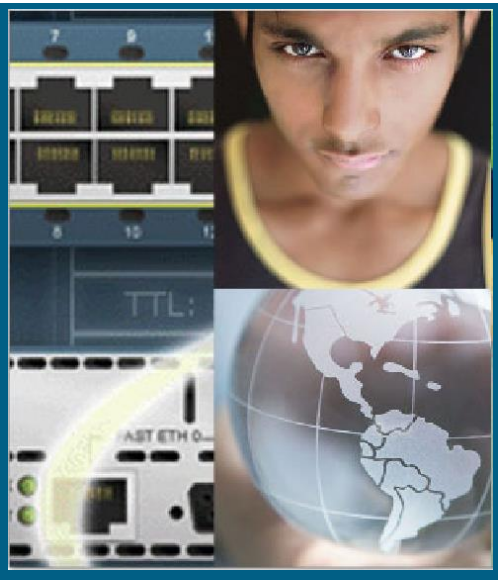
《无线网络应用》第五次课之二

4.03版在线教材 http://ebase.zju.edu.cn/ccna403
(Edge在IE模式下加载打开，要装Flash)

4. 03版 第7章
无线技术：
无线LAN的安全考虑



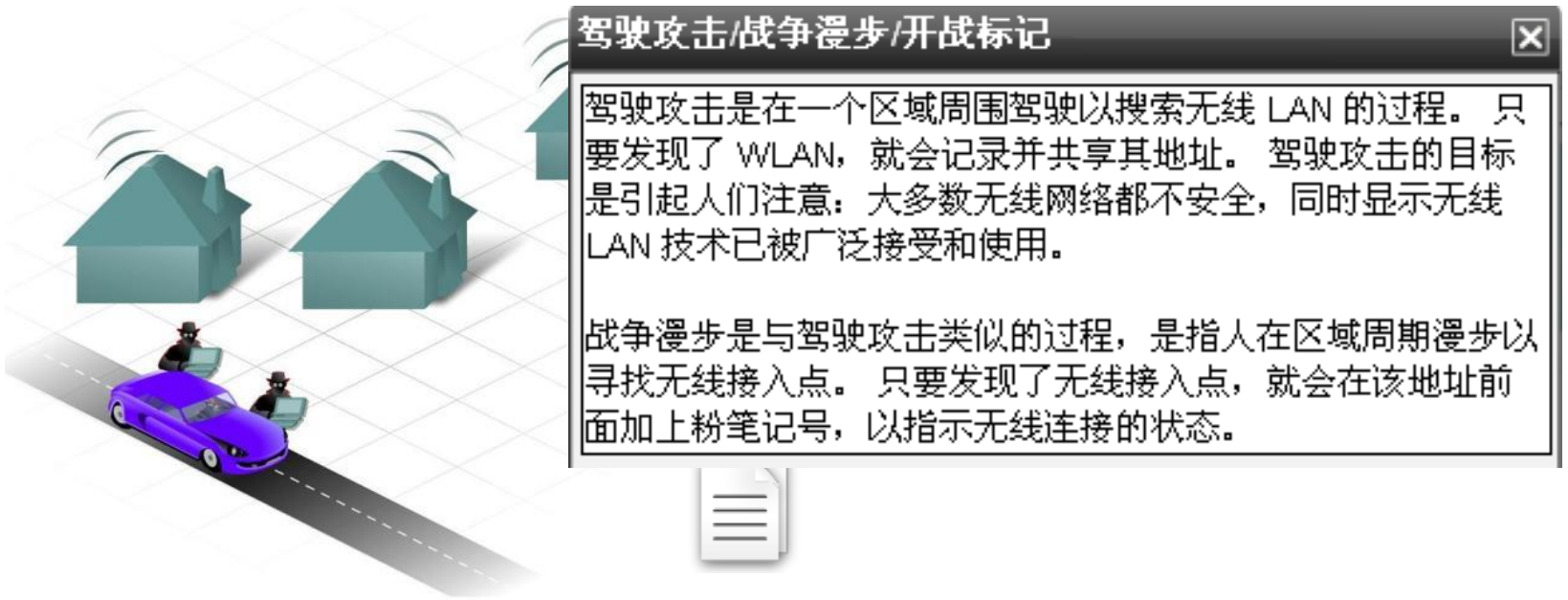
在 4. 03版 第7章 内容基础上 **增加一系列最新进展内容**

特别提示：ITN 7. 02版 期末在线考试不考这些内容！为实验准备！

一、为什么WLAN容易受到攻击

- 无线网络的一个主要优点是连接设备非常简便。
- 信息通过空间传输，容易遭受拦截和攻击。
- 攻击者可以从用户无线信号能抵达的任何地点访问其网络。*查找“开放式”网络，使用它们来自由免费接入Internet！*

