

# 甜橙金融网络架构演进的分享

-- 如何应对虚拟化、业务突发增长以及应用架构变化带来的网络冲击

- ◆ 天翼电子商务有限公司（简称“甜橙金融”）是中国电信股份有限公司的全资子公司，作为中国电信旗下唯一的互联网金融平台公司
- ◆ 甜橙金融注册资本5亿元，由中国电信股份有限公司（00728.HK）出资
- ◆ 甜橙金融是国内首家电信运营商支付公司，是中国人民银行核准的第三方支付机构；作为进军互联网金融领域从事新业态的央企子公司，是兼具“金融、电信、互联网”特点的创新企业
- ◆ 拥有**第三方支付、征信、消费金融、财富管理、保险、网络贷款**等金融牌照

# 甜橙技术Fintech体系



合作方

## SaaS服务输出

风控	风险名单服务	风险模型计算	支付	支付服务	认证	登录鉴权	反欺诈
	信任环境甄别			账户服务		实名认证	

甜橙云PaaS

全局安全服务	众测平台	平台运维服务	监控管理		自动化测试		资源调度		智能大数据服务
	威胁感知		业务实时监控	设备基础监控	自动化测试平台	环境资源管理	流式计算		
	自动化攻击防护		资源动态监控	定制监控	全链路压测	一键式发布	模型算法		
	安全审计		持久化		分布式中间件		流程管理		
	关系型数据服务	Kv数据服务	事务服务	消息服务	Hadoop				
	分布式缓存	NOSQL	数据源服务	动态配置服务	Spark				

基础设施

IAAS平台API			数据服务API				
资源虚拟化	VMWARE	负载均衡	存储	资源标准化	容量管理	节点管理	容器管理
	计算资源	DOCKER	SDN		版本管理	日志管理	CMDB

# 甜橙金融-技术架构演进历史

1.0: “一把蜡烛”

2.0: “烛台上的蜡烛”

3.0: “蛋糕上的蜡烛”

