
NETWORKERS


CISCO SYSTEMS

保护802.11无线网络

Session ACC-232

会议内容

- 基本了解 802.11网络的组成部分
- 请在会议结束前保存各种问题

议程

- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

议程

- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

主要的无线市场

- 企业/中型市场
- 教育
- 生产/仓储
- 铁路
- 卫生保健

企业/中型市场

- 职员需要无线服务
- ROI—每天最多可以使生产效率提高70分钟
- 如果没有全面部署无线服务，职员将：

  降低CompUSA公司本地的终端AP

企业/中型市场

- 低劣的部署方法暴露了公司网络
- IT部门应提供并保护 WLAN

教育

- 协作教学应用对学生和教师提供辅助作用
- 不安全的WLAN将会使内容遭受攻击：
  - 学生成绩
  - 管理数据库
  - 专用教学资料

生产/仓储/铁路

- Barcode条码扫描器和POS终端非常普遍
- 许多无线应用只支持静态WEP，或没有任何安全措施！
- 如果连接到公司网络，网络更容易遭受攻击。

卫生保健

- 无线患者管理应用和设备正在普及
- 不安全的部署方法将会使患者病例遭受攻击
  - 符合HIPAA的安全无线LANS就是一种可行的方案

议程

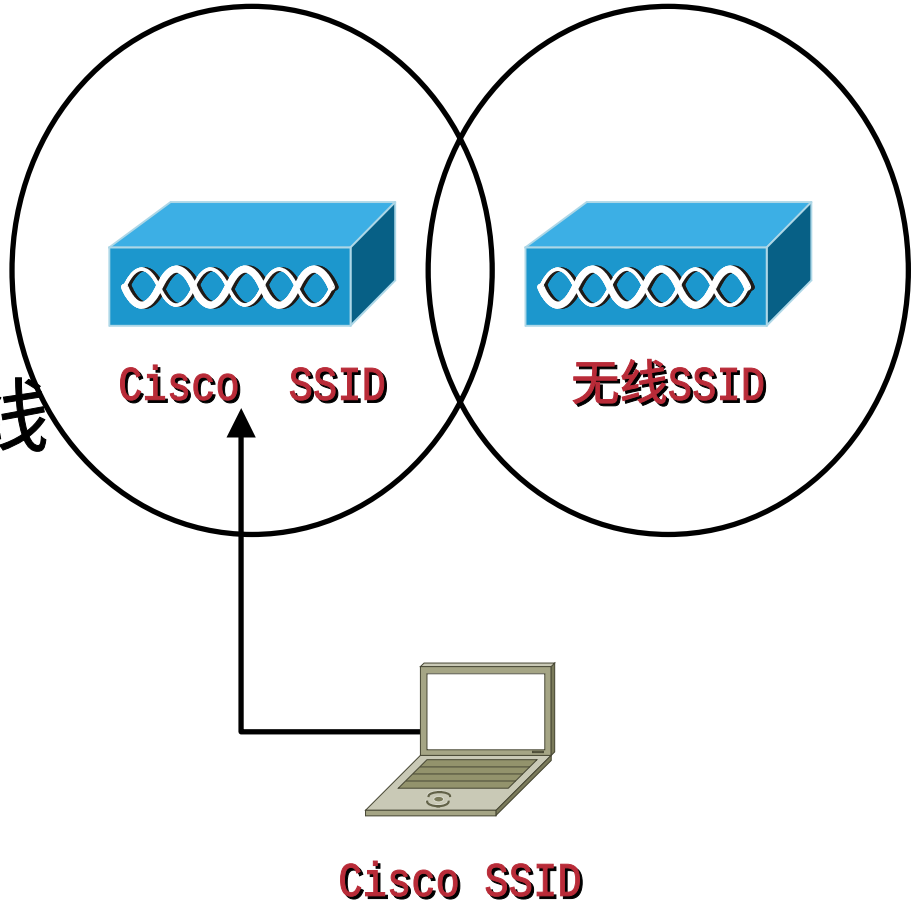
- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

802.11 无线安全性

- 服务集识别符（SSID）
- 有线对等保密（WEP）
- 开放式鉴权
- 共享密钥鉴权
- MAC地址鉴权

服务集识别符（SSID）

- 用于在逻辑上分离无线LAN

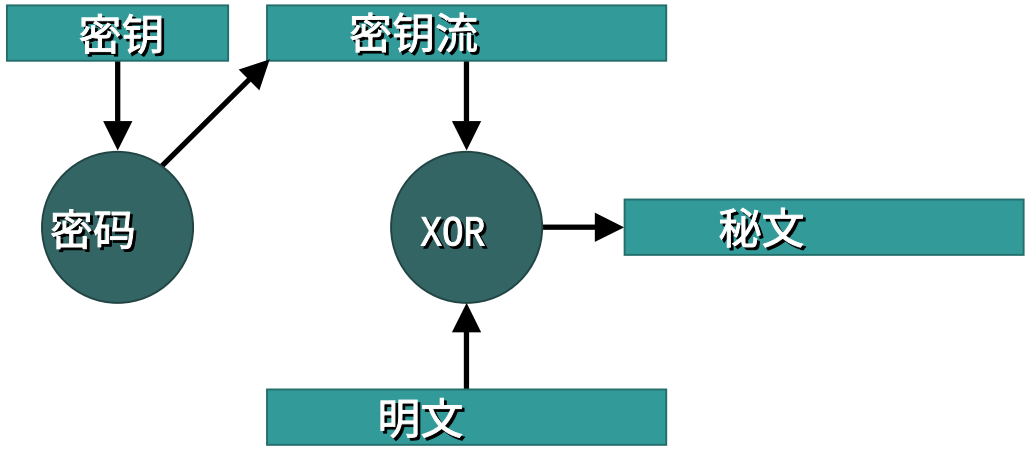


WEP加密

- 有线对等保密
- 基于RC4的对称流密码
- 在客户机和接入点上实施静态、预共享的40位或104位密钥

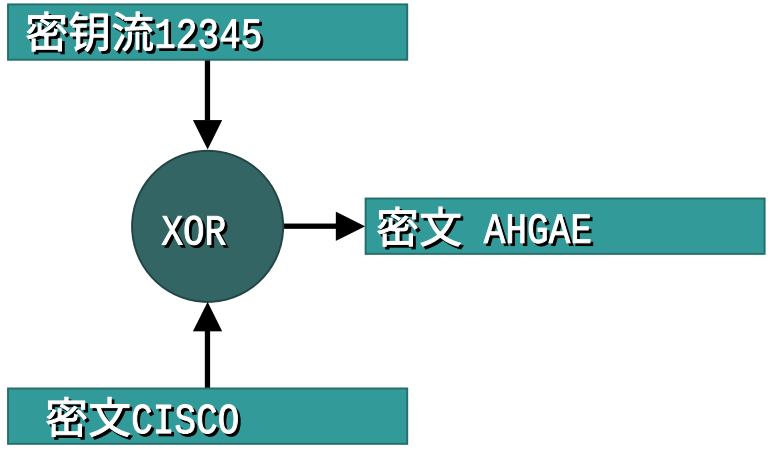
什么式流密码？

- 从密钥生成所需长度的密钥流
- 密钥流和明文数据相混合
- 结果是秘文数据



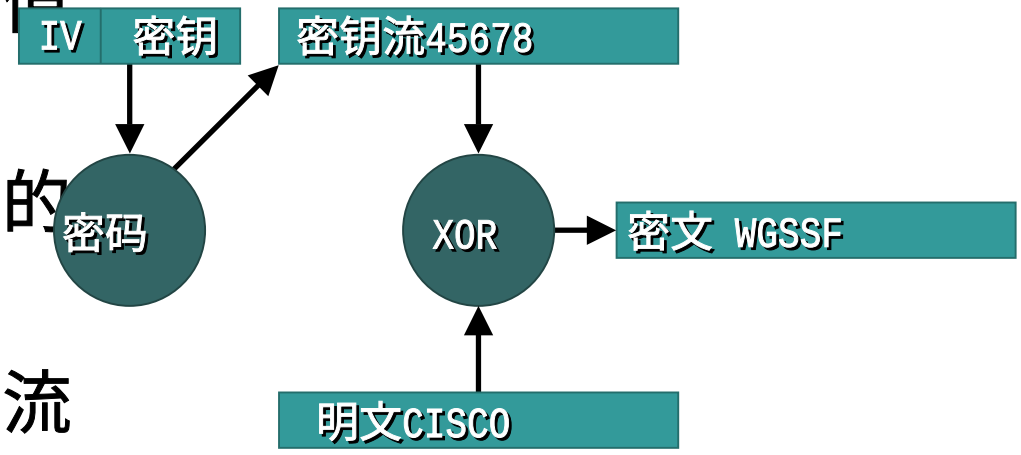
什么是流密码？

- 如果输入相同的数据，密码和数学公式一样输出相同的结果
- 这需要截听者进行“ 富有学问的猜测 ”，流密码以明文通知发生的改变



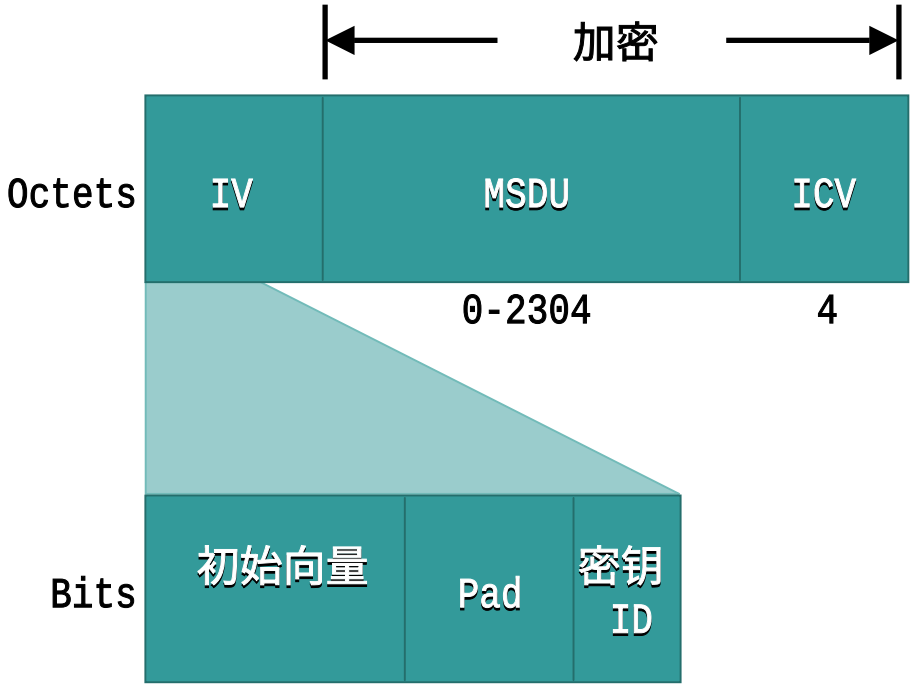
什么是初始向量？

- 初始向量（IV）是向密钥流发出告警的一个值。
- 增加密钥值，生成新的密钥流。
- 随着IV的改变，密钥流也发生改变



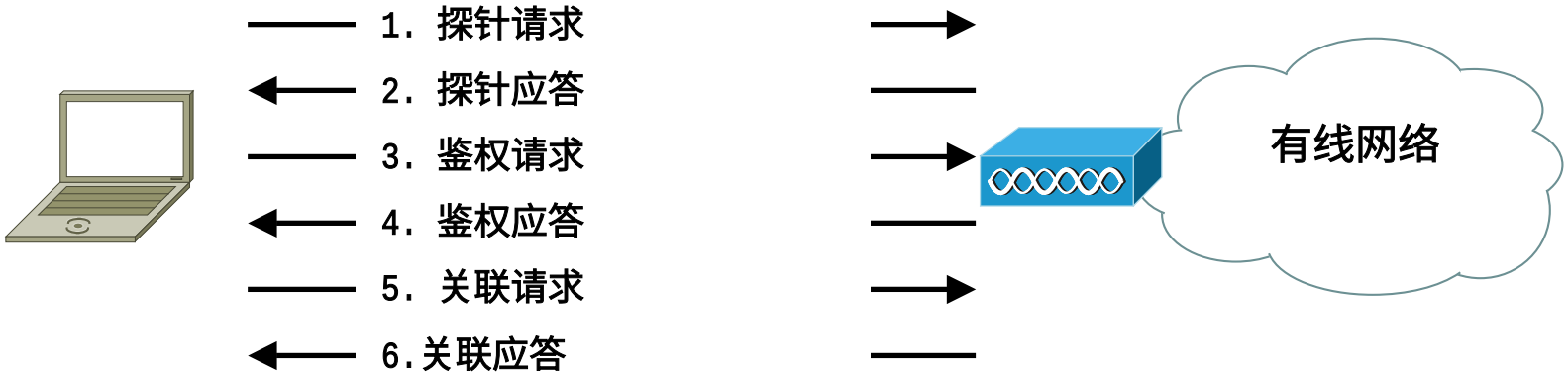
802.11 无线安全性中的IV

- 802.11 IV是 24位的整数值
- 将 40位密钥增加到64位
- 将104位密钥增加到128位
- 明文发送




```
DLC: WEP (Wired Equivalent Privacy) Header
DLC:   Initialization Vector #(1-3)= D200F8
DLC: Initialization Vector #4     = C0
DLC:                        11.. .... = 3 (Key ID 4)
DLC:                        ..00 0000 = Pad
DLC: [68 byte(s) of encrypted MSDU]
DLC: Encrypted Integrity Check Value = F9E3F873
```