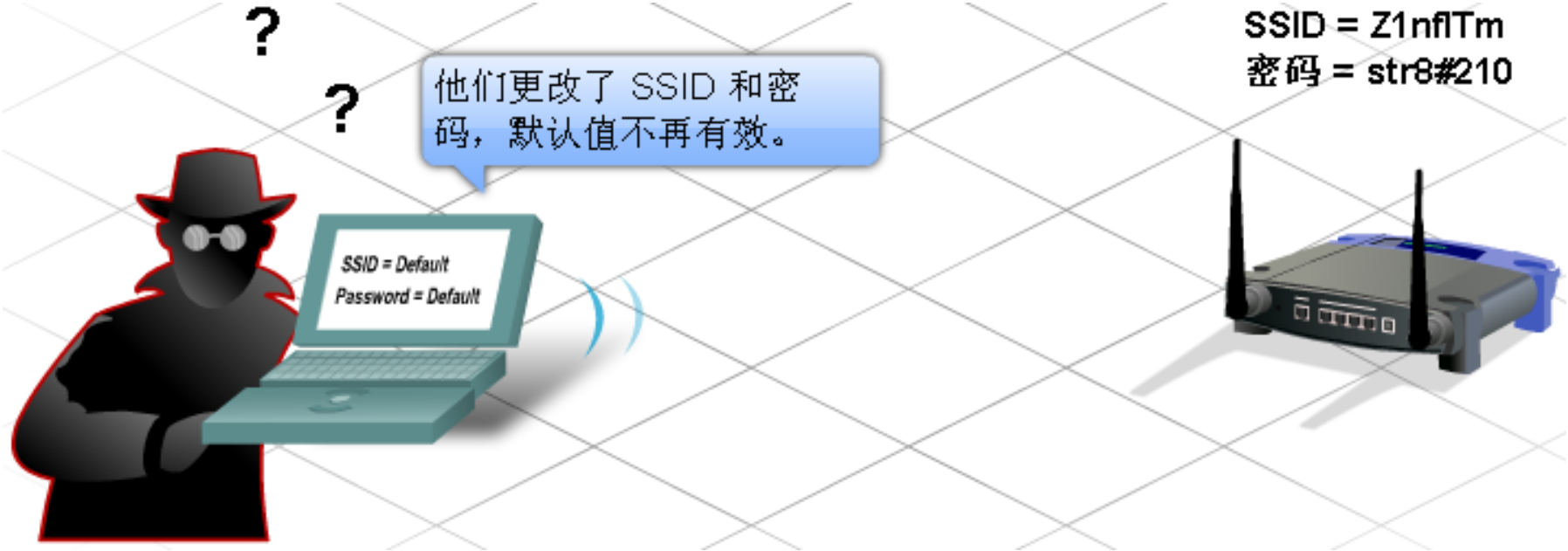
War driving/walking/chalking



二、保护WLAN安全基本措施

- 可以采用的安全防范措施包括：
  - ✓改变默认设置（例如SSID、密码和IP地址）
  - ✓禁用SSID广播功能
  - ✓配置MAC地址过滤

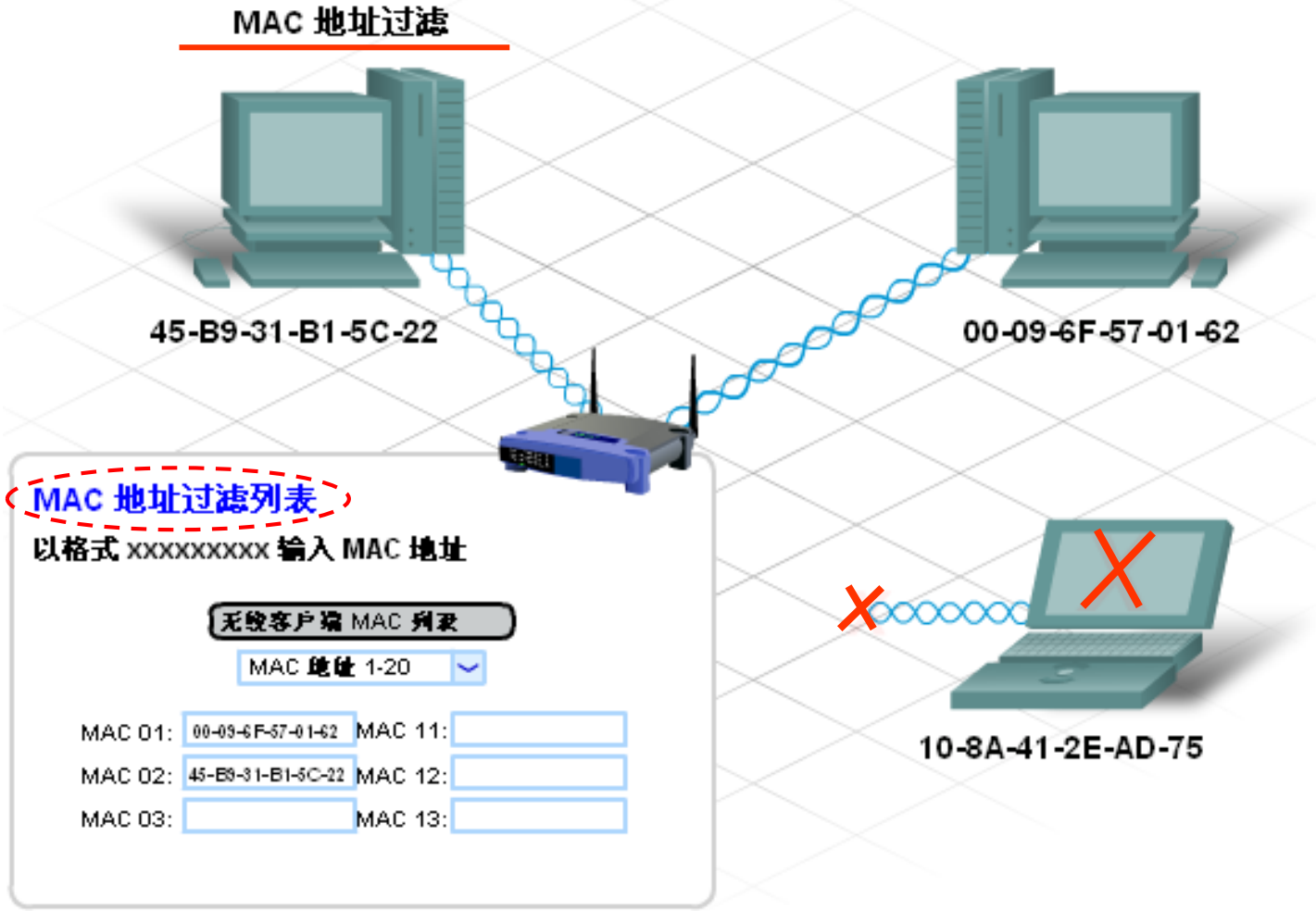
- 改变无线路由器和AP的出厂默认设置至关重要。



但注意，改变默认设置 和 禁用SSID广播功能：

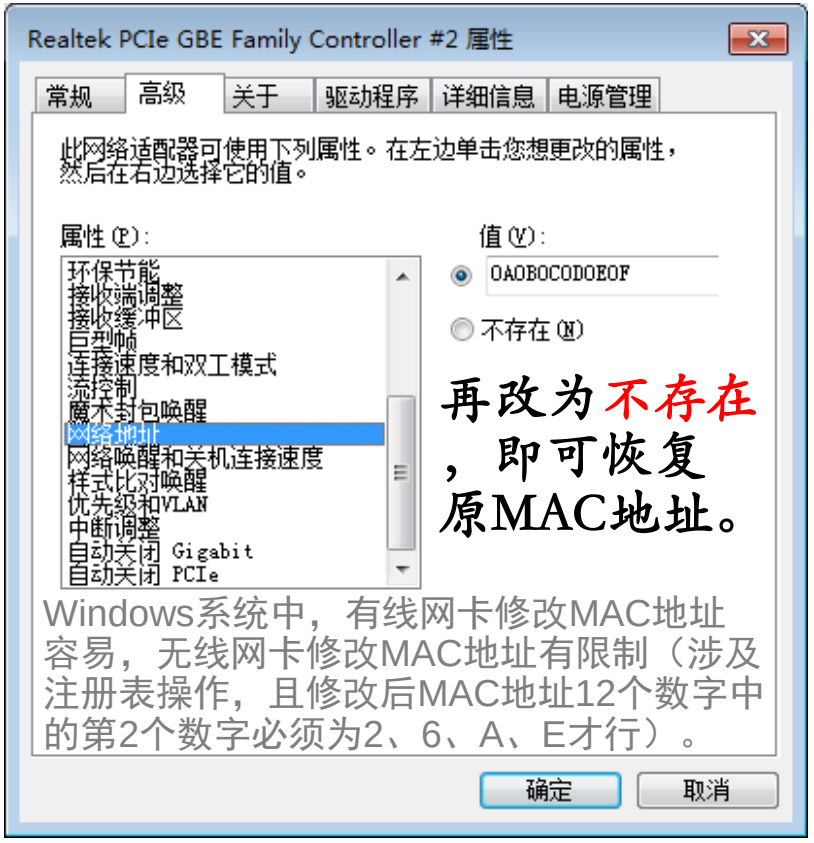
- 这些更改本身无法保护无线网络。由于SSID用明文传输，有些设备或软件能拦截无线信号，读取明文消息。
- 即使更改了默认值并且关闭了SSID广播功能，攻击者也能拦截到正在通信的无线信号，并得知无线网络的SSID名称，然后使用此信息连接到无线网络。

- MAC地址过滤：
  精确控制哪些设备可以访问无线网络。



- MAC地址过滤：精确控制哪些设备可以访问无线网络。
- 但是，这种安全保护方法也存在一些问题：

1. 所有应该访问网络的设备在尝试连接之前，必须先将其MAC地址加入过滤列表数据库中，否则将无法连接。
