数字图书馆推广工程

网络体系建设

2018.10.10

数字图书馆推广工程
DIGITAL LIBRARY PROMOTION PROJECT
www.ndlib.cn

一、数字图书馆推广工程网络平台建设

虚拟网技术介绍

推广工程虚拟网项目介绍

推广工程虚拟网建设成果

虚拟网实际操作

数字图书馆推广工程
DIGITAL LIBRARY PROMOTION PROJECT

虚拟网的概念

虚拟专用网VPN（Virtual Private Network）是指利用密码技术和访问控制技术在公共网络中建立的专用通信网络，将远程的分支机构、商业伙伴、移动办公人员等连接起来，并且提供安全的端到端的数据通信的一种技术。

虚拟：体现在并不存在一条实际的物理通路，不需要建设或租用专线，而是建立一条虚拟的通路，就可以实现属于自己的专用网络；

专用：体现在其稀有性和安全可靠性，且对数据进行加密以确保机密性。

虚拟专用网（VPN）优势

- 安全性：主要采用四项技术来保证其安全性，分别为：隧道技术、加密技术、密钥管理技术以及身份认证技术。
- 稳定性：在公用网络上建立专用的通信通道，不影响现行业业务的正常运行，保证了网络的稳定性。
- 节省成本：由于搭建VPN是利用现有的公用网络，无需租用昂贵的专线，因而降低了连接成本。
- 可扩展性：VPN使用运营商的互联网基础设施，组织可轻松的添加新用户，具有较好的可扩展性。

虚拟网技术分类

按应用场景

- 站点到站点
- 远程接入

按实现技术

- Ipsec VPN
- SSL VPN
- MPLS VPN
- L2TP
- PPTP

主流虚拟网技术

目前，常见的主流VPN技术主要包括三大类，即：IPSec VPN技术、SSL VPN技术和MPLS VPN技术。

其中IPSec VPN和SSL VPN在图书馆的资源远程访问方面更具优势，并已有所应用。

主流虚拟网技术介绍

- **IPSec VPN**

IPSec VPN工作在网络层，通过创建安全隧道提供接入，一旦隧道创建，用户终端就如同物理地处于同一局域网中，实现对整个网络的透明访问。

IPSec VPN通过保证端点到端点的网络传输通道的安全来对传输数据进行高安全级保护。由于IPSEC VPN是基于互联网进行数据传输，因此网络服务质量较难得到保证。

另外，IPSEC VPN需要解决防火墙穿越与IP地址冲突等技术问题才能保证网络良好的延展性，这成为虚拟网建设所要解决的一个关键性问题。

在经济性方面，每增加一个虚拟网络节点，就需要添加一台IPSEC VPN设备，随着建设规模的扩大，要不断购买新的设备来满足组网需要。

●SSL VPN

安全套接层（SSL，Secure Socket Layer）协议由Netscape通信公司提出，用于促进电子商务站点的发展，通过使用此协议可进行数据加密、用户验证，用户会话可以被安全的建立起来。

SSL（安全套接层）协议位于传输层和应用层之间，建立的是一条会话层的通道，是基于应用的,广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输,工作流程包括服务器认证和用户认证，主要用来认证用户和服务器、加密数据、维护数据的完整性。

主流虚拟网技术介绍

- **SSL VPN**

SSL VPN是基于SSL协议和反向代理技术建立的一种远程访问VPN技术，它为远程用户访问敏感公司数据提供了最简单最安全的解决方案。

就加密方式来说，SSL VPN只对通信双方的某个应用通道进行加密，并未对通信双方的主机之间的整个通道进行加密。

SSL VPN也是承载在公众互联网上，因此在网络服务质量方面，与IPSEC VPN一样，很难得到保证。

经济性方面，SSL VPN只需要在中心节点放置一台SSL VPN设备，就可以实现所有用户的远程安全访问，具有良好的经济性。

主流虚拟网技术介绍

● MPLS VPN

MPLS VPN是一种基于MPLS技术的IP-VPN，是在网络路由和交换设备上应用MPLS技术，利用结合传统路由技术的标记交换实现的IP虚拟专用网络，使数据包传送的延时时间减少，增加网络传输的速度，更适合多媒体信息的传送。

MPLS VPN采用路由隔离、地址隔离和信息隐藏等多种手段提供了抗攻击和标记欺骗的手段，但这种逻辑上的隔离不能很好解决管理型共享网络普遍存在的非授权访问受保护的内部(或者核心网)攻击等安全问题。

MPLS VPN将三层路由与二层交换完美结合，确保了数据传输的网络服务质量。

经济性方面，MPLS VPN尽管相比租用专线可以较大地节省成本，但需要一次性投入工程费、资源费以及本地接入费用等，这些成本是大于IPSec VPN和SSL VPN的设备费用的。

虚拟网技术介绍

推广工程虚拟网项目介绍

推广工程虚拟网建设成果

虚拟网实际操作

数字图书馆推广工程
DIGITAL LIBRARY PROMOTION PROJECT

推广工程虚拟网建设背景

- 2011年5月，财政部、文化部联合发文，在全国范围内实施“数字图书馆推广工程”。
- “数字图书馆推广工程”将推广国家数字图书馆工程的理念、技术、标准，建设分布式公共文化资源库群，形成覆盖全国的数字图书馆虚拟网，借助手机、数字电视、移动电视等为代表的新兴媒体，以互联网、移动通信网、广电网为通道，向公众提供个性化、多样化、全媒体数字图书馆服务。

推广工程虚拟网建设背景

《通知》明确提出要建设以国家数字图书馆为核心，以省级数字图书馆为主要节点的全国性数字图书馆虚拟网。虚拟网的建设是推广工程的基础性建设之一，是全国各地数字图书馆资源与服务全面共建共享的基础支撑。

数字图书馆虚拟网将连接省、市级图书馆，实现公共图书馆的网络体系纵向贯通。将国家数字图书馆已完成的标准规范、软硬件系统和资源建设成果通过虚拟网方便、快捷、安全地传输，达到在全国各地图书馆的推广使用的目的。