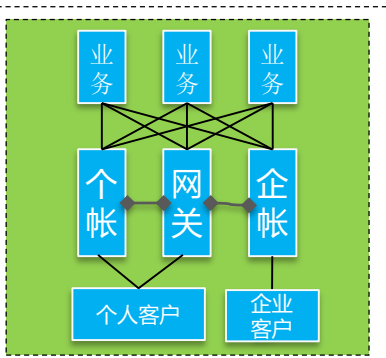
甜橙金融架构演进

流水账



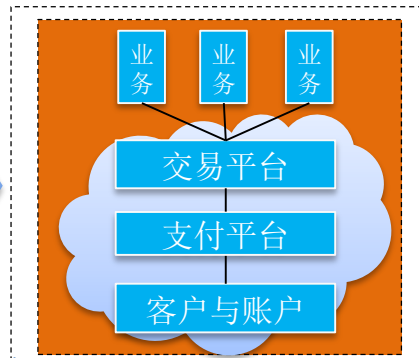
单业务条线架构

2011年~2013年



传统非金融业务架构

2014年~2015年

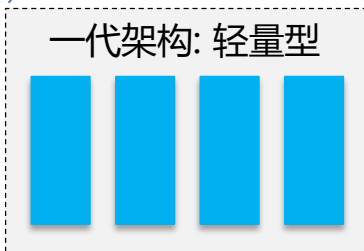


互联网云平台架构

2016年~2017年

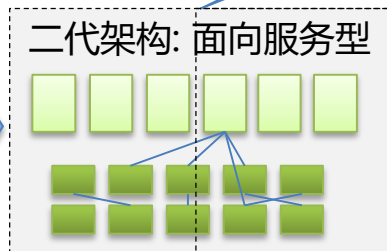
复式记账

支付宝架构演进



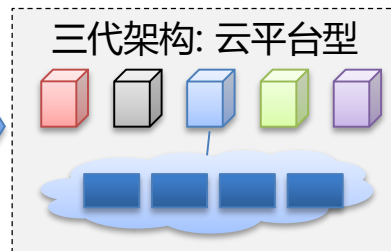
一代架构: 轻量型

2005年~2007年



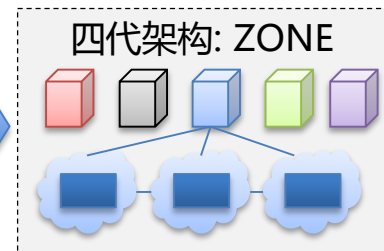
二代架构: 面向服务型

2008年~2010年



三代架构: 云平台型

2011年~2013年



四代架构: ZONE

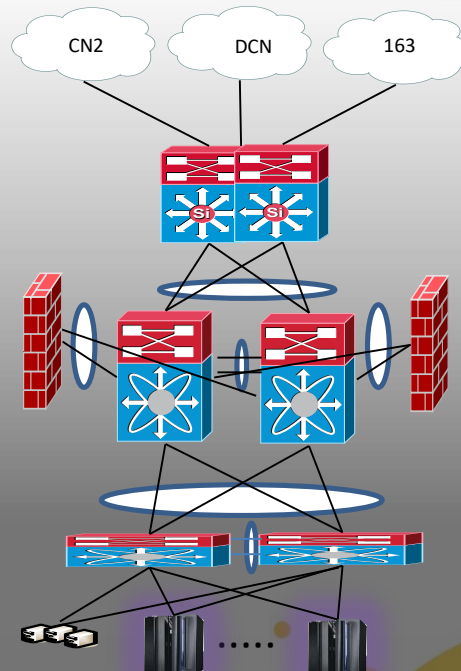
2014年~2018年

# 网络随着业务的逐步演进

## 前期较少业务

## 中期业务快速发展

## 当前业务增长迅猛

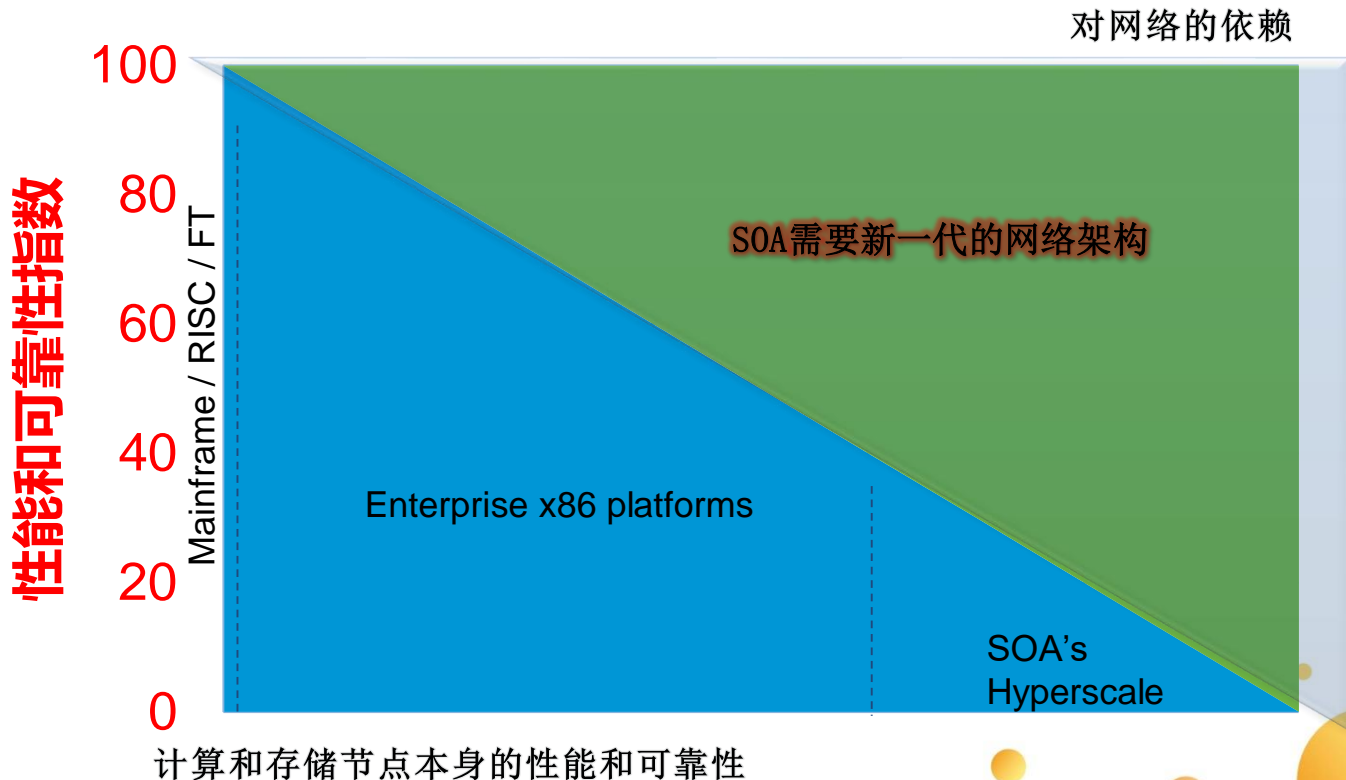


