2014年3月21日星期五

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

轻量级制造企业园区
- 密集办公条件下的信息安全

enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

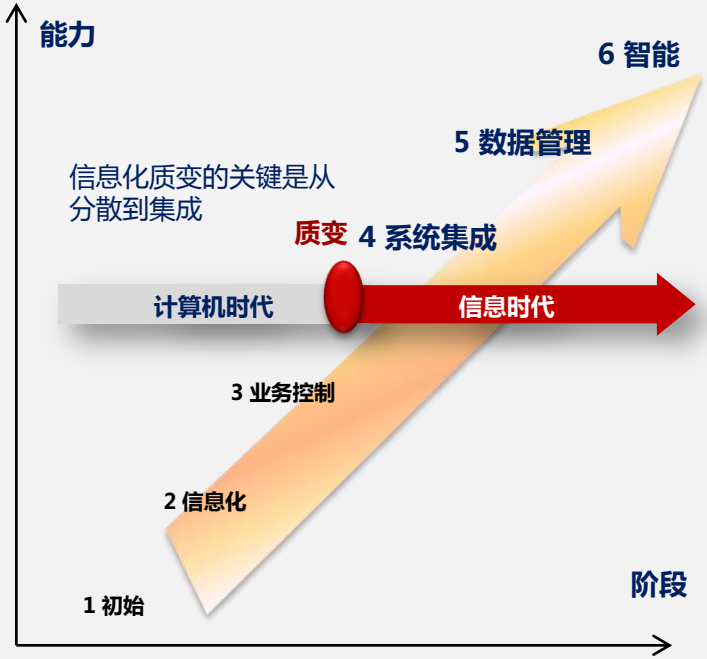
Content

1 客户关键需求理解

2 密集办公条件下的信息安全

HUAWEI

园区信息化是企业信息化的基础



诺兰模型
企业信息化发展遵循客观规律的经典模型，用于指导企业ICT系统建设，分为6个阶段。

信息共享

数据时代

企业办公系统 | 视频会议 | 无线接入 | 语音通信

品质体验

多媒体、云与移动时代

多媒体	桌面智真	临场式智真	移动视频
云	云存储	桌面云	云计算
移动	BYOD	企业应用商店	物联网

HUAWEI

轻量级制造企业园区涌现，如轻型飞机制造企业

0005852

国务院 中央军委 文件

国发〔2010〕25号

国务院 中央军委关于深化我国低空空域管理改革的意见

各省、自治区、直辖市人民政府，国务院各部委、各直属机构，各军区、各军兵种、各总部，武警部队：

低空空域是通用航空活动的主要区域，深化低空空域管理改革，是大力发展通用航空、繁荣我国航空业的重要举措，是促进我国经济社会发展的迫切需要。党中央、国务院、中央军委十分重视发展航空业和做好空管工作，在军地双方的共同努力下，我国空域管理不断改进，空域资源逐步得到有效利用，在经济社会发展和国防建设中发挥了重要作用。随

