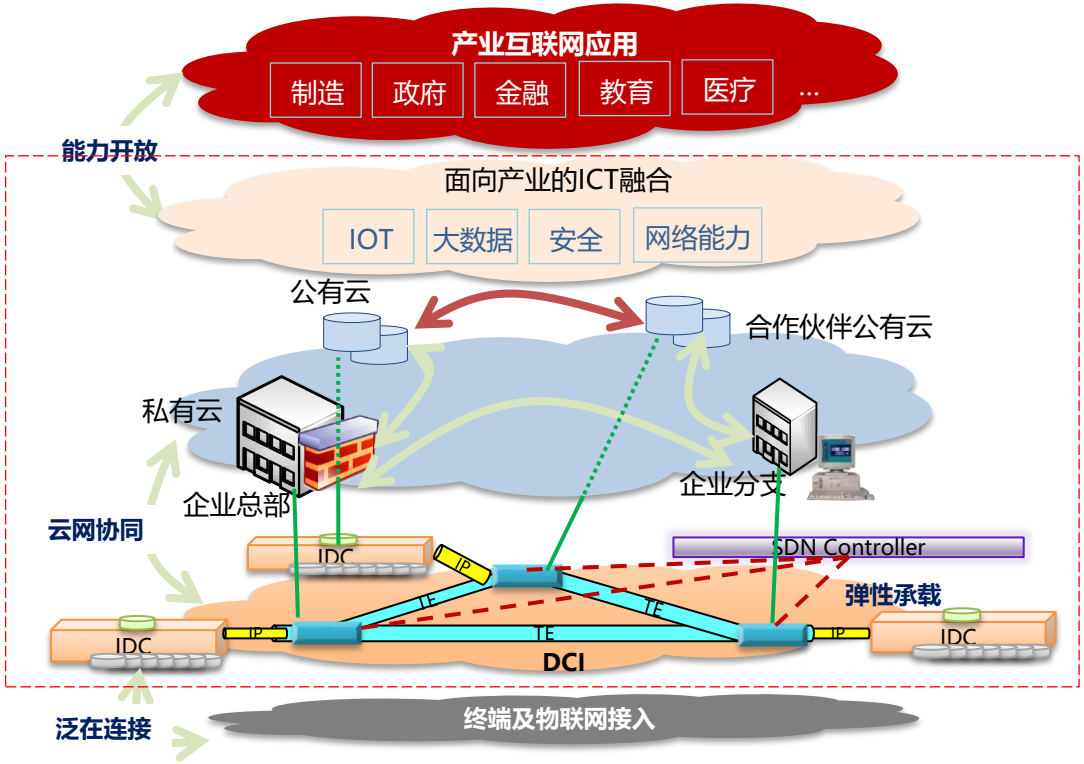
China unicom中国联通
创新·改变世界

中国联通业务提供能力分析

产业互联网产品创新中心

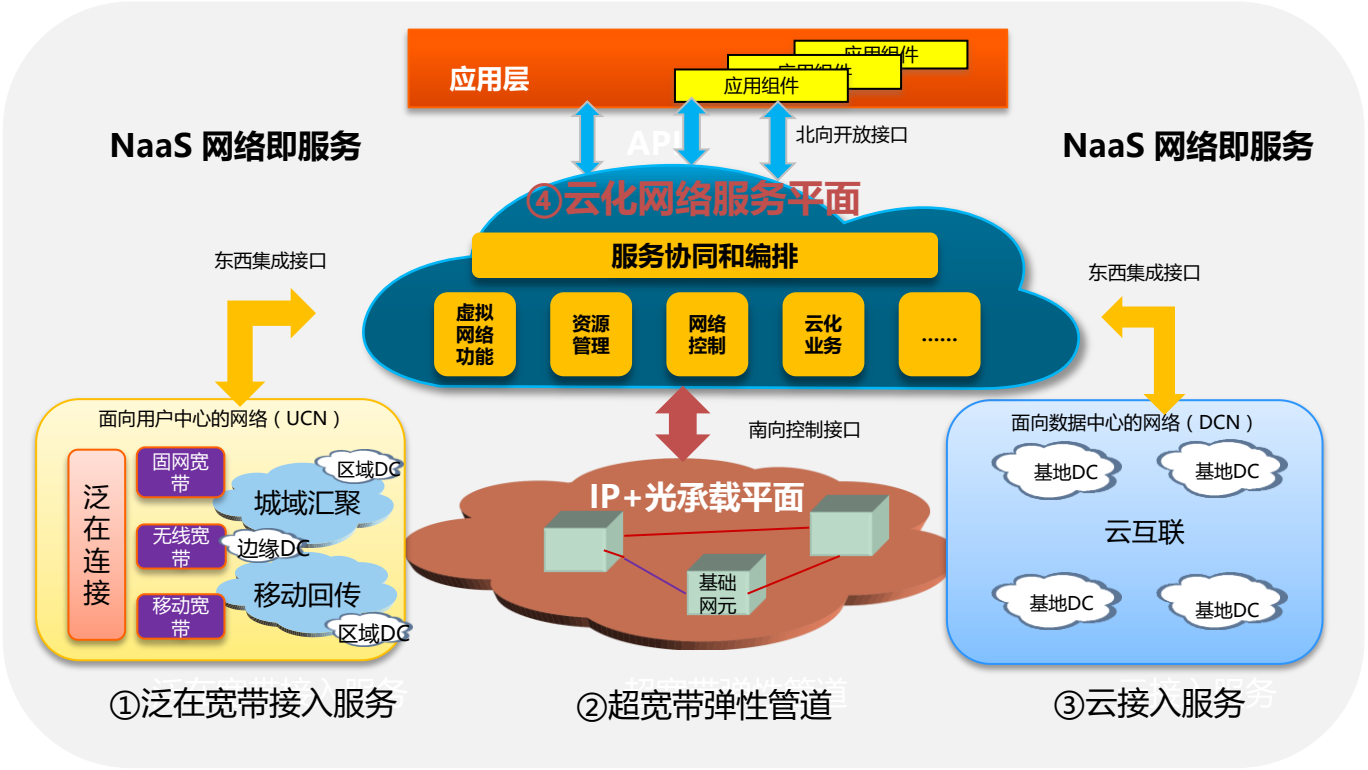
产业架构



产业互联网时代，中国联通网络的定义不只局限于承载网络本身，而是涵盖接入网络、承载网络、云服务、大数据分析以及ICT融合等内容

- 泛在的接入网络使得智能终端和物联网的接入更加自由
- 弹性的承载网络使得网络成为一种可配置的服务，为企业客户或商业合作伙伴提供了完备的NAAS服务
- 强大的云资源池为企业客户提供了灵活多样并且安全保障的云服务
- 云网协同能力为企业私有云和公有云之间的协同提供了技术保障
- 能力开放平台使得相关业务的开通和部署更为便捷，网络能力更为开放

新一代网络架构


应用层
应用组件
应用组件
NaaS 网络即服务
API
北向开放接口
NaaS 网络即服务
④云化网络服务平面
服务协同和编排
虚拟网络功能
资源管理
网络控制
云化业务
.....
东西集成接口
东西集成接口
面向用户中心的网络（UCN）
泛在连接
固网宽带
无线宽带
移动宽带
城域汇聚
区域DC
边缘DC
移动回传
区域DC
南向控制接口
IP+光承载平面
基础网元
面向数据中心的网络（DCN）
基地DC
基地DC
云互联
基地DC
基地DC
①泛在宽带接入服务
②超宽带弹性管道
③云接入服务

China unicom中国联通
创新·改变世界

1 面向产业互联的网络资源

2 面向产业互联网的DT服务

3 面向产业互联网的ICT服务

1 面向产业互联的网络资源

- 面向数据中心的网络
- 面向信息交换的网络
- 面向用户的网络

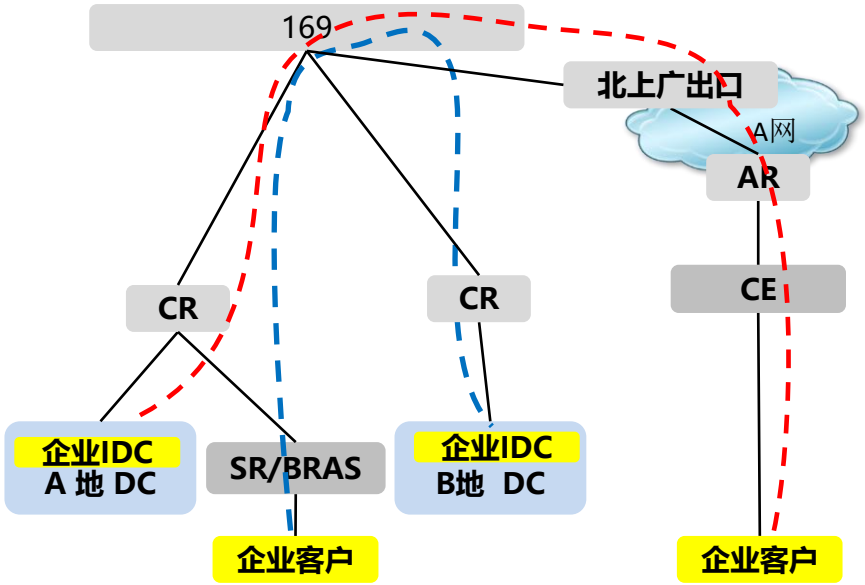
2 面向产业互联网的DT服务

3 面向产业互联网的ICT服务

面向数据中心的网络

挑战

现网架构不匹配云业务流量流向特征



- **企业**：租用运营商机架，建设本地IDC，上层根据DC负载进行流量调度，而不是根据网络物理拓扑就近调度
- **运营商**：网络架构不匹配DC流量流向的变化，无序扩容，加重省干/国干负担

传统网络难以支持自动化和能力开放

- DC互联网络的挑战：
  - R-DC与C-DC互联流量预测困难
  - 百万数量VDC跨域区域互联
  - 多样化的第三方DC互联专线
- 自动配置百万级VDC跨区域互联，实时按需提供带宽、多样化选路满足要求、对APP应用层能力开放，SDN是唯一可行技术方向
- 专线和DC缺乏协同，不具备一体化服务能力

数据中心业务现状和演进规划

China unicom中国联通
创新·改变世界

现状

1. 以设备为中心进行业务服务
2. 主要提供带宽、网络等固化基础服务
3. 产品类型单一，可定制化程度低
4. 流量混跑，通过QoS提供差异服务
5. 机架、服务器租赁为主的IDC出租业务
6. 传统通信网元节点分散、业务提供单一运营
7. IT与CT的烟囱式业务