虚拟网建设面临的挑战

VPN技术多样

- 三种主流技术优缺点各异

软硬件基础设施差距

- 省馆互联网出口带宽
- 辐射人群
- 网络安全保障

网络建设复杂、要求高

- 安全和稳定性
- 访问效率：应用系统产生大量的业务数据、读者资源，涵盖文本、图片、音乐、视频等
- 扩展性
- 适应性

➢ 技术方案选择

通过虚拟网技术的比较分析可以看出，SSL VPN是面向站点到客户端的技术，提供基于应用层的访问控制，因而更适合于大量分散移动用户的远程安全接入，而不适应于建设站点到站点的全国数字图书馆虚拟网；

MPLS VPN虽然能满足站点到站点的组网需求，但在经济性方面要求较高，而推广工程虚拟网的支持经费有限，因而也不适用于组网要求；

IPSEC VPN是站点到站点的组网技术，在经济性方面，只需要购买一台IPSEC VPN设备即可打通VPN隧道，组建虚拟网，因此，只要能够解决IPSEC VPN的防火墙穿越技术难题，便可以在不用更改各地图书馆网络拓扑的情况下完成虚拟网的建设工作。

➢ 技术选择

SSLVPN	IPSEC VPN	MPLS VPN
• 提供基于应用层的访问控制 • 不适合建设站点到站点的全国数字图书馆虚拟网	• 站点到站点的组网技术 • 经济性 • 需解决IPSEC VPN的防火墙穿越技术	• 站点到站点的组网技术 • 经济性方面要求较高

➢ 技术方案选择

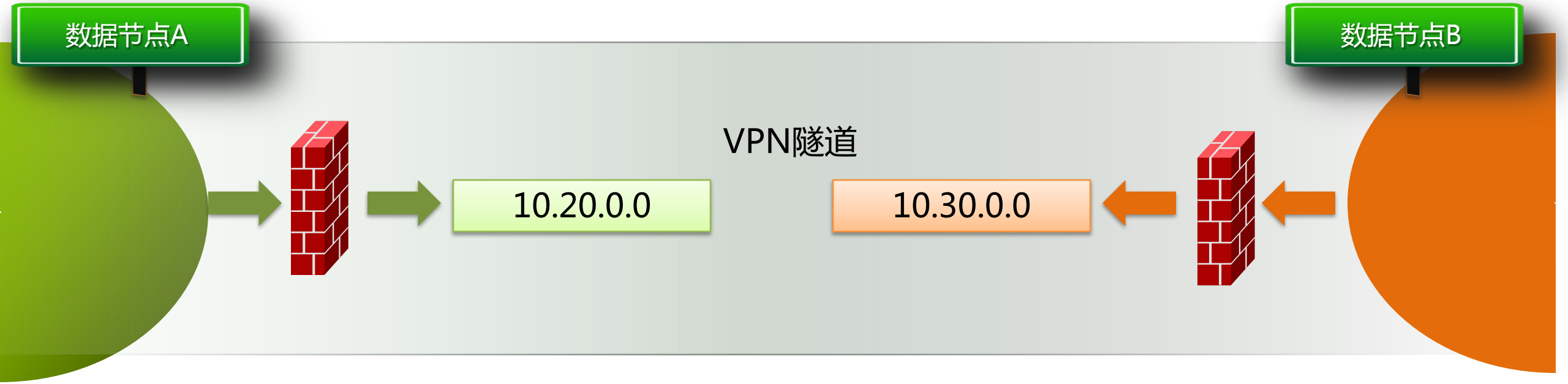
- **经过技术攻关，IP地址冲突带来的防火墙穿越问题能够被很好地解决，同时根据虚拟网上传输的数据类型，并结合各地图书馆调研情况，以及对加密性与灵活性的考虑，数字图书馆推广工程采用IPSec VPN技术来组建虚拟网。**

➢ 虚拟网架构设计

虚拟网的整体网络架构为：利用各节点自身互联网链路，通过IPSec VPN技术组成虚拟网，实现各节点的互联互通。组成国家图书馆到省馆和各个省馆到市馆的网络，两级网络能够互相连通。国家图书馆作为数字图书馆虚拟网的网络中心，与各个省馆、市馆之间能够在虚拟网上相互通信。

➢ 虚拟网IP地址规划

1 各图书馆需要访问虚拟网上的资源时，需要把图书馆的IP地址通过地址转换(NAT)转换到所分配的虚拟网地址
2 图书馆需要向虚拟网发布资源时，也要把服务器IP地址转换到所分配的虚拟网地址