— 1 —

2010年11月14日 《关于深化我国低空空域管理改革的意见》

低空空域管制的逐步**放开**，**轻型直升机**成为未来交通工具新宠

轻型飞机制造企业陆续出现

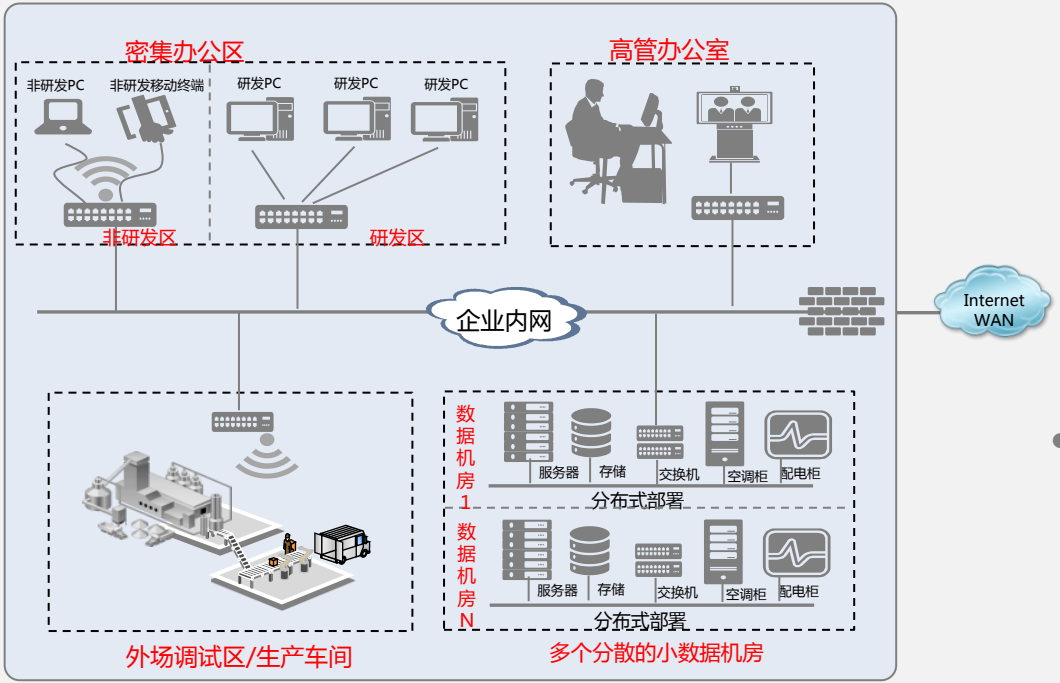
轻量级制造企业园区涌现

- **人数少**：一期30人
- **功能多**：研发，办公，制造
- **弹性大**：二期600人
- **机房小**：数个9m^{2}机房分散在园区

某典型轻量级制造园区

HUAWEI

轻量级制造园区办公及信息化建设的需求



- **密集办公**
  - ✓ 办公区域紧凑，研发、非研发员工办公区间靠近，没有物理隔离手段，存在研发核心资产泄密的隐患；
  - ✓ 数据中心机房面积小，网络、服务器、存储等设备需要分散部署在多个机房