演进

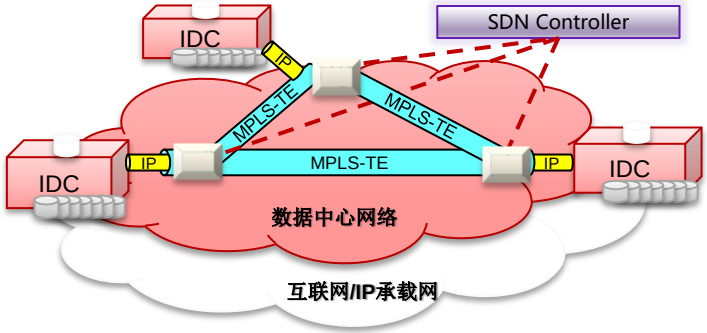
1. 以软件为中心进行业务运营
2. ICT融合一体化的服务模式
3. 提供基于网络能力开放的差异化服务
4. 开放用户自服务平台，满足不同需求
5. 叠加网络，弹性分配网络资源
6. 提供云服务的IDC虚拟化、DC池组化
7. 通信网的集中化、云化

需求驱动

- 资源整合
- 云网协同
- 差异化服务
- 能力开放

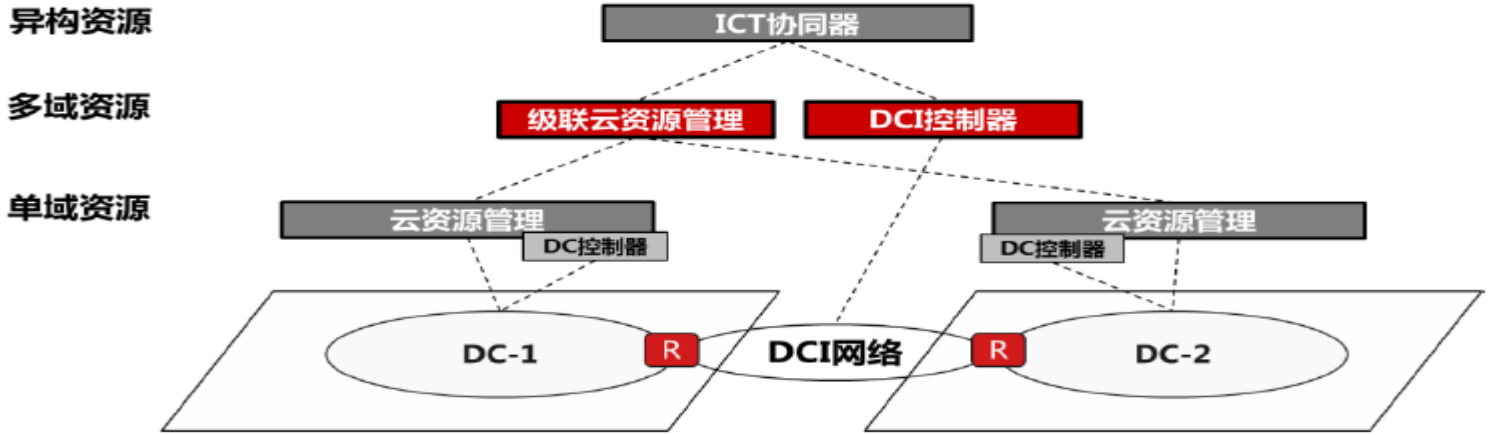
中国联通产业互联网（DCI）

- **DCI网络总体架构**
  - DCI是整合UTN、A网以及部分China169网络资源，为用户提供端到端无缝连接服务的网络。
- **DCI网络属性**
  - Overlay承载A网，以传输拓扑逻辑组网构建DCI平面，继承A网高服务质量的专线属性；
  - 在A网基础上，进行设备升级及网络结构调整，初期覆盖主要基地和重点城市数据中心。
- **DCI网络SDN化**
  - 采用MPLS TE及SDN技术满足高质量租户及云间东西向流量对网络时延优化及可编程能力的不同要求



总体方案和目标

- 基于A网构建DCI平面，基于SDN快速建立DCI连接，SDN控制器控制A网的PE设备
- 以DC-GW为CE，A网的AR为PE，建立L3VPN，通过做SLA保障

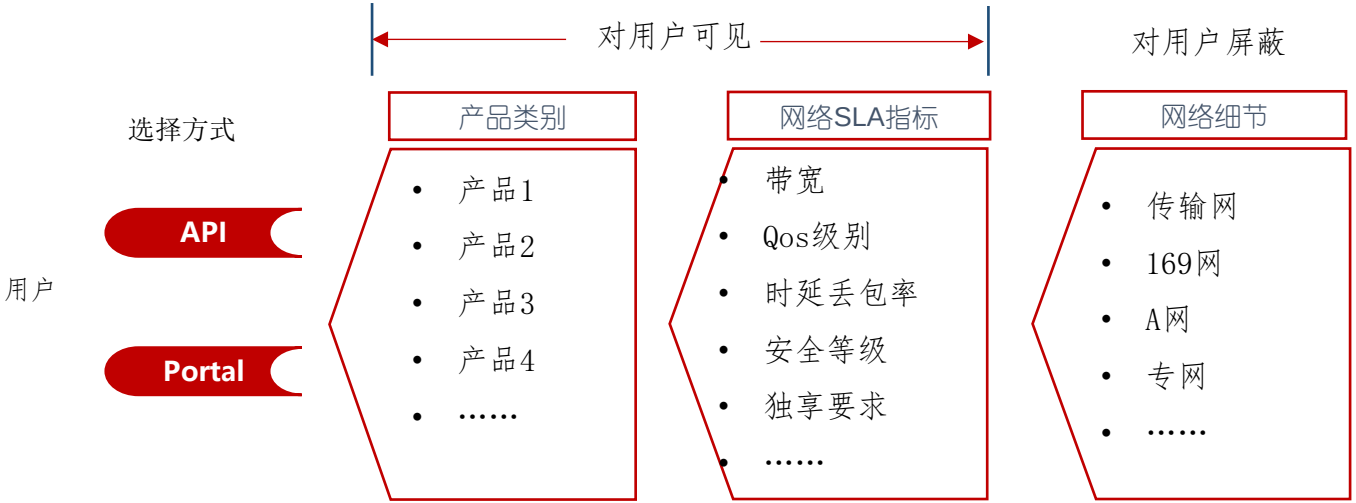


DCI网络的发展目标——以DC为核心，对各类云业务实现统一承载的专用业务网络

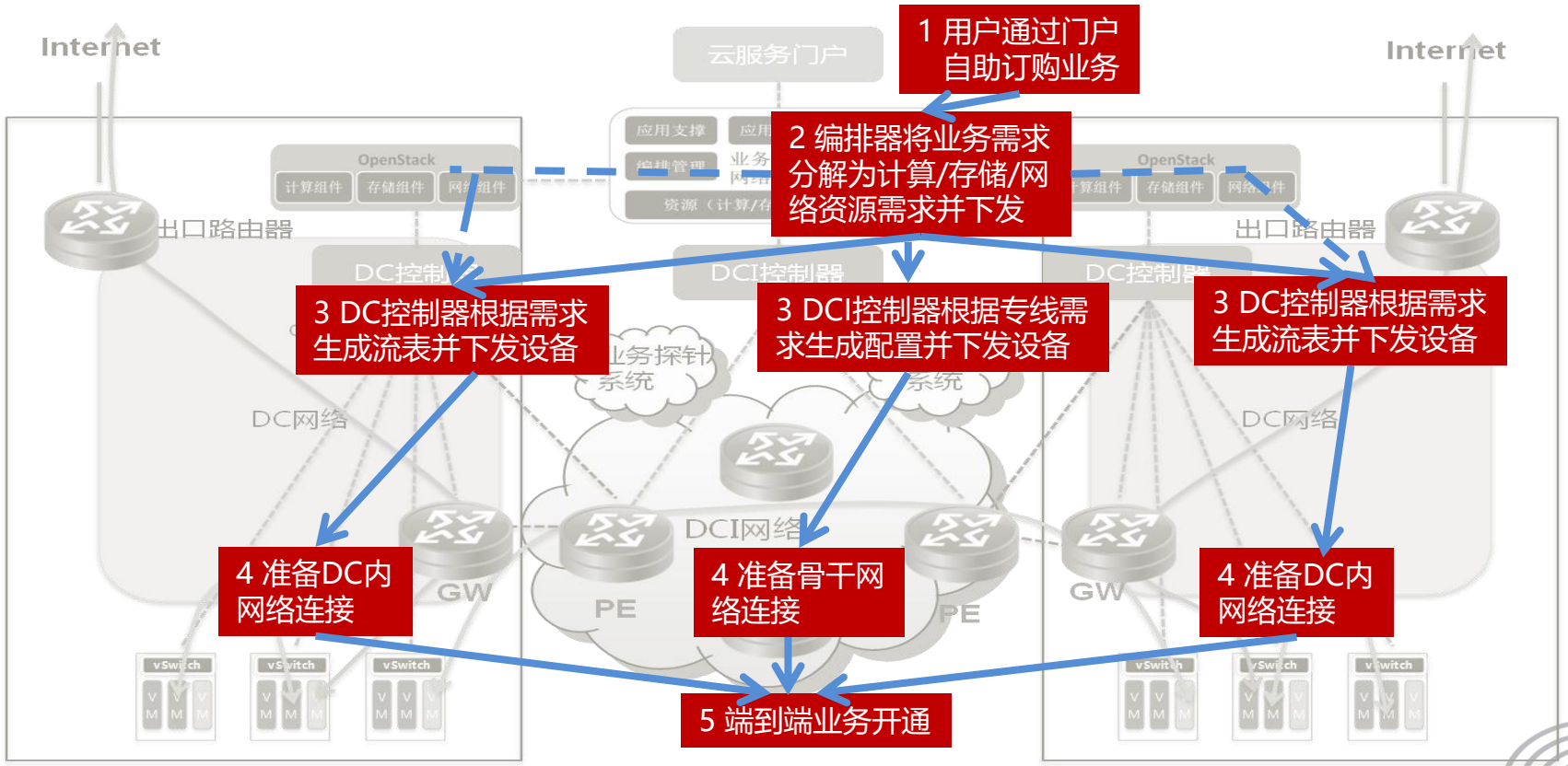
- **网络控制**：云管网络资源统一管理；根据业务需求和网络质量调整业务网络(overlay)拓扑；配置快速下发。
- **网络承载**：按业务网络(overlay)需求，在物理网络(underlay)上构建无缝传输通道，并提供带宽、QoS保障。
- **网络监测**：监控underlay各网段带宽和质量，汇总成overlay网络和业务网络质量，反馈给控制面进行参考并展示。

整体业务方案

- **为客户提供多样产品类别，并支持用户随选网络，屏蔽底层网络细节**
  - 随选网络：用户根据所提供的SLA指标，进行自由组合选择，形成最终的个性需求产品包
  - 用户可通过API或者web portal的方式选择或定制产品
  - 随着SDN技术的应用，产品中将包含更加丰富、灵活的SLA指标