➢ 虚拟网IP地址规划

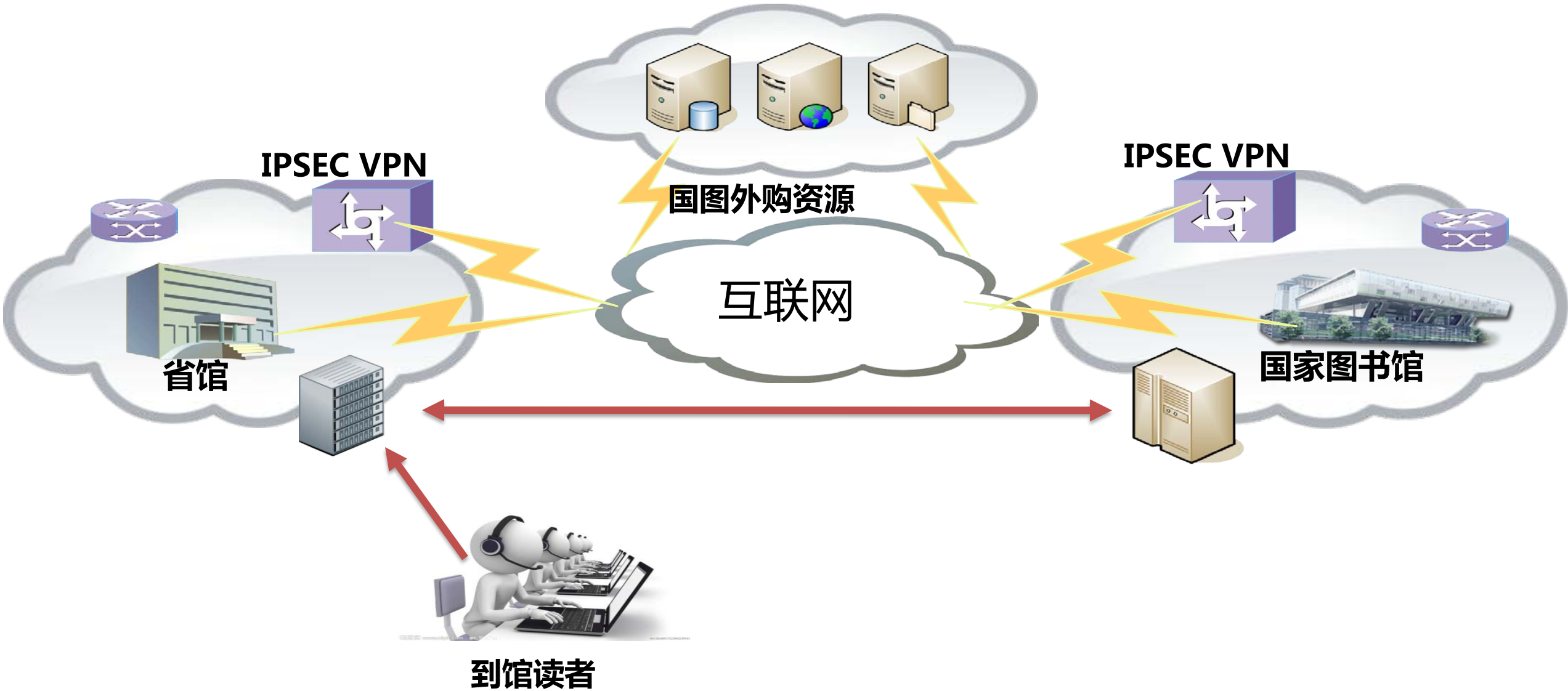
规划规则为：
第一，数字图书馆虚拟网计划使用10.0.0.0/8地址段；
第二，每个省级馆分配1个B类IP地址；
第三，每个副省级馆分配2个C类地址；
第四，每个地市级馆由所在省馆规划若干个C类地址。

虚拟网资源共享实例

A省馆访问资源时，通过对目标地址的解析确定访问路径，若访问的是虚拟网资源，则通过IPSEC VPN通道来获取国家图书馆资源（包括国家图书馆自建资源和外购资源），反之仍按照原有路由进行访问。下图展示了资源数据传输流向，要实现对虚拟网中双方多种资源的有效访问需要完成如下连接调试步骤：

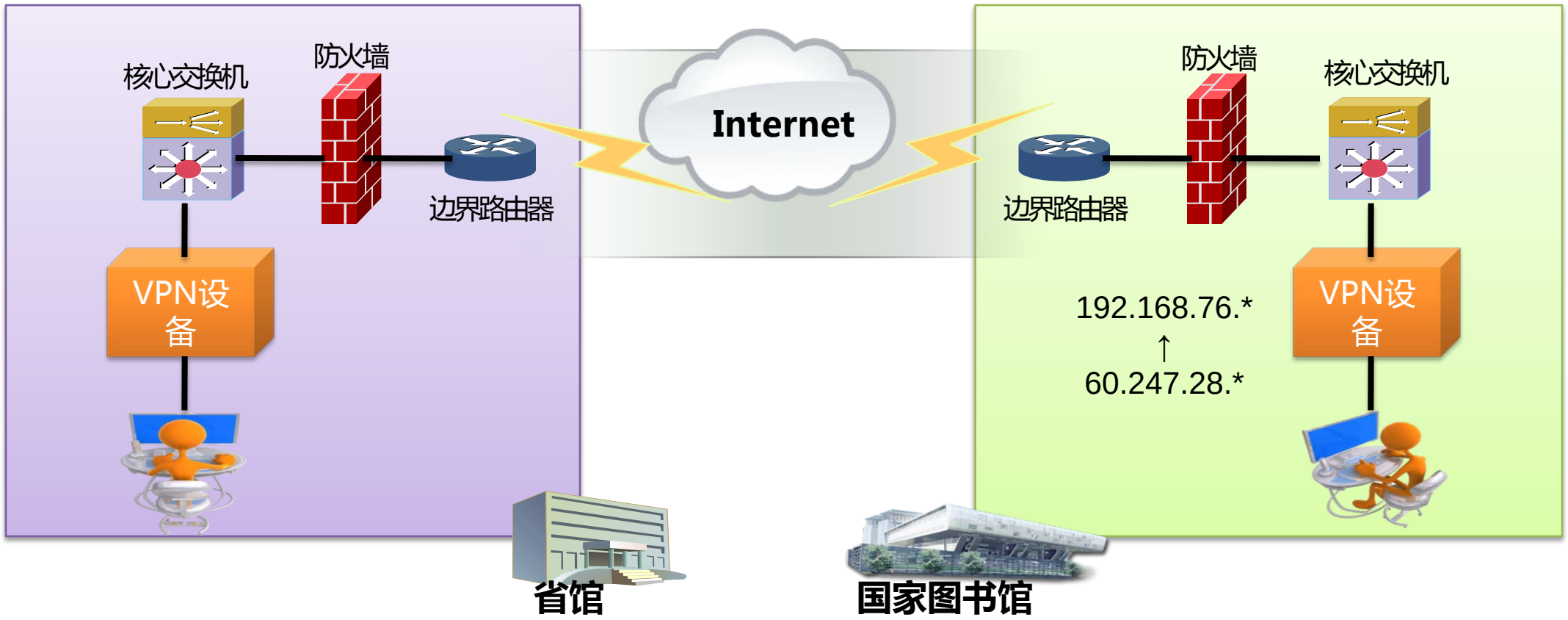
第一，使用VPN设备建立国家图书馆到A省馆的VPN隧道；
第二，使用防火墙地址转换规避两馆间内网IP地址冲突；
第三，内网资源服务器访问；
第四，静态IP外购数据库资源访问；
第五，动态IP外购数据库资源访问。

