基于同济大学的 Web 认证方式，给出下列问题的答案

1.web 上网认证系统的基本原理

Web 认证是一种基于端口对用户访问网络的权限进行控制的认证方法，这种认证方式不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行接入认证。未认证用户上网时，接入设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在 Web 认证服务器进行认证，只有认证通过后才可以使用互联网资源。

2.web 上网认证系统的基本基本流程

（1）用户连接到网络后，终端通过 DHCP 由 BAS 做 DHCP-Relay，向 DHCP Server 要 IP 地址（私网或公网）；(也可能由 BAS 直接做 DHCP Server)。

（2）用户获取到地址后，可以通过IE访问网页，BAS为该用户构造对应表项信息（基于端口号、IP），添加用户ACL服务策略（让用户只能访问portal server和一些内部服务器，个别外部服务器如DNS），并将用户访问其他地址的请求强制重定向到强制Web认证服务器进行访问。表现的结果就是用户连接上但不认证的情况下，只能访问指定的页面，浏览指定页面 上的广告、新闻等免费信息。

（3）Portal server向用户提供认证页面，在该页面中，用户输入帐号和口令，并单击"log in"按钮，也可不输入由帐号和口令，直接单击"Log in"按钮；

（4）该按钮启动portal server上的程序，该程序将用户信息（IP地址，帐号和口令）送给网络中心设备BAS；

（5)BAS利用IP地址得到用户的二层地址、物理端口号(如Vlan ID, ADSL PVC ID,PPP session ID)，利用这些信息，对用户的合法性进行检查，如果用户输入了帐号，使用用户输入的帐号和口令到Radius server对用户进行认证，如果用户未输入帐号，则认为用户是固定用户，网络设备利用Vlan ID（或PVC ID）查用户表得到用户的帐号和口令，将帐号送到Radius server进行认证；

（6）Radius Server返回认证结果给BAS；

（7）认证通过后，BAS修改该用户的ACL，用户可以访问外部因特网或特定的网络服务；BAS开始计费。

（8）用户离开网络前，连接到portal server上，单击"断开网络"按钮，系统停止计费，删除用户的ACL和转发信息，限制用户不能访问外部网络；

3.未登录时为什么输入任何网址都会转到登陆页面上？

Web认证的基本概念主要有HTTP拦截、HTTP重定向。

HTTP拦截是指接入设备将原本需要转发的HTTP报文拦截下来，不进行转发。这些HTTP报文是连接在接入设备的端口下的用户所发出的，但目的并不是接入设备本身。如果用户未登录想通过IE浏览器上网，将启动HTTP拦截，这些HTTP请求报文则不能被转发到网关。HTTP拦截之后，接入设备需要将用户的HTTP连接请求转向自己，于是接入设备和用户之间将建立起连接会话。接入设备将利用HTTP重定向功能，将重定向页面推送给用户，用户的浏览器上将弹出设定好的认证页面。