□客户建设需求

***一期：**1座办公楼+2座生产车间，30名员工（含12名研发员工），园区有多个分散的小面积的机房，每个机房9平米左右*

***二期：**计划占地7公顷，人员规模扩大到600-700人（含研发和管理人员100人）*

HUAWEI

轻量级制造园区的信息化建设挑战

密集办公

挑战：密集办公条件下的信息安全问题

- 办公区域紧凑，非研发终端接入研发区端口，造成研发核心信息资产泄密；
- 研发电脑通过厂区内的WIFI接入非研发区，外发核心信息资产。

HUAWEI

Content

1 客户关键需求理解

2 密集办公条件下的信息安全

HUAWEI

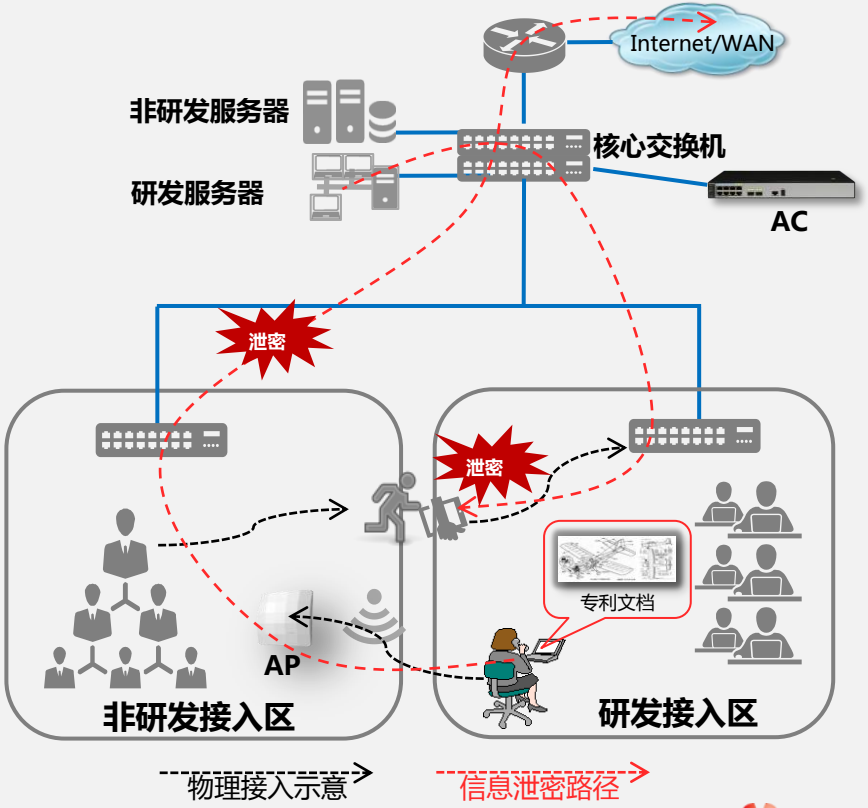
办公区域密集紧凑，存在核心信息资产泄密隐患

办公区域紧凑，端口账号混用

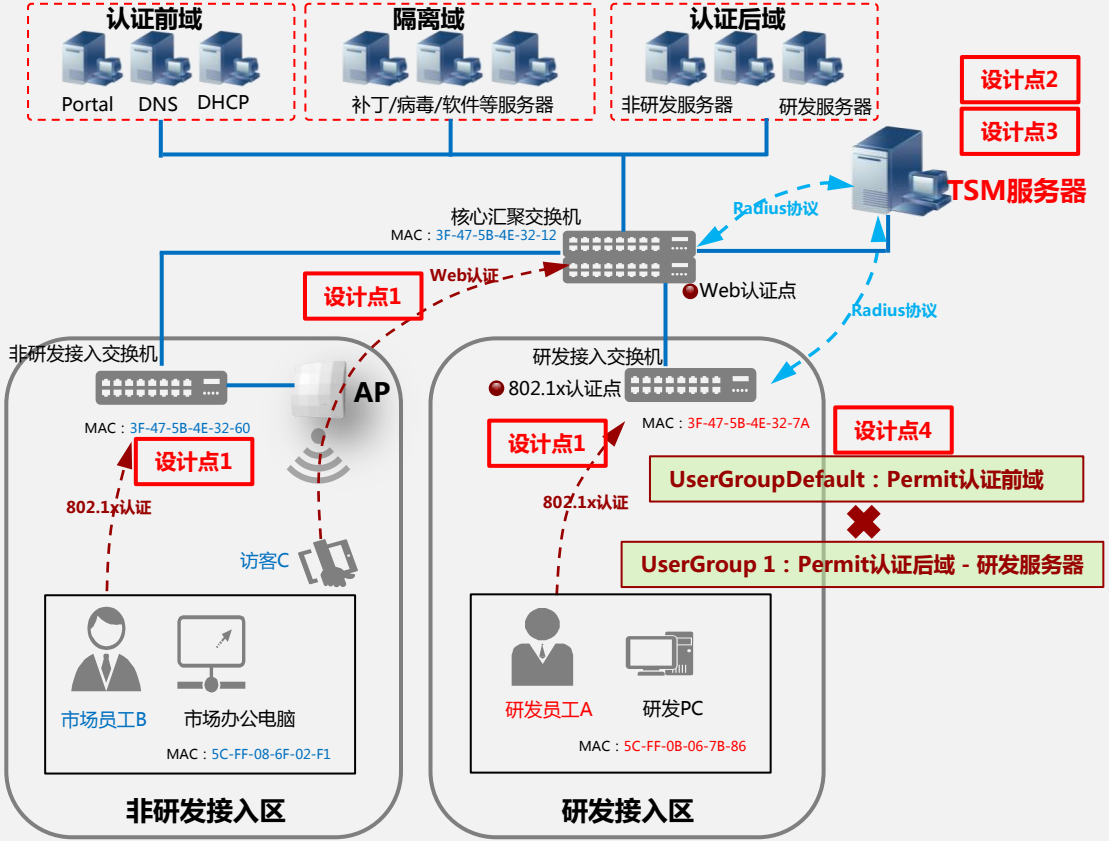
- 非研发区终端或员工私带个人便携机接入研发区端口，下载研发核心资产造成泄密；
- 研发电脑搬离研发区，在非研发区端口接入，并外发研发核心资产造成泄密

