汇聚层交换机与主干交换机之间为保证链路的可靠性，往往会形成环形链路，环形链路上某个链路或接口的故障会引起生成树的重新计算。在主链路断掉时，被生成树阻断的端口需要重新进行计算，在经过20秒的最大等待时间（Max_Age）后进入侦听（listening）状态，在经过 30 秒后被打开参与用户数据的转发。在汇聚层交换机上启动 BackboneFast 功能后，如果交换机在非直连的主链路上，即迂回链路上检测到失效，交换机快速收敛去掉最大等待时间（Max_Age）20 秒，因此可以节省生成树的计算时间至 8~30 秒。

  - 增强功能：UDLD（线路单通问题自动诊断功能），用于检测光纤或铜缆以太网链路上的故障。由于生成树具有单向的 BPDU 流，对这种故障相当敏感。在一个端口突然不能发送 BPDUs的时候，引起邻居的STP状态改变，导致邻居的 “blocking” 端口切换到 “forwarding” 状态。由于原 forwarding 端口仍然可以接收包，从而引起环路。因此，UDLD 可以监视物理电缆的配置，并将通过 “ErrDisabled” 状态将配置不正确的端口给 down 掉。避免出现单向连接，当检测到一个因为介质或端口故障导致的单向连接时，将端口 shutdown 并标识为 “ErrDisabled” 状态，同时产生一个 syslog 信息。

- 更全的链路捆绑
  - Cisco PAgP 和 IEEE 802.3ad：
    - > PAgP是一个用于在检查Channel两端的参数的一致性以及在出现增加链路或链路失效时的重新适配的一个管理协议，PAgP 协议控制每个独立的物理或逻辑端口打成 Channel 的行

为，如果一个Channel中的某个链路失效（拨掉光纤或光纤断了）了，agport会进行更新，流量会在现有的端口上重新进行hash计算，不会有包丢失。

> 源自思科ISL的802.3ad把两个或多个Link捆绑成逻辑的虚拟的单一通道，子Link之间提供自动流量负载平衡和冗余，很大程度上会简化系统集成，减少升级骨干网络的投资。

– 点到点的冗余连接

– 在重新建立的链路仍可进行负载均衡，链路恢复时间小于1秒

- 更强大的路由灾备
  – VRRP/HSRP：虚拟路由器冗余协议/热备份路由器协议，实现VRRP/HSRP的条件是系统中有多台路由器，它们组成一个“热备份组”，这个组形成一个虚拟路由器。在任一时刻，一个组内只有一个路由器是活动的，并由它来转发数据包，如果活动路由器发生了故障，将选择一个备份路由器来替代活动路由器，但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换的问题。

  – GLBP：网关负载平衡协议，相对于HSRP与VRRP，GLBP具有很多的优点，在保护第一个跳动路由器的同时能在所有可用路径上分配分组负载，使得网络带宽的利用率更高。以前，如果主路由器或路径中出现错误，则第一个跳动冗余功能只能在备份WAN路径上转发分组。GLBP可使组中的任一路由器担当备份作用，并能简化配置。最大的区别是在HSRP和VRRP中同一个GROUP中只有一个路由器在转发流量，其余路由器只是起备份作用，而在GLBP中，同一个GROUP的所有路由器（最多4个）可以同时转发流量。这样就起到了负载均衡的作用。

系统级可靠性

系统级可靠性是指软件重新加载或升级时，系统重新启动对网络运行所造成的影响。系统级可靠性在建网过程中往往容易忽略，但是对于主干网络设备来说，连接中断所造成的影响会很快波及整个网络。因此，尽可能大的缩短系统软件的加载时间才可以有效提供系统级可靠性。在有“Cisco IOS 暖升级”的情况下路由器丢失分组转发低于30秒钟。

如何在网络中嵌入安全

网络安全的发展经历了三个阶段：附属式安全、集成式安全和嵌入式安全。

第一阶段，附属式安全。这是我们最常见的一种形式，各种安全设备单独存在于网络之中，通过网络线缆连接到相应的网络设备上。这种形式比较适合于中小企业的建网模式，其性能要求不高，网络连接的可靠性要求也不高。并且当网络中存在多种安全设备（如防火墙、IDS、VPN等）时，数据包在进入内部网络之前，不得不往返于交换机和多种安全设备之间，受中间连接带宽的限制，网络传输的性能不会很高。