传统三层架构网络 + X86服务器

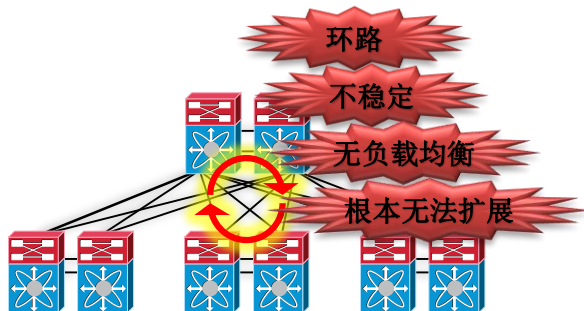
传统三层架构网络 + X86服务器 + 小型机

传统网络 + 网络虚拟化 + X86服务器 + 小型机 + 初步SOA

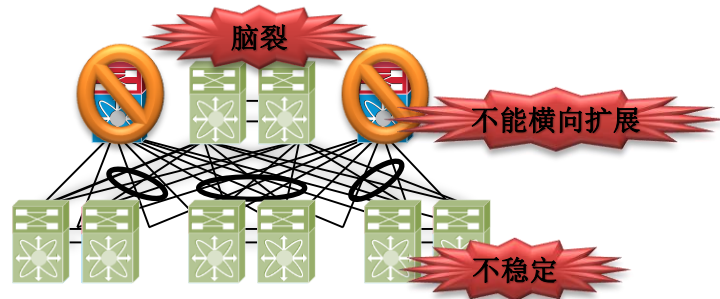
# 网络更多的参与到计算过程中



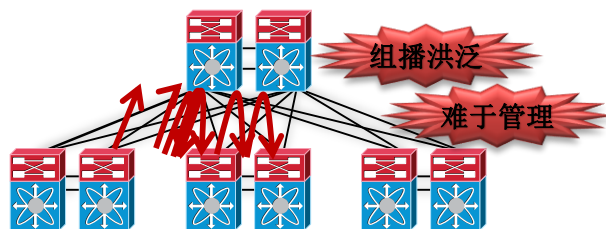
# 传统设计中遇到过的一些问题分享



传统生成树



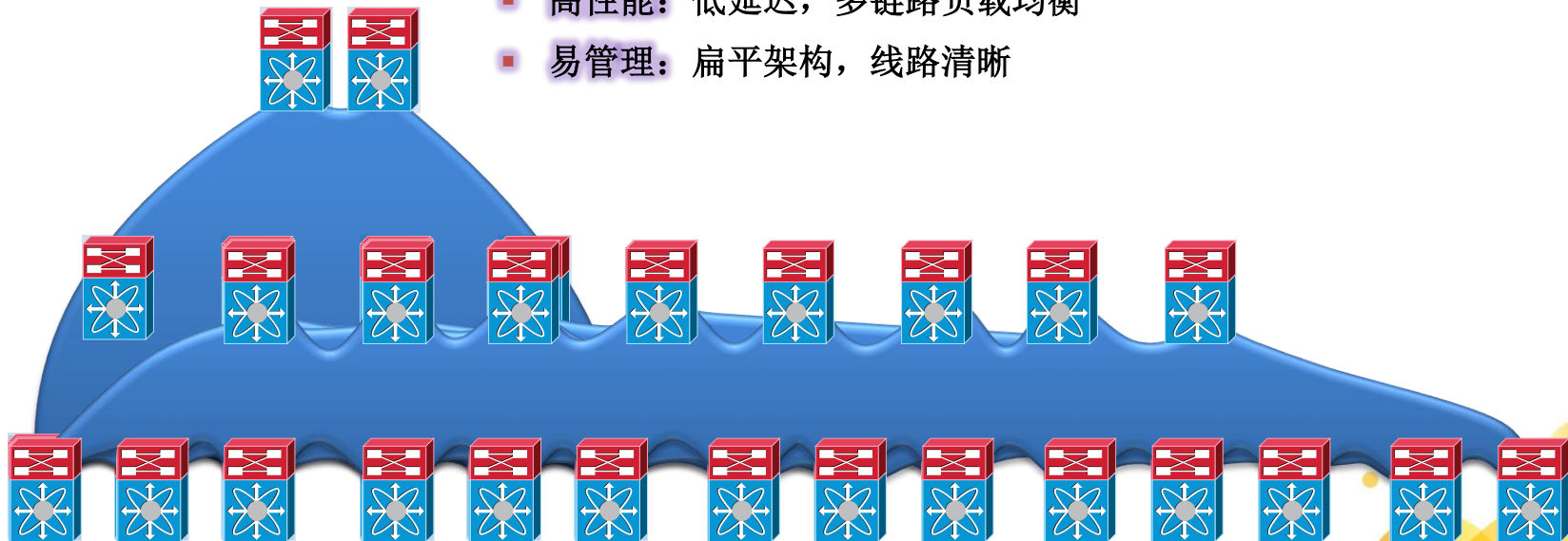
传统跨机箱捆绑



传统VXLAN

# 全新的弹性网络结构

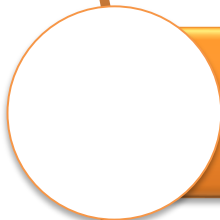
- **Pay as You Grow:** 动态横向扩展
- **VLAN Anywhere:** 二层处处可达
- **高可靠:** 广播控制、差错隔离、松耦合
- **高性能:** 低延迟, 多链路负载均衡
- **易管理:** 扁平架构, 线路清晰