研发区终端通过WiFi访问外网

- 研发终端通过WiFi接入非研发区，进而访问Internet，外发核心资产。



端口账号混用解决之道——基于位置和设备的全员认证



方案设计点

设计点1：全员认证
通过认证限制用户的访问权限

- ✓员工采用802.1x认证，认证点为接入交换机
- ✓访客采用Web认证，认证点为核心汇聚交换机

设计点2：账号/接入终端绑定
限制员工账号只能由固定的终端接入，不可混用

- ✓研发员工A→ 研发PC MAC：5C-FF-0B-06-7B-86
- ✓市场员工B→ 市场电脑 MAC：5C-FF-08-6F-02-F1

设计点3：账号/接入区域绑定
员工和访客账号只能由固定的交换机接入，不可混插

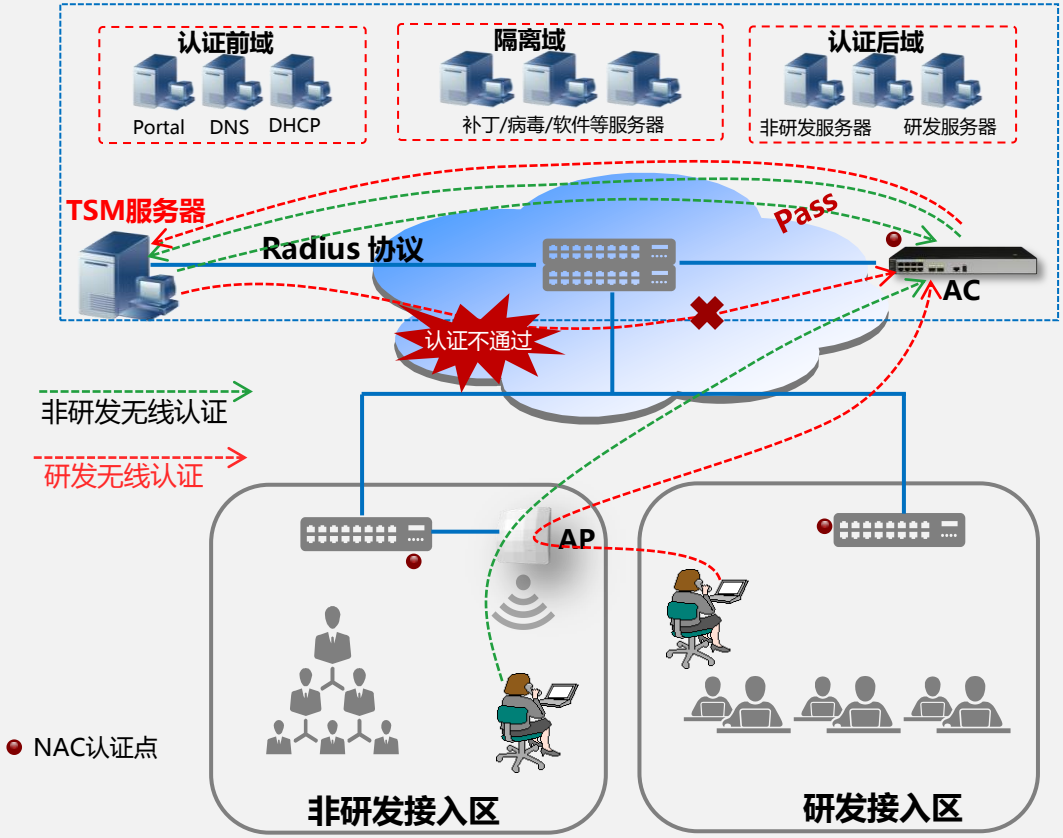
- ✓研发员工A→ 研发交换机 MAC：3F-47-5B-4E-32-7A
- ✓市场员工B→ 市场交换机 MAC： 3F-47-5B-4E-32-60
- ✓访客C → 市场交换机 MAC： 3F-47-5B-4E-32-12