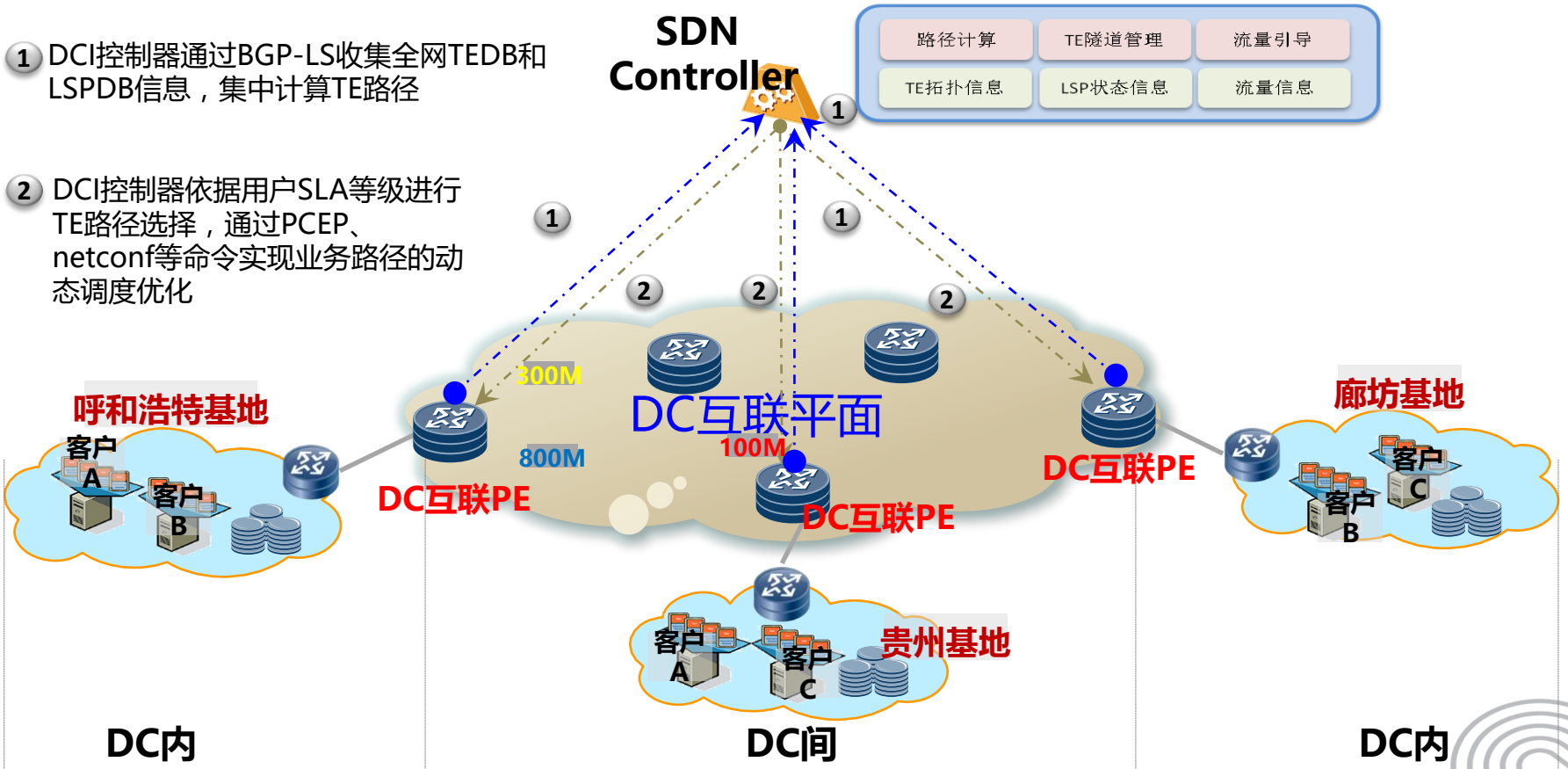
业务开通


Internet
云服务门户
1 用户通过门户自助订购业务
2 编排器将业务需求分解为计算/存储/网络资源需求并下发
Internet
OpenStack
计算组件
存储组件
网络组件
出口路由器
DC控制器
DCI控制器
3 DC控制器根据需求生成流表并下发设备
3 DCI控制器根据专线需求生成配置并下发设备
3 DC控制器根据需求生成流表并下发设备
DC网络
DCI网络
GW
PE
4 准备DC内网络连接
4 准备骨干网络连接
4 准备DC内网络连接
5 端到端业务开通
vSwitch

流量调度

1. DCI控制器通过BGP-LS收集全网TEDB和LSPDB信息，集中计算TE路径

2. DCI控制器依据用户SLA等级进行TE路径选择，通过PCEP、netconf等命令实现业务路径的动态调度优化



IP与光协同

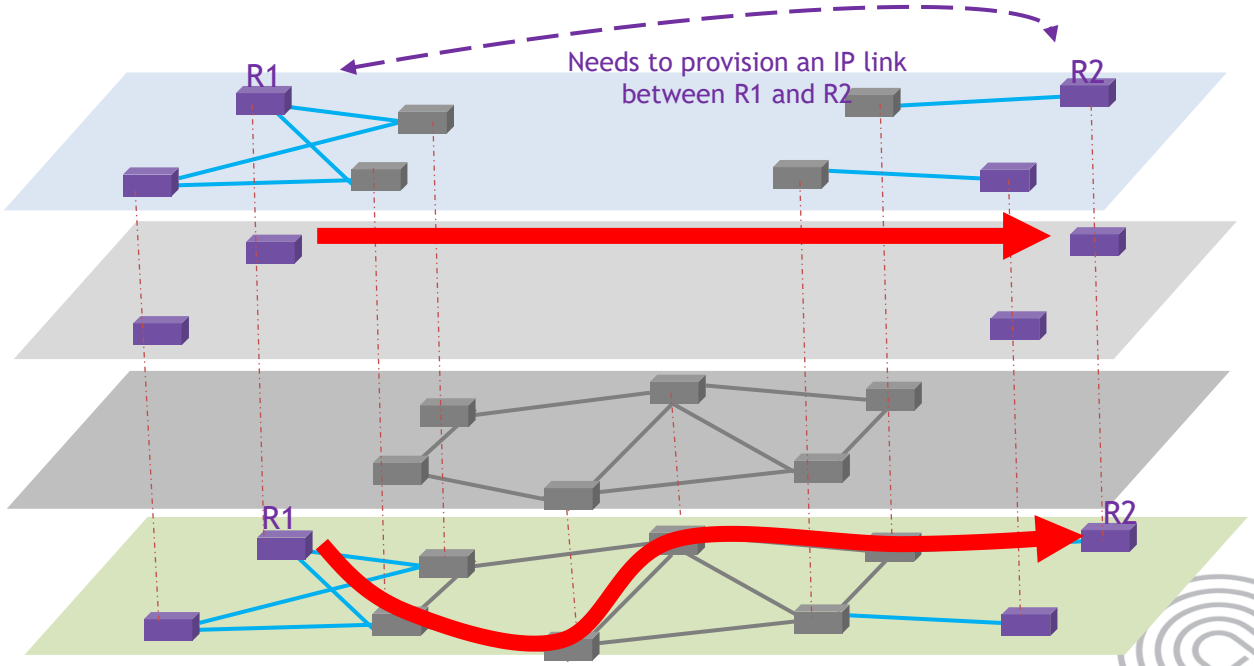
IP层感知业务、负责路径选择，光层感知网络并提供质量保障。IP层拓扑与光层拓扑联合运算，在用户接入点与DC接入点之间尽量实现一跳直达。IP与光之间的灵活分流，降低对核心路由器容量需求，达到资源要求和可靠性要求的平衡。

跨层/跨域拓扑
H-PCE可见. 涉及域间的节点和链路资源

IP 拓扑有IP PCE管理

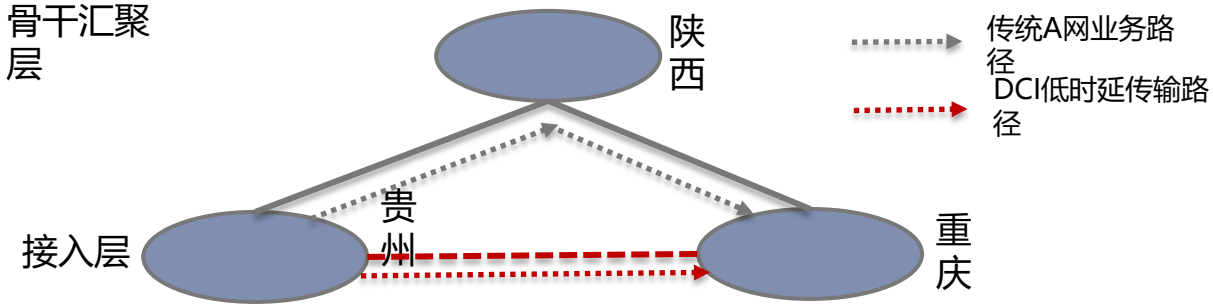
Optical 拓扑由光层PCE管理

物理层分为Ip和光两个域



低时延 | 高带宽 | 成本控制 | 灵活随选 | 本地化服务

- 摆脱A网传统网络层级，基于传输逻辑组网，协同控制器跨专业、跨网协同调度
- Overlay在A网之上，继承A网MPLS TE隧道技术，进一步保障时延和可靠性
- 能够增强CVM、网络（跨地域互联、VPN、专线）、存储与CDN等服务的服务质量



低时延 | 高带宽 | 成本控制 | 灵活随选 | 本地化服务

- DCI网络在A网基础上，增加22个省际电路方向、扩容现有25个省际电路、北上广之间开启100GE，满足用户带宽需求
- 目前网络利用率控制在30%以下，全网轻载状态，业务可扩展性强

业务产品

低时延　高带宽　成本控制　灵活随选　本地化服务

- DCI为用户提供API或Portal页面，实现业务快速开通、变更等，广泛利好多种云服务
- DCI提供的弹性管道可以由用户定制时延、带宽、闲时带宽、短租等业务形式，能够更精准的控制成本

指标选择	属性支持
带宽保障	保障、突发、尽力而为
时延	最短，尽力而为
价格敏感度	高，中，低
业务启用时间	包月/天，自定义
业务接入模式	VLAN，VxLAN
可靠性保证	路由隔离，路由保护，独立PE
资源独享选择	链路，设备
业务优先级等级	高,中，低
客户服务保障等级	钻金银铜
业务组合	推荐模板，自由定制

服务保障	钻石	金牌	银牌	铜牌
服务标准	全面解决方案咨询制定	全面解决方案咨询制定	全面解决方案咨询	全面解决方案咨询
资源确认时效	≤ 1工作日	≤ 2工作日	≤ 3工作日	≤ 5工作日
业务开通时效	≤ 5工作日	≤ 10工作日	≤ 15工作日	≤ 20工作日
故障恢复时效	≤ 6小时	≤ 12小时	≤ 18小时	≤ 24小时
年故障历时	≤ 8小时	≤ 12小时	≤ 24小时	≤ 72小时
日常维护	日常巡检、健康检查	日常巡检、健康检查	日常巡检	不提供