802.11 鉴权

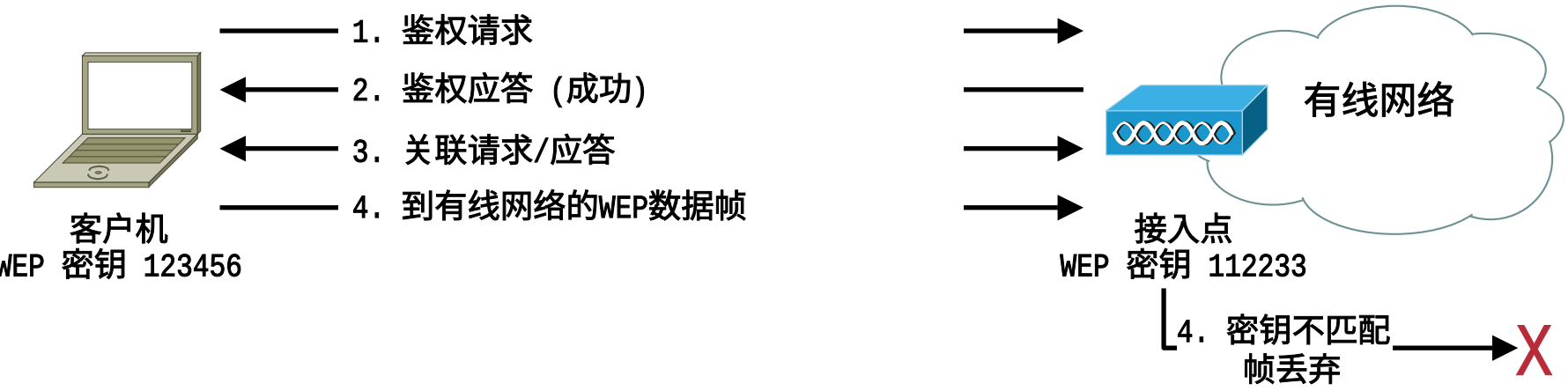


- AP客户机探针
- 客户机请求鉴权
- 客户机请求关联
- 客户机可以开始数据交换

802.11 开放式鉴权

- 面向设备的鉴权
- 不使用鉴权—准许所有请求
- 没有WEP,网络对所有用户开放
- 如果实施了WEP加密， WEP密钥将成为直接鉴权符

802.11 开放式鉴权



- 客户机发送鉴权请求
- AP 发送成功应答
- WEP 密钥匹配数据后才能通过 AP

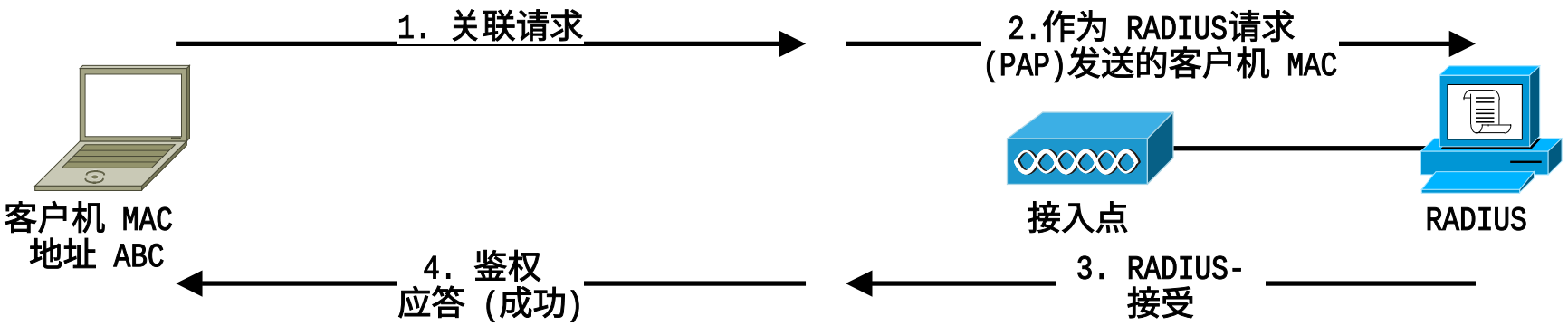
802.11 共享密钥鉴权

- 客户机和 AP必须使用具有预共享密钥的WEP
- 客户机请求共享密钥鉴权
- AP 发送明文挑战
- 客户机以WEP 密钥加密挑战并应答
- 如果AP可以解密应答，客户机有效

802.11 MAC地址鉴权

- 不是802.11规范的一部分
- 根据供应商来实施
- 用于增强开放式或共享密钥鉴权

802.11 MAC地址鉴权



- 客户机请求鉴权
- 客户机请求关联
- AP根据以下内容检查 MAC
  1) 本地许可列表
  2) 转发到AAA服务器
- 接受关联

802.11网络的无线安全性总结

- 鉴权面向设备
- 静态、预共享的WEP加密
- 没有指定密钥管理

议程

- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

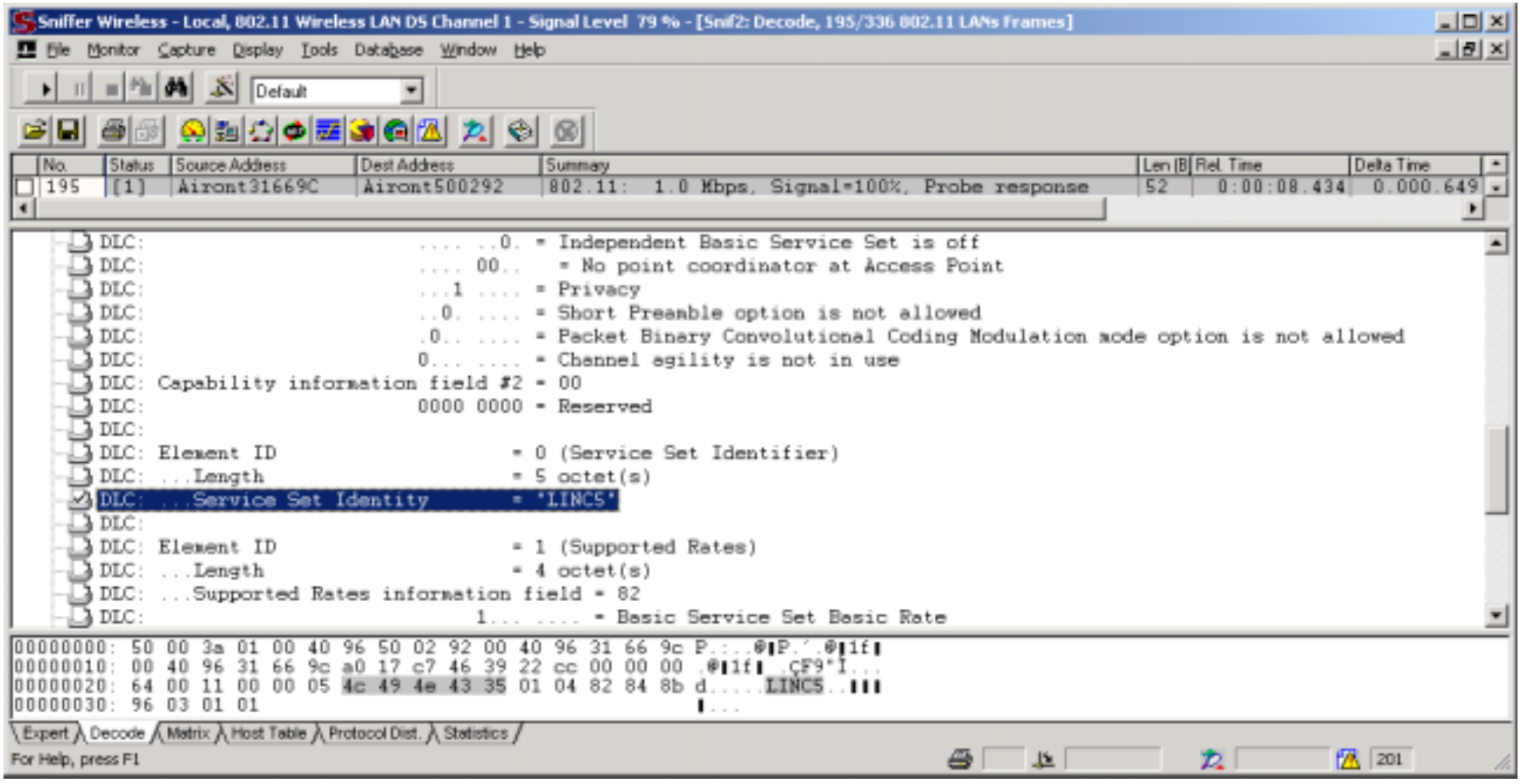
802.11无线安全性中的薄弱环节

- 鉴权薄弱环节
- 派生统计WEP密钥
- 派生感应WEP密钥

鉴权薄弱环节

- SSID 不是一种安全性机制!
- 在Beacons中抑制SSID广播不能防止攻击者的攻击
- 抑制SSID广播可能会影响与 WiFi的符合性

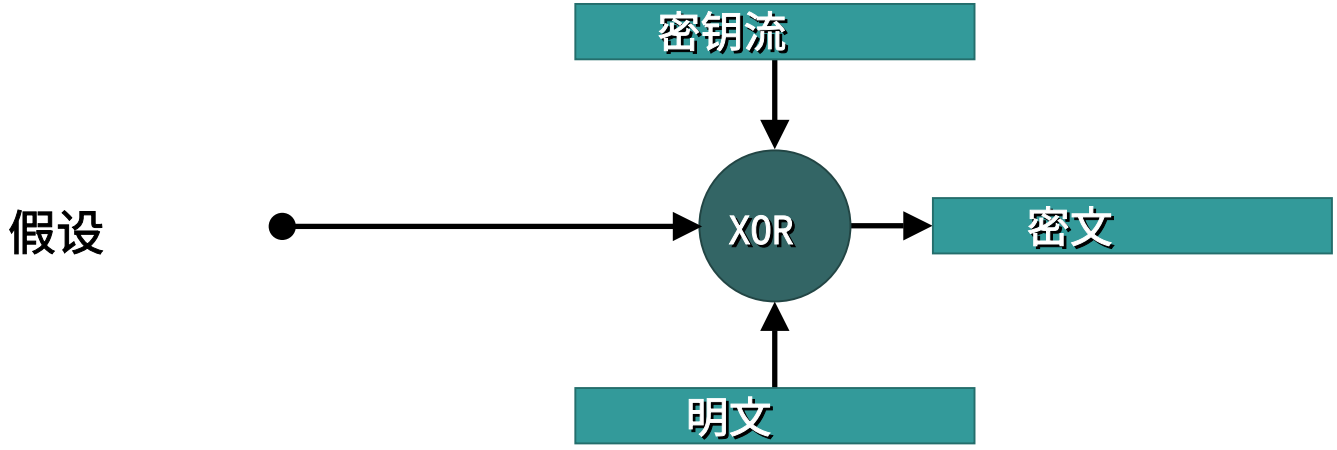
鉴权SSID

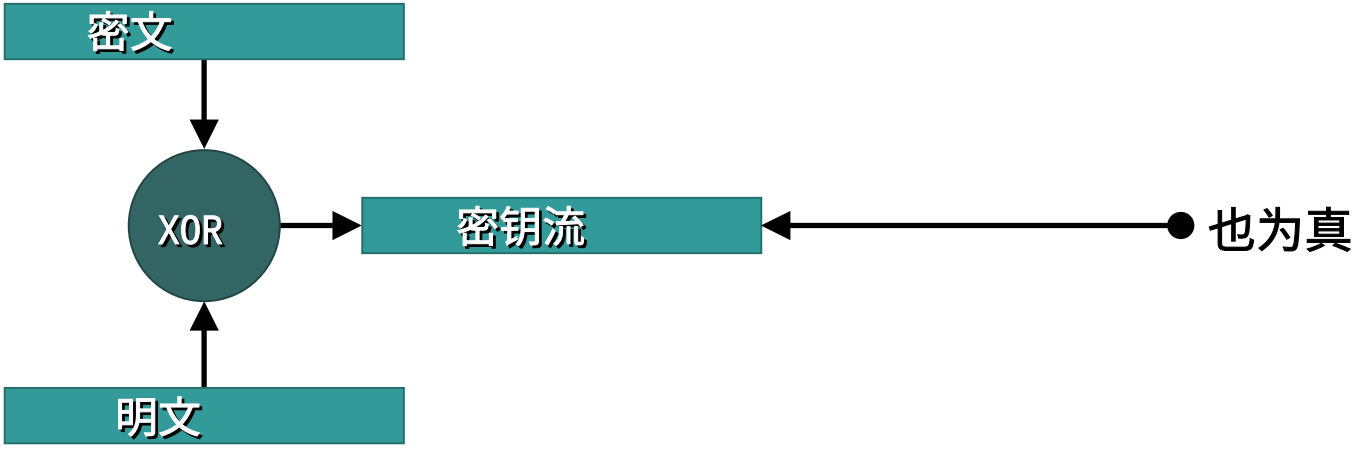

Sniffer Wireless - Local, 802.11 Wireless LAN DS Channel 1 - Signal Level 79 % - [Snif2: Decode, 195/336 802.11 LANs Frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len (B) Rel. Time Delta Time
195 [1] Airont31669C Airont500292 802.11: 1.0 Mbps, Signal=100%, Probe response 52 0:00:08.434 0.000.649
DLC: .... ..0. = Independent Basic Service Set is off
DLC: .... 00.. = No point coordinator at Access Point
DLC: ...1 .... = Privacy
DLC: ..0. .... = Short Preamble option is not allowed
DLC: .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC: 0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC: 0000 0000 = Reserved
DLC:
DLC: Element ID = 0 (Service Set Identifier)
DLC: ...Length = 5 octet(s)
DLC: ...Service Set Identity = "LINC5"
DLC:
DLC: Element ID = 1 (Supported Rates)
DLC: ...Length = 4 octet(s)
DLC: ...Supported Rates information field = 82
DLC: 1... .... = Basic Service Set Basic Rate
00000000: 50 00 3a 01 00 40 96 50 02 92 00 40 96 31 66 9c P.:..@.P...@.1f.
00000010: 00 40 96 31 66 9c a0 17 c7 46 39 22 cc 00 00 00 .@.1f....F9"....
00000020: 64 00 11 00 00 05 4c 49 4e 43 35 01 04 82 84 8b d.....LINC5.....
00000030: 96 03 01 01 ....
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
201