4.itongji-auto为什么登录一次之后能自动登录？

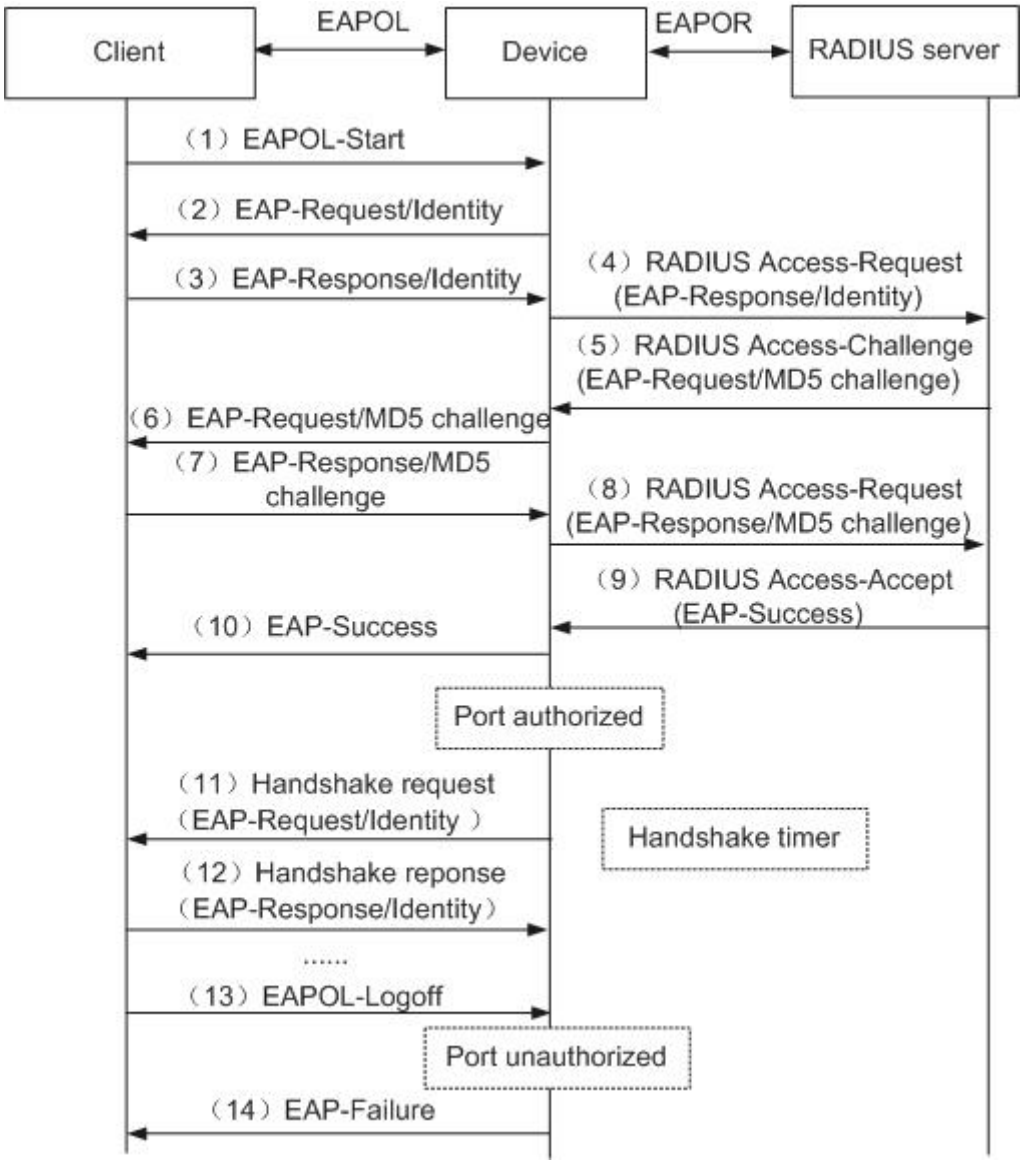
itongji-auto是基于802.1x认证的上网方式。

A.802.x的受控端口/非受控端口：

这种方式在设备端为客户端提供的接入端口被划分为两个逻辑端口：受控端口和非受控端口。“非受控端口”可看成为EAP（可扩展认证协议）端口，不进行认证控制，始终处于双向连通状态，主要用来传递在通过认证前必需的EAPOL协议帧，保证客户端始终能够发出或接收认证报文。

“受控端口”可以看作为普通业务端口，是需要进行认证控制的。它有“授权”和“非授权”两种状态（相当于在该端口上有一个控制开关）：在授权状态下处于双向连通状态（控制开关闭合），可进行正常的业务报文传递；在非授权状态下处于打开状态（控制开关打开），禁止任何业务报文的传递。设备端利用认证服务器对客户端进行认证的结果（Accept或Reject）来实现对受控端口的授权/非授权状态进行控制。

B.EAP中继认证原理：



图a EAP中继认证流程

在EAP中继认证的过程中，设备端起一个中继代理的角色，用于通过EAPOR封装和解封装的过程转发客户端和认证服务器之间的交互报文。整个认证过程是先进行用户名认证，然后再进行对应的密码认证，具体如下（对应图a中的序号）：

（1）当用户访问网络时自动打开802.1x客户端程序，根据提示输入已经在RADIUS服务器中创建的用户名和密码，发起连接请求。因为端口最初的状态是未授权状态，所以此时端口除了IEEE 802.1x协议包外不能接收和发送任何包。此时，客户端程序将向设备端发出认证请求帧（EAPOL-Start），启动认证过程。

（2）设备端在收到客户端的认证请求帧后，将发出一个Identity（标识）类型的EAP请求帧（EAP-Request/Identity），要求用户的客户端程序发送上一步用户所输入的用户名。

（3）客户端程序在收到设备端的Identity请求帧后，将用户名信息通过Identity类型的EAP响应帧（EAP-Response/Identity）发送给设备端，响应设备端发出的请求。

（4）设备端将客户端发送的Identity响应帧中的EAP报文原封不动地使用EAPOR格式封装在RADIUS报文（ RADIUS Access-Request）中，发送给认证服务器进行处理。

（5）RADIUS服务器收到设备端发来的RADIUS报文后从中提取用户名信息后，将该信息与数据库中的用户名列表中对比，找到该用户名对应的密码信息，并用随机生成的一个MD5 Challenge消息对密码进行加密处理，然后将此MD5 Challenge消息同样通过EAPOR格式封装以RADIUS Access-Challenge报文发送给设备端。