第二阶段，集成式安全。为了解决附属式安全的问题，以思科为代表的众多网络设备厂商在防火墙、路由器和三层交换机的软硬件中集成了防火墙或者IDS或者VPN等单项安全防护功能，类似于叠加的模式。这样做虽然有效地解决了中间连接线缆的不可靠性问题，同时也减少了信息包往返于交换机和多种安全设备之间所带来的网络延迟，但是由于这些设备多属网络边缘设备，因此设备自身的性能不够高，限制了在大型网络中的应用。并且功能的缺憾是集成式安全无法完全满足网络安全要求的症结所在。特别是在城域网骨干网中，大量数据进行路由、交换、安全控制所带来的处理压力要求在大型的核心骨干设备上支持这些功能，并且完全模块化，独立处理。这就使得网络安全进入了第三个阶段。

第三阶段，嵌入式安全。为了解决前两个阶段一直未能解决的性能和功能缺失的问题。思科公司重新对路由器和交换机的软硬件结构进行了设计，提出了嵌入式安全的概念。尤其是在城域网的核心骨干设备上，多种安全服务模块的集成使得网络核心交换机真正做到了：

- 基于网络的安全特性；

- 更容易捕捉到病毒和攻击；
- 自我防御、保护、复原和预防；
- 控制访问与被访问的对象；
- 性能大大提高；
- 网络拓扑得到简化；

思科核心交换机 / 路由器上的安全服务模块包括：

模块	性能	模块	性能
防火墙模块	• 4-20Gbp 处理能力 • 3-12Mpp 包转发能力 • 可处理 1-400 万个并发连接 • 可形成 256 个虚拟防火墙	IDS 模块	• 600Mbps 处理能力 • 可处理 50 万个并发连接 • 启发式分析、异常分析能力
VPN 模块	• 保持 8000 个并发隧道 • 1.9Gbps 包转发能力	网络分析模块	• 性能监控及分析 • 故障定位 • 流量分析 • 容量设计
SSL 模块	• 300Mpps~1.2Gpps 吞吐量 • 6 万 ~24 万并发连接	内容交换模块	• 20 万应用连接 • 100 万并发连接

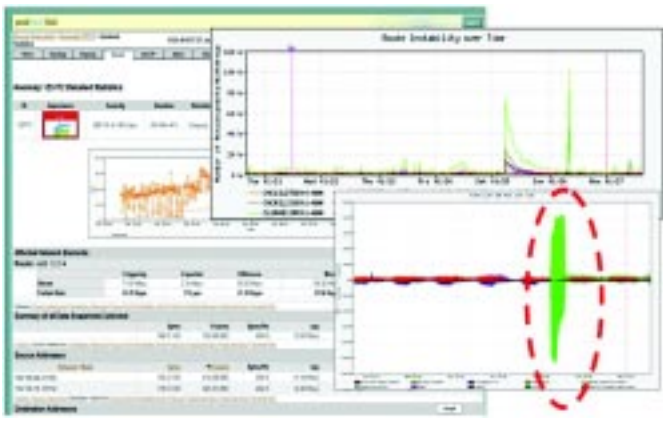
这些模块为每一种安全处理提供了独立的高性能硬件处理平台，同时利用核心交换机/路由器的高速交换矩阵将处理完后安全的信息快速地在网络中进行传递。由于多种安全模块可以同时集成在核心设备内部，因此它不仅有效解决了安全功能的缺失，同时更为城域网核心骨干设备带来了高性能的安全处理，解决了长期以来一直困扰城域网核心设备的“牺牲性能保证安全”的问题。

在这些安全服务模块中，网络分析模块的引入增强了安全服务管理和控制能力：

- 支持 7 层分析功能；
- 对网络中的任意端口、模块、网段、虚拟网进行数据采集和分析；
- 通过图形化界面有效显示、识别和管理；
- 可扩展至多个，提高处理性能。