智能化之前的困境



智能化以后的效果



智能化运维的解决基石

# 智能化之前的困境 (一)

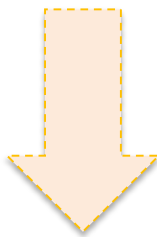


VS



瓶颈  
有状态  
延迟增加  
SOA高并发场景下选型困难

监管要求  
隔离  
管控



一次访问操作3套防火墙，配置超过50行







智能化之前的困境



智能化以后的效果



智能化运维的解决基石

# 智能化之后的效果 (一)

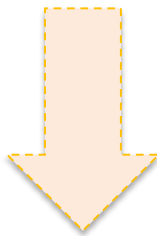


&



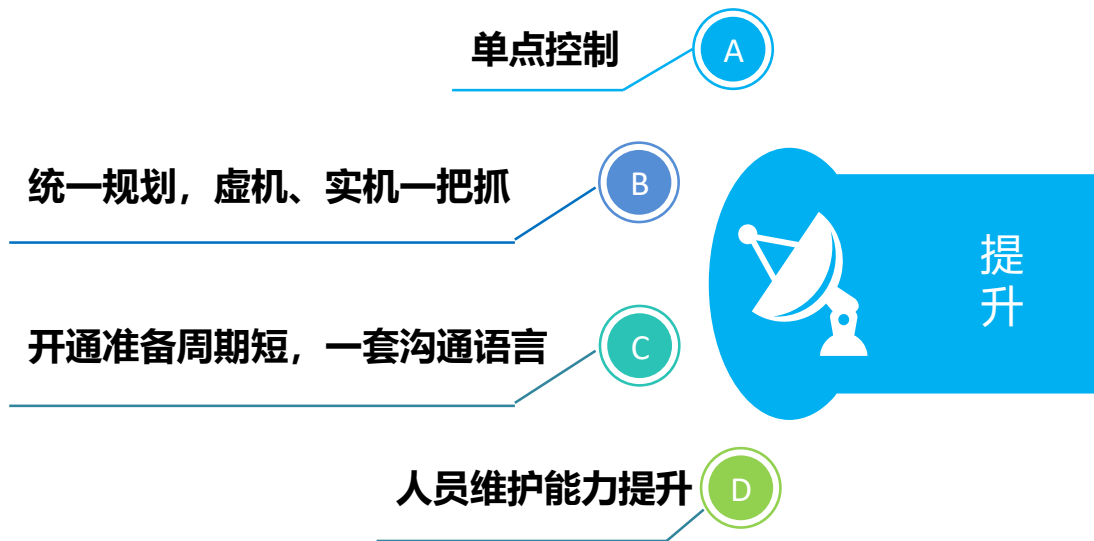
低延迟  
无状态 (切换不断长链接)  
无瓶颈可扩展  
适合SOA场景, 适合分布式场景

监管要求  
隔离  
管控



一次访问操作, 一分钟搞定

## 智能化以后带来的提升（二）



# 智能化以后带来的提升(三)

## 平台能力提升

稳

快

1. 后续系统升级服务不中断，用户无感知（现在部分业务有影响）
2. 平台服务可用率大幅提升（98.6%→99.99%）
3. 运维可用率提升到99.996%
4. 水电煤、话费充值、理财等业务系统故障发生后恢复效率提升30%（平均70分钟→50分钟）

1. 客户端登陆更流畅，活动高峰期登陆3s内（现有5s左右）
2. 营业厅业务办理更顺畅，效率更高（交费助手开通、翼支付开户）
3. 全国业务(营业厅、pos)并发受理能力大幅提升（1000笔/s→3000笔/s，还可以持续提升）
4. 套餐红包返利更快、高效（1小时→10分钟内）
5. 单机处理能力和支付宝、微信等水平一致

## 3.0 平台整体性能目标一览表

各支付平台	账务处理能力				交易处理能力	
	单个会计事件的事务处理时长(ms/笔)	单次余额更新的事务处理时长(ms/笔)	单机并发会计事件目标数(台)	单机并发余额更新事务处理目标数(台)	单个交易处理时长(ms/笔)	单机并发交易处理数(ms/笔)
支付宝	9	8	3500	7000	30	7000
微信	12	10	2200	5000	40	5000
翼支付	10	8	3000	5000	50	5000

各支付平台	客户平台能力		风控平台能力		中间件统一服务能力		登录状态
	单次客户信息查询处理时长(ms/笔)	单次客户信息查询并发处理数(W/台)	风控事件的单点判断处理能力(ms/笔)	单次消息通信速度(ms/条)	单机并发处理消息数(ms/笔)	同时登录保持在线数(W/台)	
支付宝	15	10	10	4	4	5	
微信	15	10	20	8	7	8	
翼支付	15	10	15	5	5	5	

对比图

支付宝 微信 翼支付

备注：整体性能指标阐述按单台标准机器的处理能力进行列示，单台标准机器的配置为（双核8G内存），这个配置后面将作为信息技术部的唯一标准进行衡量。



# 通过建规范及推行应用改造、权限把控、自动化平台搭建等解决问题

部分应用仅支持单点部署

集群的节点隐藏着差异：比如定时任务

对本地环境依赖

个性化的应用

无法准确判断节点的健康状态，特别假死

难以快速复制的网络

问  
题

## 一 建规范；推改造

1. 统一架构
2. 健康检查页面
3. 会话共享
4. 文件存储规范

1. 涉及改造应用：413个
2. 剩余95个应用为非标或者厂商应用

## 二 试迁移；爆问题

1. 通过迁移应用，提前暴露各种不规范问题。通过试迁移100多个应用，提前发现各种问题

## 三 控权限，避免二次不规范

1. 严格控制服务器权限，避免二次不规范的产生，回收了消费金融、征信、预付卡等的权限

## 四 通过EPG管理应用及网络

1. 内部调用：标准端口网络互通
2. 对外提供的地址：全部通过NGINX，有据可查；网络关系更清晰
3. 网络开通按照epg开通，快速扩容中的网络卡点将不复存在