虚拟网资源共享实例



虚拟网资源共享实例

1.建立连接&VPN隧道
使用单臂连接



虚拟网资源共享实例

2.地址转换（NAT）

使用防火墙地址转换规避两馆间内网IP地址冲突

两馆均使用防火墙对原IP地址段进行转换：
A省馆：
国家图书馆：

使用ping命令可以彼此连通对方的虚拟网地址

虚拟网资源共享实例

3.内网服务器访问
服务器地址：192.168.180.97，国家图书馆通过虚拟网设备进行地址转换，转换成10.100.1.1，通过虚拟网隧道进行数据传输，

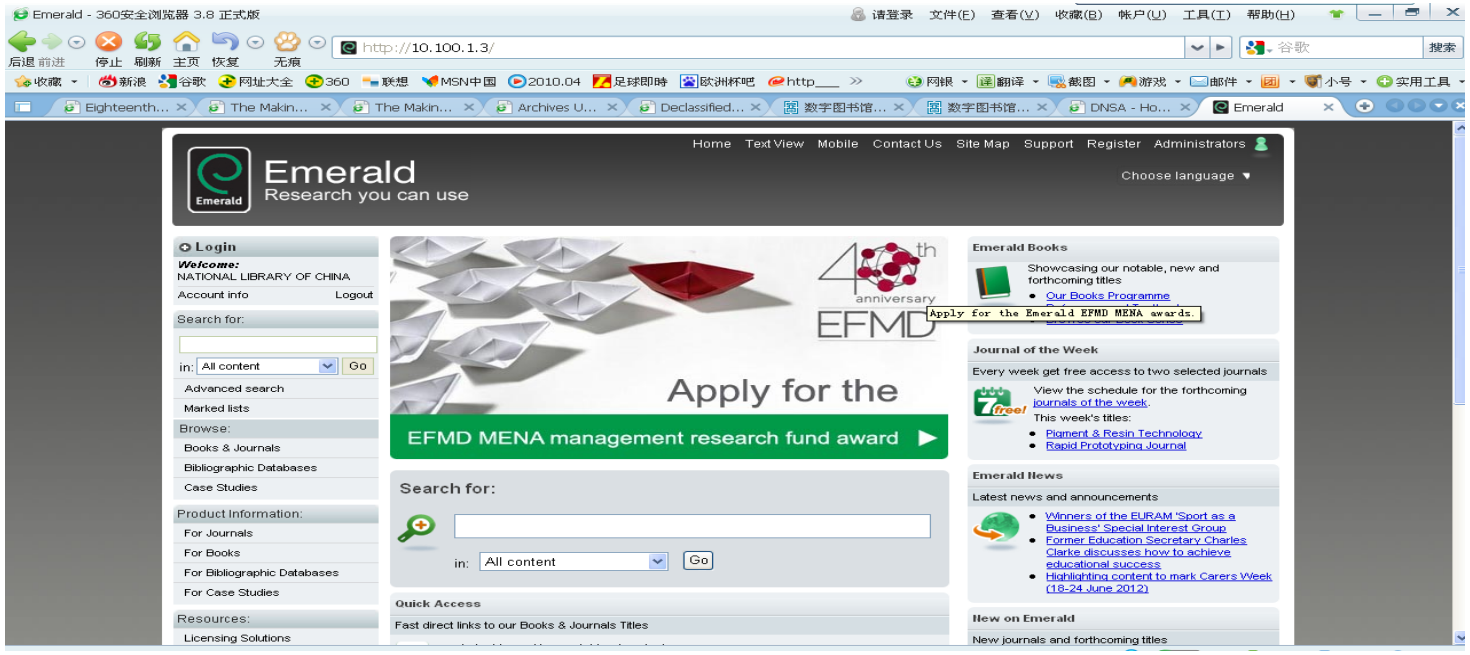
虚拟网资源共享实例

4.静态IP外购数据库资源访问

国家图书馆外购数据库资源Emerald回溯期刊数据库

公网地址为195.92.228.61，虚拟网转换后地址为10.100.1.3

A省馆直接访问转换后的地址10.100.1.3，便可以通过虚拟网隧道进行传输，该请求在国家图书馆防火墙转换成该资源登记的公网地址195.92.228.61，并且从国家图书馆网络出去访问该资源



虚拟网资源共享实例

5.动态IP外购数据库资源访问

首先找到某一资源对应的所有IP地址，在省馆的核心交换机上面配置路由，凡是访问这几段IP地址的请求全部指向省馆VPN设备，然后再通过与国家图书馆建立的VPN隧道，进行数据的传输，实现资源的访问。

省馆到馆读者可通过域名来访问某一资源

推广工程虚拟网实施规划

实施时间

2011-2012年为虚拟网基础构建阶段，主要完成省级数字图书馆和部分市级数字图书馆的硬件平台搭建工作。
2011年在全国范围内选择15个省馆和152个市馆实施推广工程的硬件平台搭建工作，其中东、中、西部地区各5个省馆。这部分已经全部连通。
2012年完成其他省馆（含新疆生产建设兵团）和部分市馆的虚拟网搭建工作，并着手进行推广工程资源共享的建设工作。完成了15家。
2013年完成剩余19家副省级以上图书馆的虚拟网连接工作。
目前共完成54家省市级图书馆的虚拟网连接工作。