鉴权薄弱环节

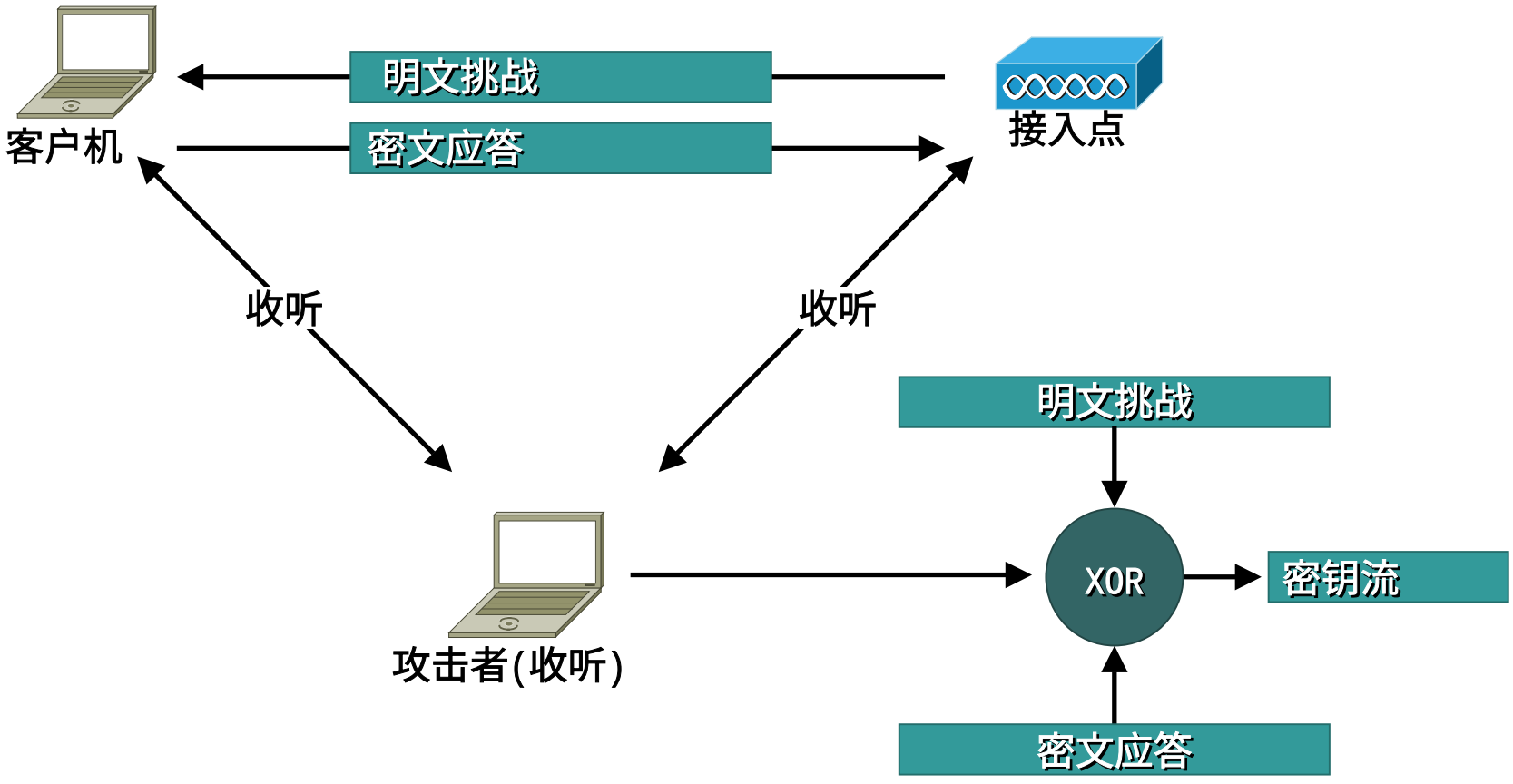
- 无线NIC被鉴权，而不是用户
- 非法用户可以使用合法设备
  - 笔记本电脑丢失或被盗窃
  - 有不满情绪的职员

鉴权薄弱环节





鉴权薄弱环节



- 共享密钥容易遭受中间人的攻击

鉴权薄弱环节

- MAC 鉴权易遭攻击
- MAC 地址以明文发送
- MAC 地址会被盗窃和盗用

派生统计密钥

- 802.11 WEP存在缺陷
- WEP 密钥可以使用统计分析以 1M 到4M 的帧发送
- 攻击者被动“ 收听 ”无线LAN
- AirSnort应用中实施

派生感应密钥

- 攻击者可以从无线LAN中获得信息来派生密钥
- 一般方法

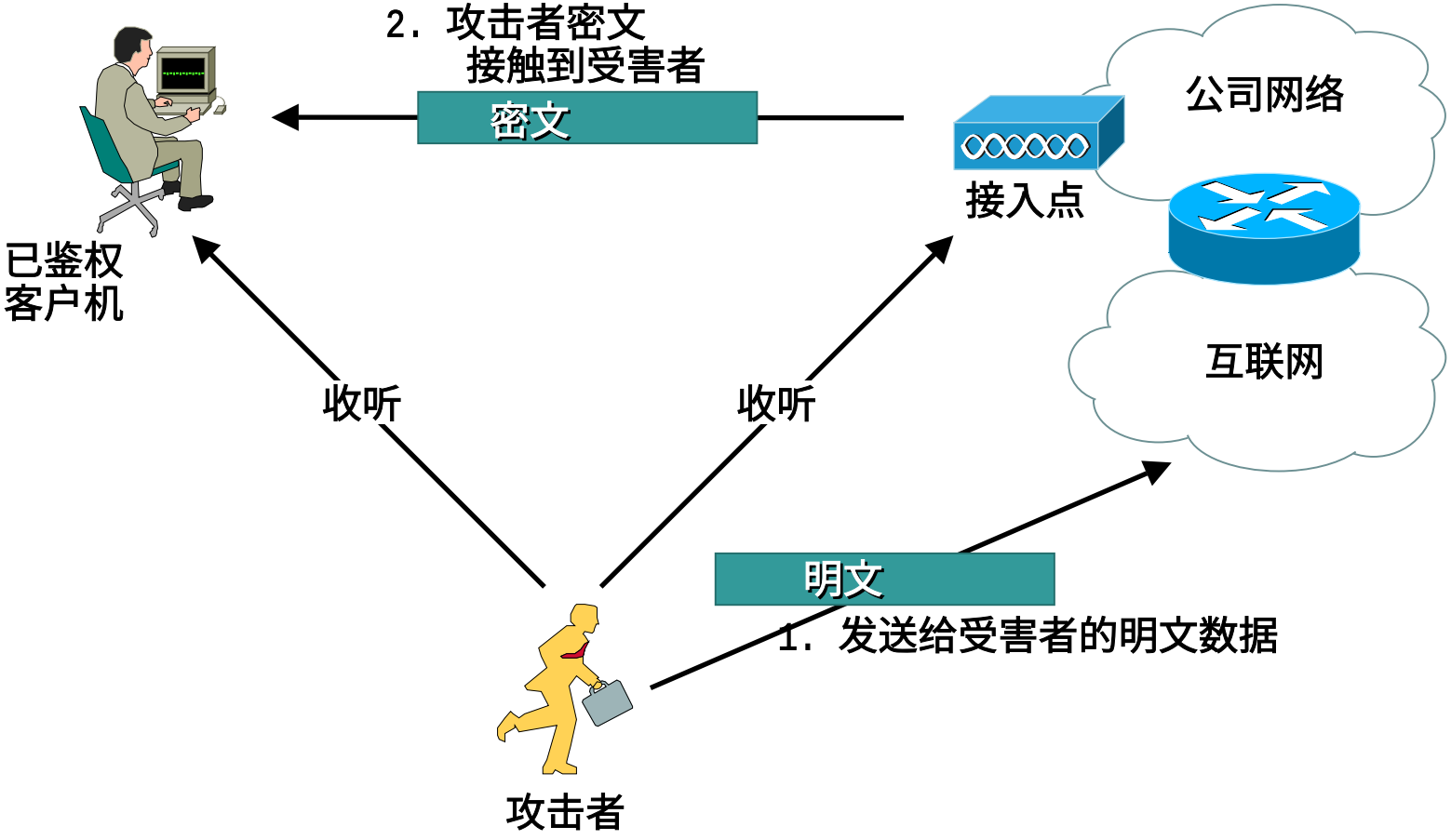
  重新使用IV/WEP 密钥

  帧位反转

IV/WEP 密钥重新使用的薄弱环节

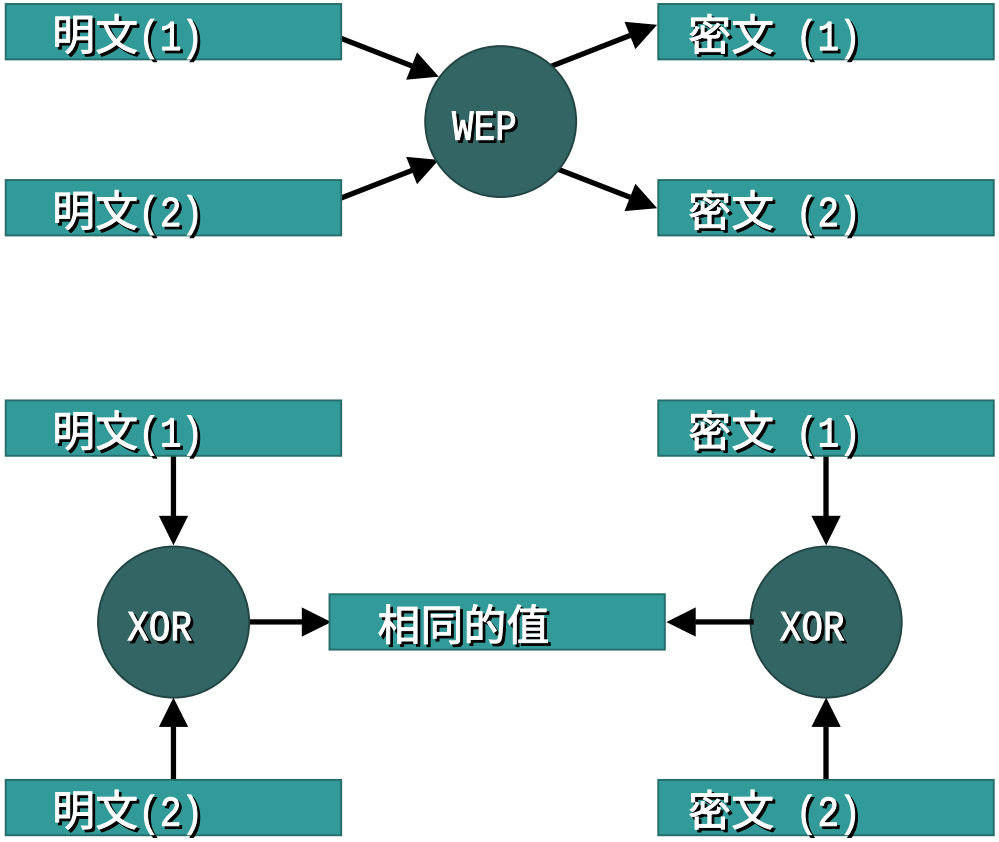
- 攻击者可以向易引起注意的无线客户机发送已知明文（即通过电子邮件。）
- 攻击者将“收听”无线LAN，等待查看预测密文
- 一旦攻击者“看到” 密文，便派生出了密钥流
- 密钥流只对具体IV有效