设计点4：基于用户组设定权限
只需要指定员工所属的用户组，权限由用户组决定

- ✓研发员工A→ UserGroup_RD
- ✓市场员工B→ UserGroup_MK
- ✓未认证员工C→ UserGroupDefault

HUAWEI

无线集中认证，研发用户无线认证不通过



方案设计点

①有线无线一体化认证保证非研发无线用户的正常访问

1、员工终端发起802.1X认证。
2、AC接受请求，向TSM服务器发起认证请求。
3、TSM服务器进行身份认证，通过后，向AC发送用户的所属的用户组权限信息。
4、AC放开用户的访问权限

② 研发用户接入AP，认证不通过

1、员工终端发起802.1X认证。
2、AC接受请求，向TSM服务器发起认证请求。
3、TSM服务器中无研发账号和AC设备的对应记录，认证不通过
4、AC禁止用户的访问权限

HUAWEI

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

Copyright©2012 Huawei Technologies Co., Ltd. All Rights Reserved.
The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

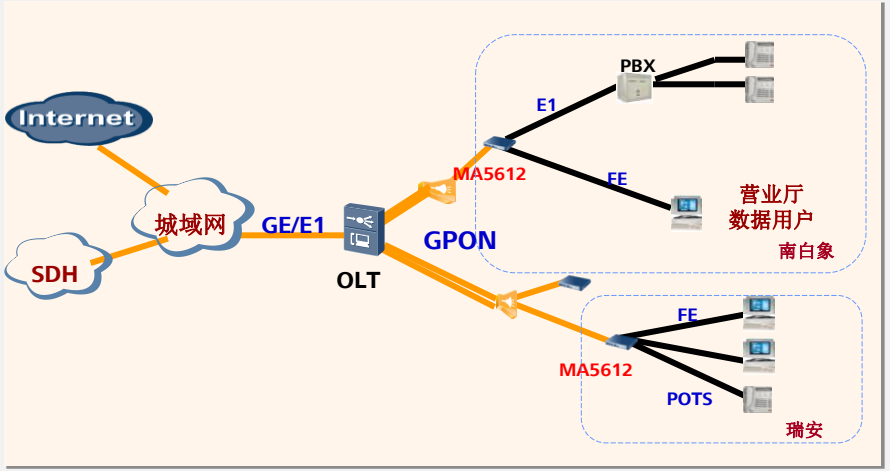
温州中小企业园区

项目背景

- 温州市中小企业数量庞大，由于企业用户收益高，发展这类用户对运营商至关重要
- 竞争激烈，光接入成为主流

华为方案

- MA5612通过E1接入企业专线及PBX。专线业务通过GPON传输后在OLT上再出E1接口接入SDH网络
- MA5612通过FE接入移动营业厅的数据用户，提供宽带上网业务。
- MA5612提供POTS端口，为企业用户提供VOIP业务。



