

什么是Captive Portal

大家肯定都连过公共场所的wifi热点，比如麦当劳等地方的。他们的wifi往往一连上去就会弹出一个要求登录或者微信关注之类的页面，只有在这个页面完成操作了才能正常访问网络的。之前看到这个很神奇，为什么一连wifi，手机就会自动打开这个网页的，就知道android系统应该是提供了一些接口的。最近接触到这个，查了一下才知道这个东西叫做“captive portal”，就是专门用来给后端的网关提供鉴权计费之类的服务的。很多公共场合的wifi热点应该都用了这么一个技术，比如酒店，商场，银行等等。

Apple的Captive Network Assistant

1. 发送一个HTTP/1.0的请求到 <http://www.apple.com/library/test/success.html>
2. 接收一个回应，如果回应跟它预计的结果一致，那么认为网络是通的，就不会自动弹出页面。同时，状态栏的WIFI图标出现。流程结束。否则，进入下一步。
3. 如果收到的回应不是它想要的那个，它就认为有CWP存在。
4. 如果有CWP存在，iOS就会自动打开一个页面，在这个页面中再请求一次 <http://www.apple.com/library/test/success.html>，这一次使用的是HTTP/1.1。
5. 然后就可以打开Login页面了。

1.一个通常的认证流程是什么样的，从设备接入到认证前后发生了哪些动作？

具体的实施方式有不只一种，例如：

- Redirection by HTTP (HTTP 重定向)
- ICMP Redirect (ICMP 重定向)
- Redirection by DNS (DNS 重定向)

在设备第一次接入到无线网络的时候，会通过 DHCP 服务获取到一个 IP 地址，可能是公有地址也可能是私有地址。不论分配到的 IP 地址属于公有或者私有，此时客户端都只具备访问指定站点的权限，需要在 Portal 页面上完成认证（确认接受使用条款，验证账号密码等），在 Portal 页面完成认证后，这个系统通常会立即执行一系列的动作包括，重新分配地址（在原本是私有地址时可选），更新这台设备对应的权限控制列表（ACL）中的信息解除访问限制，并开始计时/计费等动作。

当用户需要停止使用这类网络时，通常在 Portal 页面上会提供主动断开的按钮，或者服务器会在一段时间没有检测到该客户端网络流量时将你的设备做下线处理，以保证计费准确并及时释放占用的 IP 地址。

以上就是一台新设备接入到需要 Portal 认证的网络环境中在获得访问互联网权限之前的大致步骤。那在一台设备完成介入后，以后再访问这类网络是否可以不必进行重复的认证就直接接入网络呢？答案当然是肯定的，否则在网络条件不好时无穷无尽的输入账号密码登陆不用强调也知道是一件折磨死人的事情，而这个问题的解决使用了叫做无感知认证的解决方案。关于无感知认证在参考资料中给出了常见的认证方式下实现无感知认证的方案。无感知认证的思想总结起来就是在完成了首次认证后再次接入时会利用已保存的信息进行后台验证，不需要用户主动输入口令进行登陆。不过这并不是我想了解的重点，于是不再继续深入了解。

当时产生这个疑问的时候，是用 iPhone 连接到热点后，系统会弹出一个类似浏览器的窗口，那么这个窗口是怎么弹出来的，触发的条件又是什么呢。根据前面收集到的信息，我使用 Captive Portal iOS 作为关键字在谷歌进行搜索，找到了一些相关的信息，大致介绍了这里面相关的细节。iOS设备所弹出的认证窗口是由 Apple Captive Network Assistant(CNA) 来完成的。大体的流程是当你首先链接到 Wi-Fi 网络后，iOS 设备会从它所属的众多域名下的特定域名选择一个或多个进行访问，例如

- www.appleiphoncell.com
- captive.apple.com

- captive.apple.com
- www.apple.com
- www.itools.info
- www.ibook.info
- www.airport.us
- www.thinkdifferent.us

当域名能够被解析且对特定的网页访问得到正确的响应（通常是 Success ）时，CNA 会判定设备成功的链接到了互联网，比如这个[页面](#)，。如果域名被解析但访问特定页面返回的内容不是预期的结果，那么 CNA 会认为设备所处网络存在Captive Portal，因此会调用一个专门的类似浏览器的页面来发起网络请求并触发 Portal 页面，来引导用户进行登录或者认证。

```
1 GET /library/test/success.html
2 HTTP/1.0
3 Host: www.apple.com
4 User-Agent:CaptiveNetworkSupport/1.0 wispr
5 Connection: close
```

可以看到，在请求特定的页面时，CNA 也使用了一个自定的 User-Agent，这有助于我们识别iOS设备的 Captive Portal 探测请求并选择性的绕过，来实现自定的认证方式

标签: [Captive Portal](#)

posted on 2017-06-21 13:45 [清明-心若淡定](#) 阅读(15155) 评论(2) [编辑](#) [收藏](#) [举报](#)