2. 攻击者也可使用其设备克隆其它具有访问权限的设备的MAC地址。例：网卡→属性→“网络”选项卡→配置→“高级”选项卡→属性→“网络地址”或“Network Address”可修改为欲克隆的其它网卡的MAC地址（“哄骗spoofing”），修改后可用ipconfig /all命令看到效果。



三、WLAN上的身份验证

- 控制谁能连接的另一方法是实施身份验证。身份验证是根据一组证书允许登录网络的过程，验证尝试连接网络的设备是否可信。

- 用户名和密码是最常见的身份验证形式。
- 在无线环境中，身份验证用于确保连接的主机已经过验证。

- 无线身份验证方法有三种：
  - ✓**Open Authentication(开放式身份验证)**
  - ✓PSK(预共享密钥)　　详情参见4.03版教材7.3.3.1
  - ✓EAP(可扩展身份验证协议)

默认情况下，无线设备不要求身份验证，任何身份的客户端均可关联（只要知道SSID），这称为开放式身份验证。

比如我校的ZJUWLAN、ZJUWLAN-NEW（连上后网页身份验证）

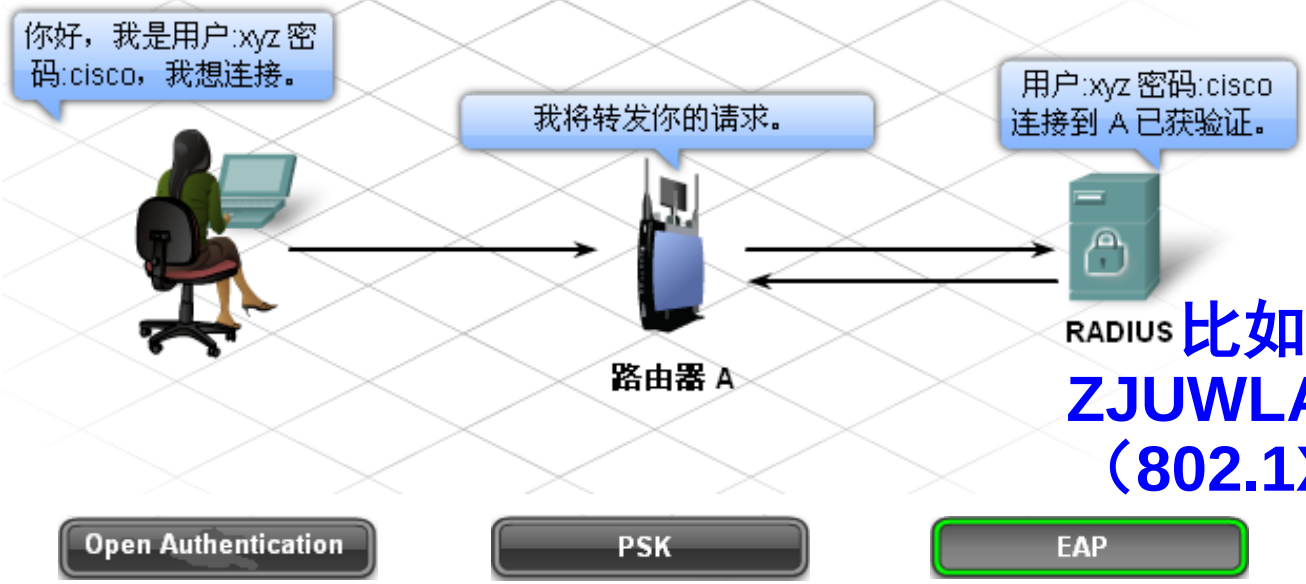
- 无线身份验证方法有三种：
  - ✓Open Authentication(开放式身份验证)
  - ✓**PSK(预共享密钥)**　　详情参见4.03版教材7.3.3.2
  - ✓EAP(可扩展身份验证协议)
  - 使用PSK时，AP和客户端必须配置相同的密钥或密码。
  - PSK执行单向身份验证，即只向AP验证主机身份。

(AP或无线路由器)