职责分工

国家图书馆在文化部、财政部的指导下负责虚拟网的顶层规划和总体方案、组织实施和日常管理工作，对各省、市级机构进行全面指导。

副省级以上图书馆的虚拟网搭建工作，由国家图书馆牵头负责实施。省级馆在国家图书馆的指导下负责本省范围内地市级图书馆虚拟网的搭建、监督与管理工作。

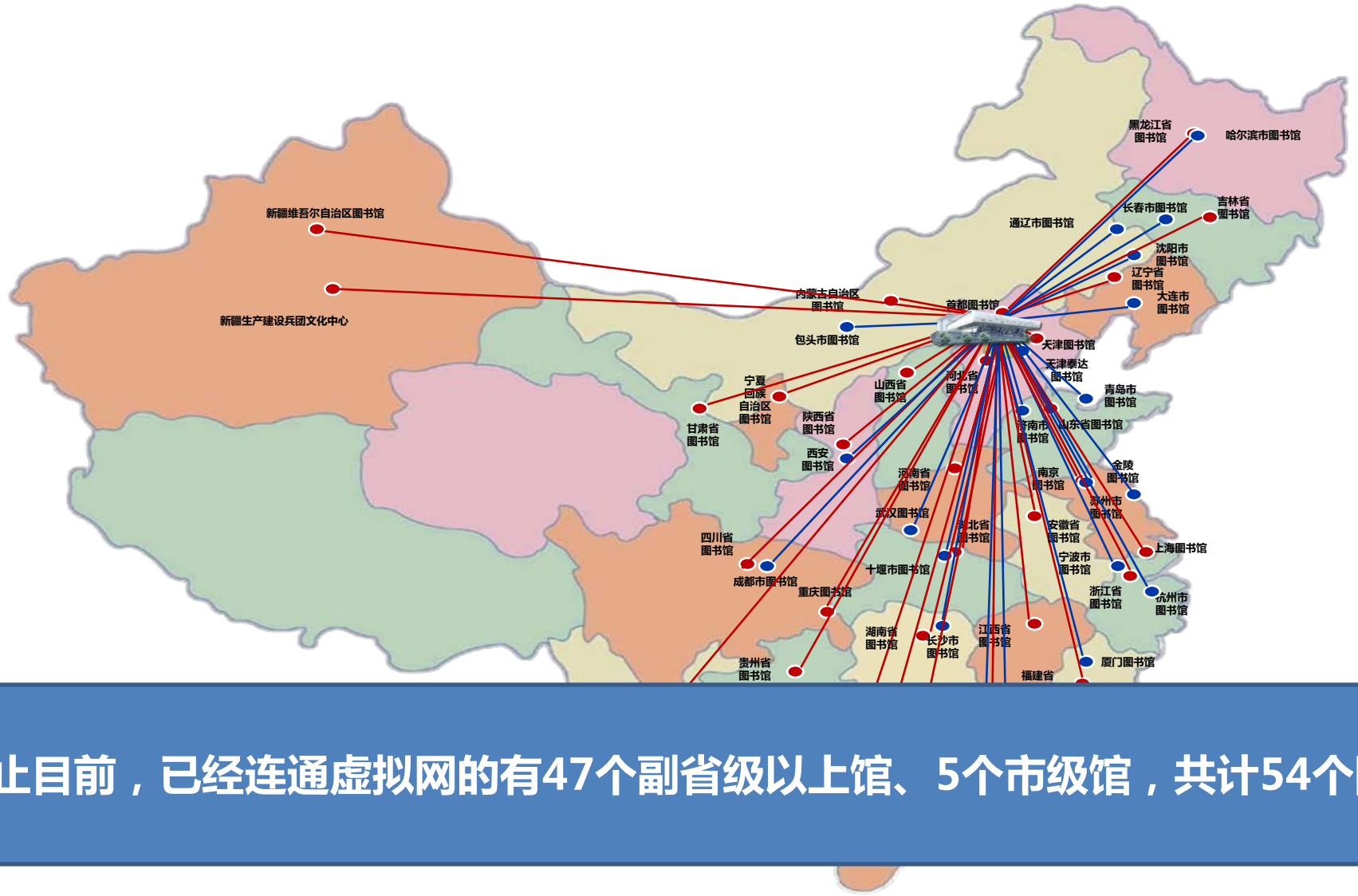
虚拟网技术介绍

推广工程虚拟网项目介绍

推广工程虚拟网建设成果

虚拟网实际操作

推广工程虚拟网建设成果



截止目前，已经连通虚拟网的有47个副省级以上馆、5个市级馆，共计54个图书馆。

推广工程虚拟网建设成果

国家图书馆已向每个开通虚拟网的图书馆开放总量超过145TB的中外文数字资源。

中外文期刊
700余种

教学课件
7万余个

档案全文
18万余份

讲座和地方戏曲
3000余种

中外文图书
100余万册

中文报纸
300余种

图片
1万余种

音乐
10万余首

虚拟网技术介绍

推广工程虚拟网项目介绍

推广工程虚拟网建设成果

虚拟网实际操作

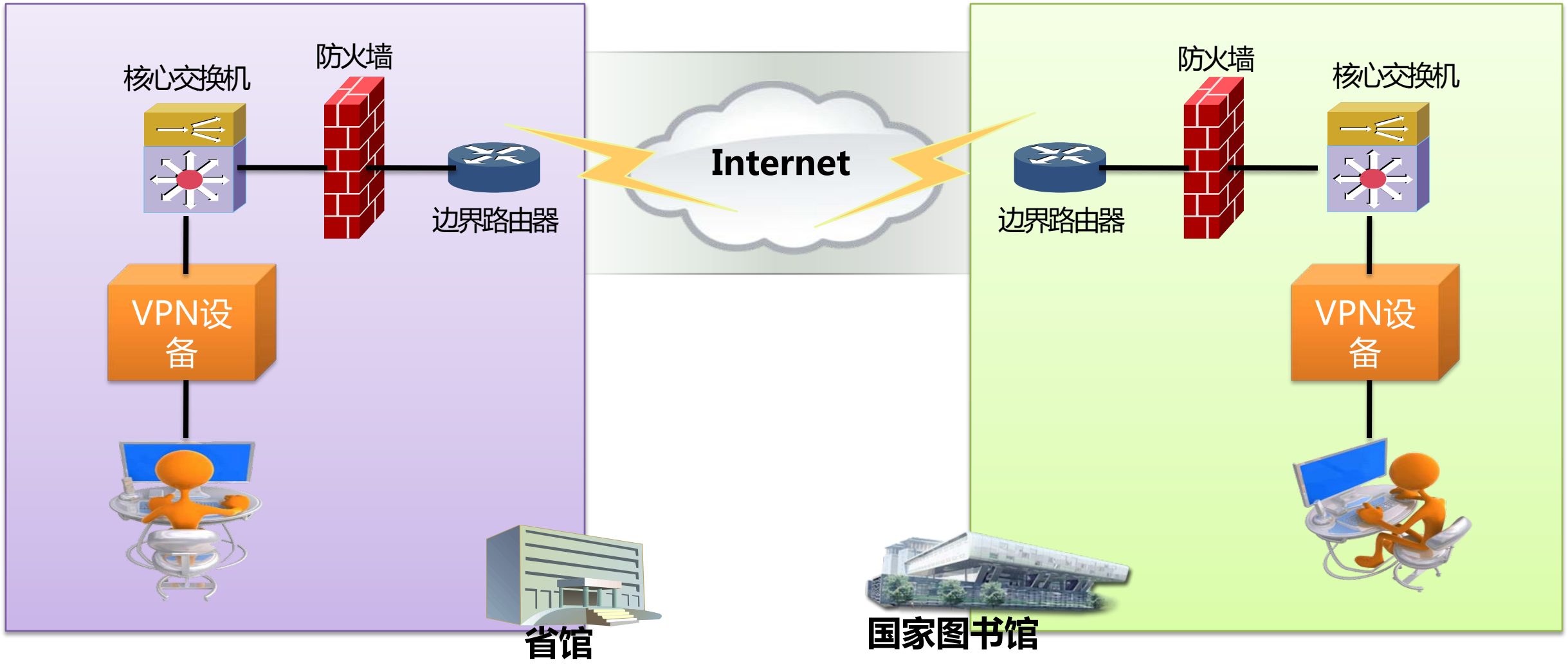
数字图书馆推广工程
DIGITAL LIBRARY PROMOTION PROJECT

虚拟网实际操作

让我们一起搭建虚拟网吧！

虚拟网实际操作

➢ 前期准备



2、内网路由配置

当内网用户访问虚拟网资源时，应指向虚拟网设备，应在相关网络设备上添加对应路由。

以国图访问某省馆资源为例，路由如下 ：
ip route-static 10.*.*.* 255.255.0.0 192.168.*.1
当访问某省馆资源时，路由指向虚拟网设备地址192.168.*.1，优先级不设置，默认为60

ip route-static 10.*.*.* 255.255.0.0 192.168.*.2 preference 10 当访问某省馆资源时，路由指向专网设备地址192.168.*.1，优先级为10，高于虚拟网路由

