SANGFOR
深信服科技

金融网点无线覆盖

技术建议书

深信服科技有限公司

SANGFOR
深信服科技

目录

1应用背景

近年来随着无线技术的迅速发展，企业的无线应用需求急剧增长，而随着手持智能终端（平板电脑，智能手机等）的迅速普及，用户使用习惯也随之改变。越来越多用户习惯通过智能终端访问互联网。国内同行如城/农业银行、光大银行，通过部署无线营业厅，向用户提供免费 WIFI 无线上网， 受到广泛认可。经调研，通过部署无线营业厅，可为银行带来如下好处：

1、可分流 20%以上前来办理业务的人员，通过手机网上银行办理业务，平均节省 30%的排队等候时间（手机银行体验区）。

2、当客户在等候时，可使用 WIFI 免费上网，分散等待注意力，从而减少客户排队等待时间过长的抱怨，提升客户满意度。

3、通过与短信，或者微信等社交媒体结合，形成灵活的营销模式，有助于银行业务的提升。

综上，通过部署覆盖营业厅的 WIFI 网络，为客户提供免费 WIFI 服务，符合银行业未来发展的大趋势，能有效提升客户满意度，同时通过微信或短信等营销手段增强客户粘性，提升银行业务的竞争力。

除此之前，随着办公笔记本以及其他移动终端的普及，银行工作人员对无线办公的需求也越来越迫切，安全快速的无线办公环境，增加了员工认同感，也提高了员工办公的效率。

2关键点分析

银行营业厅和办公 WIFI 覆盖，需考虑如下几个关键点：

1. 方案合规性：公安部 82 号令规定，凡提供互联网上网服务的单位，需具备技术措施，

能留存实名用户上网行为记录，对应到具体用户，并至少保存六十天记录备份。

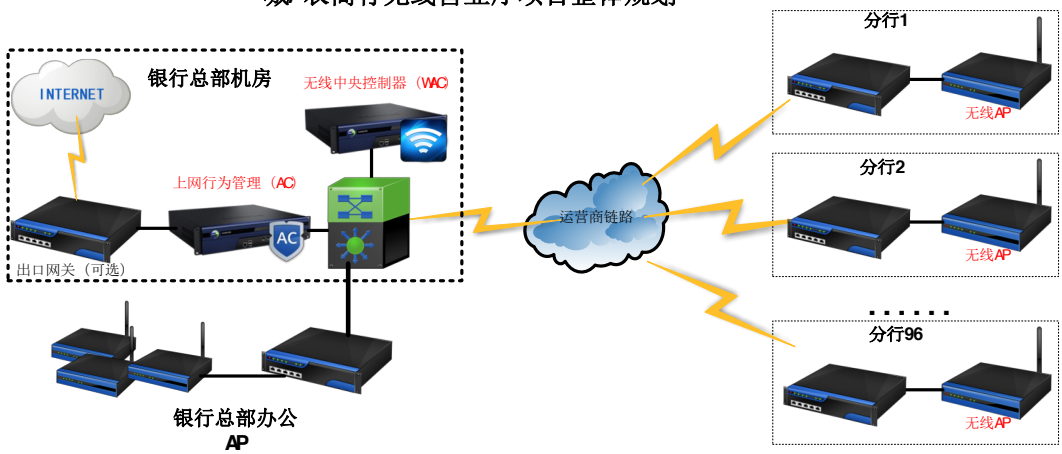
2. 用户体验：WIFI 覆盖区域，需具备足够的用户接入数量冗余度，并有速度保障机制，保证接入用户均能享受到流畅的网络服务。
3. 管理便利性：WIFI 覆盖分布在各营业网点，地理位置分散，而营业网点技术维护力量不足，需要集中管控。而总部办公则需要考虑不同员工的认证和内部权限管理等问题。
4. 广告营销能力：WIFI 网络接入，可收集客户手机号码、或者关注微信公共平台，具备广告推送功能，可给接入用户推送指定广告，推广银行各项增值业务。