（6)设备端在收到来自RADIUS服务器的EAPOR格式的Access-Challenge报文后，通过解封装，将其中的MD5 Challenge消息转发给客户端。

（7）客户端在收到由设备端传来的MD5 Challenge消息后，用该Challenge消息对密码部分进行加密处理，然后生成EAP-Response/MD5 Challenge报文，并发送给设备端。

（8）设备端又将此EAP-Response/MD5 Challenge报文以EAPOR格式封装在RADIUS报文（ RADIUS Access-Request）中发送给RADIUS服务器。

（9）RADIUS服务器将收到的已加密的密码信息后，与第（5）步在本地经过加密运算后的密码信息进行对比，如果相同则认为为合法用户，并向设备端发送认证通过报文（RADIUS Access-Accept）。

（10）设备收到RADIUS Access-Accept报文后，经过EAPOR解封装再以EAP-Success报文向客户端发送，并将端口改为授权状态，允许用户通过端口访问网络。**因此不需要重复登录。**

（11)用户在线期间设备端会通过向客户端定期发送握手报文,对用户的在线情况进行监测。

（12）客户端收到握手报文后向设备发送应答报文，表示用户仍然在线。缺省情况下，若设备端发送的两次握手请求报文都未得到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

（13）客户端可以发送EAPOL-Logoff帧给设备端，主动要求下线。

（14）在设备端收到客户端发来的EAPOL-Logoff帧后，把端口状态从授权状态改变成未授权状态，并向客户端发送EAP-Failure报文，确认对应客户端下线。

5.web/portal认证和802.1x认证的主要区别

（1）IP地址的获得

有时为了避免IP地址冲突，需要采用DHCP服务器动态分配IP地址，普通的交换机在这种应用当中没有问题，用户机器开机后即能从DHCPServer上获得可用的IP。

①在传统的Web / Portal认证中，无论什么用户都可以先获得IP地址，再上网通过客户端认证。Web / Portal方式在认证前就为用户分配了IP地址，对目前网络珍贵的IP地址来说造成了浪费，而且分配IP地址的Web认证服务器对用户而言是完全裸露的，容易造成被恶意攻击，一旦受攻击瘫痪，整网就没法认证。

②802．1x交换机端口启用认证以后，用户开机时(在没有通过认证前)，网络对该用户来讲是不可用的，因此该用户在开机后(认证通过前)不能与DHCP服务器连通，因此该用户得不到可用的IP地址。在通过认证后，发送DHCP Renew报文到DHCP服务器，从而得到可用的IP地址，进而可以使用网络。

（2）认证过程的效率

①Web／Portal认证是基于业务类型的认证，不需要安装其他客户端软件，只需浏览器就能完成，就用户来说较为方便。但是由于Web认证走的是7层协议，从逻辑上来说为了达到网络2层的连接而跑到7层做认证，这首先不符合网络逻辑。其次由于认证走的是7层协议，对设备必然提出更高的要求，增加了建网成本。

②由于802．1x的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，因此，用户的认证与控制由Radius和交换机利用不可控的逻辑端口共同完成，而业务报文则直接承载在正常的2层报文上通过可控端口进行交换，有效地实现了业务与认证的分离。此业务与认证分离的特性是对传统网络认证方式的一种革命性创新，有效解决了传统的PPPOE和Web／Portal认证方式带来的问题。

（3）对异常情况的处理

①由于Web／Portal认证是基于7层的认证,4层以下的网络问题往往检测不到。如断电、突发故障等异常离线情况必须在2层做检测，而Web／Portal对此束手无策。因此Web肌rtal认证用户连接性差，不容易检测用户离线，基于时间的计费较难实现。

②802．1x协议为简单的二层协议，不需要到达三层，解决异常离线情况游刃有余，比较容易实现了基于时间的计费。

（4）认证后上网方案的区别

①Web认证方案中：用户先得IP地址，再认证上网。因此认证前，局域网内是通的，这是不利的。因为大家只要一个人上网，这台电脑装上代理服务器，其他人均可将网关指向代理服务器，靠代理服务器来上网，这样电信运营商就只能收到一个用户的钱了。因此要在交换机上划分VLAN，把每个端口隔开，这样大家就无法实现局域网共享。我们认为高校的宿舍网如建设成这“梳子”模型，将严重压抑同学们的网上交流。将来同学们建设的FTP,Web等交流站点，校园内大家都访问不到。当然，我们可以在三层交换机上做ARP代理实现局域网互通，但这无疑又加重了三层交换机的负担。

②802．1x认证是先认证，后得IP地址。设立了服务区的概念，用户认证到不同的服务区，取得不同的访问权限，能访问不同程度的资源。交换机能识别不同的类别后缀，标识不同的服务区。认证服务器依不同的类别后缀，对各服务区划分不同的VLAN。