IV/WEP 密钥重新使用的薄弱环节



IV/WEP 密钥重复使用的薄弱环节

- 两条明文XORed和它们的密文XORed具有相同的输出结果。
- 这样为盗窃者提供了更多的预测明文机会。



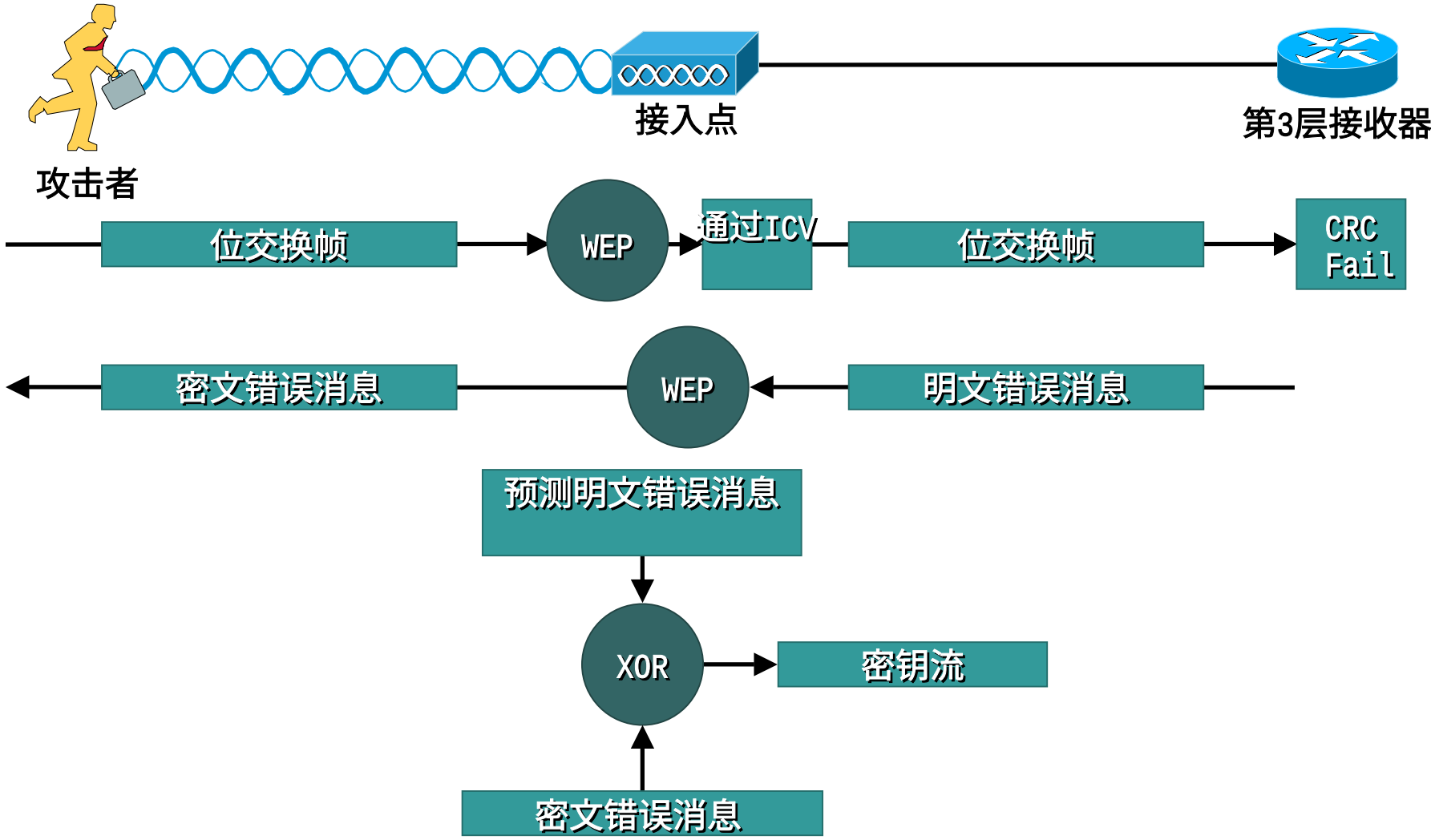
位交换薄弱环节

- 攻击者从无线LAN中捕获帧
- 帧被摇摆位修改
- 攻击者预测更高层的错误
- 攻击者等待预测错误密文
- 密钥流根据“看到”的预测密文来派生

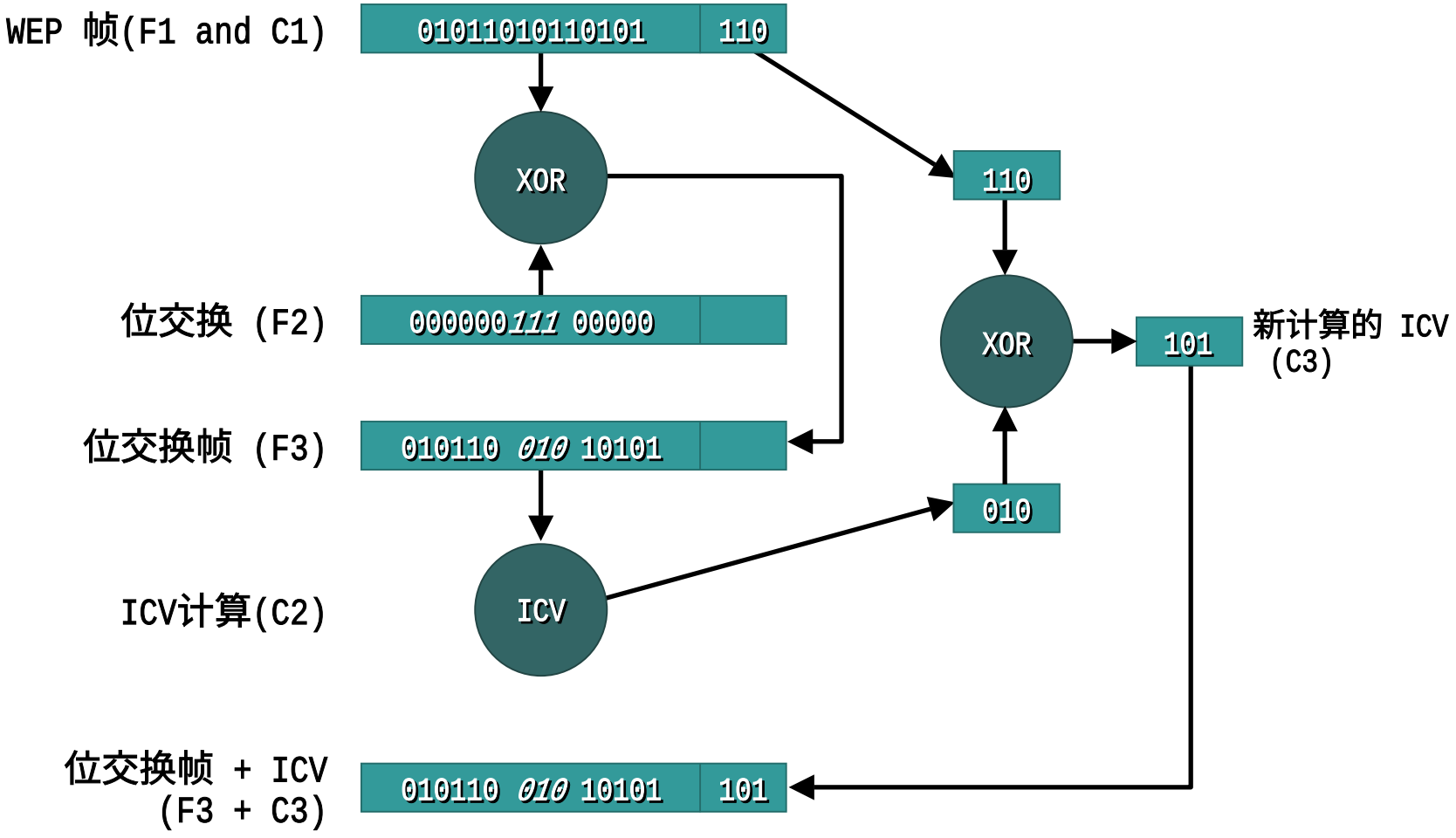
位交换薄弱环节

- 完整性检查值 (ICV)基于 CRC-32多项式
- ICV的已知数学漏洞可以改变加密帧和 ICV
- 由于该漏洞，AP或客户机将该帧接收为有效帧

位交换薄弱环节


攻击者
接入点
第3层接收器
位交换帧
WEP
通过ICV
位交换帧
CRC Fail
密文错误消息
WEP
明文错误消息
预测明文错误消息
XOR
密钥流
密文错误消息

位交换过程


WEP 帧(F1 and C1)
010110101101010 110
XOR
110
位交换 (F2)
000000111 00000
XOR
101
新计算的 ICV
(C3)
位交换帧 (F3)
010110 010 10101
010
ICV计算(C2)
ICV
位交换帧 + ICV
(F3 + C3)
010110 010 10101 101

802.11 安全性总结

- 1997 802.11规范中的安全性机制存在缺陷。
  - 开放式鉴权
  - 共享密钥鉴权
  - WEP
- 这些无法保护您的无线 LAN!!

802.11 安全性总结

- 无线鉴权要求
  - 基于用户、集中式、可靠的鉴权
  - 客户机和网络同时鉴权
- 无线保密性要求
  - 可靠、有效的加密
  - 有效的消息完整性检查
  - 集中式、动态WEP 密钥管理。

议程

- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

安全的无线LAN
客户机考虑因素

- 单一登录
- 可扩展鉴权支持
- 最小的安全性开销

安全的无线LAN
基础设施考虑因素

- 成本
  - 附加服务器硬件
  - 附加网络基础设施
- 快速部署
- 维护和支持
  - 对客户机和基础设施的影响
- 将来的802.11增强
  - 与增强功能的互操作性

保护无线LAN的技术

- VPN
- 具有TKIP加密的802.1X

安全的鉴权要求

- 通过AAA服务器实现的集中式鉴权
- 客户和网络同时鉴权
- 支持动态、基于用户的加密密钥

  改变密钥的可选功能

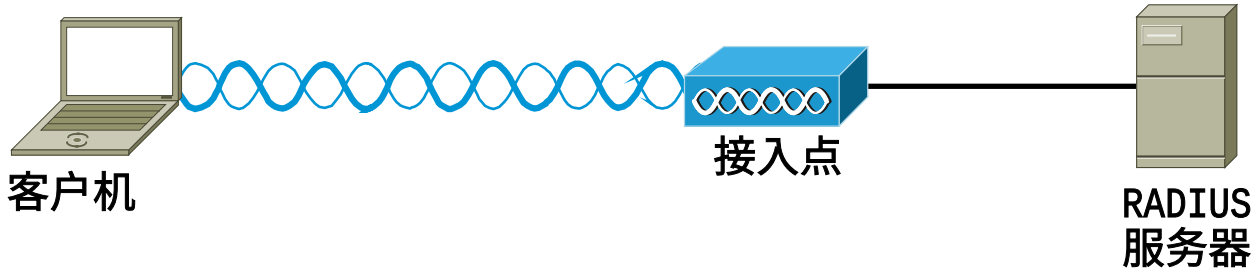
802.11上的VPN

- 两阶段鉴权
  - 通过预共享密钥或PKI实现的设备鉴权
  - 通过AAA服务器实现的用户鉴权
- 相互鉴权
- 可扩展的用户鉴权类型

用于802.11 的802.1X

- 第2层链路支持可扩展鉴权协议（EAP）
- 便于在客户机、 AP和AAA服务器之间进行鉴权的框架
- 可扩展的鉴权算法
  - 基于口令
  - 给予PKI
  - 生物测定
  - 其他...

802.1X 鉴权流程



开始

AP阻塞所有请求，直到
鉴权完成

请求识别符

识别符

识别符

RADIUS 服务器鉴权客户机

客户机 鉴权RADIUS 服务器

成功

成功

EAP 鉴权
无线LAN类型

- EAP-Cisco (aka LEAP)
  基于口令
- EAP-TLS (传输层安全性)
  基于证书
- EAP-PEAP (保护EAP)
  综合—证书/口令
- EAP-TTLS (隧道化TLS)
  综合—证书/口令

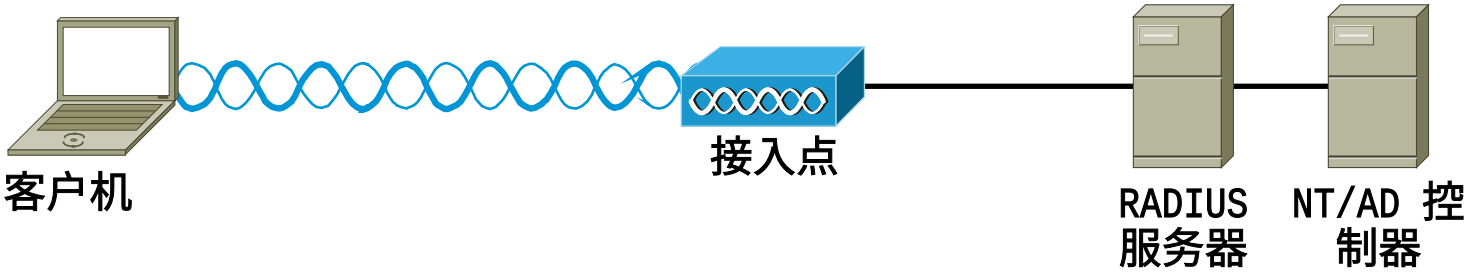
EAP-Cisco 鉴权

- 客户机支持
  - Windows 95-XP
  - Windows CE
  - Macintosh OS 9.X 和 10.X
  - Linux
- 设备支持
  - 工作组桥接 (WGB 340 和 350)
  - 点到点桥接 (BR350系列)

EAP-Cisco 鉴权

- RADIUS 服务器
  - Cisco ACS
  - Cisco AR
  - Funk Steel Belted RADIUS
  - Interlink Merit
- 用于后端鉴权的Microsoft域或 Active Directory (可选)

EAP-Cisco 鉴权



开始

AP阻塞所有请求，直到鉴权完成

请求识别符

识别符

识别符

RADIUS 服务器 鉴权客户机

派生密钥

客户机鉴权RADIUS 服务器

派生密钥

广播密钥

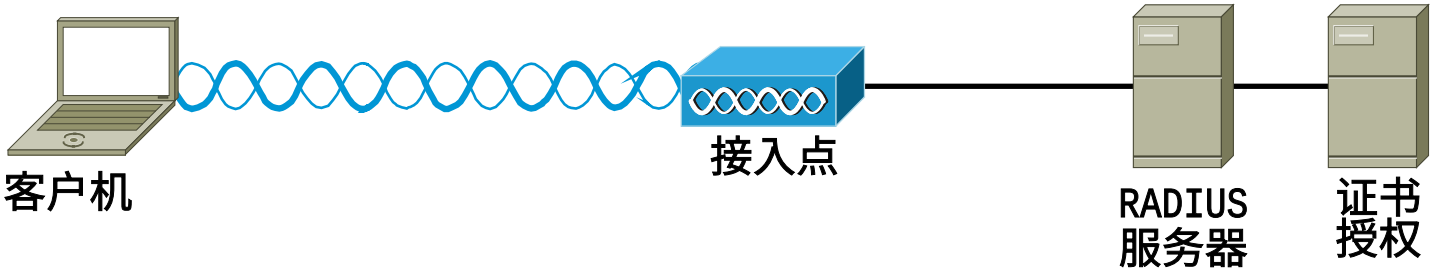
密钥长度

AP发送客户机广播密钥，通过会话密钥加密

EAP-TLS 鉴权

- 客户机支持
  - Windows 2000, XP
  - 客户机要求本地用户或机器证书
- 基础设施要求
  - 支持EAP-TLS的RADIUS 服务器
    - Cisco ACS, Cisco AR, MS IAS
    - RADIUS 服务器要求服务器
  - 证书授权服务器
    - Windows 2000 Server

EAP-TLS 鉴权



开始

AP阻塞所有请求，直到鉴权完成

请求识别符

识别符 识别符

服务器证书 服务器证书

客户机证书 客户机证书

加密 交换

生成随机会话密钥

广播密钥

密钥长度

AP 发送客户机
广播密钥，通过会话密钥加密

综合鉴权

- EAP-TTLS

  服务器端的TLS鉴权

  客户机端通过传统鉴权类型进行的鉴权 (CHAP, PAP等)

- EAP-PEAP

  服务器端的TLS鉴权

  客户机端根据EAP鉴权类型进行的鉴权 (EAP-GTC, EAP-MD5等)