## 五 梳理了网络和dns

1. 梳理完成：1100条网络
2. Dns迁移：209条

后续所有应用信息以及网络信息均会维护在自动化运维平台里



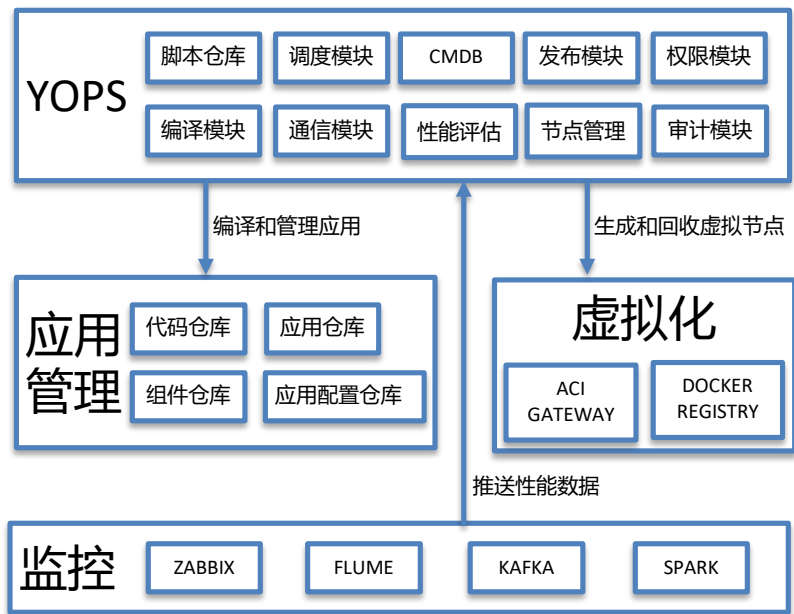
智能化之前的困境



智能化以后的效果



智能化运维的解决基石

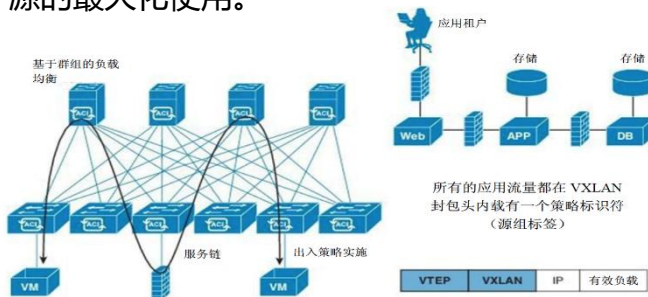


- 全平台采用PYTHON自主研发，并结合了MAVEN、GIT、ZABBIX等业界实践过的优秀开源组件
- 通信模块采用主流的自动化配置管理工具SALTSTACK，高效稳定且集群易于扩展
- 主机虚拟化采用轻量化容器DOCKER并做了定制化，在实现应用有效隔离的同时最大化利用主机资源
- 网络虚拟化采用行业领先的CISCO ACI技术，完全实现SDN
- 系统监控采用老牌组件ZABBIX，应用监控采用最新的FLUME+KAFKA+SPARK，实时感知应用压力变化，并通过自主开发的智能学习模型感知扩容阈值，实现弹性计算
- 权限和审计模块做到每次线上操作事前有管控，事后可回溯，保证线上生产环境安全稳定

## 智能化运维的解决基石

### 基于全局资源虚拟化的自动化运维平台

1. 甜橙云引入了**全局资源虚拟化**的体系，对计算、存储、网络资源分别进行统一的池化，在统一资源调度平台的融合下形成全局的弹性。
2. 通过对运行时状态下的应用在Load、IO、流量等数据的动态监控，弹性地增减资源使用情况，达成在低运维成本情况下对设备资源的最大化使用。



### SDN建设

#### SDN的价值

提升运维效率

降低运维成本

快速自动化部署

#### 近期成果

工单模板调研及目标制定

部署安装  
TOOLKIT及SDK

编写PYTHON SDN程序V1.0及配置下发验证

## ACI环境SDN工单模板调研及模板制定完成

H19												
	A	B	C	D	E	F	G	H	I	J	K	L
1	Tenant	Contract	Provide_EPG	P_AppPrf	Consume_EPG	C_AppPrf	FilterEntry	Protocol	sFromPort	sToPort	dFromPort	dToPort
2	sunzhibin	APP_CON	APP_EPG	APP_PRF	WEB_EPG	APP_PRF	TCP_25	TCP	1	65535	25	25
3	sunzhibin	DB_CON	DB_EPG	APP_PRF	APP_EPG	APP_PRF	TCP_1433	tcp	1	65535	1433	1433
4	sunzhibin	DB_CON	DB_EPG	APP_PRF	APP_EPG	APP_PRF	UDP_3306	Udp	1	65535	3306	3306
5	sunzhibin	WEB_CON	DB_EPG	APP_PRF	WEB_EPG	APP_PRF	ICMP	icmp	unspecified	unspecified	unspecified	unspecified
6												
7												

	A	B	C	D	E	F	G
1	Tenant	Context	BD	Subnets	Subnets_Scope	AppProfile	EPG
2	sunzhibin	sunzhibin_VRF	APP_BD	192.168.10.254/24	private	APP_PRF	APP_EPG
3	sunzhibin	sunzhibin_VRF	APP_BD	192.168.15.254/24	public	APP_PRF	APP_EPG
4	sunzhibin	sunzhibin_VRF	WEB_BD	192.168.20.254/24	private, shared	APP_PRF	WEB_EPG
5	sunzhibin	sunzhibin_VRF	DB_BD	192.168.30.254/24	private	APP_PRF	DB_EPG
6	sunzhibin	other_VRF	other_BD	10.10.10.254/24	private	other_PRF	other_EPG
7	test	test_vrf	test_bd	1.1.1.1/24	public, shared	test_prf	test_epg
8							
9							