3解决方案

3.1组网方案

城/农商行及各营业网点 WIFI 网络 ,可采用 802.11n 技术实现无线局域网覆盖 ,802.11n AP 实现用户的无线接入和数据转发，并通过部署于电信 IDC 机房的无线控制器实现无线 AP 的集中管理和状态监控，另外所有的无线流量经过上网行为设备（AC）做流量控制和审计。

城/ 农商行无线营业厅项目整体规划



部署情况：

1、 营业厅：在每个营业网点的路由下部署一个 AP，使得每一个接入的无线用户路由可达；

2、 总行办公： 部署多个瘦 AP 点，用于员工的办公接入；

3、 总部机房：以网桥的模式部署一台上网行为管理设备，用于对无线用户做上网行为的管理和审计。另外以旁路的模式在交换机处部署一台无线控制器（WAC），用于对营业厅及城/农商行办公的瘦 AP 进行认证和管控，根据不同的位置划分不同的 VLAN，由无线中央

控制器做统一 DHCP。

3.2方案说明如下：

3.2.1互联网接入及 WIFI 覆盖

本方案采用集中部署方式管理和维护各营业网点及总部办公的瘦 AP，对所有营业网点的客户及总部员工的上网需求进行统一网管，瘦 AP 实现无线信号的处理，而用户管理、加密、漫游、AP 管理等功能全部集中到总行的无线控制器上进行。AP 的供电采用以太网交换机供电（Power Over Ethernet，PoE 交换机），通过以太网线来汇聚 AP 的流量，同时为 AP 提供电源，这样可以简化布线，同时减少故障点，提高网络的可靠性。具体规划如下：

1、 营业网点，考虑网络规模及客户流量，按一到两台即可实现 AP 覆盖。

2、 为了便于安全和管理策略的实现 ,客户自带的终端设备接入及电子银行服务器终端设备接入两种场景，需要 AP 至少支持 2 个 SSID，同时两个 SSID 需要采用不同的认证策略、使用时长限制和访问控制策略等。

3、 各营业厅网点，部署无线 AP、POE 交换机，无线 AP 安装在弱电井、吊顶上方等较隐蔽的位置，不影响整体美观，并可通过吸顶式天线增强信号覆盖。POE 交换机用来给无线 AP 供电，避免各营业厅二次布线，影响美观。每个营业厅需要给路由器分配一个固定的 IP 地址，同时路由给终端用户动态分配 IP 地址。

4、总行部署多台瘦 AP，用于总部员工访问互联网，可根据不同的部门设置不同的分组，方便权限的管理；

5、可在总部机房选择性的部署两台无线控制器（双机热备），两台上网行为管理设备（双机热备），从而进一步提高整体网络的稳定性，并通过无线控制器集中配置管理所有营业网点 AP 设备，做到自动下发配置，管理维护简单。上网行为

管理设备用来对所有终端用户的上网行为进行审计 ,对违法、违规网页进行屏蔽等，满足公安部 82 号信令等要求

3.2.2SSID 规划

为了便于安全与管理策略的实现，客户自带设备接入与电子银行服务区终端接入两个场景，使用不同的SSID，请见下表：

场景	SSID名称	广播	加密	终端
分行：客户自带设备接入	CCB	是	否	客户自带终端（笔记本电脑、平板、手机等）
分行：电子银行服务区终端接入	DZYH	否	否	电子银行服务区终端（PC、笔记本电脑、平板）
总行：无线办公	NRCB	是	否	银行需要上互联网的电脑以及员工的移动终端

3.2.3用户认证审计及流量控制

各营业网点部署的，除对营业网点用户提供路由上网功能外，同时需实现如下的网络安全监控和管理功能。

1、手机号码认证准入

营业网点 WIFI 用户暂时限定为客户。用户接入 WIFI 都必须先通过手机短信认证才能使用上网服务。

本方案采用 Web Portal 认证方式对用户进行认证。WIFI 网络强制未认证用户跳转到银行专用认证门户，用户登录成功后，自动跳转到指定的广告页面后，客户方可继续正常访问互联网。