综合鉴权

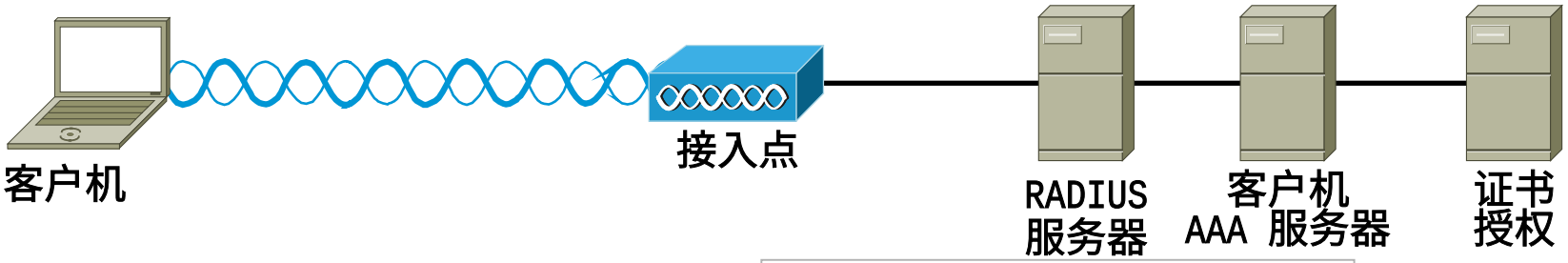
- 两者都要求CA，和 EAP-TLS一样
- 客户机不要求证书

  简化了终端用户/设备的管理
- 允许使用单向鉴权类型

  一个时间口令

  LDAP代理、 Unix、 NT/AD、 Kerberos等

EAP-TLS 鉴权



开始

请求识别符

识别符

识别符

AP阻塞所有请求直到鉴权完成

服务器证书

服务器证书

服务器 端
鉴权

建立加密隧道

传统鉴权

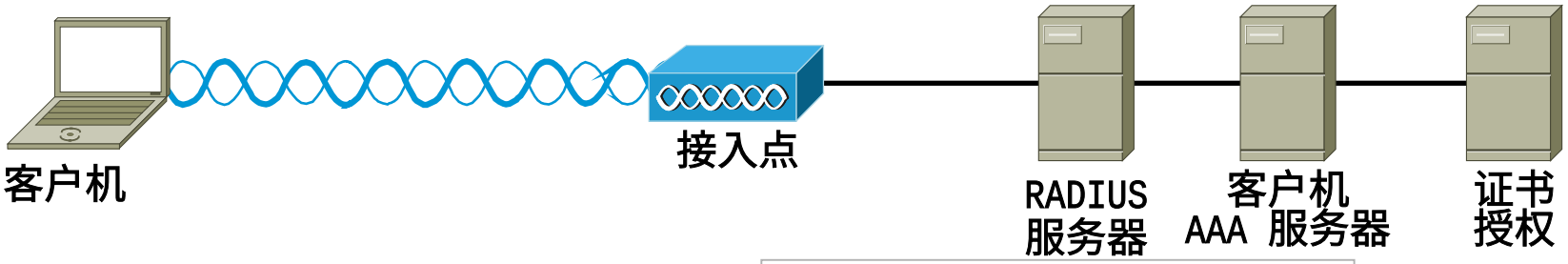
客户机端
鉴权

广播密钥

密钥长度

AP 发送客户机
广播密钥，通过会话密钥加密

EAP-TLS 鉴权



开始

请求识别符

识别符

识别符

AP阻塞所有请求直到鉴权完成

服务器证书

服务器证书

服务器 端
鉴权

建立加密隧道

客户机 端
鉴权

EAP 鉴权中的EAP

广播密钥

密钥长度

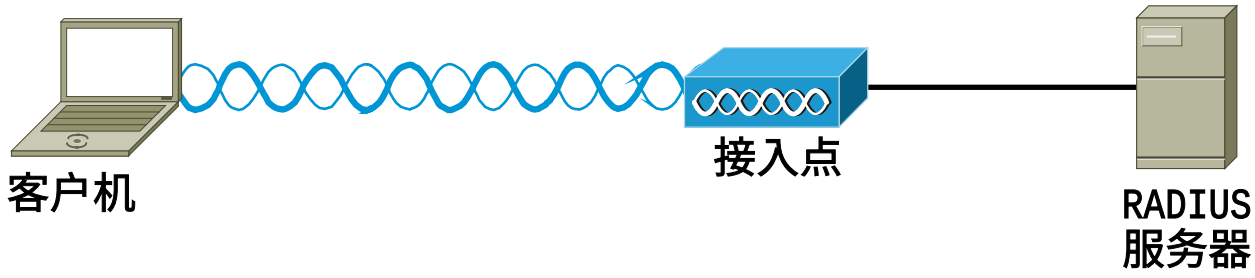
AP 发送客户机
广播密钥，通过会话密钥加密

EAP-MD5 鉴权

- 在WLAN中不使用的一个例子
- 单向鉴权

  网络鉴权客户机
- 不支持动态密钥

EAP-Cisco 鉴权



开始

AP阻塞所有请求，直到鉴权完成。

请求识别符

识别符

识别符

RADIUS 服务器 鉴权客户机

成功

成功

鉴权攻击缓解

	EAP-MD5	EAP-Cisco	EAP-TLS	EAP-TTLS/PEAP	VPN
恶意AP		X	X	X	X
会话攻击		X	X	X	X
中间人攻击		X	X	X	X
目录攻击	X*	X*	X	X	X

X：弥补薄弱缓解

*要求使用可靠的口令

可靠加密的要求

- 正确的加密算法
- 有效的消息完整性

可靠的加密

- TI临时密钥完整性协议（TKIP）
  - 增强WEP加密
  - 每数据包加密
  - 消息完整性检查
- 无线VPN
  - 3DES加密—历经考验的真正加密
  - HMAC-SHA1或HMAC-MD5 消息鉴权

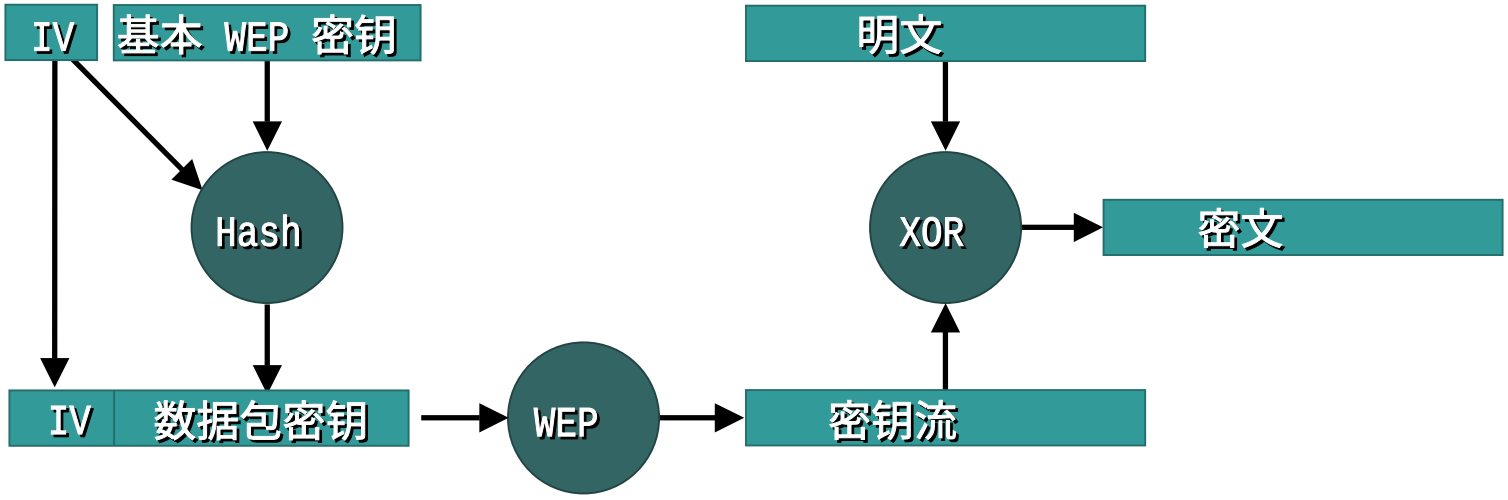
TKIP加密

- Cisco提供预标准实施
- 每数据包加密
- 消息完整性检查
- 广播密钥旋转

每数据包加密操作

- IV 排序—IV逐一递增
- 每个数据包IV都充斥着基本 WEP 密钥
- 结果是生成新的 “ 数据包 ” WEP 密钥
- 数据包WEP 密钥根据 IV改变

每数据包加密操作



- IV排序—IV逐一递增
- 每个数据包IV都充斥着基本 WEP 密钥
- 结果是生成新的“数据包” WEP 密钥
- 数据包WEP 密钥根据IV改变

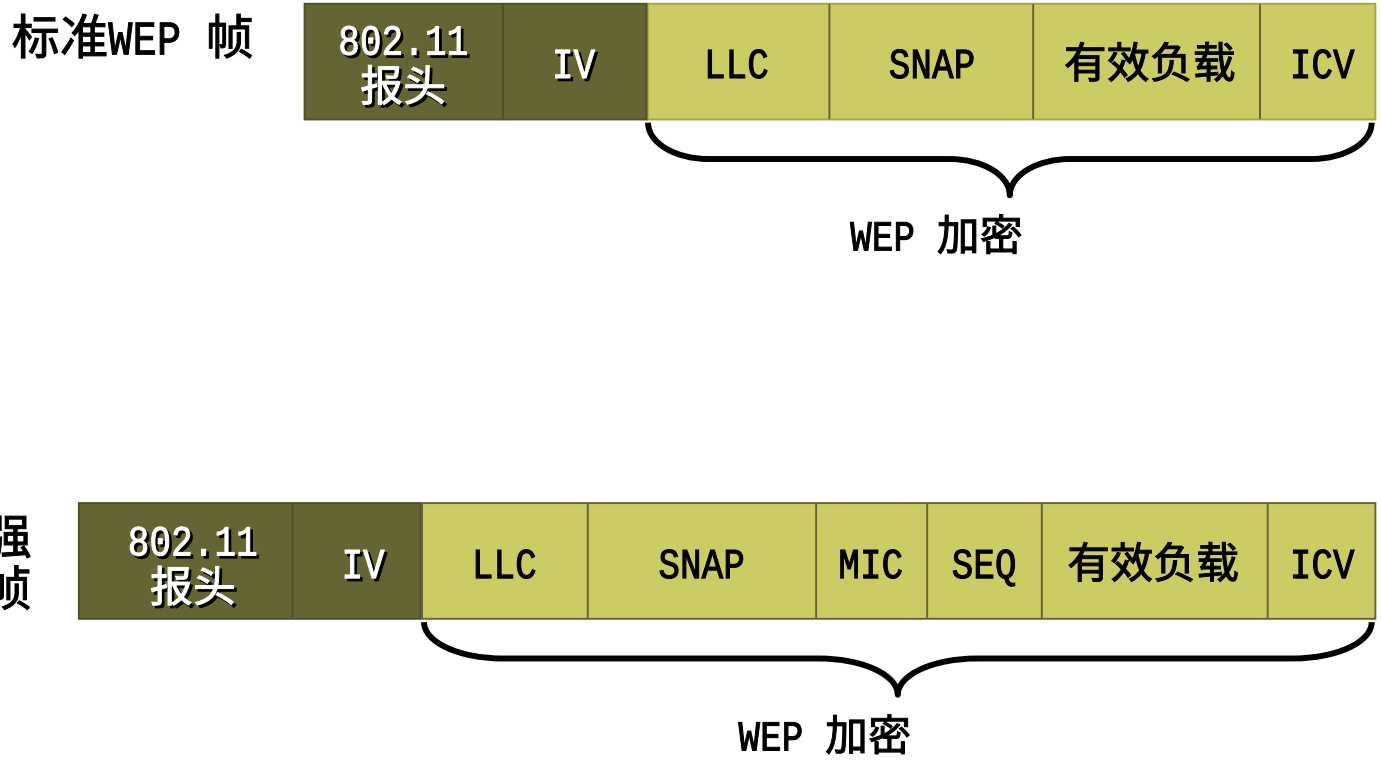
每数据包加密原则

- 只要IV是唯一的，数据包密钥就是唯一的。
- 802.11 IV可能具有 2^24个整数 (约从 0到 16.7M)
- 基本WEP密钥必须通过802.1X改变，以便避免IV/数据包密钥流的派生

消息完整性检查 (MIC)

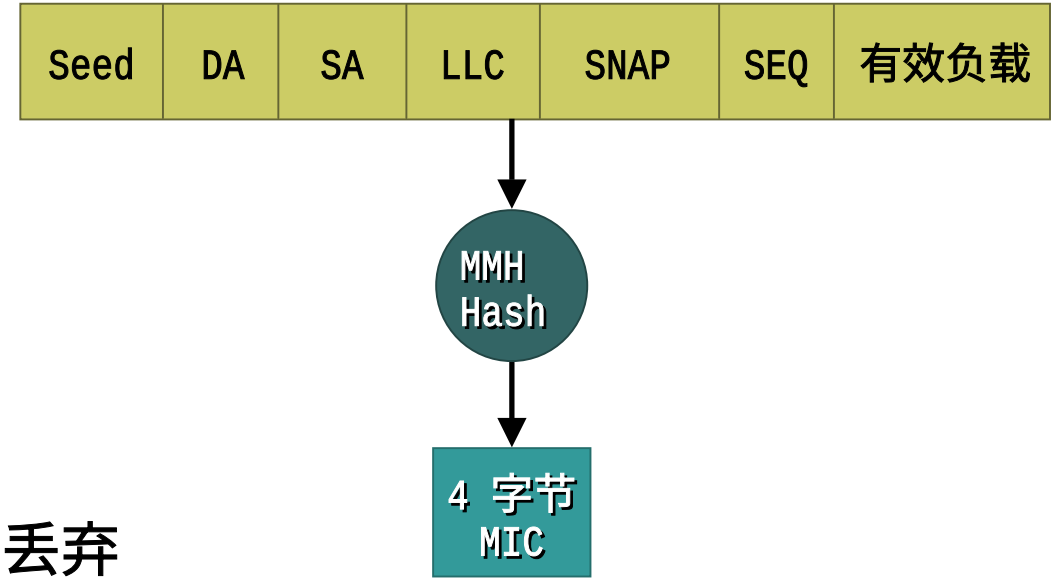
- 防止重新使用 IV/WEP 密钥
- 防止破坏帧

消息完整性检查（MIC）


标准WEP 帧
802.11 报头
IV
LLC
SNAP
有效负载
ICV
WEP 加密
MIC增强 WEP 帧
802.11 报头
IV
LLC
SNAP
MIC
SEQ
有效负载
ICV
WEP 加密