现处于虚拟网和专网的并行阶段，虚拟网的优先级低于专网，因此当同时存在虚拟网和专网时，优先选择专网，虚拟网用于备份

3、常见问题解答

Q：隧道不能成功协商，一直处于“正在协商”状态，是由何原因造成的？

A：如果一直处于正在协商，请仔细检查两端配置的各参数是否一致，包括加密算法、认证算法等，另外有些设备的密钥为非明文显示，可重新输入进行再次确认。

虚拟网实际操作

Q：为何第一阶段协商、第二阶段协商两端参数配置完成且无误时，隧道不能成功建立？

A：此时可能受双方网络架构的影响，如果两端的VPN设备均处于内网，配置有内网地址，即不在边界，通过其外部的网络设备将其映射至公网地址。此种情况下，通常可将一方的对端地址设置为动态地址，即0.0.0.0，本地/对方标识与其它隧道不重复，IKE协商模式为主模式，主动发起隧道协商选“否”，由另一端进行主动发起隧道。

虚拟网实际操作

Q:为何建立多条隧道？

A：由于有些资源不能通过IP地址进行访问或者其IP地址不固定，此时不能按静态地址转换方式进行访问，因此提供给省馆的地址并非规划的虚拟网地址，不在隧道的保护子网范围，而省馆的VPN设备不支持添加虚拟路由，此时，采用新建隧道的方式实现此类资源的访问。

数字图书馆专网背景

数字图书馆专网建设面临的挑战

数字图书馆专网架构及组网技术实现方案

数字图书馆专网展望

数字图书馆专网背景

随着推广工程建设的推进，加之传统图书馆的业务交互不断扩展，各地图书馆的互联网既承载普通互联网服务、又承担图书馆间业务系统的虚拟网互联。因此，依托互联网链路的IPSEC虚拟网在可用带宽、传输速率、稳定性等诸多方面逐步不再满足推广工程建设的要求。要突破虚拟网的瓶颈，满足数字图书馆开放式、联合式的发展需求，通过专线的方式组建数字图书馆专网，且实现与原推广工程虚拟网链路的互相备份，是提升推广工程网络服务体验的唯一方法。