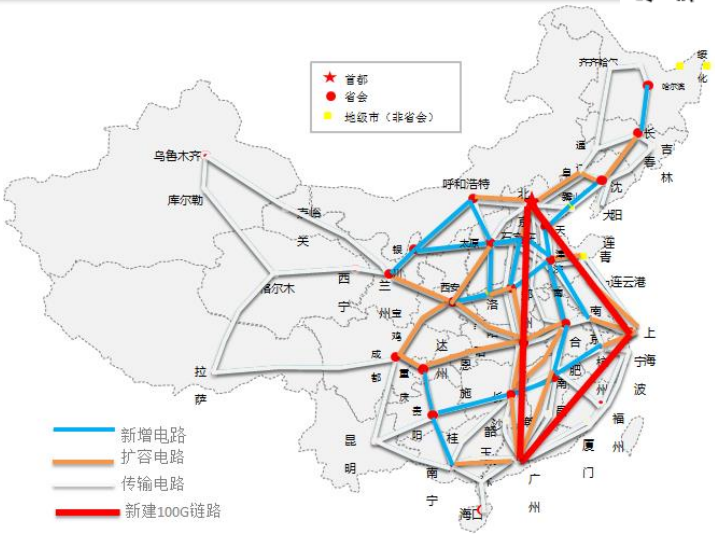
低时延 | 高带宽 | 成本控制 | 灵活随选 | 本地化服务

- DCI网络为联通DC、企业自建DC以及第三方IDC提供DC间以及用户到DC的连接服务
- DCI网络由UTN作为本地接入网，覆盖全国300多个本地网，有与基站同等密度的接入范围，满足用户接入广度需求
- UTN网络能够承载多种业务，L2/L3 VPN等，满足用户业务接入需求
- 有完善的、成体系的市场响应能力和业务支撑能力，为用户直接提供订制化的ICT技术服务

面向信息交换的网络

A网架构

- 网络概述
  - 分层架构，核心层、汇聚层以及接入层
  - 覆盖范围：7个核心节点、31个汇聚节点、334个接入节点
- 网络结构
  - 核心层为双平面结构，核心节点之间采用全互联，每个汇接节点至少连接到其他两个核心节点，保证可靠性
- 高服务质量
  - 95%的地区最大单向时延不超过50毫秒，全部大陆地区最大单向时延不超过60毫秒
  - 保证各类业务的QoS等级要求



- 高可靠性
  - 核心层全部启用MPLS TE FRR，收敛时间小于100毫秒
  - 全网IGP收敛小于1秒
  - VPN路由的快速收敛时间小于700毫秒
- IPv6
  - 网络协议全面支持IPv6版本，包括OSPFv3、ISISv6、BGP4+、IPv6 MPLS等
  - 支持多种过渡技术，全网能够平滑过渡到IPv6

China169

- 网络概述
  - China169骨干网覆盖全国31省，除北京、内蒙外，其余各省均设置2台路由器设备；
  - 全网网络容量年底达到200T，国际出口2260G；
  - 省际电路以100G电路为主

    (采用纠错能力强且便于故障定位的100GE OTN板卡)。
- 网络结构
  - 十三核心省全互联，非核心就近双上联核心省实现流量转发，并保证可靠性；
  - 流量较大省间开通直连电路，实现一跳可达，进而减少转发，提高效率。
- 时延优化
  - 根据工信部最新通报结果，China169全网平均时延达到36ms，为全国最优。

- 差异化服务
  - 与IP承载A网互联
  - 国际出口部署SDN
- QoS
  - 已部署大客户保障，具有针对移动互联网用户和国际流量的保障

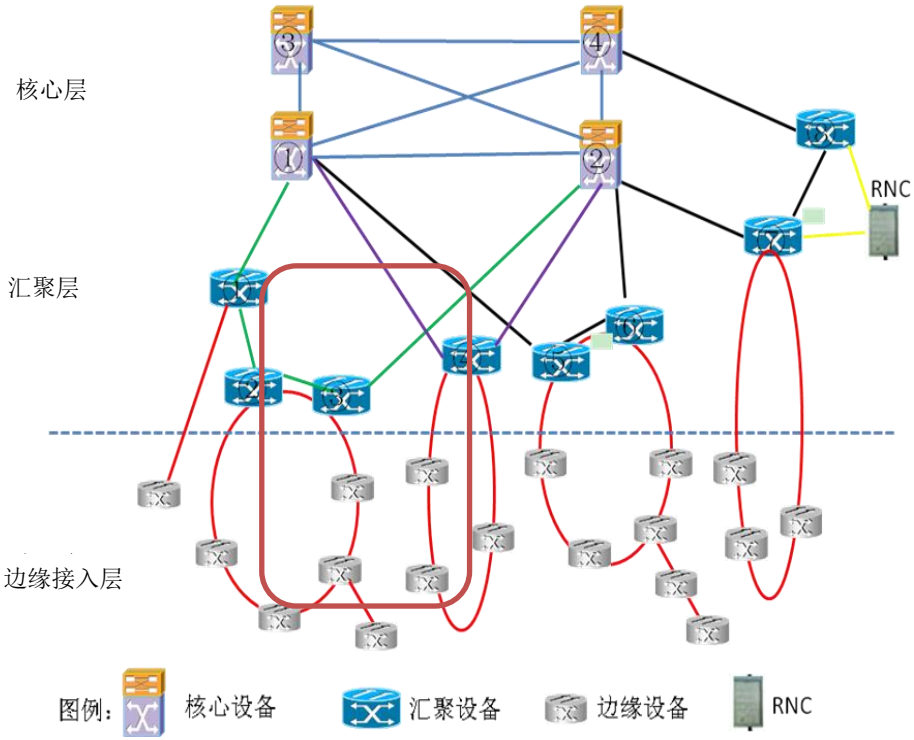
传输网

- **中国联通传输网能够覆盖全国所有本地网，提供2M到100G的刚性管道；**
- **SDH/MSTP，OTN/WDM是应用ASON控制技术的两张大客户专用网络；**
- **中国联通传输网络应用多种保护技术，满足业务高可靠性的要求；**

网络名称	覆盖范围	颗粒度	保护方式
ASON网	31省，37个节点	622M/155M/2M/FE	环网/MSP/SNCP/恢复
10G WDM	31省	10G/10GE/2.5G/GE	部分系统采用OMSP保护方式,提供光层保护
40G WDM	24省	40Gb/s	80%以上的系统建设了OMSP保护,提供光层保护
100G WDM	31省及集团/省IDC节点	100G OTN/100GE	90%以上的系统采用OMSP保护,提供光层保护
OTN智能网	31省	GE/2.5G/10G/40G/100G OTN和以太网	OMSP/环网、MSP/SNCP/恢复

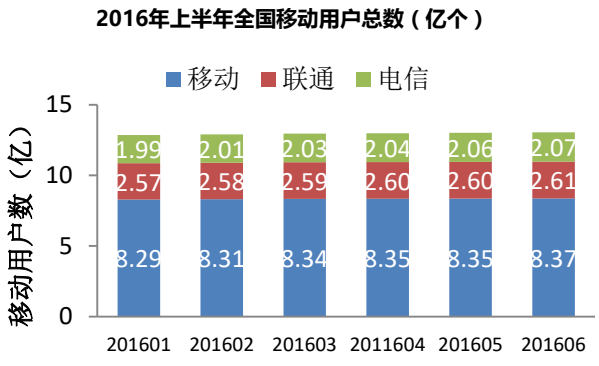
面向用户的网络

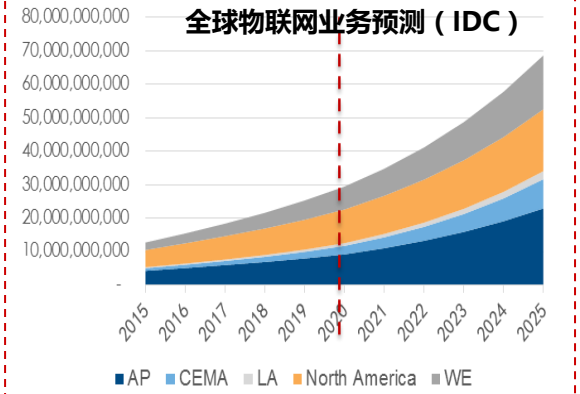
UTN

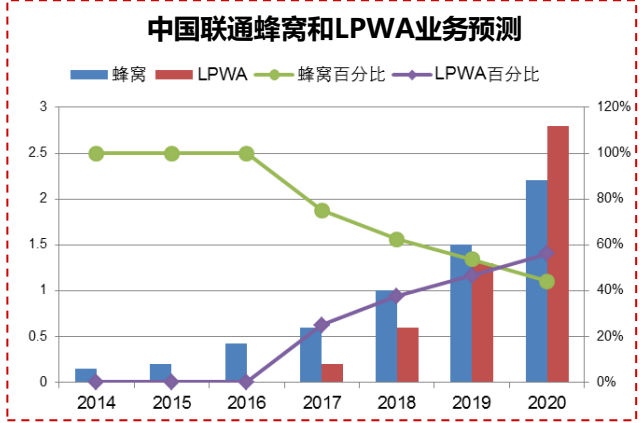


1. **核心层**
   - ✓ 网状网/口字型结构
   - ✓ 负责业务转发和与其他网络互连
   - ✓ 上联A网、B网
2. **汇聚层**
   - ✓ 口字型与核心层设备相连
   - ✓ 负责边缘接入层业务汇聚和转发
3. **边缘接入层**
   - ✓ 4-6台设备与汇聚层设备成环组网，利于业务保障
   - ✓ 负责用户侧业务接入
4. **中继链路**
   - ✓ UTN网络整体处于轻载状态
   - ✓ 核心/汇聚层中继链路无传输保护情况下利用率（峰值）不超过33%，有保护不超过45%
   - ✓ 边缘接入层在保护情况下，利用率不超过80%
5. **网络覆盖**
   - ✓ 全国300多个本地网

人人互联已趋饱和，万物互联催生海量链接需求，为运营商提供新的商业契机和利润增长点







- 国内移动用户数已趋于饱和，未来移动业务发展空间有限，运营商纷纷瞄准广阔的物联网业务空间；
- 物联网业务增长迅猛，预计到2020年，全球物联网总连接将达到300亿，国内年复合增长率达50%（全球CAGR24%），但目前传统蜂窝占比较低(<6%)；
- LPWA（低功耗广域网）发展潜力巨大。凭借深覆盖、低功耗、低成本的优势，逐步侵蚀一部分“短距+网关”业务市场。2020年中国联通LPWA连接数将达3亿，2017年是培育期(<2千万)；在2018-2019年迎来爆发式增长（近亿链接）。