消息完整性检查（MIC）

- MIC根据以下值来计算：
  - 随机速度值
  - MAC 报头
  - 顺序号
  - 数据有效负载
- 混合各组分以派生32位MIC
- 必须顺序分配SEQ号，或丢弃帧



广播密钥旋转

- 在802.1X环境中要求广播密钥
- 广播密钥和静态WEP密钥一样易遭同样的攻击
- 和单点发送密钥一样，广播密钥需要旋转

加密攻击缓解

	WEP	TKIP	VPN
位交换		X	X
IV 重新使用		X	X
AirS否rt		X	X

议程

- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

部署安全性的无线LAN

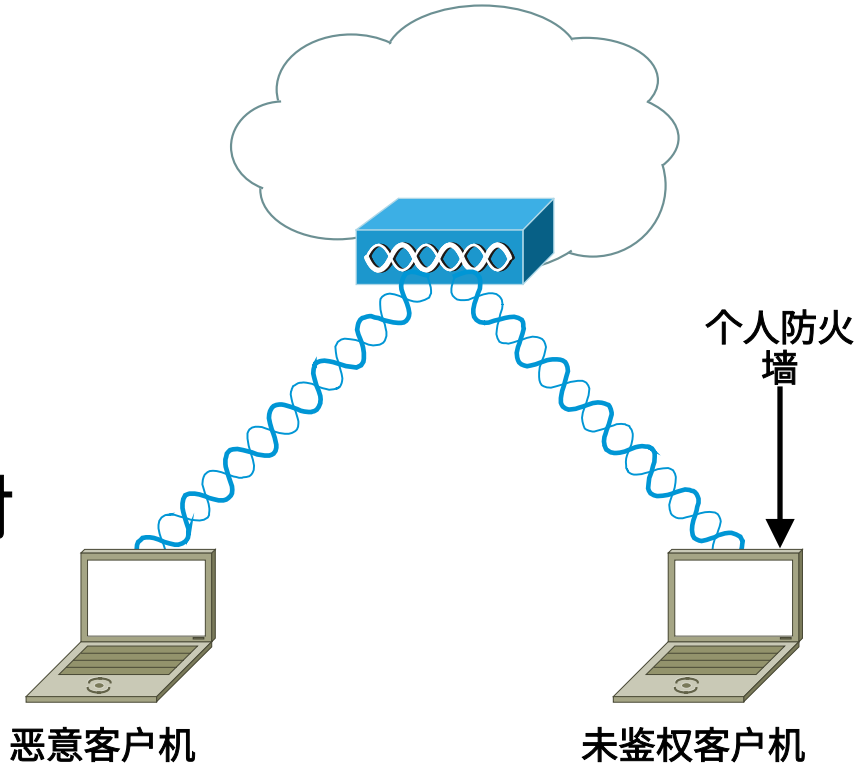
- 802.11上的VPN
- 具有TKIP加密的802.1X

802.11上的VPN—客户机

- 要求单独登录VPN

802.11上的VPN—客户机

- 在VPN 鉴权前，客户机在未受保护的WLAN上
- 个人防火墙可以缓解对这些客户机的攻击。

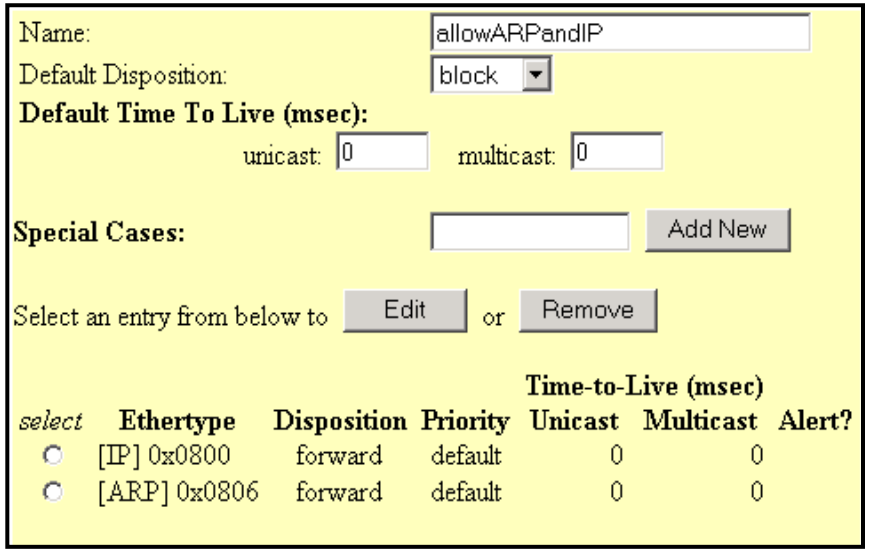


802.11上的VPN—接入点

- AP设置为开放式鉴权
- 无加密

802.11上的VPN—接入点

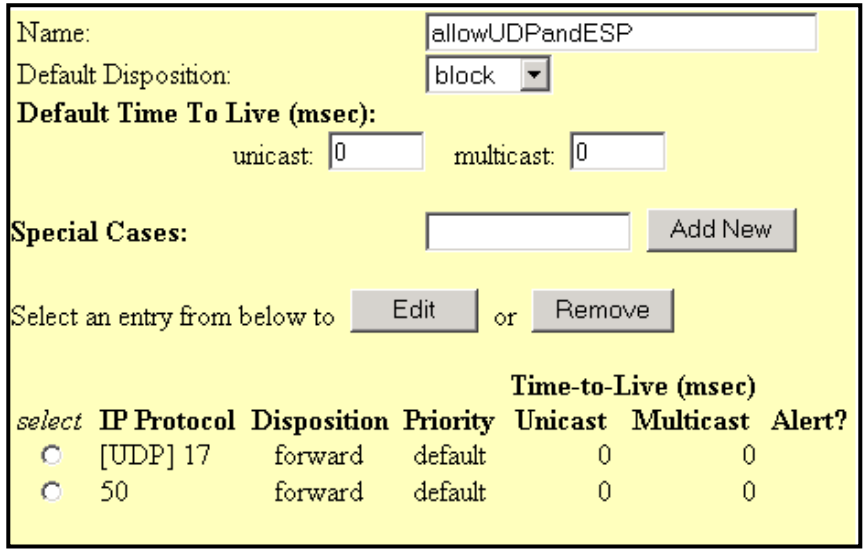
- 建立加密过滤器
- 缺省设置为阻塞（全部拒绝）
- 允许实现IP和 ARP



802.11上的VPN—接入点

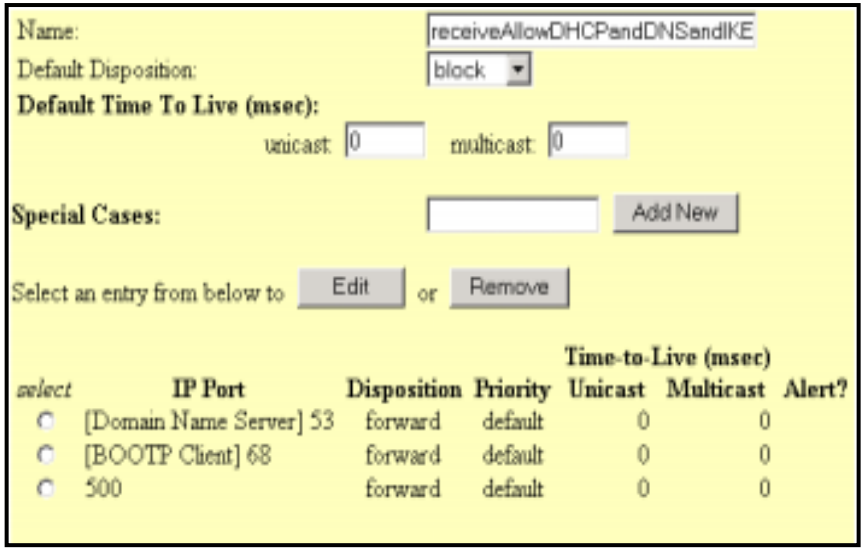
- 创建IP协议过滤器
- 缺省设置为阻塞(全部拒绝)
- 允许实现UDP

  对于 DNS和DHCP
- 允许实现ESP (端口 50)



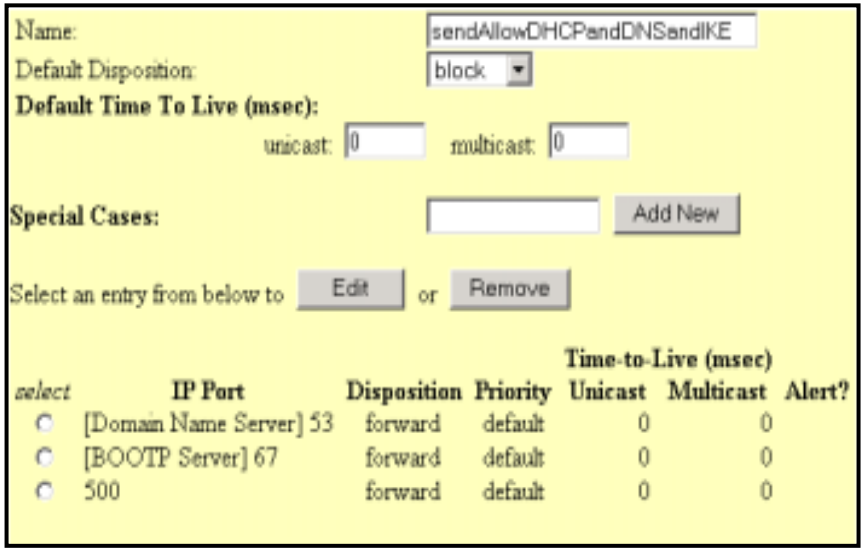
802.11上的VPN—接入点

- 创建IP端口接收过滤器
- 缺省设置为阻塞（全部拒绝）
- 允许实现DNS和DHCP 客户机
- 允许实现IKE（端口500）



802.11上的VPN—接入点

- 创建IP端口发送过滤器
- 缺省设置为阻塞（全部拒绝）
- 允许实现DNS和DHCP客户机
- 允许实现IKE（端口500）



802.11上的VPN—接入点

- 将过滤器应用到AP无线接口

	Receive	Transmit
EtherType	[1] allowARPandIP	[0] -None-
IP Protocol	[1] allowUDPandESP	[0] -None-
IP Port	[1] receiveAllowDHCPandDNSandIKE	[2] sendAllowDHCPandDNSandIKE

802.11上的VPN—第3层入局ACL

- 允许实现ESP和IKE
- 允许实现ICMP
- 允许实现DHCP和DNS
- 拒绝模糊性

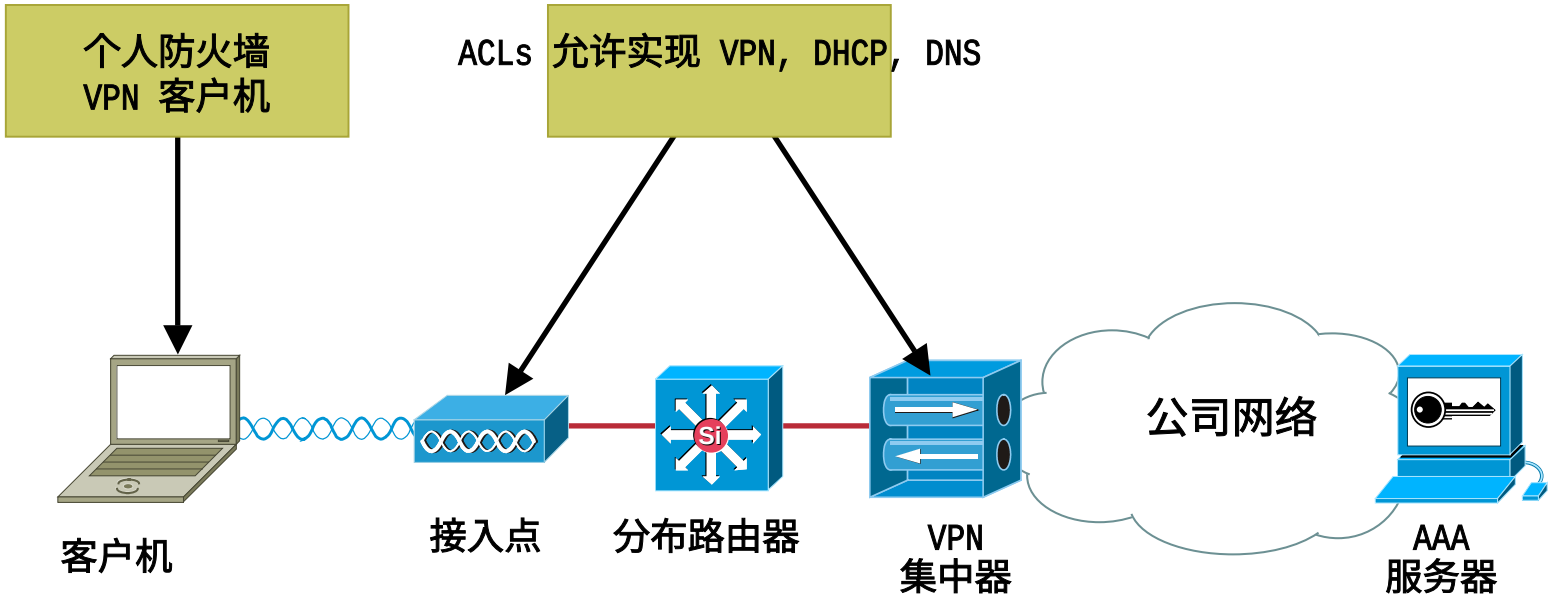
```
! Permit IPSec traffic to the VPN gateway subnet
access-list 100 permit esp <wlan subnet> <vpn subnet>
access-list 100 permit udp <wlan subnet> eq isakmp <vpn subnet> eq isakmp

! Permit Full ICMP for troubleshooting
access-list 100 permit icmp <wlan subnet> <vpn subnet>

! Permit DHCP requests for the initial IP assignment for the wireless client
access-list 100 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 100 permit udp <wlan subnet> eq bootpc host 255.255.255.255 eq
bootps
access-list 100 permit udp <wlan subnet> eq bootpc host <DHCP server> eq bootps

! Deny all other traffic, don't log Windows file share broadcasts
access-list 100 deny udp <wlan subnet> any eq netbios-ns
access-list 100 deny udp <wlan subnet> any eq netbios-dgm
access-list 100 deny ip any any log
```