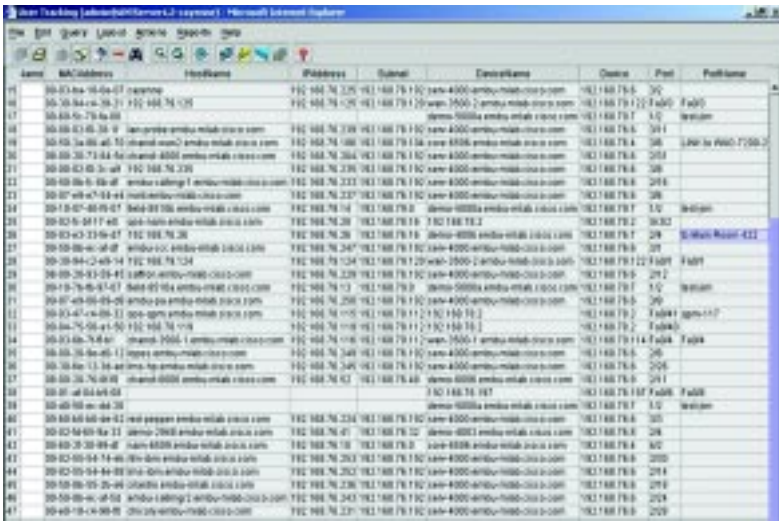
高性能的网络分析模块使得网络安全技术能够更准确及时地看到问题源点，找到安全问题的始作俑者。

图 11
网络流量分析——及时发现网络攻击



以“SQL的Slammer蠕虫”病毒为例，网络分析模块可以通过图形化的方式显示病毒发生的时间段、流量的大小和变化情况。

图12
定位用户——USER TRACK功能



通过网络分析软件中的用户定位功能，我们不仅可以看到问题源点的IP地址和MAC地址，同时我们也可以更具体的看到问题源点多连接的交换机和相应的接口，准确地定位，找到问题源点。

如何确保网络、应用的高性能

设备级高性能

安装于Cisco Catalyst 6500系列交换机和Cisco 7600系列路由器上的Supervisor Engine 720-3BXL（Sup 720-3BXL）是面向万兆骨干网络设备的第三代超级引擎。该模块提供了硬件加速IPv4、IPv6和多协议标记交换（MPLS）等可扩展的增强式服务，从而满足了服务供应商和企业客户不断增长的数据板要求。Cisco Sup 720-3BXL集成了一个高容量的交叉式交换矩阵，每插槽可提供40Gbps的容量，总系统容量可达720Gbps。

Cisco Sup 720-3BXL在单个模块中集成了一个高性能的720Gbps交换矩阵，该矩阵带有一个新的路由和转发引擎。这一集成的交换矩阵可提供每插槽40Gbps的全双工容量，因此能够支持第三代的高性能、高密度千兆位以太网和10千兆位以太网接口以及所有现有的LAN、WAN和服务模块，包括已被广泛采用的FlexWAN和光服务模块，因此可支持各种WAN边缘汇聚部署，从DS-0到OC-48/STM-16。Sup 720-3BXL建立在已得到验证的思科快速转发架构（CEF）的基础上，支持集中式转发（思科快速转发）和分布式转发（分布式思科快速转发），提供了一个高度可扩展的和经济有效的平台。

Cisco Sup 720-3BXL提供了一个具有模块性、永续性、可扩展性和安全性的第2层和第3层解决方案。Cisco Sup 720-3BXL支持各种特性，包括QoS、基于硬件的普通路由封装（GRE）隧道机制和访问控制列表（ACL），使客户能够构建高性能的、特性丰富的网络，提供MPLS VPN，城域汇聚和各种WAN边缘服务。

在硬件指标的背后，思科公司所采用的先进的软件技术支撑起了系统在城域网核心骨干上，面对多种业务流的大负载冲击下仍然能够出色的发挥“多业务，高性能”的作用。这其中我们要提到两种业界领先的技术：TCAM（三重可寻址内存）和CEF（思科快速转发技术）。

三重内容可寻址内存：交换机和路由器在转发数据时，如果转发数据在决定向何处转发时花了很长的时间，那么以线速转发数据是不可能的。目前表查询所采用的主要机制是内容可寻址内存（Content Addressable Memory，CAM）和三重内容可寻址内存（Ternary Content Addressable Memory，TCAM）。

在常规的CAM查询中，所有信息都是重要的，换句话说，我们不希望错过任何内容。这是只有2个数据位“0”和“1”的二进制带来的功能。但由于查询整个数据结构的匹配（MAC地址是48位，IP地址是32位）需要花费时间，因此这个功能是受到约束的。

TCAM的三重机制为二进制的潜力增加了又一个选项，即“不必关注”，通常被显示为字母X。这意味着数据可以使用标记技术进行查找，即我们希望匹配“1”和“0”的位，而忽略X的位。