比如一般无线热点（只需输入一个密码即可连接）

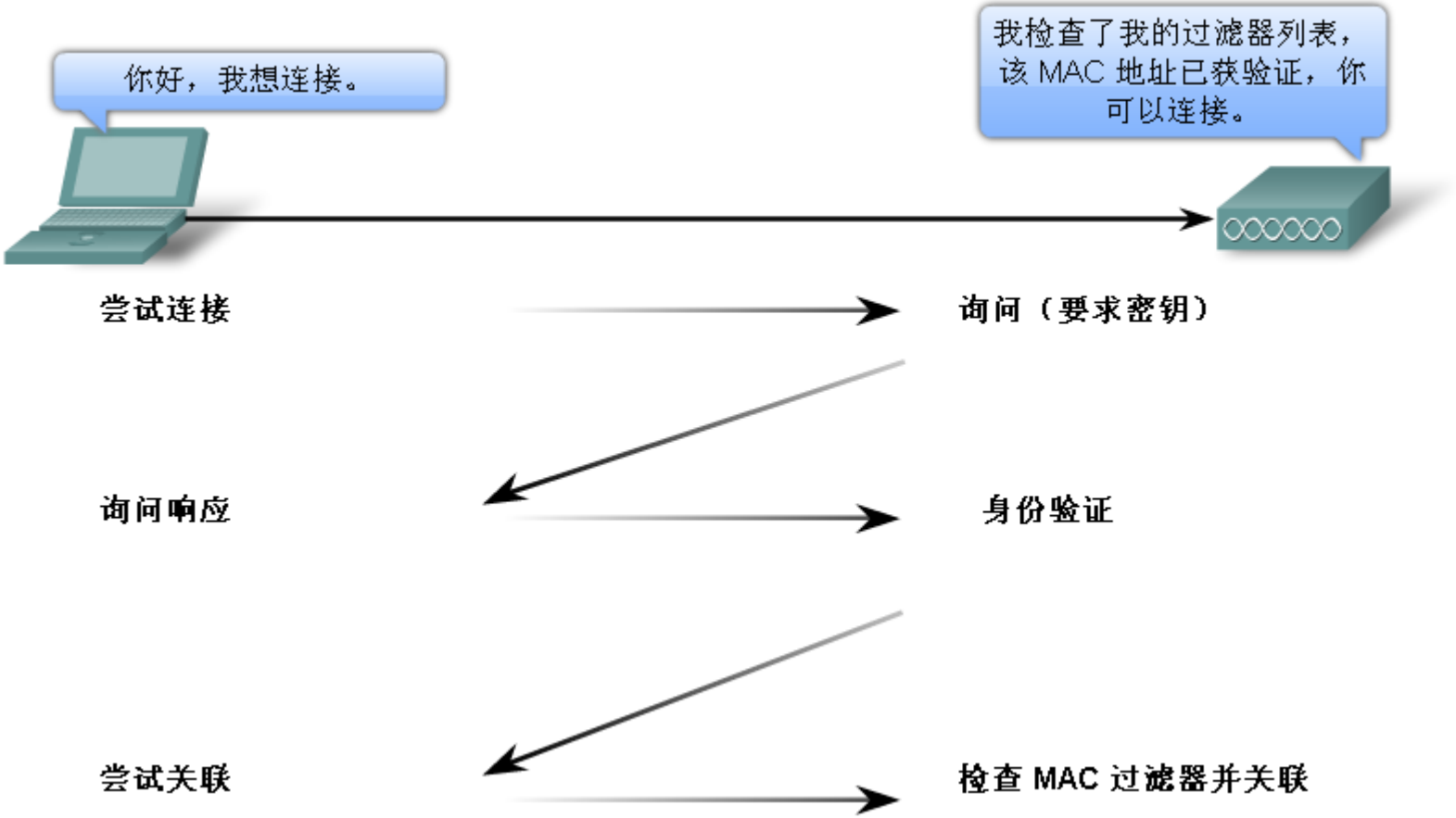
- 无线身份验证方法有三种：
  - ✓Open Authentication(开放式身份验证)
  - ✓PSK(预共享密钥)　　详情参见4.03版教材7.3.3.2
  - ✓**EAP(可扩展身份验证协议)**

• EAP提供双向身份验证及用户身份验证。身份验证工作转交给专业的后端身份验证服务器（如RADIUS服务器）来进行。



比如我校的ZJUWLAN-Secure（802.1X + EAP）

- 如果同时启用了身份验证和MAC地址过滤，则会先进行身份验证，然后再检查MAC地址。



参见4.03版教材动画7.3.3.3

四、WLAN上的加密

- 身份验证和MAC地址过滤可以阻止攻击者连接无线网络，但无法阻止他们拦截在空间中传输的数据。
- 因为无线网络没有单独的边界，并且所有通信量都通过空间传输，所以攻击者很容易拦截或窃听无线帧。
- 而经过加密后，攻击者即使拦截了传输的数据，也无法理解和使用它们。

- WEP(有线等效协议)是一种防范攻击者拦截数据的安全功能，使用预配置的密钥加密和解密通过空间传送的网络通信数据。
- WEP密钥是一个由数字和英文字母组成的字符串，长度为64或128或256位。
- 为使WEP生效，必须为AP或无线路由器以及每台可以访问网络的无线设备都设置输入相同的WEP密钥。若没有此密钥，设备将无法理解无线传输的内容。

参见4.03版教材动画7.3.4.1

安全性差的RC4加密算法

- 但WEP有缺陷。所有启用WEP的设备都用**静态密钥**，而且攻击者现已可用一些软件来破解WEP密钥。

参见4.03版教材动画7.3.4.2

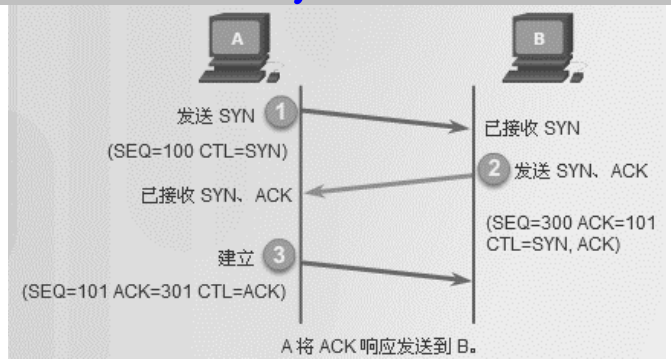
- 填补此漏洞的一种方法是：频繁更改密钥。
- 另一种方法是：使用更高级、更安全的加密：Wi-Fi保护访问(Wi-Fi Protected Access, WPA)。
- WPA也用加密密钥，其长度为64位~256位，但每当客户端与AP或无线路由器建立连接时，WPA都会生成**新的动态随机密钥** 仅供本次连接使用。而且WPA所用的加密算法本身也更强更复杂，因此WPA比WEP更安全，几乎无法破解 (☺) 。