802.11上的VPN—第3 层出局ACL

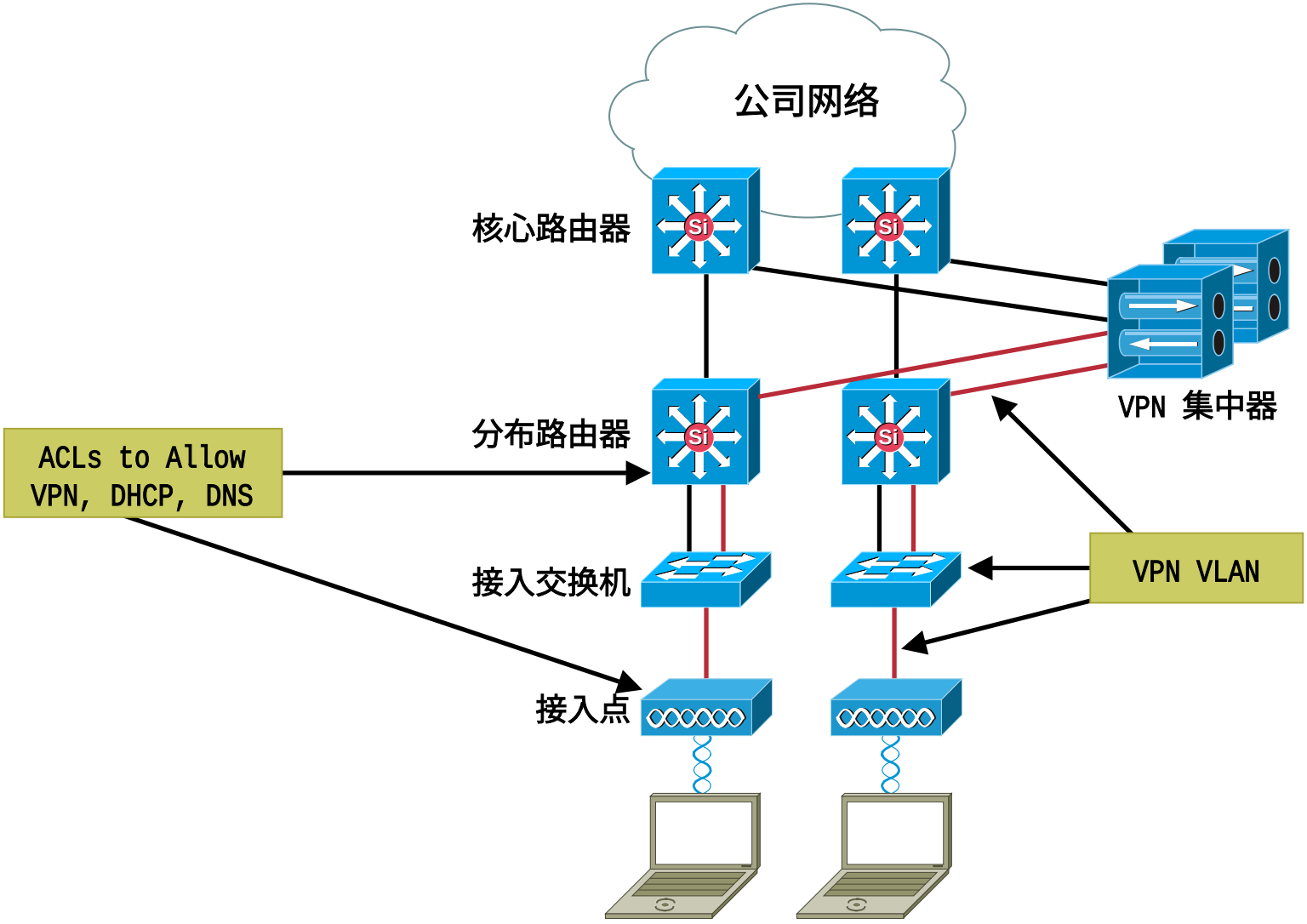
- 允许实现ESP和IKE
- 允许实现ICMP
- 允许实现DHCP和DNS
- 拒绝模糊性

```
! Permit IPSec traffic to the wireless subnet
access-list 101 permit esp <vpn subnet> <wlan subnet>
access-list 101 permit udp <vpn subnet> eq isakmp <wlan subnet> eq isakmp

! Permit Full ICMP for troubleshooting
access-list 101 permit icmp <vpn subnet> <wlan subnet>

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 101 permit udp host <DHCP server> eq bootps host 255.255.255.255 eq
bootpc
access-list 101 permit udp host <DHCP server> eq bootps <wlan subnet> eq bootpc

! Deny all other traffic
access-list 101 deny ip any any log
```

VPN逻辑拓扑结构

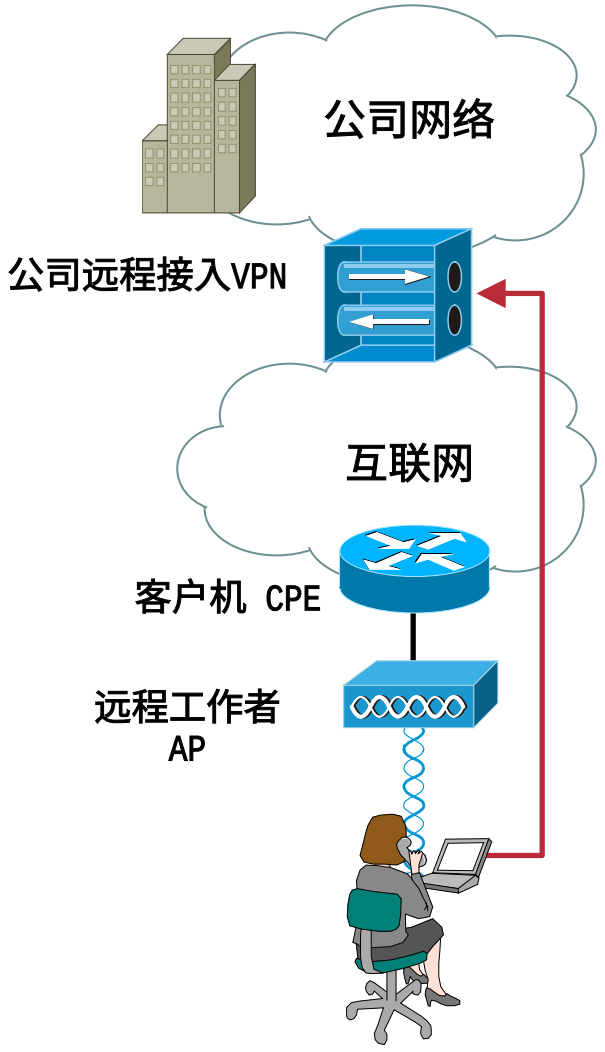

个人防火墙
VPN 客户机
ACLs 允许实现 VPN, DHCP, DNS
客户机
接入点
分布路由器
VPN
集中器
公司网络
AAA
服务器

802.11上的VPN—大型部署

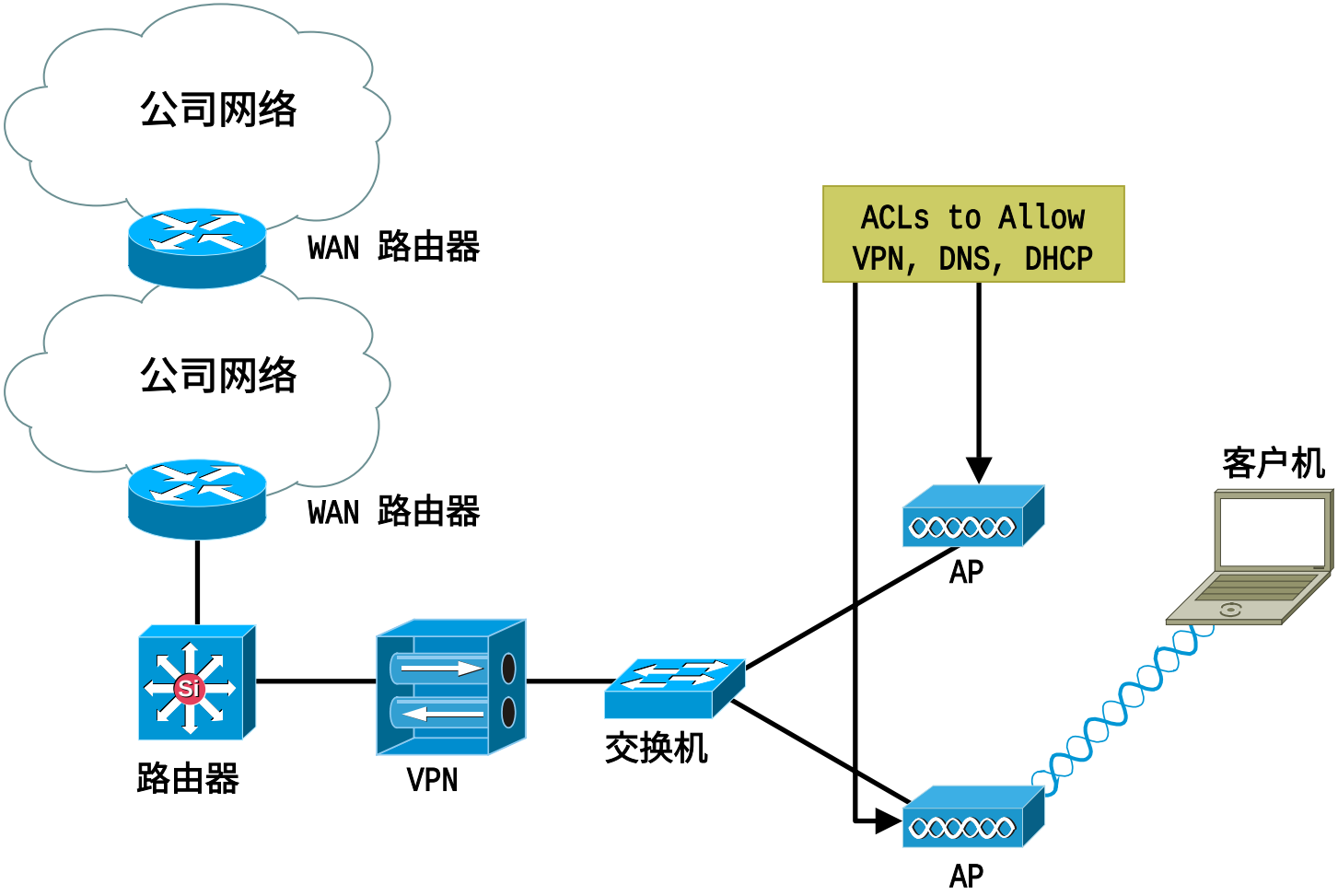


802.11上的VPN—远程工作者

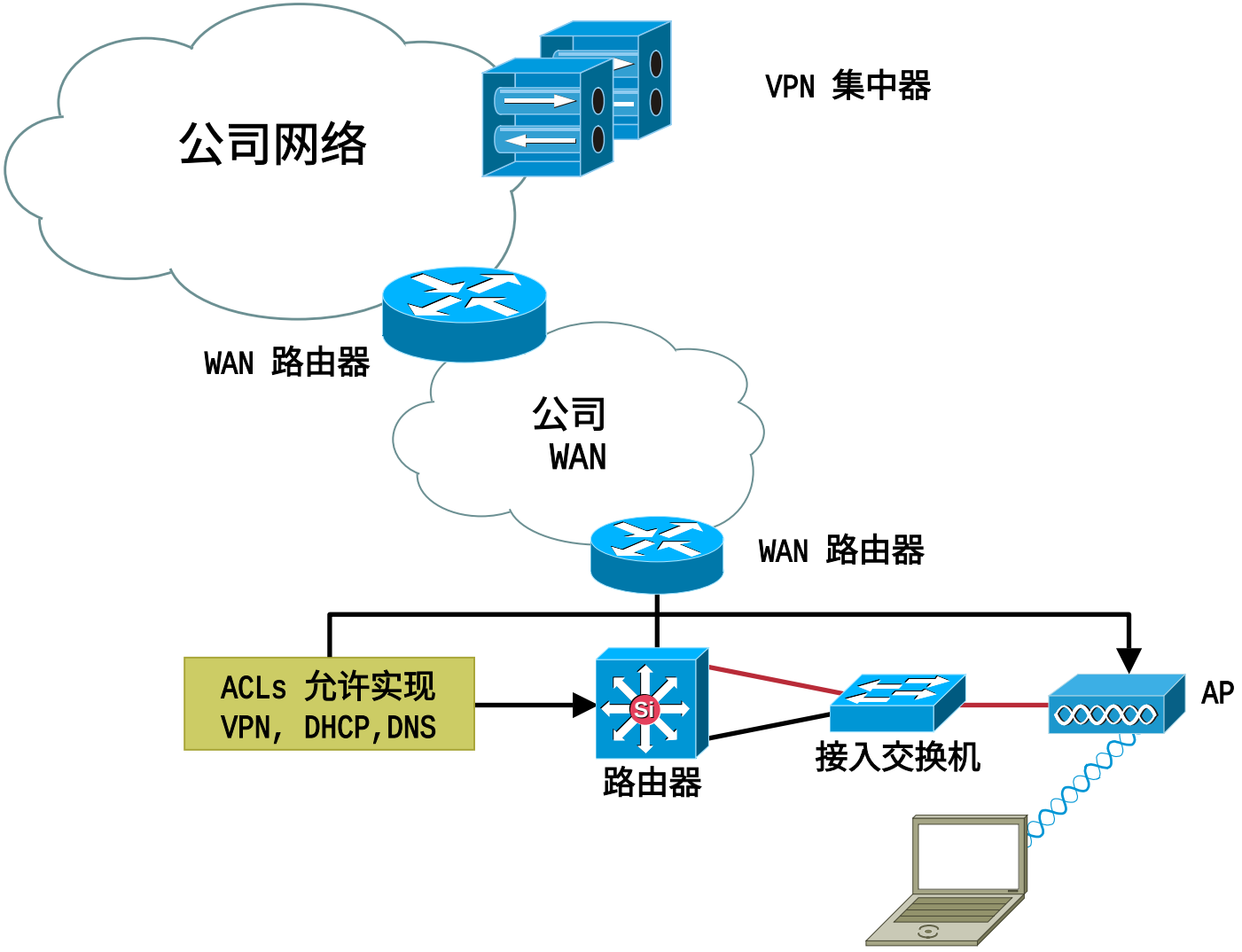
- 客户机作为远程接入用户接入公司网络
- 客户机和公司网络通过IPSec隧道来保护