- 完成ACI环境SDN的SDK部署与安装;
- 完成ACI环境SDN的Toolkit部署;

## APIC Python SDK – cobra

[https://developer.cisco.com/media/apicDcPythonAPI\\_v0.1/install.html](https://developer.cisco.com/media/apicDcPythonAPI_v0.1/install.html)

```
C:\>cd Python27
C:\Python27>dir
Volume Serial Number is 8865-1272

Directory of C:\Python27

2016-03-28 14:47 <DIR> .
2016-03-28 14:47 <DIR> ..
2016-03-28 21:58 98,388 acicobra-1.2.2b-py2.7.egg
2016-03-28 21:58 69,254,122 acimodel-1.2.2b-py2.7.egg
2016-03-28 17:45 <DIR> acikitoolkit-master
2016-03-28 09:15 <DIR> bin
2016-03-28 09:16 <DIR> doc
2016-03-28 17:41 <DIR> etc
2016-03-28 09:16 <DIR> include
2016-03-28 09:16 <DIR> lib
2016-03-28 09:16 <DIR> lib\
2016-12-06 20:26 28,534 libffi-1.2.10-1.exe
2016-12-06 20:26 444,788 libffi-1.2.10-1.exe
2016-12-06 20:33 27,136 python.exe
2016-12-06 20:33 27,548 python.exe
2016-11-21 23:00 54,557 setup.exe
2016-03-28 09:16 <DIR> scripts
2016-03-28 09:16 <DIR> test
2016-03-28 09:16 <DIR> tools
2016-12-06 20:33 111,616 vcpkg.exe
2016-03-28 14:48 <DIR> wsgy-master
2016-12-06 20:33 8 Files(s) 78,158,743 bytes free
2016-12-06 20:33 11 Dir(s) 5,637,653,948 bytes free

C:\Python27>python setup.py install acicobra-1.2.2b-py2.7.egg
Processing acicobra-1.2.2b-py2.7.egg
removing 'c:\python27\lib\site-packages\acicobra-1.2.2b-py2.7.egg' (and everything under it)
installing acicobra-1.2.2b-py2.7.egg to c:\python27\lib\site-packages
Extracting acicobra-1.2.2b-py2.7.egg to c:\python27\lib\site-packages
acicobra-1.2.2b is already the active version in easy-install.pth

Installed c:\python27\lib\site-packages\acicobra-1.2.2b-py2.7.egg
Processing dependencies for acicobra-1.2.2b-py2.7.egg
Finished processing dependencies for acicobra-1.2.2b

C:\Python27>python setup.py install acimodel-1.2.2b-py2.7.egg
Processing acimodel-1.2.2b-py2.7.egg
removing 'c:\python27\lib\site-packages\acimodel-1.2.2b-py2.7.egg' (and everything under it)
installing acimodel-1.2.2b-py2.7.egg to c:\python27\lib\site-packages
Extracting acimodel-1.2.2b-py2.7.egg to c:\python27\lib\site-packages
acimodel-1.2.2b is already the active version in easy-install.pth

Installed c:\python27\lib\site-packages\acimodel-1.2.2b-py2.7.egg
Processing dependencies for acimodel-1.2.2b
Finished processing dependencies for acimodel-1.2.2b

C:\Python27>
```

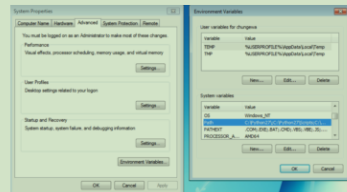
acicobra

acimodel

## Python环境

[https://developer.cisco.com/media/apicDcPythonAPI\\_v0.1/install.html](https://developer.cisco.com/media/apicDcPythonAPI_v0.1/install.html)

- 目前为止，Python2.7版本依然是ACI编程的不二选择
  - 目前:不要试图选择高版本^^
  - 确保安装姿势正确!!! ☺ 否则，就没有然后鸟.....
  - Python2.7、easy\_install、pip是必备安装包; 没有install难度，只有安装过程是否正确
  - Virtualenv用虚拟空间跑不同的APIC SDK版本环境; 不是必须
  - Python: <https://www.python.org/>
  - Easy\_install: <https://pypi.python.org/pypi/setuptools>
  - PIP: <https://pypi.python.org/pypi/pip>
  - Virtualenv: <https://pypi.python.org/pypi/virtualenv>
- Pyopenssl
  - SSL support for connecting to the APIC and fabric nodes
  - 不是必须安装工具
- Python脚本编写工具:
  - 参考: JetBrains PyCharm Community Edition 5.0.3
  - 工具不唯一，各有所爱
- 针对Windows，修改环境变量:
  - 增加 ;C:\Python27\Scripts (以安装目录为C:\Python27为例)