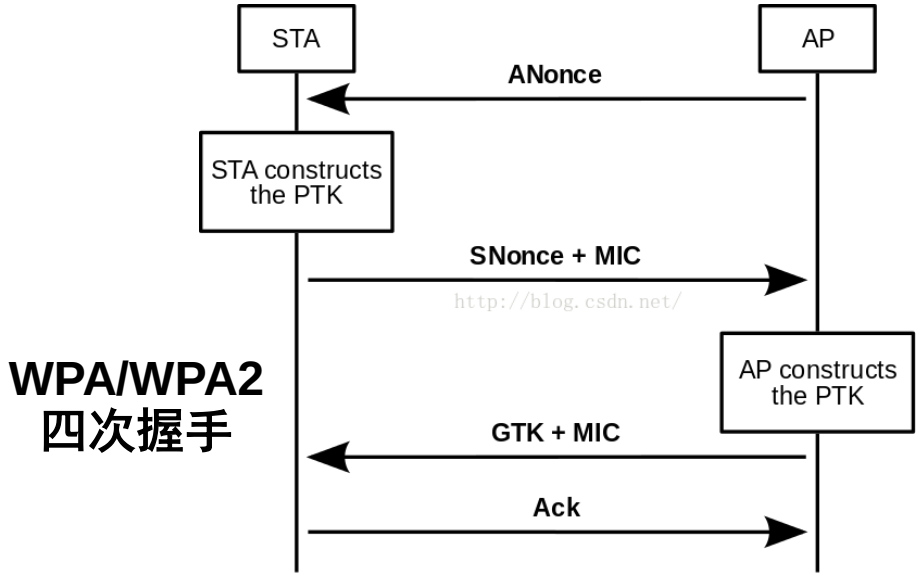
WPA2漏洞新闻

- 171016消息：比利时鲁汶大学Mathy Vanhoef发表报告称，
  他发现已有13年历史的WPA2协议有重大漏洞，利用该漏洞的攻击称为：
  KRACK，Key Reinstallation Attacks，即“密钥重安装攻击”。

- WPA/WPA2协议的工作机制包含一个四次握手（4-Way Handshake）过程，
  是发生在 用户客户端STA 与 无线AP或无线路由器 之间，如右下图（参见备注）。
  当客户端希望加入受保护的无线网络时都会先执行四次握手动作，
  这被用来证实客户端及访问者拥有正确的入网凭证。

➢ 注：7.02版教材模块14传输层14.5.2节
TCP在建立连接的时候有一个类似的
三次握手（3-Way Handshake）过程。





- **WPA2**每次安全加密是使用仅能用一次的动态随机密钥，
  下一次再连、再加入时就不能再用旧的了，就要变成用新的了，
  而这个密钥正是通过四次握手过程来协商完成的。

- 注：最常用的WPA2/PSK安全模式下，一开始输入的密码是身份验证协议PSK的密码，并不是上面说的WPA2动态随机加密密钥！

KRACK攻击者能入侵这个四次握手过程，
操控并重放（Replay回放重播）加密握手信息，
以此诱骗受害者重装已经在使用的密钥。
这样就使得一个曾用过或已在用的旧密钥
也能再次使用、也能成功完成四次握手的验证。

●KRACK攻击过程大致如下（仅供参考）：

1.在被攻击客户端与正常AP建立连接时，黑客克隆这个正常AP，
建立一个SSID相同但信道不同的热点——伪AP（Rogue AP）。

2.然后黑客发送断开连接迫使客户端与正常AP断开，这样客户端尝试重连。

3.在客户端准备与正常AP重连时，黑客发出信息使信道切换到伪AP信道。

4.客户端继续完成四次握手，黑客发送四次握手中的消息3（含旧密钥）
实施KRACK攻击，从而使客户端与伪AP建立正常安全连接并正常通信。

5.黑客实施中间人攻击（参见7.02版16.2.3：威胁发起者会置身于
两个合法实体之间，以便读取或修改双方之间传输的数据），
抓取客户端通过伪AP所发出的非加密数据如HTTP明文数据。

- KRACK攻击主要针对用户无线客户端（电脑、智能手机、平板等）。而对处于默认工作模式的无线AP或路由器并没有影响。但若无线AP或路由器处于类似一般用户客户端角色的桥接、中继、客户端等模式（参见无线AP组网实验），则也能被KRACK攻击。
- 但最重要的是，这一漏洞不会影响采用标准WPA2加密之外的保护方式的信息。即安全的HTTPS网站仍安全（现在大部分网站都已转HTTPS，包括百度、netacad.cn等）。另外，虚拟专用网络（VPN）和SSH通讯等加密连接也是安全的。
- 订阅服务Iron首席技术官Alex Hudson表示，现在“保持冷静”非常重要：“该漏洞所能带来的安全威胁非常有限：因为攻击者必须在受害者附近。所以说，你不是突然间就会被攻击了。另外，很有可能你没那么多单纯依赖WPA2安全性的协议。每次你打开HTTPS网站时，你的浏览器都会和HTTPS的独立的加密层谈判。所以通过WiFi登陆安全HTTPS网站仍然是完全安全的”。回顾：史上最大的漏洞—SSL心脏滴血安全漏洞

➢ 客户端生产商方面的反应：（上述WPA2漏洞于171016公布）

✓ 微软已先知先觉地于171010发布Windows漏洞修复补丁。

✓ 苹果于171017发布iOS的安全更新补丁。

✓ 谷歌的反应慢一拍，于171106为安卓系统发布安全补丁程序。

- ✓ HTTP并非一种安全的协议。对安全HTTP服务的请求将发送到端口443，此类请求需使用https://开头的网址，多用于网上银行、加密用户服务等场合。
- HTTPS的安全基础是SSL(Secure Socket Layer)。

- 140408新闻－HTTPS“心脏滴血”Heartbleed安全漏洞：OpenSSL的协议中，刚刚曝光了一个“毁灭性”的安全漏洞，或暴露某些重量级服务的加密密钥和私有通信。网站服务器请务必立即升级到OpenSSL 1.0.1g。
- 据了解国内大量网站存在该漏洞，网友更称该漏洞为史上最强大的漏洞。网络安全专家建议：2014年4月7日、8日使用过电商和第三方支付平台购物的用户，有必要检查一下自己的账户是否遭到攻击，并及时更改密码。