数字图书馆专网背景

2013年启动

选取基于电路交换技术的光传输网络

独享信道级网络

国家图书馆的专线带宽为2.5G，各省级馆到国家图书馆的专线带宽为155M

数字图书馆专网背景

数字图书馆专网建设面临的挑战

数字图书馆专网架构及组网技术实现方案

数字图书馆专网展望

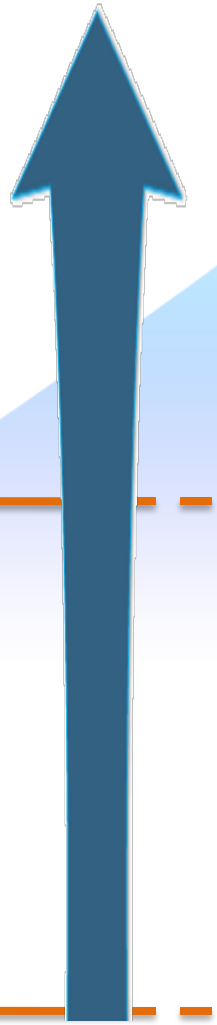
数字图书馆专网建设面临的挑战

SDH	***WDM***	***OTN***	***PTN***	*复杂多样*

数字图书馆专网建设面临的挑战

2013

调研



主要完成：

- 开展调研
- 东部地区
- 中部地区
- 西部地区

数字图书馆专网建设面临的挑战

- （1）高可靠性要求
- （2）实用性要求
- （3）安全性要求
- （4）可扩展性要求
- （5）灵活性要求
- （6）技术先进性要求

数字图书馆专网背景

数字图书馆专网建设面临的挑战

数字图书馆专网架构及组网技术实现方案

数字图书馆专网展望

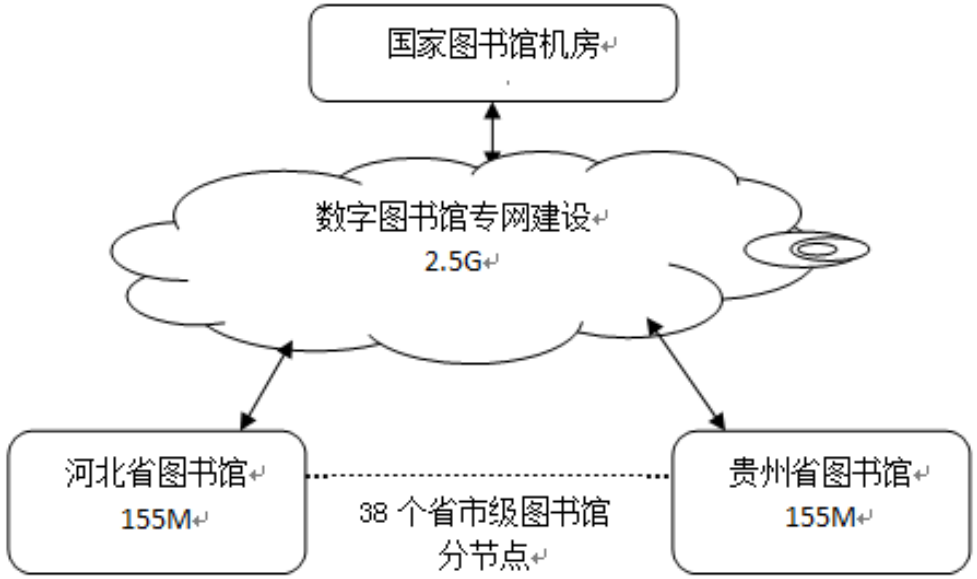
数字图书馆专网架构及组网技术实现方案

专网组网技术选择：

数字图书馆专网承载业务种类既有图文数据，又有语音视频，且业务总量伸缩性较大，业务的丰富性带来对网络带宽的更高需求，直接反映为对传送网能力及性能的要求。且数字图书馆专网的组网范围是连通全国各地图书馆，建设的终极目标是形成以专网为骨干以虚拟网为基础，联接省市县数字图书馆、乡镇综合文化站、村级文化活动室，服务覆盖全国的公共文化网络体系。经过对SDH、WDM、OTN、PTN等各种组网技术的比较分析、对各地图书馆网络情况的调研以及对专网建设要求的分析，SDH技术无论从安全性、传输质量、可靠性方面都可满足推广工程数字图书馆专网的多业务及保护要求，更加适合数字图书馆专网，因此，数字图书馆专网建设可选用SDH技术进行网络构建。