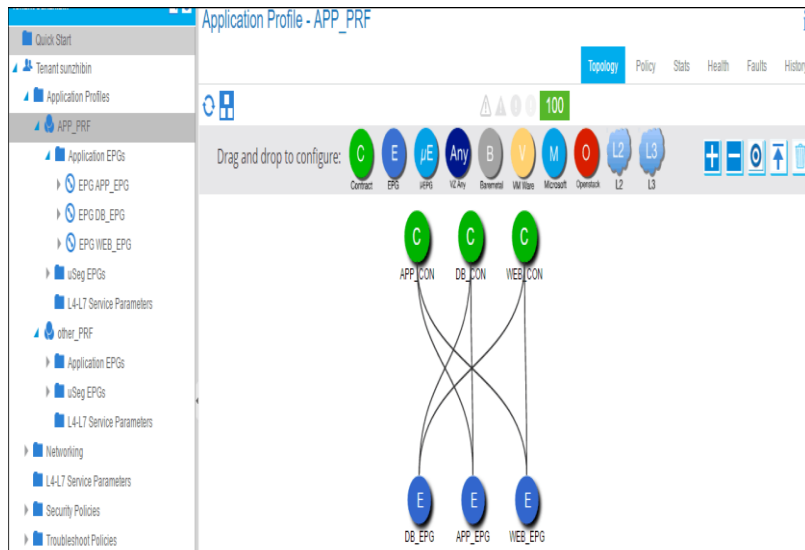


# SDN建设的近期成果- PYTHON SDN程序V1.0编写及配置下



- 调用ACI API接口的Python SDN程序v1.0编写完成;
- 工单的一键实施, 配置自动下发及验证完成;

```
文件(E) 编辑(E) 搜索(S) 查看(V) 文档(O) 项目(P) 生成(G) 工具(T) 帮助(H)
新建 打开 保存 全部保存 还原 关闭 后退 前进 编译 生成 执行 颜色选择器
标记 文档
ACI_Python.py
9 f = open('log_json.txt', 'w')
10
11 # Get the APIC login credentials
12 description = 'scitoolkit tutorial application'
13 creds = Credentials('apic', description)
14 creds.add_argument('--delete', action='store_true',
15 help='Delete the configuration from the APIC')
16 args = creds.get()
17
18 # Login to APIC and push the config
19
20 for sheet_n in xls_data.keys():
21
22     if (sheet_n == "CreatEPG") & (len(xls_data[sheet_n]) != 0):
23         print "\nSheet", sheet_n, "Input:\n", xls_data[sheet_n], "\n\n"
24         EPGList = [(i[0] + 7) for i in range(1000)]
25         EPGList = xls_data[sheet_n]
26         for m in range(0, len(EPGList)):
27             tenant = Tenant(EPGList[m][0])
28             app = AppProfile(EPGList[m][5], tenant)
29             epg = EPG(EPGList[m][6], app)
30             context = Context(EPGList[m][1], tenant)
31             bd = BridgeDomain(EPGList[m][2], tenant)
```



# SDN的价值-提升运维效率

现状	未来
<b>运维人员角色</b>	工单实施人员 (人工写配置)
<b>实施人</b>	工单审核人员 (定义好的工单模板格式和内容)
<b>工单时长</b>	通过工单模板输入到调用SDN API接口的Python程序 瞬间完成配置推送, 缩短到分钟级别



	A	B	C	D	E	F	G
1	Tenant	Context	BD	Subnets	Subnets_Scope	AppProfile	EPG
2	sunzhbin	sunzhbin_VRF	APP_BD	192.168.10.254/24	private	APP_PRF	APP_EPG
3	sunzhbin	sunzhbin_VRF	APP_BD	192.168.15.254/24	public	APP_PRF	APP_EPG
4	sunzhbin	sunzhbin_VRF	WEB_BD	192.168.20.254/24	private, shared	APP_PRF	WEB_EPG
5	sunzhbin	sunzhbin_VRF	DB_BD	192.168.30.254/24	private	APP_PRF	DB_EPG
6	sunzhbin	other_VRF	other_BD	10.10.10.254/24	private	other_PRF	other_EPG
7	test	test_vrf	test_bd	1.1.1.1/24	public, shared	test_prf	test_epg
8							
9							

```

Application Profile - APP_PRF
-----
Tenant: sunzhbin
Application Profile: APP_PRF
Application EPGs:
  - EPG_APP_EPG
  - EPG_DB_EPG
  - EPG_WEB_EPG
L4-L7 Service Parameters:
  - other_PRF
  - Application EPGs
  - other_VRF
  - L4-L7 Service Parameters
Networking:
  - L4-L7 Service Parameters
  - Security Policies
  - Authentication Policies
  
```

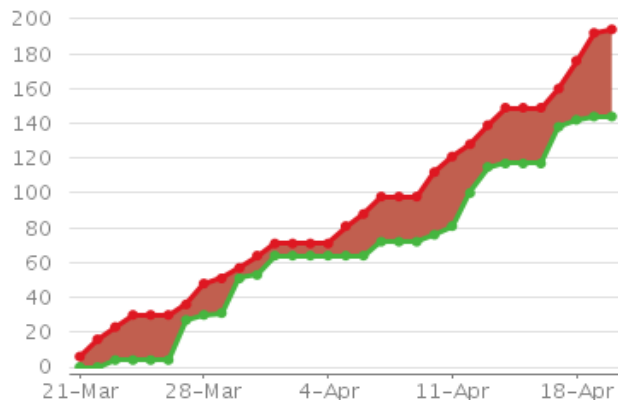


# SDN的价值-降低运维成本

1. 随着公司数据中心不断扩充和工单不断增加（人员未增加），目前面临**人人都需要参与到工单实施**的工作当中。
2. 采用SDN技术后可大大降低运维成本，以工单为例：目前日均工单10张，每人至少1-2张工单（30日工单量统计）。SDN使用后可单人即可完成日均所有工单审查与复核，可**提升网络运维效率50%**。