举例来说，在一个标准的CAM中，IP地址172.16.0.0的查询需要匹配32个1和0的位。但是如果我们希望找到网络172.16.0.0/16的匹配，那么我们真正只需要映射前16位。由于我们只要寻找我们希望匹配的那些位，无关的位将被标记为X，因此查询速度将大大加快。

思科快速转发技术：CEF不同于其它的多层交换技术，即它没有传统意义上的缓存。缓存导致了很多问题需要解决。例如，缓存保持有效的时间应该是多少？缓存增长的大小允许是多少？我们如何处理那些使缓存条目是小的路由拓扑变化？

Cisco公司一直致力于试图对缓存的工作进行优化，但是问题依然存在。看起来只有使用路由标记才是进行第3层数据转发的好办法。但是所有的工作又都会变慢。实际上，没有必要这样做。如果建立了一个拆开形式的路由表，和一个分离的邻接表（它与分离的ARP缓存很相似），那么大家就可以一举两得。表位于接口附近，将数据从繁忙的路由处理器和总线分离出来。并且由于表与主路由标保持联络，因此总是保持最新的内容。

CEF维护着两个分开的但又相关的表，转发表（forwarding table）和邻接表（adjacency table）。转发表包含路由信息，邻接表包含第2层下一定址信息。CEF使用trie代替树。trie是与数据结构一起使用的指针，其中数据结够并不真正包含数据。

数据结构上的分离意味着查询过程可以递归进行，准许为连续的信息包选择不同的路由，因而实现逐包的负载分担。而且，如果缓存中的信息发生了改变，由于查询每次都是独立进行的，因此总是会采用最新的信息进行。

CEF转发带来了更高的吞吐量。实际上，速度增长的大部分都归因于交换机或路由器内部的专有结构，包括ASIC的使用和专门的总线和内存的分配。而且信息包不再需要通过内部总线转发到繁忙的路由处理器，大多数路由器延迟都会在那里发生。CEF还有一些其它的优点，比如支持逐包负载分担的能力，这一点是旧有的交换技术使用缓存条目所无法达到的。

正是依托上述这些先进的技术，Cisco Sup 720-3BXL才能够在城域网核心骨干上，面对多种业务流的大负载冲击下仍然能够发挥出色的 “多业务，高性能”的作用。

应用级高性能

在信息服务业日趋发达的今天，不仅上网用户数指数增长，而且服务的业务种类也逐日增加。而其中十分受用户欢迎的多媒体应用如视频点播（VOD）、远程教育、视频会议、IP电话、IP/TV等，不仅仅是在带宽方面提出了更高的要求，而且在服务优化方面提出了更加深层次的要求。

在实际网络中，用户的环境是复杂的，面临着数据、视频等IP实时业务的混合使用，IP数据的传输特性是突发性的，有可能造成瞬间网络线路阻塞，干扰其它应用的传输，而IP语音视频的传输特性是实时性的，允许少量丢包，但不允许出现延迟。因此，实现QoS（服务质量）的IP网络是成功企业网络建设的关键。

Cisco 端到端的服务质量管理由 Cisco IOS 的 QoS 服务充分体现出来。Cisco IOS QoS 服务由三个关键主件构成：一个快速发展的构件和功能集；一个高度灵活、用于制定策略的工具，它利用构件控制网络资源的分配，以支持客户和应用程序的要求；以及一个功能分布主件，它优化了网络在服务配置和带宽 / 容量增长方面的可伸缩性。

Cisco IOS QoS 服务允许网络边缘和主干之间划分网络功能。功能的分布能力使网络具有性能和服务的可伸缩性。

在网络边缘，能够灵活地设置：
- 制定划分业务类和服务级别的策略。
- 定义网络资源的分配和控制策略。
- 高效地将分组包映射到业务类。
- 运用策略满足客户的应用程序和安全性要求。
- 收集和输出关于网络流量和服务资源的详细统计数据。

在网络的主干上，Cisco IOS QoS 及其支持技术提供如下功能：
- 调整网络，以提供高容量、高性能和高可靠性。
- 提供策略管理和强制功能。
- 提供合理的排队和拥塞管理功能。