WPA2漏洞新闻

- 180808消息：研究人员发现一种破坏WPA/WPA2安全协议的新方法。这种攻击手段会危害WPA/WPA2路由器，破解基于“成对主密钥标识符”（PMKID）功能的WiFi密码。在本月早些时候的Hashcat论坛上，安全研究员兼Hashcat密码破解工具开发者Jens Atom Steube公布这一发现，并分享了调查结果。
- 据称，新型攻击方法不依赖于窃取WiFi密码的传统手段。目前流行的方案是等待用户连接到WiFi，在进行四步认证握手时捕获此信息，以暴力使用密码。
- 相反，新技术在单个EAPOL帧的鲁棒安全网络信息元素（RSN IE）上执行。如此一来，攻击不需要常规用户参与任何阶段。收集的信息将以常规的16进制白马字符串进行转换，这意味着没有特殊的转换（或输出格式）可以阻止攻击或导致延迟。如利用该新方法破坏WiFi网络，攻击者或可窃取预共享登录密码、窃听通信、以及执行中间人（MiTTM）攻击。
- 万幸的是，上述攻击手段并不会对最新的WPA3产生影响，因其使用了更加先进的SAE (Simultaneous Authentication of Equals) 密钥建立协议。

破解再见！WPA3 WiFi加密！

- 为解决WPA2被KRACK破解的尴尬，2018年1月8日，WiFi联盟在2018年国际消费电子展(CES)上发布了WiFi新加密协议WPA3。WiFi安全标准WPA2在时隔11年后终于升级。

- WPA3全称WiFi Protected Access 3

  即第三代无线网络安全标准，主要变化有：

  1、128bit升为192bit安全套件

  2、使用新的握手重传方法Dragonfly交握

  (Dragonfly-Handshake) 取代WPA2的四次握手

  3、支持为设备分配不同密钥

- **2018年6月26日，WiFi联盟宣布WPA3协议已最终完成。**

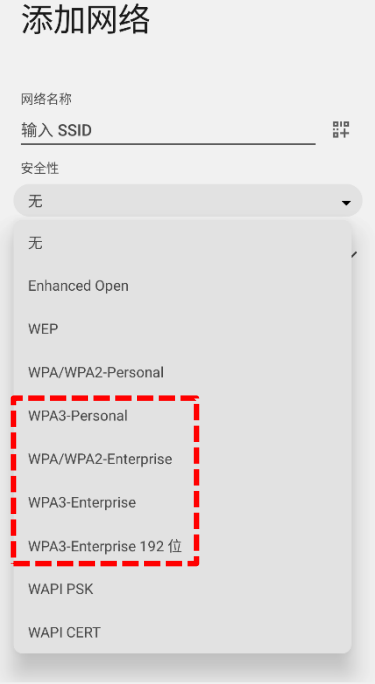
破解再见！WPA3 WiFi加密！

- ✓ 高通旗舰移动平台处理器骁龙845、855、865、870、888、8 Gen 1、8 Gen 2、8 Gen 3支持WPA3
- ✓ iPhone X、11、12、13、14、15支持WPA3（见其 网络安全性选项 ）
- ✓ 支持WPA3的无线路由器：华硕RT-AX88U、网件RAX120、TP-LINK TL-XDR6060等

目前华为WiFi设备均支持WPA3

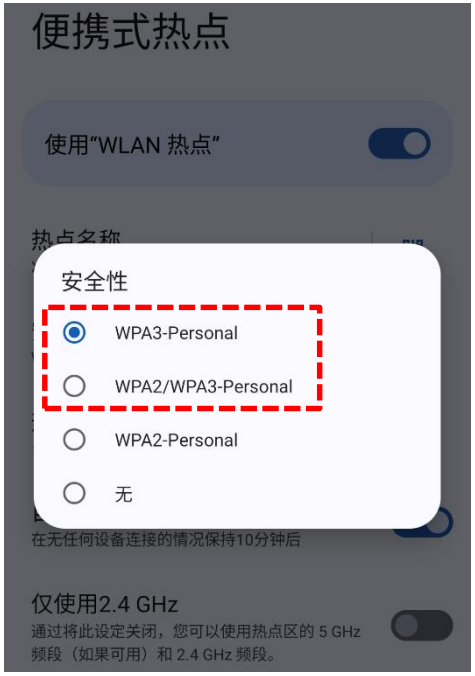
某款基于骁龙8 Gen 2
安卓14系统手机
支持WPA3

网络和互联网→
互联网→
WLAN→
添加网络→
安全性



某款基于骁龙8 Gen 2
安卓14系统手机
支持WPA3

网络和互联网→
热点和网络共享→
便携式热点→
安全性



研究人员揭露WPA3标准多个漏洞

- 190412消息：两位专家本周对外揭露了WPA3的五个漏洞（统称DRAGONBLOOD）。**幸好WPA3尚未普及，WiFi联盟也已及时发布修补程序。**
- WPA3的优点之一是以Dragonfly交握（Dragonfly-Handshake，或称Simultaneous Authentication of Equals）取代了WPA2的四向交握（4-Way Handshake），让黑客更难破解密码。但他们却发现，就算用了WPA3，一定距离内的黑客依然能恢复WiFi密码，继而读取WPA3自以为已经安全加密的讯息。
- WPA3中发现的设计漏洞主要可归类为降级攻击与旁路攻击两种型态，这些漏洞或攻击型态都允许黑客取得WiFi密码，被称为DRAGONBLOOD漏洞。
- **WiFi联盟随后发布了WPA3的安全更新**，并表示：这些问题都可以通过软件更新得到缓解，而不会影响设备的协同工作能力，WiFi产品供应商现在必须通过固件更新将这些更新应用到他们的产品中。
- 190807消息：上述两位专家近期又披露了WPA3另外两个新的漏洞。

小结：WLAN安全的主要里程碑

开放式访问	第一代加密技术	过渡技术	最新技术
SSID	WEP	WPA	802.11i/WPA2/WPA3
• 未加密 • 基本身份验证 • 并非安全之举	• 没有严格的身份认证 • 静态、可破解的密钥 • 不可扩展	• 标准化 • 改进的加密技术 • 基于用户、严格的身份验证（例如 LEAP、PEAP、EAP-FAST）	• AES 加密 • 身份验证：802.1X • 动态密钥管理 • WPA2 是 Wi-Fi 联盟版的 802.11i

WAPI：中国自主知识产权的WLAN安全协议，优于WEP。

TP-LINK无线路由器和无线AP一般支持三种安全模式(身份验证+加密)：

- **WEP**（RC4加密算法、开放式或PSK身份验证；密钥既用于身份验证又用于加密）
- **WPA/WPA2**（TKIP/AES加密协议、802.1X EAP (Radius)身份验证）
- ✓ **WPA-PSK/WPA2-PSK**（TKIP/AES加密协议、PSK身份验证）