中国联通IOT网络

■ 业务现状：聚焦6大典型行业应用，精细化深耕物联网业务新空间

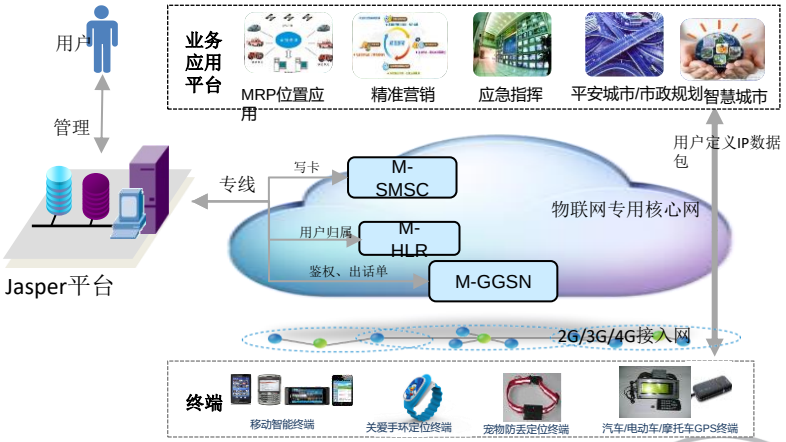
- **业务分布情况：**2G网络接入用户数比例最高接近60%；3G网络上产生的上下行流量最高分别达到68%和59%；4G接入用户数则最少（终端价格较高）。
- **业务发展趋势：**用户呈现由2G向3G，由3G向4G转网的趋势；2G连接数逐年递减，3G与4G连接数快速增长。
- **高ARPU值业务情况：**车辆服务类业务ARPU值最高且增长速度最快。消费电子类和生产环境监控类增长较快。
- **连接数总量情况：**截止2016年6月，**中国联通物联网连接数达3400万（其中集中平台1600万），全国占比超过20%**（移动7000万，电信1000万）。

■ 网络现状

- **无线网：** 依托GPRS/3G/4G蜂窝移动网，为物联网提供多种接入方式。
- **核心网：**在**南京和广州**，建设物联网专用核心网网元HSS和GGSN，以提供高可靠网络支撑。

■ 平台现状

- **管理平台集中化运营：**采用一级平台管理及运营模式，引入**Jasper连接管理**平台，对用户进行统一计费和管理。
- **业务应用平台分布各省**：各省根据业务发展需求建设业务平台，并以**创新合作的方式**接入南京统一运营的Jasper管理平台。



中国联通IOT网络目标

China unicom 中国联通 创新·改变世界

■ **以业务需求为导向，分阶段稳步推进物联网网络建设，提升平台开放能力，拓展物联网业务新空间。**

	2017年	2018-2019年
无线	◻ 以业务需求为导向，推进**重点城市、重点区域NB-IoT商用部署**； ◻ 开展LTE-eMTC(Cat-M)、LTE-V、5G等技术试验，**适时引入Cat.M；**	◻ 持续推进低功率广覆盖NB-IoT、 LTE-eMTC(Cat-M)业务覆盖，部分企业级业务应用部署LoRa作为特殊场景覆盖解决方案。
核心网	◻ 推进物联网专用虚拟化EPC部署，结合各省业务需求逐步完善核心网建设。	◻ 推进**核心网专网全面虚拟化**，结合各省业务发展情况实现P-GW网元向省内下沉。
平台	◻ 实施平台基础能力建设，打造以平台为核心的业务拓展样板工程，探索运营商物联网业务的商业闭环。	◻ 增强平台的业务支撑、数据分析等能力建设，深入垂直行业应用，形成良性的产业生态，拓展业务增长新空间。
终端	结合行业应用及中国联通物联网业务应用需求，持续推动定制化模组、芯片产品的研制与商用。	

1 面向产业互联的网络资源

2 面向产业互联网的DT服务

- 面向产业的云服务
- 全面的数据服务

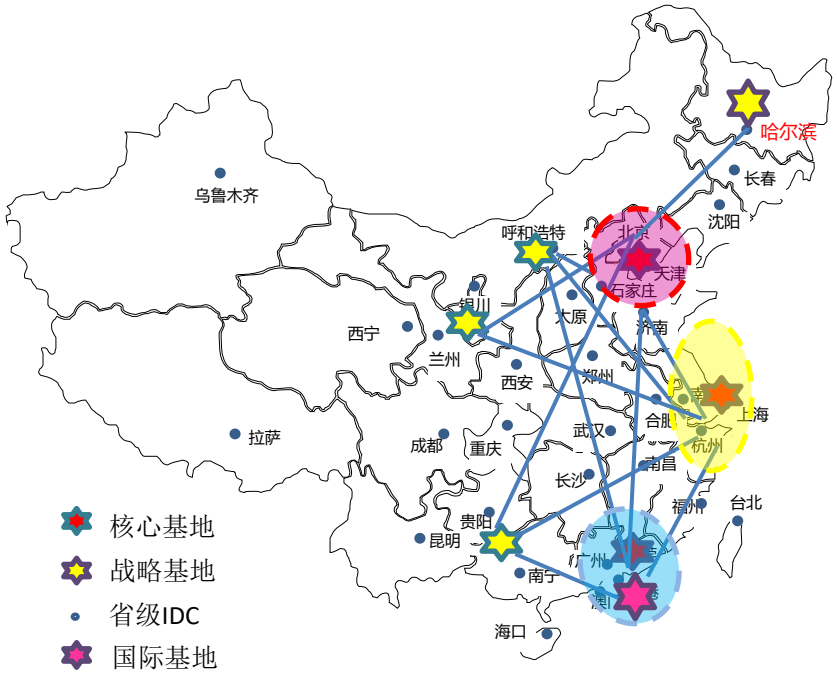
3 面向产业互联网的ICT服务

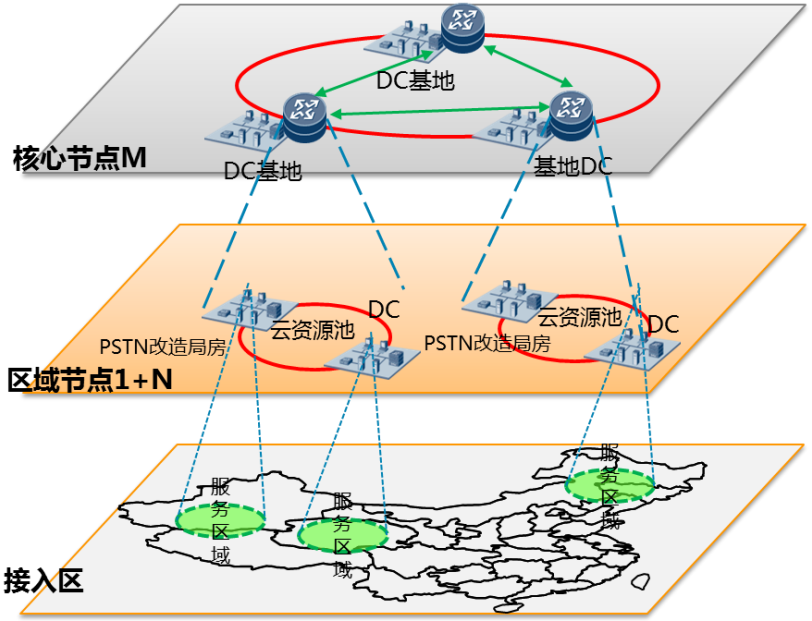
China unicom中国联通
创新·改变世界

面向产业的云服务

中国联通云数据中心

规划布局“M+1+N”云数据中心体系，构筑高性能、全覆盖、任意调度的差异化服务网络

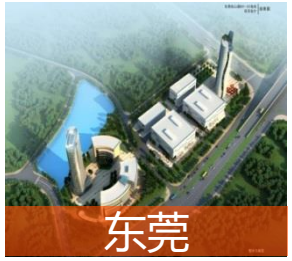


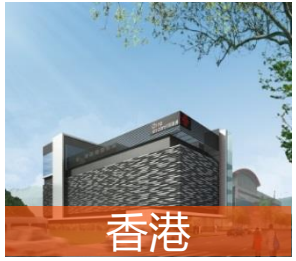


立体式、可扩展、自动保护的云服务能力

云基地

十二大基地总机架≥32万架，总出口带宽>30T，PUE<1.5；采用SDN智能网络架构





业务定位:

◆ **高端数据中心（IDC）**

面向国内政府、金融、大企业的战略级客户和TOP50互联网客户，提供国际标准VIP服务的五星级IDC

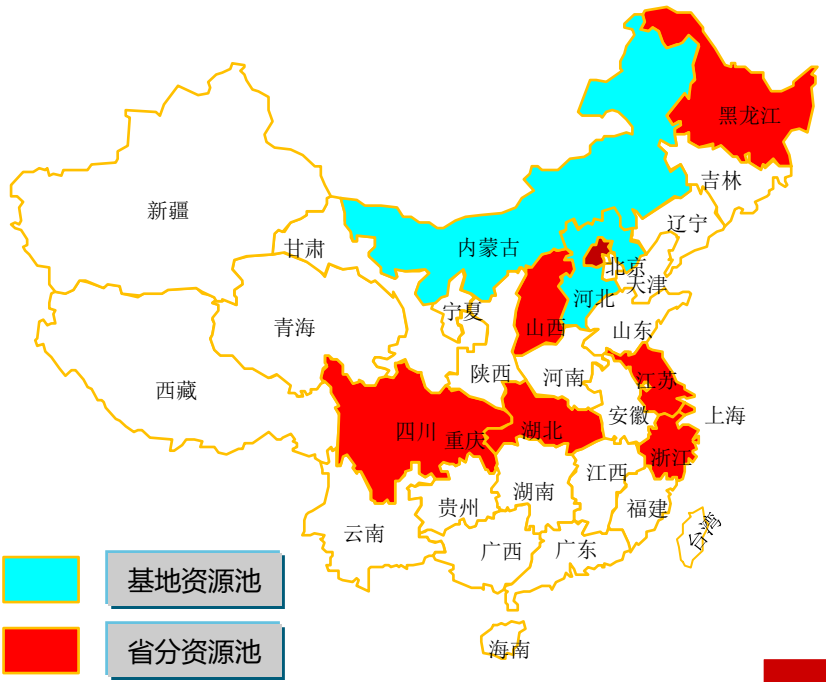
◆ **全国共享灾备中心（DRC）**

服务全国和海外大客户，建立容灾备份服务体系

◆ **云计算服务中心（VDC）**

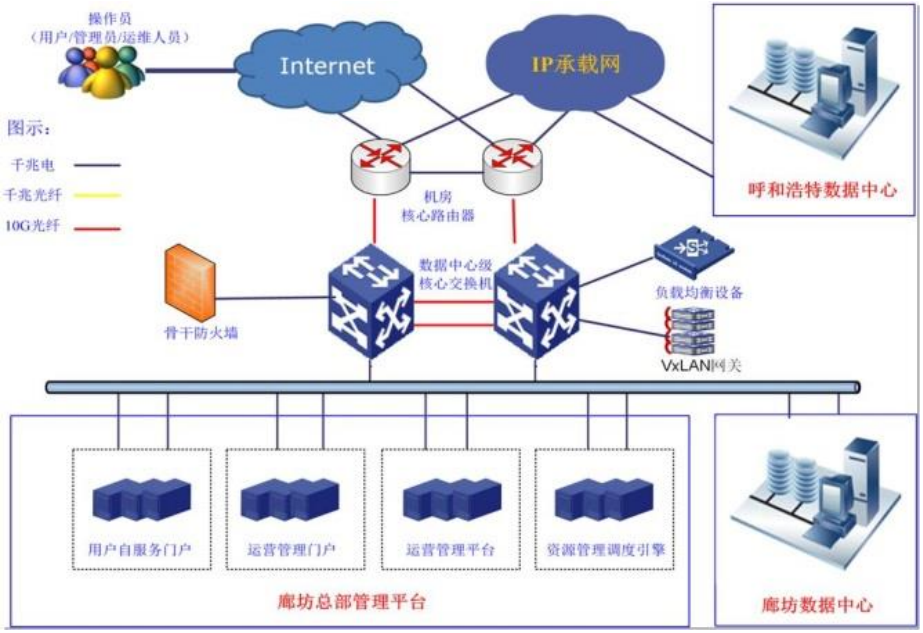
以企业专享云为主，探索全新的云服务商业运营模式，满足随需的扩展、使用和付费等

云资源池



基地资源池
计算：不低于5000核vcpu
存储：不低于800T
网络：不低于10G

节点资源池
计算：不低于1024核vcpu
存储：不低于120T
网络：不低于2G



云平台管理节点通过IP承载网与资源池实现管理，实现资源统一调度
各数据中心资源池通过各自的互联网出口为用户提供服务

沃云

China unicom中国联通
创新·改变世界

2013.12 — 沃云2.0

- 沃云商用,中国联通云计算业务品牌“沃云”
- 发布沃云公有云服务
- 发布十大云数据中心规划

2014.5 — 资源池部署

- 呼和浩特、廊坊、郑州云数据中心交付,完成核心资源池部署
- 覆盖政府、金融、互联网、医疗、教育、环保、制造业等多个行业领域

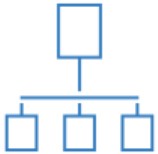
2014.12 — 沃云3.0

- 全国分布式资源池节点完成部署
- 2014 年 9 月 沃 云 SDN商用发布

2016.3 — 沃云4.0

- 推出云网一体化解决方案
- 完全满足私有云、混合云及复杂组网类需求


弹性云主机


弹性负载均衡


云安全

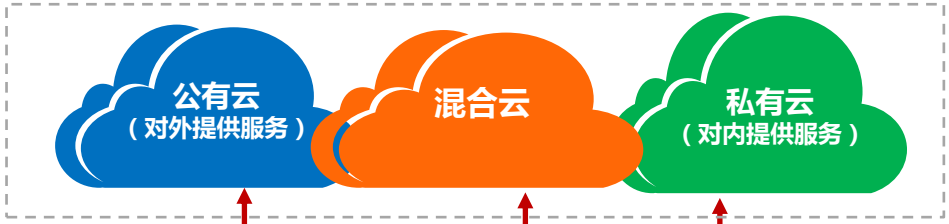

云桌面


分布式数据库


云存储

沃云服务能力

云计算提供的是：
服务



SaaS

（Software as a Service）软件即服务

SaaS侧重于服务，以软件程序提供服务，如CRM、ERP、OA等

PaaS

（Platform as a Service ）平台即服务

PaaS侧重于服务，以应用服务器平台或开发环境提供服务，云管理平台。

IaaS

（Infrastructure as a Service）基础设施即服务

IaaS注重计算资源的共享 ，消费者通过 Internet 可以获得虚拟的服务器、存储和网络。

2016年公有云资源	
计算能力	25万核vCPU
存储能力	20PB
互联网总带宽	240G

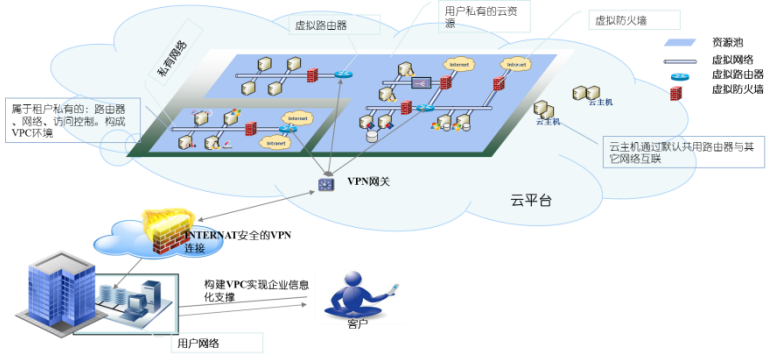
产品样例

云主机

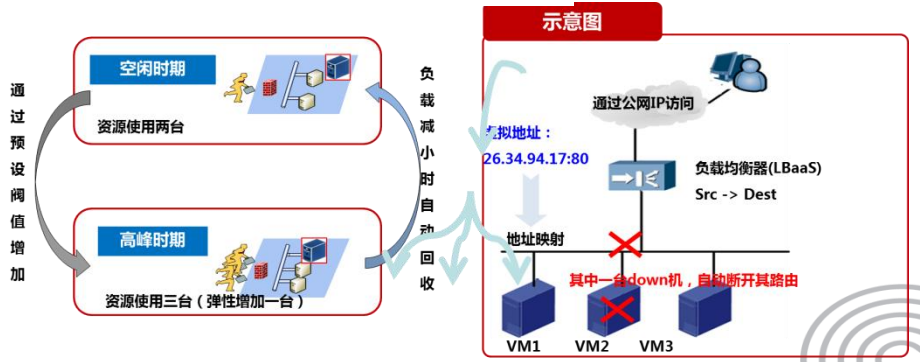
云存储

弹性块存储可理解为我们日常生活中使用的移动硬盘，可以挂载到任意一台云主机上，使数据更安全、更具灵活性。

虚拟私有云



弹性负载均衡



China unicom中国联通
创新·改变世界

全面的数据服务

中国联通数据中心主要内容

工作要点

- 基础体系构建
- 数据采集与处理
- 能力沉淀与服务

01

基础体系构建

跟踪主流技术发展路线，结合联通业务、数据诉求构建平台基础体系，支撑数据采集、处理及服务；

02

数据集中采集与处理

分层分专业构建数据模型，集中采集并整合联通及外部数据，支撑数据深度挖掘及各类服务；

03

能力沉淀与服务支撑

聚焦数据核心价值，沉淀统一、通用的数据能力，面向其他平台、省分、外部合作伙伴的能力诉求提供标准化服务。

数据运营（总体）

- **综合各类硬件与技术搭建一体化生产服务平台，集中采集并整合联通及外部各类分离、分散的数据，深度挖掘数据价值并进行能力沉淀，通过标准、安全的服务模型支撑集团、省分及外部伙伴的各类需求。**

一点 数据采集

集团总部：
- 19个B域系统，274个接口
- 13个M域系统，457个接口

31省分：
- 各省O域2个接口
- 各省BSS系统，169个接口

数据采集规模
日采集BM域170亿记录，Gn口3800亿记录，约43TB存储

集中 数据整合

跨M\B\O域整合：
- 明细层编码统一映射
- 汇总\衍生层\立方体层转换公共维度和核心事实

映射转换规模
构建标准编码表170个
转换事实维度11类

深度挖掘 与能力沉淀

数据挖掘：
- 用户互联网偏好标签库；
- 客服养卡、双卡识别、重入网识别等10类模型；
- 终端库；

数据量规模
包括用户视图等在内的数据资产占用存储7PB

标准 数据服务

集团省分两级服务：
- 系统服务，30余万人次
- 离线数据，2200余份
- 系统间文件接口，300余个
- 分析报告，60余份

数据服务范围
集团28个部门400余人
31个省分公司8600余人

基础设施

✓主机设备：Hadoop集群节点规模 2000+
✓存储能力：50PB

数据采集

■ **生产服务平台集中采集两级（*集团/省分*）三域（*B/O/M*）各类系统数据，为后续数据处理及服务提供保障。**

数据整合

- **生产服务平台采集各域生产系统及外部互联网等数据，数据清洗后统一进行整合并沉淀标准化数据资产以支撑后续的深度数据挖掘和数据服务。**

数据挖掘

- **以整合后的数据为基础，围绕潜在、通用、可扩展的业务诉求对数据进行挖掘并沉淀结果，支撑后续的标准化服务。**

数据服务

- **生产服务平台为数据中心、其他业务部门、省分公司及外部合作伙伴提供各类标准化的服务，涵盖数据共享、分析报告、个性化定制等多类内容。**

数据运营方向

数据运营目的：让采集来的数据发挥更大的价值

数据运营方向：利用好数据中心的数据、设备及技术，支撑集团各个部门、分公司、子公司、合资公司提高生产效率、创造收入

目前在已开展的大数据业务中，主要存在以上六大运营方向

对外应用

与六大行业合作

蚂蚁金服 ANT FINANCIAL　geo 集奥聚合 领先的互联网大数据服务商　Miaozhen Systems　PayEco 易联支付　前海融通　中国平安 PING AN 平安数据科技　康得投资集团　南方航空

上海大众汽车 SHANGHAI VOLKSWAGEN　招商银行 CHINA MERCHANTS BANK　国家旅游局　36Kr　广发银行 CGB　Brilliance Auto 华晨汽车