对于客户，采用手机号作为其认证账号，认证密码采用手机动态密码，通过短信发送到认证手机 ;只要是授权使用 WIFI 网络的客户 ,无论其手机号码属于何运营商 ,均可使用 WIFI 网络。另外，可选择性的使用微信认证，只要用户关注了银行的微信公共账号，通过微信账号内的定制化服务链接，就可以连接上无线。

对于总行办公员工，可采用固定用户名/密码的方式接入，也可以采用 IP/MAC 绑定的方式，这样可以保证只有我们允许的终端的才能接入互联网。

3、网页过滤

通过上网行为管理内置的 URL 数据库，对色情、暴力、毒品等各种含有有害内容的网页进行及时有效的识别，并根据管理策略进行记录或者封堵，确保用户访问网站合法合规，规避法律风险。

4、流量识别及控制

对接入 WIFI 用户的上网流量进行精确识别，对 P2P 流量能根据类型进行自动分类，对 bt 等上传下载类流量进行限制，避免此类应用抢占有限的出口带宽，影响其他用户上网体验，同时应能精确识别网页视频、客户端视频等视频流的 P2P 流量，对此类流量提供一定量的带宽保证，保证用户能顺畅的访问视频资源，建议预留 50%带宽通道保障此类应用。此外，需对用户访问银行相关业务网站专门预留通道，确保用户访问城/农商行网站及用户能获取最流畅的访问体验。设备应具备弹性带宽管理功能，在预留带宽应用无流量时，能智能将预留带宽分配给其他应用使用。

5、安全内容审计和过滤

通过设备自带数据中心，对 WIFI 用户的上网行为记录留存完整日志，以符合公安部 82 号令要求。

6、上网时段自动控制，为避免 WIFI 网络被恶意使用，对代理上网功能做时段控制，仅在营业厅工作时段开启免费上网功能，其余时段关闭。开放时段为：早 8:00~晚 7:00。

7、紧急断网及用户访问控制

当出现用户访问互联网不良信息或者制造、传播不当言论等情况时，可以事先通过对安全网关配置的策略，切断此用户或者整个覆盖范围内的互联网接入以进行遏制。可以实现报

警，人工进行断网控制，实现网络自动监控及干预。

3.2.4安全防护

1、钓鱼 AP 的检测

在网点互联网 WIFI 针对钓鱼 AP 等非法 AP 启用检测功能，在发现非法 AP 或冒用 SSID 等情况下，能及时通报。

2.钓鱼 AP 的抑制

一旦发现有钓鱼 AP 等非法 AP，其可以通过发送伪造的解除认证数据包到非法 AP 以及连接在非法 AP 的客户端使其掉线，并能抑制非法 AP 对客户端的接入功能。

3.用户私设 IP 地址控制

用户私设 IP 地址，会造成 IP 地址使用的不可控以及 IP 地址冲突。部署的 WIFI 网络禁止 IP 地址私设行为，只允许通过 DHCP 获得 IP 地址的客户端访问。

4.防 ARP 欺骗功能

ARP 欺骗是最常见的网络攻击，能造成很严重的网络故障，甚至大面积的网络瘫痪。客户端发起 ARP 欺骗的原因有可能为客户端感染 ARP 病毒或者是客户端安装网关软件所致。部署的上网行为管理设备开启防 ARP 欺骗功能，以防止客户端发起的 ARP 欺骗攻击。

5.入侵检测功能

WIFI 所接的客户端类型多种多样，客户端的多样化提高了设备安全管理的难度和复杂度，同时提高了 WIFI 的安全风险。上网行为管理开启入侵检测功能，包括但不限于如下基本攻击入侵检测：蠕虫、间谍软件、广告软件、网络病毒、网络攻击等。

6.禁止用户互访

连接到 WIFI 网络的用户互访，会对用户终端安全造成威胁，造成数据流量的不可控并占用大量带宽，部署的 WIFI 网络支持禁止用户之间的互访功能。

3.2.5广告页面推送

客户接收短信后，在登陆页面（接入认证Portal页面）输入验证码，认证通过后，自动弹出广告页面。客户必须观看完广告后，允许用户正常上网。

另外一种方式就是微信推送，只要关注银行的公共账号，微信平台就会定时推送相应的信息，并长期保留在手机里。