NETWORK-365	光大-outerbank准生产机器开通光大银行网络工单	张怀志	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17
NETWORK-364	燃气专线开通常京网络	曹锦华	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17
NETWORK-363	征信添加综测白名单	张怀志	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17
NETWORK-362	商户宣城云海-浦东网络开通-刘超	孙志斌	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17
NETWORK-361	打通开发环境与外网(支付宝, 微信, 翼支付个人账户)的网络	张元舜	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17
NETWORK-360	outerbank开通光大专线	张怀志	吴佳琦	已解决	验证通过	14/四月/17	17/四月/17	17/四月/17
NETWORK-359	办公网访问上海综测, 鉴权中心	张怀志	吴佳琦	已解决	验证通过	13/四月/17	17/四月/17	17/四月/17
NETWORK-357	准生产中间件F5内负载地址申请	孙耀松	陈苏强	已解决	验证通过	13/四月/17	19/四月/17	17/四月/17
NETWORK-356	通联综测网络开通	孙耀松	吴佳琦	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17
NETWORK-355	陕西综测环境网络开通	孙耀松	吴佳琦	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17
NETWORK-354	电子货币手机充值业务联调	孙耀松	吴佳琦	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17
NETWORK-353	生产中间件F5内负载地址申请	李伊仁	陈苏强	已解决	验证通过	13/四月/17	18/四月/17	17/四月/17
NETWORK-351	梳理172.17.49.121的专线向上策略	刘涛	张长双	已解决	验证通过	13/四月/17	14/四月/17	17/四月/17
NETWORK-350	开通商户调用账单应用网络白名单	刘涛	吴佳琦	已解决	验证通过	13/四月/17	17/四月/17	14/四月/17

问题: 30 天汇总



已创建 194 个问题, 已解决 144 个问题

# DeepFlow®

接入网络 / 回溯分析

时间范围: 2018-05-14 10:19 - 2018-05-14 11:19

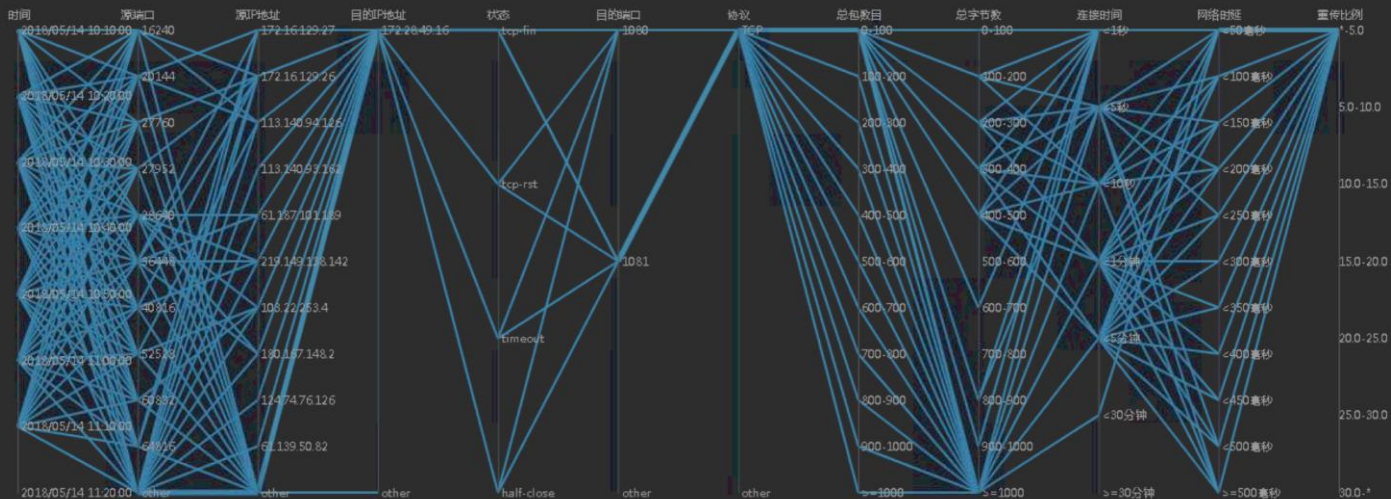
流量总览 | **回溯分析** | 流量特征 | 会话回溯 | 服务记录

回溯分析（多维图）是用来检索历史数据，并展示出Flow数据在相邻两个维度的映射关系。每个维度坐标按照关联性排列（如时间）或该维度的TOP排序，您也可以自定义维度展示顺序。

目的IP地址=172.28.49.16 × 回溯过滤规则，以回车结束

搜索 保存 打开 维度

目前共回溯到 158213 条 Flow 数据，耗时 12.614 秒



# Thank you!

天翼电子商务有限公司

北京：西城区复兴门南大街乙2号天银大厦A东座

上海：虹口区四川北路859号中信广场6F

广州：珠江新城花城大道18号建滔广场20F