招联

- 构建征信模型
- 提供征信服务

西电

- 组建合资公司
- 提供位置服务

沃指数

- 乌镇发布
- 综合评价产品

合作拓展

- 战略合作：国家旅游局、交通部、北京银行等
- 筹建征信运营公司

1 面向产业互联的网络资源

2 面向产业互联网的DT服务

3 面向产业互联网的ICT服务

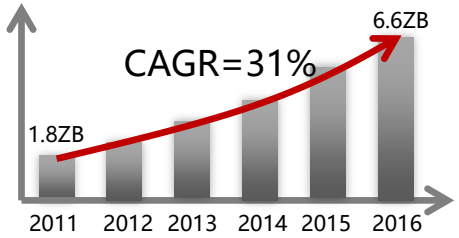
- 专业的安全服务
- 完备的CDN部署

专业的安全服务

安全现状

网络流量保持高速增长

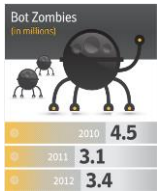
全球IDC流量将保持31%的年复合增长率



来源：CISCO《云计算产业调研（2011-2016）》

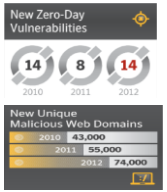
网络安全威胁日益复杂多样化

在虚拟化、移动技术和云计算等趋势作用下，网络攻击的手段也更加复杂和多样化



僵尸病毒

网站木马



DDoS

不良信息扩散范围大，势头猛

不法分子利用即时通讯工具、社交软件、BBS等散播谣言、非法言论等扩散快，误导社会舆论，引发社会矛盾

工信部和国务院联合出台【2012】551号、【2012】247号、【2013】467号，加强和扩大对网络信息安全的监管

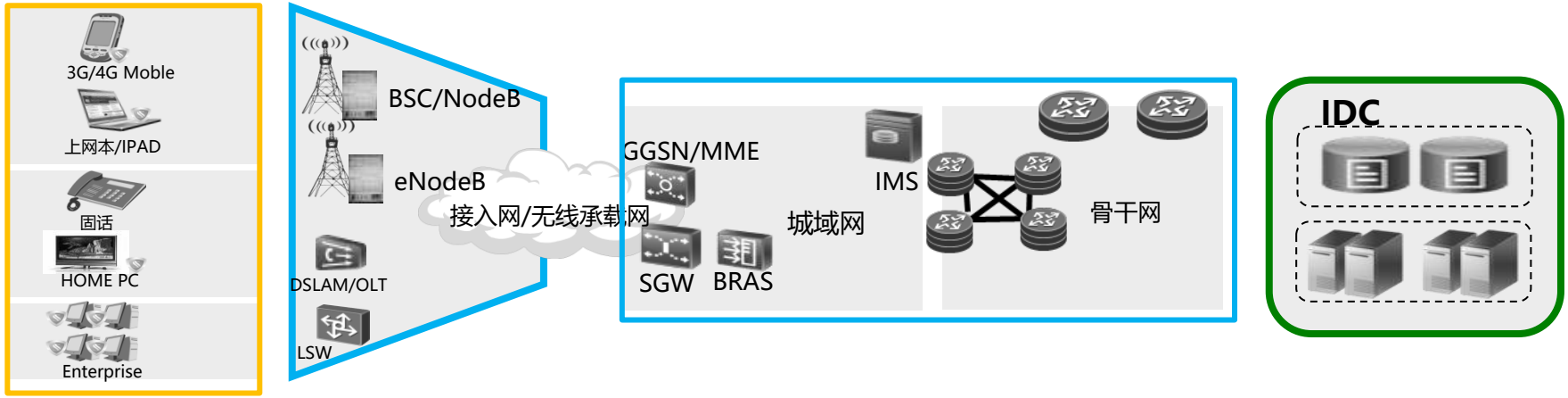
运营商安全需求

网络流量需要有效控制

带宽资源需要监管

业务需要精细化运营

运营商网络安全威胁



终端及CPE	接入网/无线承载网	PS域、城域网	关口局、互联互通口	IDC、业务系统
端威胁	**管威胁**	**管威胁**	**管威胁**	**云威胁**
◆蠕虫/木马/僵尸 ◆信息窃取 ◆垃圾邮件 ◆黄赌毒 ◆垃圾广告	◆非法接入 ◆网络资源滥用 ◆信息监听	◆DDOS攻击 ◆网络资源滥用 ◆垃圾邮件/广告 ◆黄赌毒 ◆非法接入	◆DDOS攻击 ◆网络资源滥用	◆DDOS攻击 ◆网络资源滥用 ◆入侵/挂马 ◆网页篡改 ◆非法接入

安全防御技术

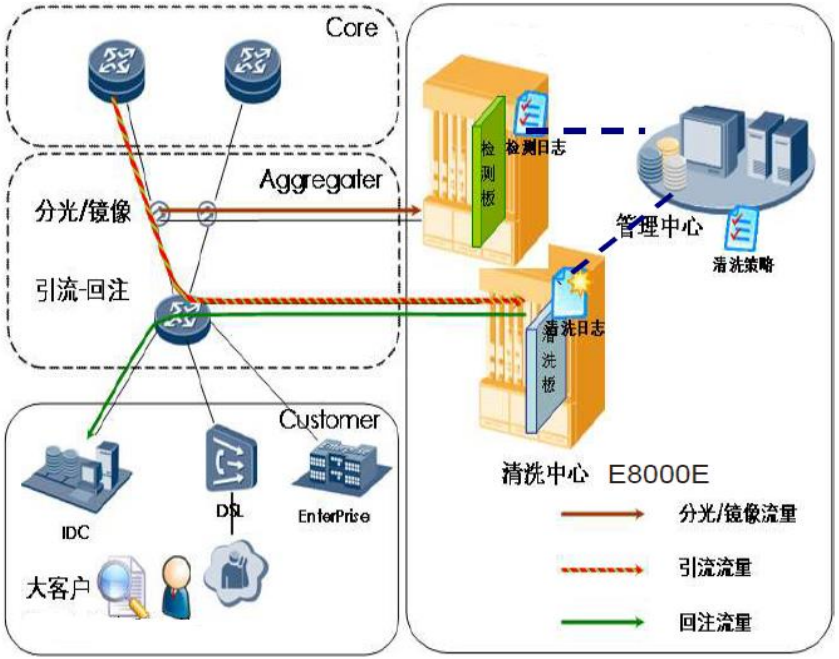
异常流量检测 联动 **DDoS流量处理**

DPI
- 深度包检测，应用层识别
- 基于数据包的逐包检测
- 主流厂家有华为、宽广等

DFI
- NetFlow/NetStream检测
- 网络层流检测
- 现网主流厂家Genie、Arbor

流量封堵、流量压制
- 通过黑洞路由、ACL实现，或限速实现
- 真实用户流量也会丢弃
- 响应快，成本低

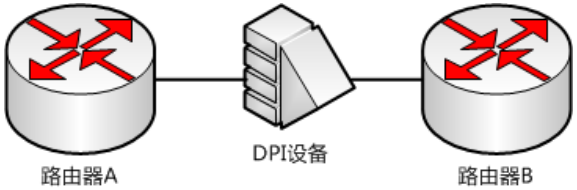
流量清洗
- 近源或近目的牵引流量至清洗系统
- 过滤DDOS攻击流量，将真正流量回注给用户
- 响应时延较大，成本高



- 异常流量检测可以采用DFI和DPI结合方式，综合判定
- 流量处理一般采用部署专用清洗设备和过滤、封堵相结合的方式

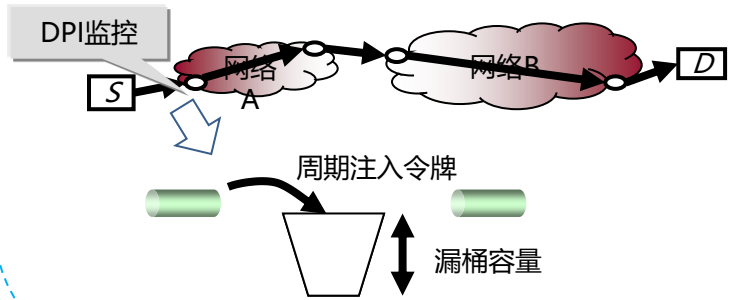
DPI技术（深度包检测）

串联方式

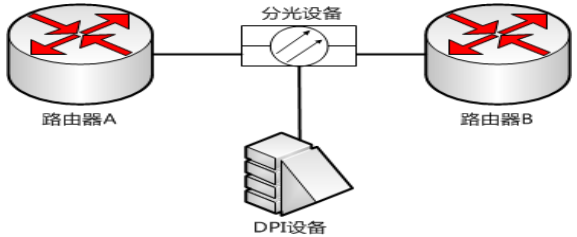


- 部署方式
  - 部署风险大
- 控制方式和能力
  - 控制精准
  - 方式灵活
- 法律纠纷
  - 非侵入式控制，法律风险低

报文控制方式

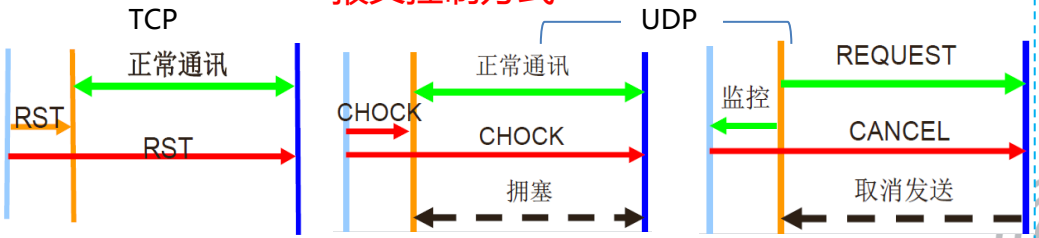


并联方式



- 部署方式
  - 部署风险小
- 控制方式和能力
  - 控制精准较差
  - 扩展性差
- 法律纠纷
  - 面临法律风险

报文控制方式



- 通过伪造A-B之间的RST报文，使双方TCP连接中止
- 限流：发送伪造数据包造成拥塞状态，控制流速如BT协议的CHOCK消息
- 限连接数：发送伪造报文进行连接拆除，如BT协议的cancel消息

流量清洗系统现状

流量清洗系统

- 截至15年底，已建或在建流量清洗系统的省分有28个，至2016年规划期末，30个省将具备流量清洗能力。
- 各省现有系统均基于保护本地用户建设，为近目的端防护
- 绝大多数已覆盖本省IDC和城域网
- 主要设备：华为、绿盟、迪普、ARBOR等
- 北京、上海等分公司已形成独立产品推出

流量封堵

- 目前骨干网设有一台专用路由器，可以在全网范围内下发黑洞路由，实现对去往某个目的地址的所有流量进行封堵。
- 包括国内流量封堵、国内网间流量封堵和国际网间流量封堵
- 可实现对去往用户IP的流量全部封堵，后期可实现攻击源区分封堵

现状：各省基于其城域网结构、流量特征以及业务需求等，独立建设和部署流量清洗系统

流量监控与分析系统

- 对出入城域网流量和内部交换流量进行分析检测
- 对异常攻击流量进行检测和定位
- 与流量清洗设备联动，保障城域网的安全性和可靠性
- 部署位置：城域网核心节点
- 监控范围：出口核心、汇聚层、IDC
- 主要技术：DPI、DFI
- 现状：各省独立部署，以Netflow设备为主，部分省分部署DPI设备
- Netflow设备以流量五元组为基础，可实现流量采集和分析
- DPI设备相对成本更高，可实现应用层流量识别及统计分析

北京

北京联通IP 城域网目前部署有基于Flow 监测方式的 “IP 城域网流量分析系统”和基于DPI+DFI 监测方式的 “IP 网流量识别与控制系统”

山东

流量监控与分析系统
流量流向分析系统在济南集中部署，采集全省17地市城域网核心路由器、省网核心设备、济南青岛IDC核心设备的出口流量flow信息，实现对全网城域网核心路由器数据流量的采集和分析。

广东

流量检测与清洗系统主要包括流量清洗中心系统和专用流量清洗系统
流量清洗中心采用Netflow采用检测，可发现攻击并告知清洗中心
专用流量清洗系统为专用的大客户安全防御DDoS系统，可针对大流量洪水攻击和小流量应用层攻击进行识别和清洗

在建DDoS统一防护系统

总体架构：以规划新建的DDoS统一管理平台为全国控制中心，通过骨干网流量流向分析系统提供异常流量监测手段，通过骨干网运维系统提供地址溯源及路由控制功能，利用本期新建的骨干网流量清洗系统，在China169网内提供近源/近目的流量清洗及流量封堵服务；对于国内网间互联及国际互联，提供流量封堵服务；与集团B-BSS系统接口，同步客户信息和产品订购信息，并向第三方零售系统开放API；与省分流量DDoS监测系统对接，获取省分内部DDoS攻击数据，完善全网DDoS攻击数据的统计。