WPA2优于WPA！AES优于TKIP！

补充：中国的WAPI协议

Wireless LAN Authentication and Privacy Infrastructure

- **中美博弈：**
  - ✓ 美国千方百计阻挠中国的WAPI成为国际标准
- **知识产权：**
  - ✓ WAPI是中国人自己提出的WLAN安全标准，具有完全的自主知识产权及核心技术，采用的加密算法也是我国具有自主知识产权的国密算法。
- **国家安全：**
  - ✓ “棱镜门”事件暴露美国通过标准监控世界
  - ✓ WAPI双向加密认证 优于 WiFi单向加密认证
  - ✓ 加密算法使用国密算法对国家安全意义重大
- **经济利益：**
  - ✓ 以前我国在高科技产品方面丧失了很多机会，因极少有自主核心技术和自己业界标准的产品而造成了被动局面（如DVD、3G、4G等）。
  - ✓ 近年来我国WAPI产业链持续发展和推进，已颇具厚度，涉及数十亿芯片、移动终端及三大运营商设备，并在电力、金融、教育等行业逐步推广。

补充：中国的WAPI协议

- WAPI，无线局域网WLAN鉴别和保密基础结构，是一种安全协议，是中国无线局域网安全强制性标准，与国际上现行的WiFi 802.11i安全传输协议比较相近（以下“WiFi”均指基于802.11i安全协议的WiFi）。
- WAPI是一种应用于WLAN系统的安全性协议，只是它采用了比WiFi“更高级”的加密方式，而更重要的是，它是我国自主研发的WLAN标准，普遍使用的话可以比WiFi更有利于保护我国的信息安全。
- WAPI是在中国无线局域网国家标准GB15629.11中提出的WLAN安全解决方案。同时，WAPI已在2009年由ISO/IEC授权的机构IEEE Registration Authority（IEEE注册权威机构）审查并获得认可而成为国际标准。

补充：WAPI的缘起和策略

- 3G/4G时代的无线局域网(WLAN)被认为是最炙手可热的市场，中国电信、移动和联通正投入巨资打造“无线城市”战略。不过，这块“蛋糕”的国际标准是英特尔和IBM等大公司所掌握的WiFi，即“IEEE 802.11”，现在其安全标准是802.11i。中国担心若美国人和IEEE在802.11i上留有一手的话，以后不仅会使中国在无线网络信息安全方面受制于人，而且使用WiFi不得不向美国人支付大笔的专利费等费用，从而影响经济利益和国家利益。在2003年中国推出自己的WLAN安全标准WAPI，然后中国就一直努力让WAPI成为国际标准，但道路很坎坷，甚至美国曾不止一次拒绝给中国WAPI提案技术专家赴美参加国际组织会议发放签证。

补充：WAPI的缘起和策略

- 美国人认为“WAPI仅仅是贸易限制的武器”，而中国人真心认为它可以成为一种标准。政府采用了一种“市场扩张从而培育标准竞争力”的策略，要求以手机为主的设备生产商必须用“捆绑”的方式在接受WiFi的同时也接受WAPI，即过去国外行货手机在中国销售是不能带WiFi功能的，以后要带WiFi的话也要有WAPI才行。

补充：WAPI的历史

- 1992年，中国开始无线局域网研究
- 1994年，中国第一台WLAN样机，通过部级鉴定
- 2003年5月，国家强制标准GB 15629.11/1102-2003批准发布，即WAPI
- 2003年11月，质检总局、认监委发布公告，宣布2004年6月1日起对无线局域网产品实施强制性产品认证
- 2004年3月，美国务卿、商务部长和贸易代表联名致信，要求中国放弃WAPI标准
- 2004年4月，国家质检总局、国家认监委、国家标准委联合发布公告：将无限期延期强制实施WAPI标准
- 2004年7月，中国向国际标准化组织ISO提交了WAPI提案，试图推进其成为国际标准，遭到美国方面的强烈阻挠（ISO会议在美举行时，美拒绝给中方WAPI技术人员签证）
- 2006年1月，GB15629.11-2003第1号修改单和2项WLAN扩展子项国家强制性标准颁布
- 2006年3月，在ISO的投票中，WAPI以悬殊的得票率负于美国标准802.11i
- 2006年6月，质检总局、国标委联合发布《关于发布无线局域网国家标准的公告》
- 2008年4月，在ISO/IEC日内瓦会议上，中国第二次启动WAPI提案
- 2009年4月，工信部召集手机厂商开会宣布国内所有行货手机都可使用WAPI技术
- 2009年6月，在ISO/IEC东京会议上，包括美国代表在内的参会成员一致同意，将WAPI作为无线局域网络接入安全机制独立标准形式推进为国际标准
- 截至2019年12月，全球支持WAPI的WLAN芯片达500多个型号、出货量超过140亿颗，支持WAPI的移动终端和网络侧设备超过14000款
- 由于WAPI是中国无线局域网安全强制性标准，因此包括iPhone在内的智能手机均已支持WAPI标准（这些手机均同时支持WiFi标准）

补充：WAPI与WiFi的区别

项目		WAPI	IEEE 802.11i（WiFi标准）
鉴别	鉴别机制	双向鉴别（AP和移动终端MT即Mobile Terminal通过认证服务器AS即Authenti-cation Server实现相互的身份鉴别）	单向和双向鉴别（MT和Radius之间），MT不能够鉴别AP的合法性
	鉴别方法	鉴别过程简单易行；身份凭证为公钥数字证书；无线用户与无线接入点地位对等，不仅实现无线接入点的接入控制，而且保证无线用户接入的安全性；客户端支持多证书，方便用户多处使用，充分保证其漫游功能	鉴别过程较为复杂；用户身份通常为用户名和口令；AP后端的Radius服务器对用户进行认证
	鉴别对象	用户	用户
	密钥管理	全集中（局域网内统一由AS管理）	AP和Radius服务器之间需手工设置共享密钥；AP和MT之间只定义了认证体系结构，不同厂商的具体设计可能不兼容；实现兼容性的成本较高
	安全漏洞	未查明	用户身份凭证简单，易被盗取，且被盗取后可任意使用；共享密钥管理存在安全隐患
加密	密钥	动态（基于用户、基于鉴别、通信过程中动态更新）	动态
	算法	国密办批准的分组加密算法（SMS4）	128 bit AES和128 bit RC4