下面介绍几种 QoS 技术：

用于业务分类的 IP 优先权

IP 优先权提供了将业务划分为多个服务类的功能。网络管理员可以定义多达六个服务类，并利用扩展访问控制列表（扩展 ACL），为每个服务类定义拥塞处理和带宽分配策略。IP 优先权功能利用在 IP 头上用于标识服务类型（Type-of-Service）的三个比特位,确定 每个分组的服务 类。IP 优先权功能为预定分配提供了相当的灵活性，包括客户分配（如根据应用程序和访问服务器）和基于 IP 或 MAC 地址、物理 端口或 应用程序的网络分配。

IP 优先权功能既可采用被动模式（接收客户分配的优先权），也可采用主动模式,此时，网络根据预先定义的策略设置优先权或超越客户分配的优先权。IP 优先权可被映射到邻接技术（如标记交换、帧中继 或 ATM），在非均匀网络环境下提供端到端的 QoS 策略。在不改变现有应用程序，不需要复杂化网络信令的前提下，仅利用 IP 优先权功能就可建立服务类等级。

用允许访问速率（CommittedAccessRate）管理访问带宽

CAR为网络管理员提供了一个为业务目的地分配带宽,并制定超过带宽分配额度时的业务处理策略的工具。CAR 既可以用于网络入口也可以用于网络出口。CAR 阈值可根据访问端口、IP 地址和应用程序设定。CAR 测量业务负载，限制带宽资源分配，能适应 IP 业务固有的流量突增特点。

CAR 利用扩展 ACL 对超出分配带宽的业务制定处理策略，包括重新定义带宽可用阈值、修改分组的优先级、制定分组丢弃原则等。CAR 策略的选择包括：
- FirmCAR：丢弃超过分配带宽的分组。
- CAR+Premium：为分组重新定义更高或更低的优先级。
- CAR+BestEffort：丢弃之前先为其分配一个极大的阈值。
- PerApplicationCAR：为不同的应用程序制定不同的策略。

用于拥塞管理的随机早期预测（RED）

RED为网络管理员提供了灵活制定流量控制策略的能力，使其能在拥塞情况下保持尽可能大的吞吐量。RED 与抗干扰的传输协议（如TCP）协同工作，可根据如下的实现算法智能化地避免网络拥塞：

- 区分网络可适应的临时性流量爆炸和将耗尽网络资源的极度超载；
- 提供公平的带宽递减策略，按比例减少带宽的可用额度。RED 和 TCP 协同工作，在大流量出现时，能预先控制拥塞，并用丢弃分组的方式，保持大吞吐量。同时，RED 也为网络管理员提供了相当灵活的参数设置手段，包括调整队列长度阈值的最大值和最小值、分组丢弃几率和MIB，分组交换和分组丢弃的管理策略等。

加权 RED，基于服务类的拥塞管理（WRED）

WRED 结合了 IP 优先权和 RED 功能，为不同类别的服务提供不同的性能——对优先权较高的分组优先处理。 WRED 在拥塞情况下仍 能进行优先处理，而且不会加剧拥塞。网络管理员可以灵活地为不同的服务类定义排队长度最大和最小阈值以及分组丢弃率。系统还为每个服务级别提供MIB，以实现网络管理的可见性。

根据服务类别加权公平排队（WFQ）

WFQ提供了这样一种能力，在为较低优先级业务公平分配现有带宽的同时，保证要求低延时的高优先级和低优先级流。高优先级流立即得到处理，低优先级流则插入队列，按比例共享现存带宽。在出现拥塞时，低优先级流的分组可能被丢弃。CiscoIOS QoS 服务提供了基于服务类型的分布式WFQ，从而提高了性能和可扩展性。

资源保留协议（RSVP）

多媒体应用可以使用 RSVP 对必需的网络资源进行动态的请求和保留，从而满足其特定的 QoS 要求。通过代理 RSVP 功能，Cisco 的路由器可使用 RSVP 代表那些无 RSVP 功能的应用对资源发出请求。

QoS 机制是保障数据网络中多媒体应用（IP 视频）、关键应用（等）实时、及时、可靠、快速无阻塞传输的重要手段。思科公司可以提供业界最完整、最完善、最灵活的实现和保障机制。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19一21层
邮编：100738
电话：(8610)85155000
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32一33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)85193000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86961000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn

欢迎下载电子文档，http://www.cisco.com/cn/power/industry/edu/index.shtml

2005 年 3 月印刷