骨干网流量清洗系统部署方案

- **清洗系统组成：**

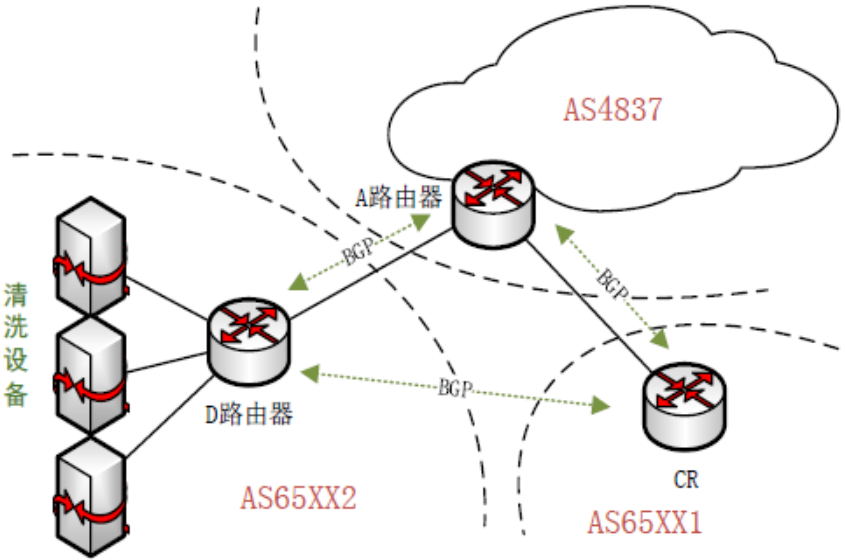
由引流路由器（D路由器）和清洗设备两部分组成，部署在全国31个省。

- **功能：**

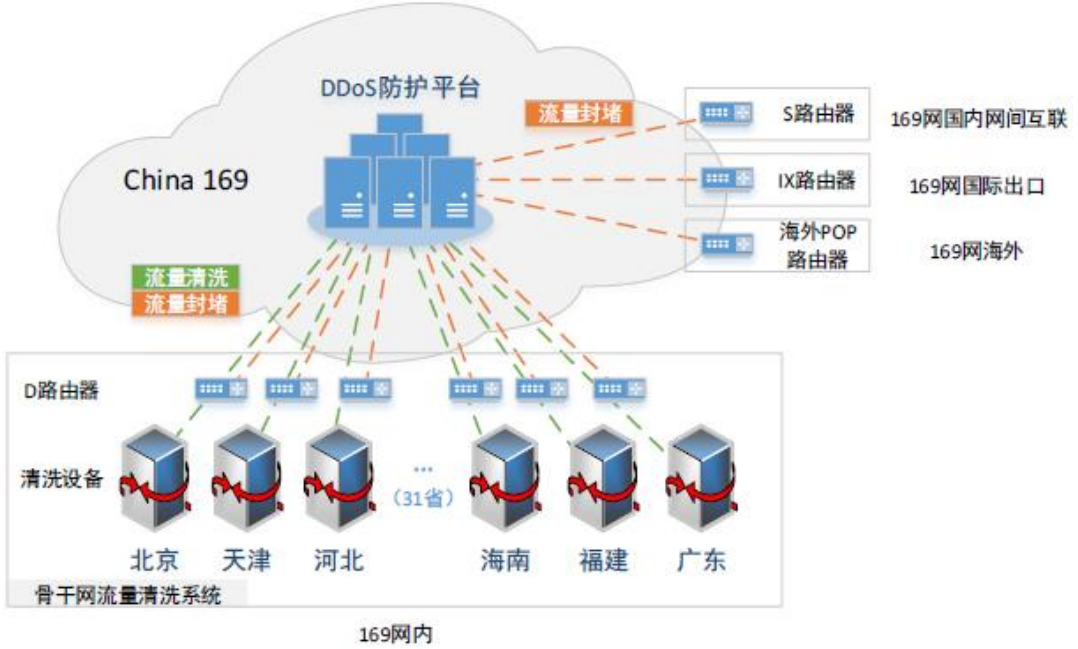
D路由器在清洗设备和骨干网A/C路由器之间做流量汇聚，执行流量引流和回注过程中的隧道终结，负责引流路由和黑洞路由的发布；清洗设备主要完成流量的清洗和回送。

- **自治域：**

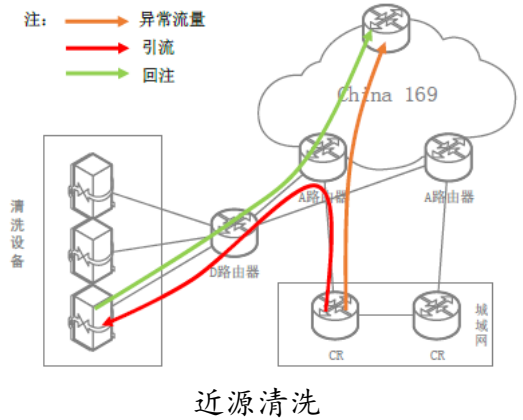
建议每个省为清洗系统分配一个私有AS号，清洗系统与骨干网、城域网等省内网络之间启用BGP路由协议。



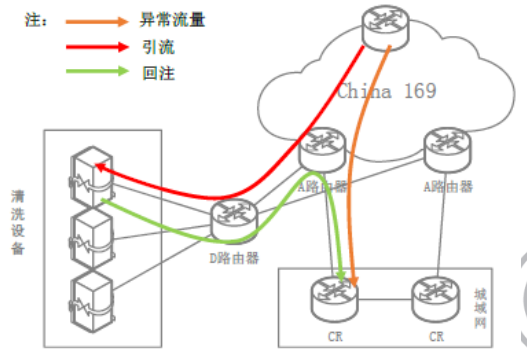
骨干网流量清洗系统部署方案_2



169网内



近源清洗



近目的清洗

网内

新建骨干网流量清洗系统，形成覆盖全网的近源及近目的清洗能力

全网

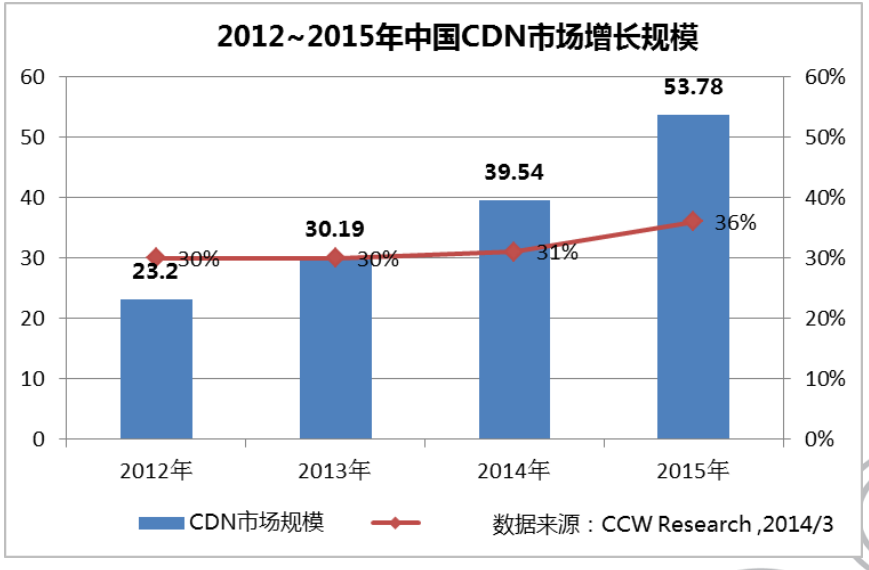
与骨干网运维系统通过接口协作，共同完成联通网内、国内互联、国际互联三个方面的流量封堵

完备的CDN部署

现状

	TV类CDN	互联网CDN
承载网络	专网承载	公网承载
加速业务	企业内容服务为主，以视频及内容下载为主	互联网内容服务为主，各类互联网内容加速
调度方式	基于IP调度	基于DNS调度
内容注入	内容以注入为主	内容以拉取为主
内容路由	内容路由根据网络拓扑	内容路由根据时延探测
典型例子	广电数字电视CDN、电信的IPTV CDN、企业流媒体CDN	蓝汛CDN、百度CDN

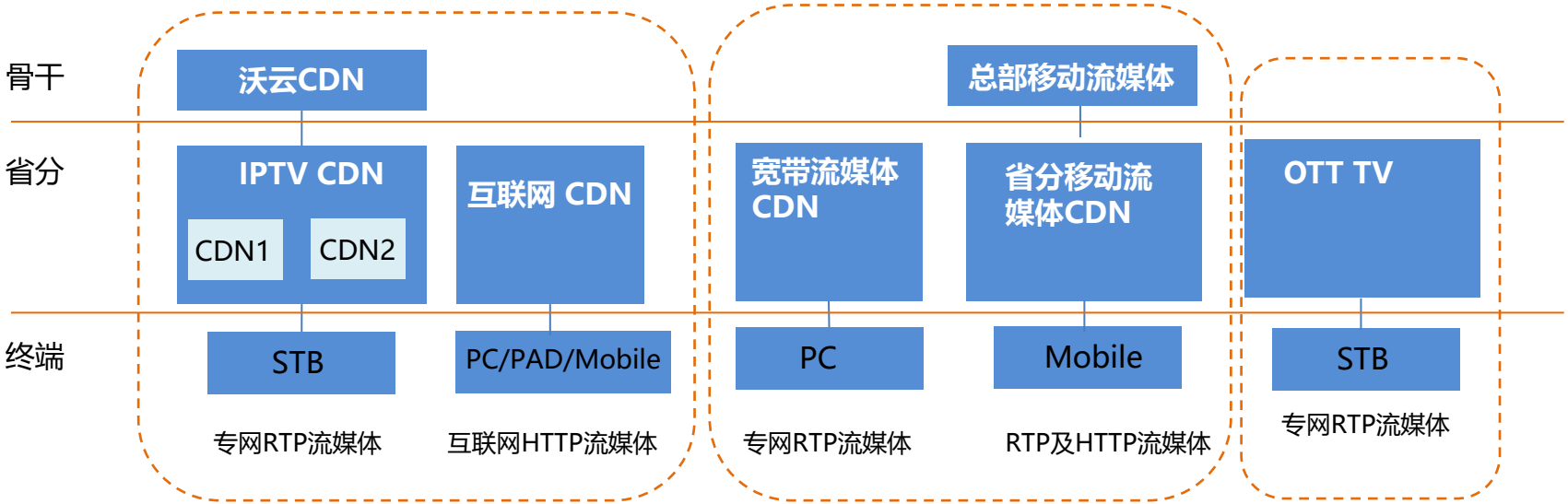
CDN现状及分类对比



中国CDN市场规模

中国联通CDN服务

中国联通综合CDN业务定位为，利用云计算、带宽、IDC等优势资源，部署高效的云CDN业务系统，打造“IDC租赁服务+云计算服务+CDN服务”的一体化经营体系



- 以提供互联网业务内容分发服务为目标，启动建设覆盖全国，超过100个节点的CDN网络
- 利用广泛的机房资源，与合作伙伴积极开展合作，发挥各自CDN业务优势，实现协同服务

China unicom中国联通
创新·改变世界

谢　谢！