补充：WAPI与国家安全

- 棱镜门事件暴露美国通过标准监控世界
  - ✓这为各国的网络与信息安全敲响了警钟，各国都开始重新审视WiFi安全性和美国阻击WAPI的真实用心，这也成为WAPI重获新生的机遇。
- WAPI双向加密认证优于WiFi单向加密认证
  - ✓WAPI由于采用了更加合理的双向认证加密技术，因此比802.11更先进、更安全。
  - ✓WAPI从应用模式上分为单点式和集中式两种，可彻底扭转WLAN采用多种安全机制并存且互不兼容的现状，从根本上解决安全问题和兼容性问题。
- 加密算法使用国密算法意义重大
  - ✓WAPI采用国家密码管理委员会办公室批准的公开密钥体制的椭圆曲线密码算法和秘密密钥体制的分组密码算法，实现了设备的身份鉴别、链路验证、访问控制和用户信息在无线传输状态下的加密保护。

补充：WAPI与经济利益

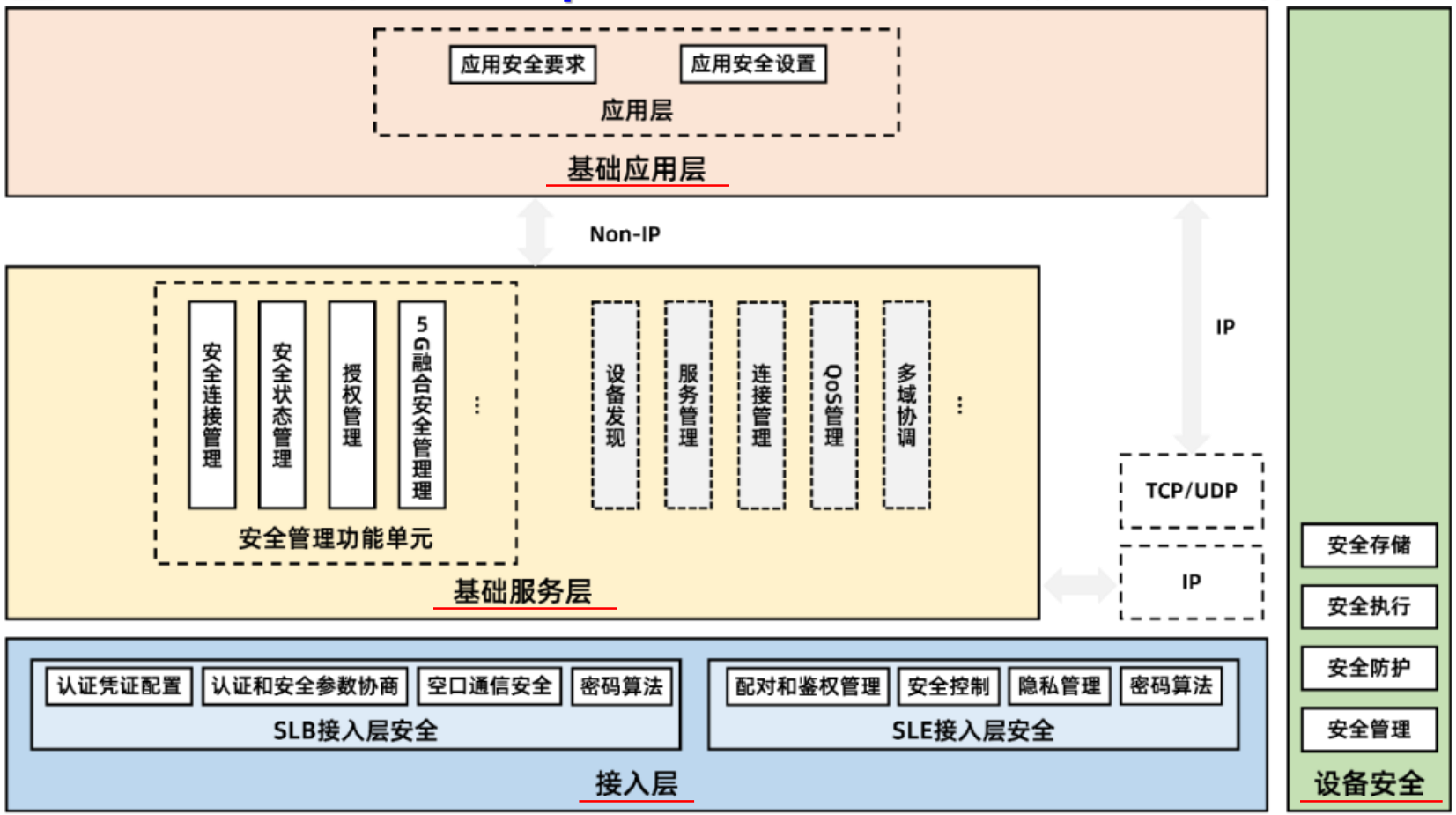
- 我国是个经济蓬勃发展的发展中国家，许多产品都拥有巨大的发展空间，尤其是高科技产品。但是，在以前，我国在高科技产品方面丧失了很多的机会，由于极少有自主核心技术和自己业界标准的产品，造成了颇为被动的局面：DVD要被外国人收取大量的专利费，GPRS、CDMA、3G、4G等很多标准都掌握在外国人手里，我们只能乖乖地将大把的钞票送给人家去买人家的标准，而自己则像个替人“打工”的工人，只能去搞OEM、去帮人组装产品。所以，有人说“一流的企业卖标准、二流的企业卖技术、三流的企业卖产品”。
- 事实上，近年来我国WAPI产业链在持续地发展和推进，已颇具厚度，具有WAPI功能的芯片全球出货量累计已超过40亿颗，移动终端产品型号超过7000款/近6亿部，国内三大电信运营商建设的公共无线局域网络设备均具备WAPI能力，累计约有700万个无线局域网热点，并已在电力、金融、教育等行业逐步推广。

补充：星闪技术的安全性

2023年7月1日，星闪无线短距通信联盟启航峰会，发布了

《星闪无线短距通信技术（SparkLink 1.0）安全白皮书 — 网络安全》

星闪无线通信系统安全架构



星闪不追求单一的安全解决方案实现所谓的一劳永逸，

而是非常严谨地提供了全周期的高安全规格、强认证机制和全面安全防护。

参考链接：解读《星闪安全白皮书——网络安全》

五、WLAN上的通信过滤

- ✓ 通信过滤可以阻止不适当的通信传入或传出无线网络。
- 可删除来自或发往特定IP地址或MAC地址的通信数据。
- 可通过端口号拦截特定应用程序或服务。
  例如，可阻止发往Radius身份验证服务器的所有Telnet（端口号23）通信量，任何想Telnet到身份验证服务器的尝试都被视为可疑通信数据而被拦截。

谢谢。

Cisco Networking Academy

Mind Wide Open