数字图书馆专网架构及组网技术实现方案

网络架构：



数字图书馆专网架构及组网技术实现方案

专网组网技术实现方案-网络拓扑：

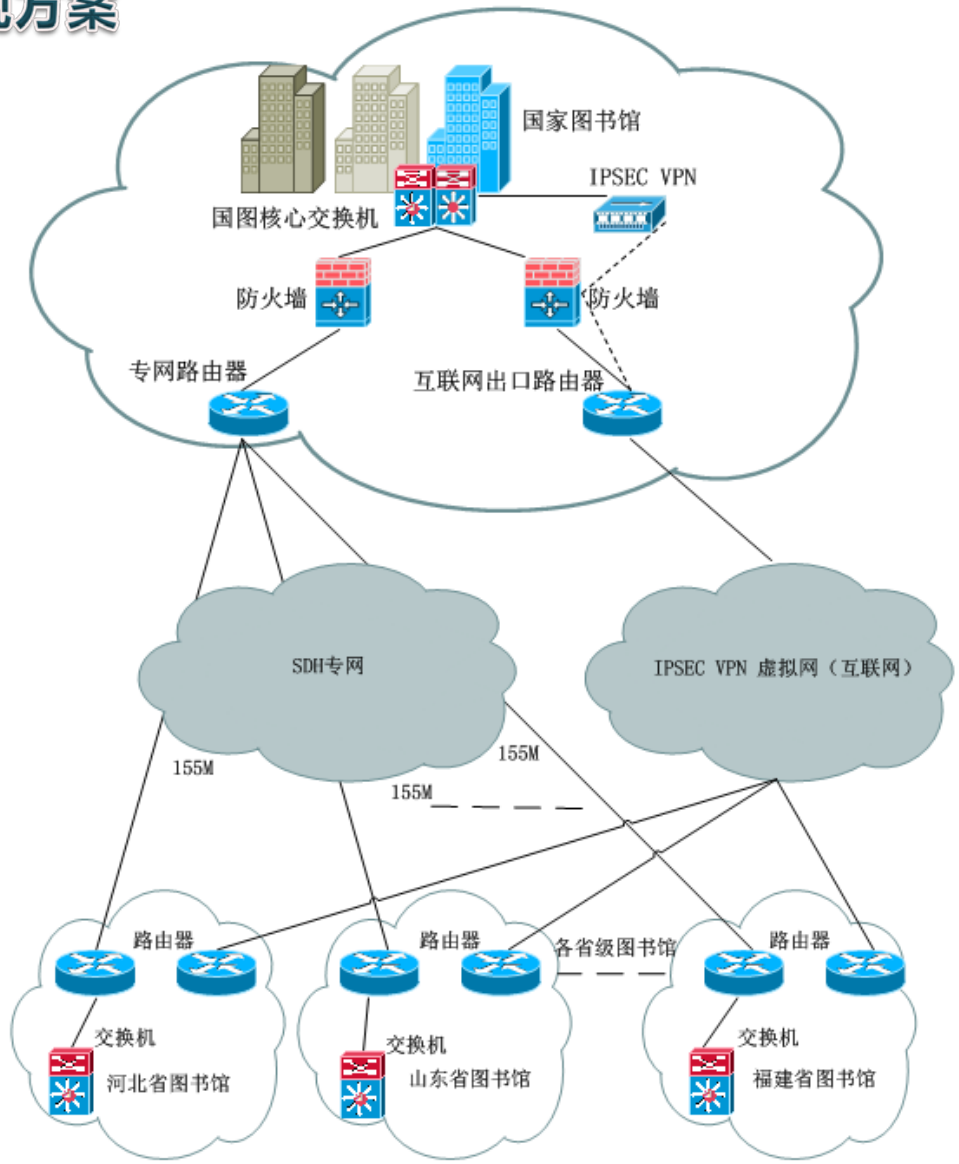


图 2 数字图书馆专网拓扑结构示意图

专网路由设计：

路由协议的选择：一是选用OSPF动态路由协议，二是选用静态路由协议。

路由主备切换设计：在国家图书馆核心交换机上添加静态路由，下一跳地址指向国家图书馆专网防火墙互联地址，并将静态路由优先级设置为50（缺省为60）以实现将原有路由切换到新专线上，如需要切回IPSEC VPN线路只要删除该新增路由配置即可。

专网IP地址规划：延用虚拟网地址。

专网防火墙配置设计：

数字图书馆专网的第一项业务应用是将国家图书馆统一采购的近140TB数字资源通过远程访问的方式开放给各省级图书馆，因此在国家图书馆端需要考虑防火墙的配置。防火墙的工作模式分为路由/NAT模式、透明（桥）模式以及混合模式。基于网络结构清晰明朗、路由跳数少，同时考虑到与专网的接入环境，以及NAT的需求，设计中防火墙采用路由/NAT模式。

网络安全策略规划：

隔离安全区域

访问控制策略

抗攻击策略

日志记录策略

QoS和安全访问控制设计：

数字图书馆专网建设完成后将承载多种数字图书馆推广工程业务，包括统一用户管理系统、唯一标识符系统、中国政府公开信息整合服务平台、文献数字化加工系统、文津搜索系统等，业务类型及数据类型多样，因此要求专网具有一定的应用服务能力。比如用户可根据需要自定义各应用服务质量保证优先级等。而各类业务承载的数据类型各有特点：

语音系统对网络传输要求较高，延迟超过150ms，就会出现断音，因此要实现好的效果，就需在带宽和延迟上加以保障，建议将其作为最关键业务进行保障；

视讯业务按照清晰度来计算，4CIF的图像清晰度占用带宽为1Mbps，高清为1～2 Mbps，而且视频对传输的要求高，建议其作为关键业务处理；

数据业务主要以办公和业务系统为主，带宽占用较大，而且使用的人数众多，建议其作为非关键业务处理。

随着数字图书馆推广工程的业务的开展，可以预见链路拥塞情况加重，会影响语音、视讯关键业务的传输质量。因此需要重点考虑QoS的部署，以达到对网络的基本要求。

QoS规划：

对于视频流量的业务，在国家图书馆的专网路由器上启用ACL识别视频流（如视频服务器的IP地址），打上优先级DSCP标记AF31；并启用CBQ或PQ，将视频流放入到高优先队列中，优先转发，直到发送完后才发送其他类对应的队列的报文。在各省级图书馆专网路由器上配置QoS策略，首先启用ACL识别视频流（如视频会议终端的IP地址），打上优先级DSCP标记AF31；再启用CBQ（基于类的队列），将其引入CBQ的紧急队列，由CBQ进行队列调度，抢占足够带宽，优先转发紧急队列中的报文，直到发送完后才发送其他类对应的队列的报文。

对于语音类流量，与视频流的实现方式类似，将其流量打上优先级DSCP标记AF41即可，其他相同。

对于数据业务，可将数据业务标记为0，尽力转发。

数字图书馆专网背景

数字图书馆专网建设面临的挑战

数字图书馆专网架构及组网技术实现方案

数字图书馆专网展望

数字图书馆专网展望

专网服务

数字图书馆专网的建设能够从根本上解决各图书馆互联网出口带宽紧张的状态，使很多交互业务可以通过专网来进行数据传输，为各图书馆节省因达到推广工程要求而新增支付的高额带宽租用费用。同时，专网的建设，使读者远程资源访问从共享互联网带宽转变为独享信道带宽，不仅能够提升读者访问体验，还能通过安全的加密机制，保护读者信息的安全性，是我国公共文化服务能力的提升。截止目前，已经有38家图书馆实现了与国家图书馆的专网连接，数字图书馆专网基本建成。在数字图书馆共建方面，专网的建设可以加快推进国家数字图书馆工程的成果转换，例如文献数字化加工系统、唯一标识符系统、统一用户管理系统等系统的部署与大数据量传输可通过专网来实现，将国家对数字图书馆工程的投入尽快得到应用，产生较好地投资回报。

基层图书馆互联互通项目

为了解决基层图书馆网络连通存在的问题，提升数字图书馆服务效能，推广工程从2016年开始实施基层图书馆互联互通项目，通过建设专线网络，将县级公共图书馆接入数字图书馆推广工程服务平台，完善国家数字图书馆网络体系，促进各级公共图书馆数字资源的整合与共享。通过基层图书馆互联互通建设，将数字图书馆推广工程建设成果向全国基层深度服务推广，引导文化资源向城乡基层倾斜，打通公共文化服务的“最后一公里”，提升区域性数字图书馆服务能力，更好地满足基层人民群众日益增长的文化需求。

基层图书馆互联互通项目-----工作要求

工作要求

1. **由省馆统筹面向县级图书馆开展数字图书馆网络互联互通建设规划实施等具体工作；**

2. **通过专线建设（10M以上物理链路）将县级图书馆接入国家数字图书馆网络体系，保障基层图书馆的数字图书馆专网服务和安全运行；**

3. **由省馆统筹采购交换机、无线设备等网络基础设施，为县级图书馆建设馆内局域网及无线网络接入。**

谢谢！