成就客户

- 一站式解决企业用户业务需求，包括语音、上网、专线等业务
- 利用GPON的FTTO方案，各种业务可以快速推向市场，快速部署

HUAWEI

合肥平安校园战略项目

项目背景

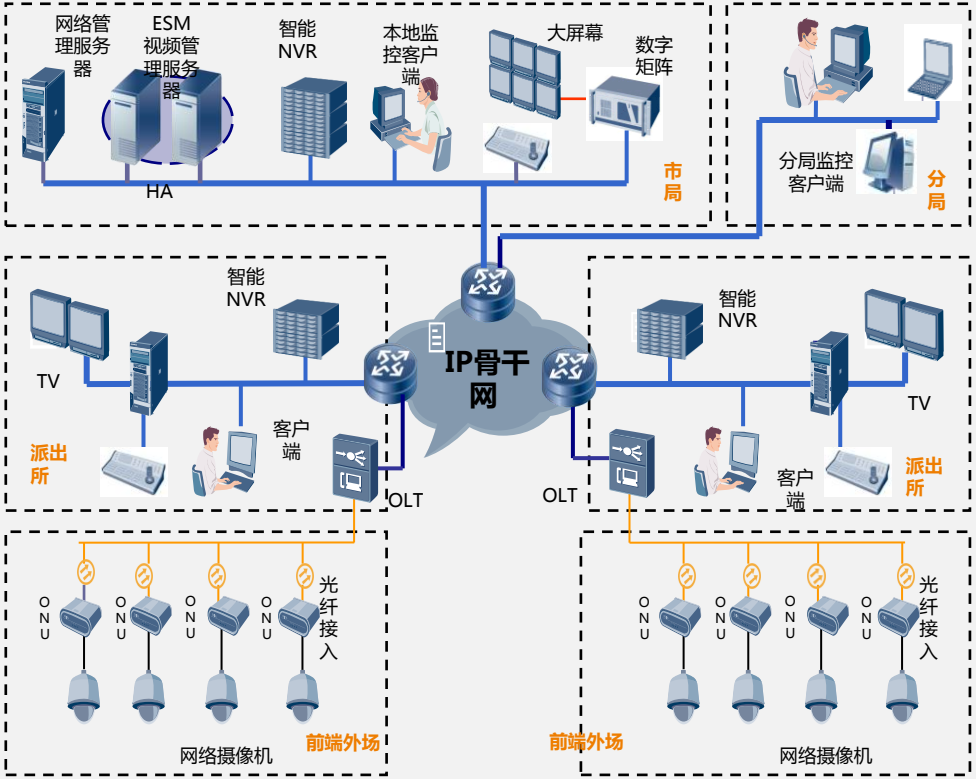
- 为了保护国家人民财产安全，建设一个良好的治安环境，合肥市计划将城市治安监控系统建设作为搞好社会治安、构建和谐社会的一项战略性措施

华为方案

- 采用华为MA5680T系列OLT和多种ONU组建全光接入层网络，还提供包含华为服务器、USG5350防火墙、监控平台软件、V1300N存储在内的监控整体解决方案。
- 方案涉及58派出所，7个分局，1个市局所属片区的中小学，近1000个点

成就客户

- 华为PON接入网降低组网复杂度，有效避免多点故障
- 丰富的智能分析能力，便被动记录为主动预警



HUAWEI

Etisalat – GPON全业务

项目背景

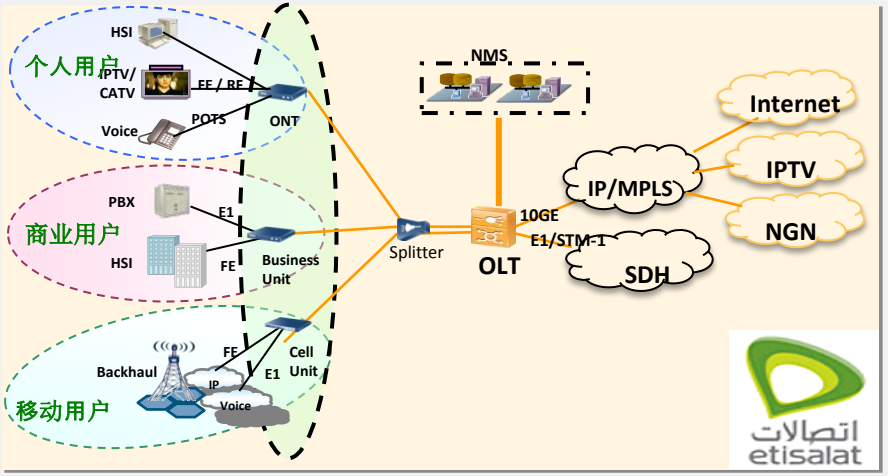
- 必须是面向未来的宽带网络
- 必须是全业务覆盖的接入网络
- 必须有利于降低长期 OPEX

华为方案

- 统一的GPON全业务网络接入个人用户、商业用户、移动回传业务
- 商业用户和移动回传业务采用Native TDM方案，E1/STM-1接入SDH网络，并采用TypeB提高网络可靠性
- 后续专线业务在OLT上行将演进到PWE3方案，全网IP化

成就客户

- 接入层产品统一，维护方便，OPEX降低
- 目前已经部署100多万线FTTH用户，其中包括数千套专供企业接入的SBU设备



HUAWEI