802.11上的VPN—远端站点



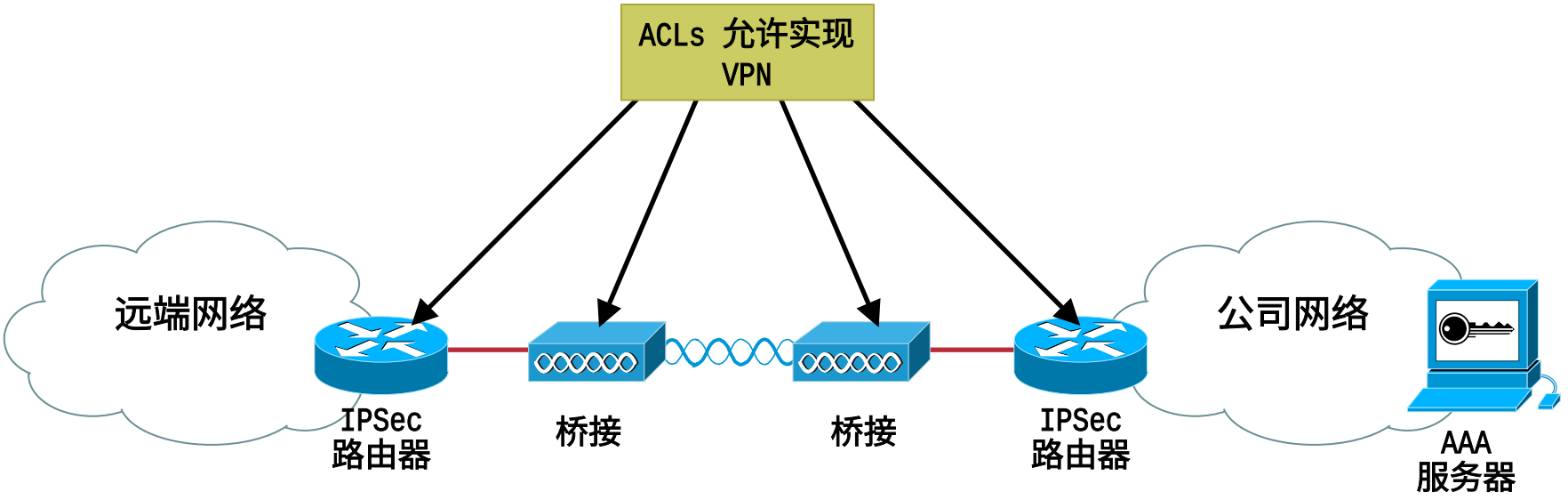
802.11上的VPN—集中式远端站点



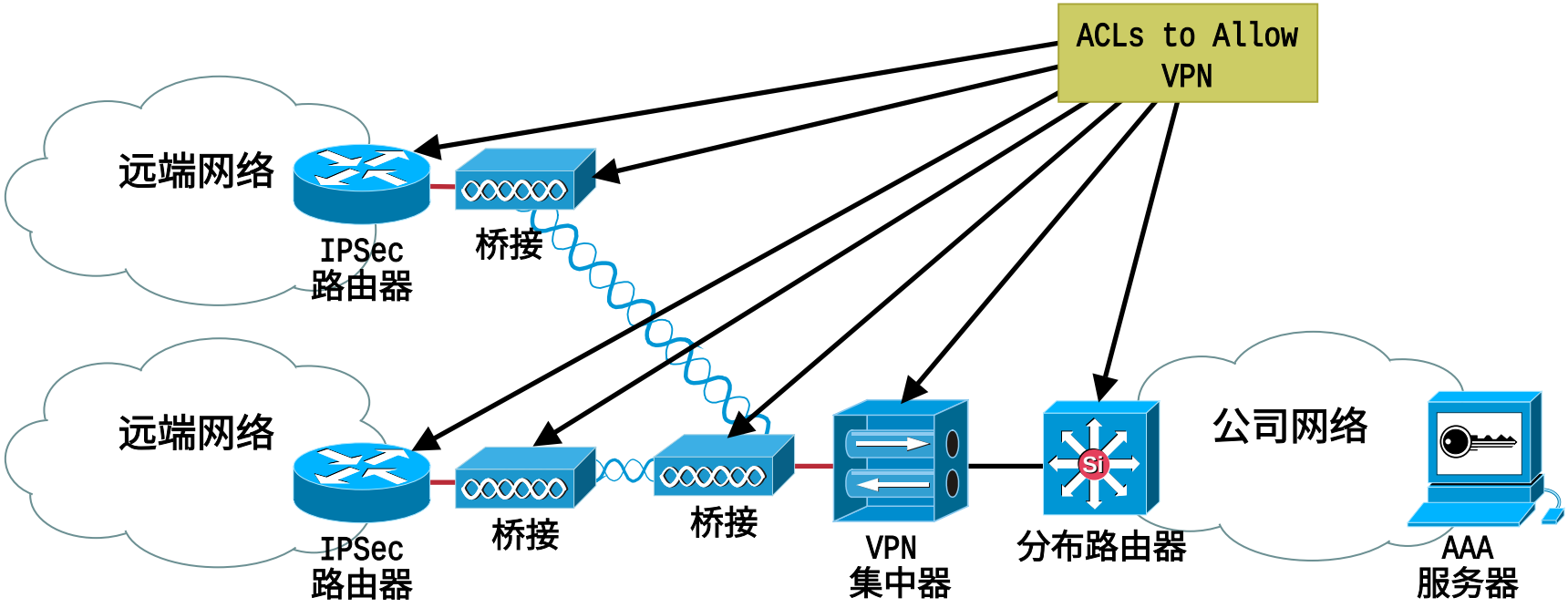
802.11上的VPN—远端站点

- VPN总是进出终接点
- 集中器应在远端站点本地，以便最大程度降低WAN使用率
- 增加额外费用

802.11上的VPN桥接方案s



802.11上的VPN桥接方案



802.11上的VPN—性能

- 在软件中进行所有消息鉴权和加密
- 平均30%到40% 的性能影响

802.11上的VPN—问题

- 客户机吞吐量可能要求多个集中器
- 只支持IP单点发送

  不支持 IPX、 AppleTalk

  不支持组播

- 802.11e QoS增强对 VPN WLAN 客户机没有意义

  所有流量都封装IP/ESP

802.11上的VPN—问题

- 不支持 WLAN设备|

  Barcode条码扫描器, 802.11电话

- 漫游问题

  第 2层—ESP会话超时

  第 3层—与移动IP的互操作性

符合TKIP协议的802.1X—配置

- EAP-Cisco
- EAP-TLS
- 两者都要求 Cisco 客户机和AP

符合TKIP协议的802.1X—接入点

- AP固件要求：|

  VPN—无，建议11.10T1

  TKIP—11.10T1

- 客户机固件/驱动程序要求：

  VPN—4.25.10 和 NDIS 6.97

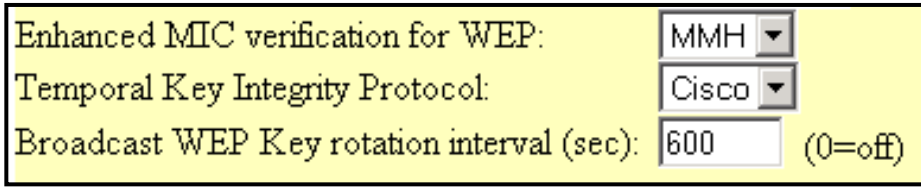
  TKIP—4.25.23 和 NDIS 8.01.06

符合TKIP协议的802.1X—RADIUS

- EAP-Cisco
  - ACS v2.6或v3.0
  - AR v1.7
  - Funk Steel Belted RADIUS 3.0
  - Interlink RAD-E v5.1
- EAP-TLS
  - ACS v3.0
  - MS IAS 2000

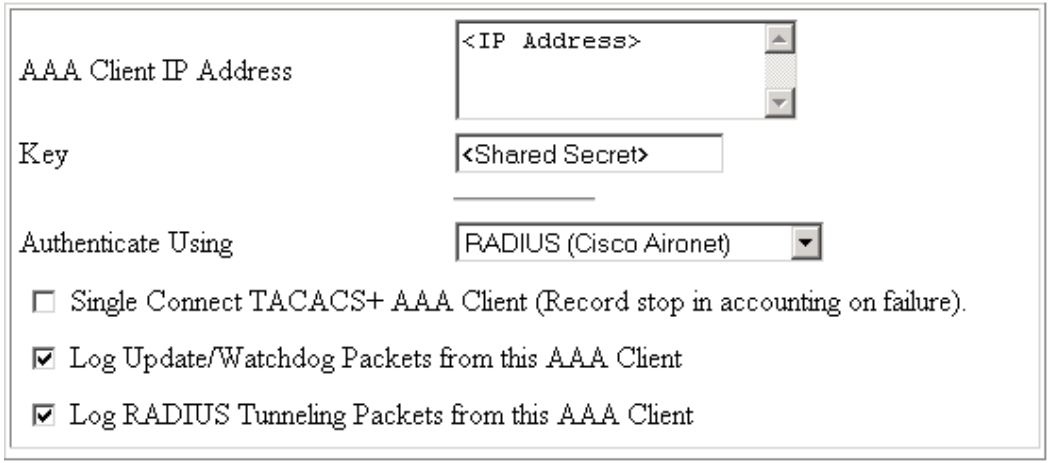
符合TKIP协议的802.1X—接入点

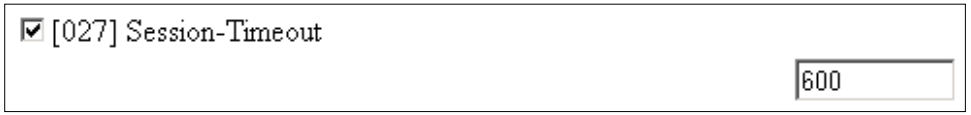
- 简单TKIP 配置
- 广播密钥旋转应与单点发送密钥间隔相匹配



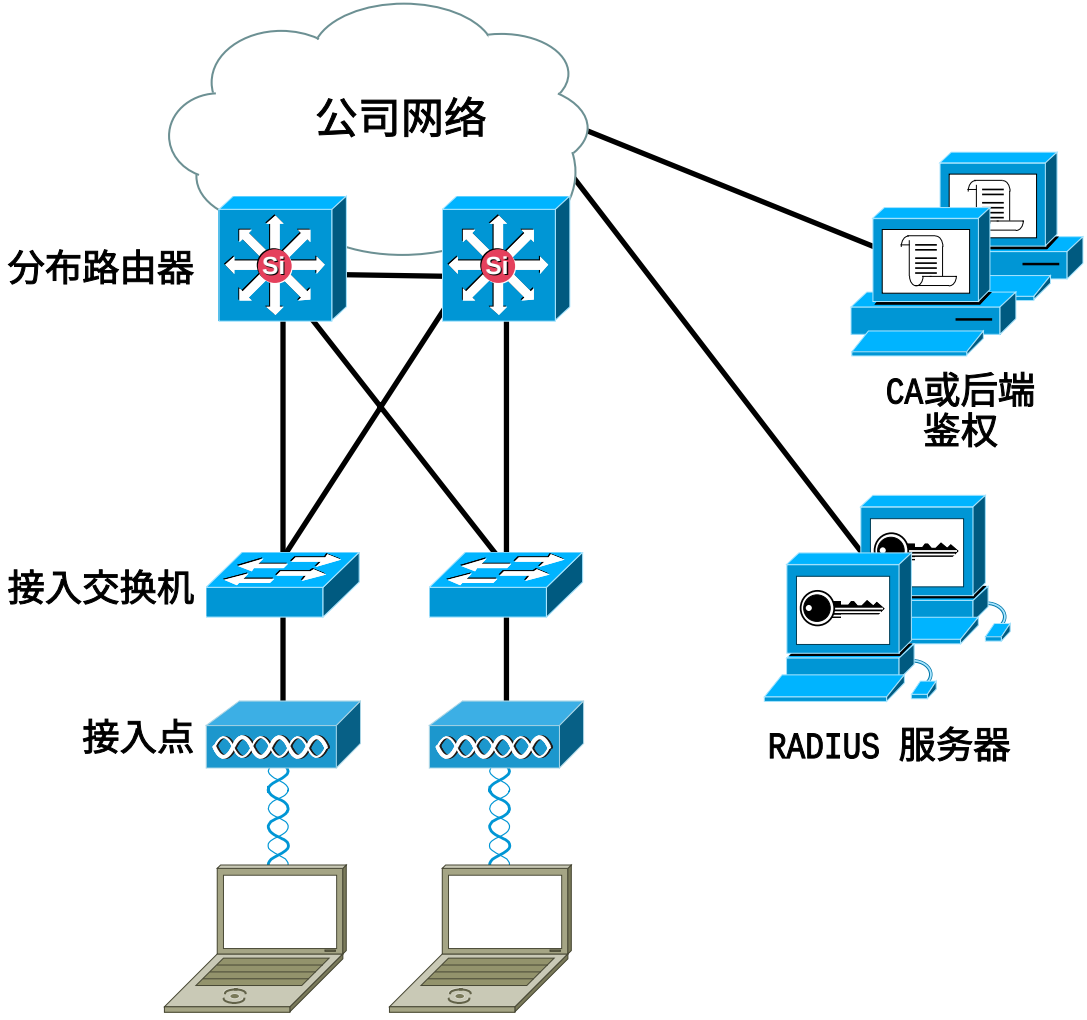
符合TKIP协议的802.1X—RADIUS

- AP作为 NAS增加到RADIUS 服务器中
- RADIUS选项27用于设置重新鉴权并生成新的密钥



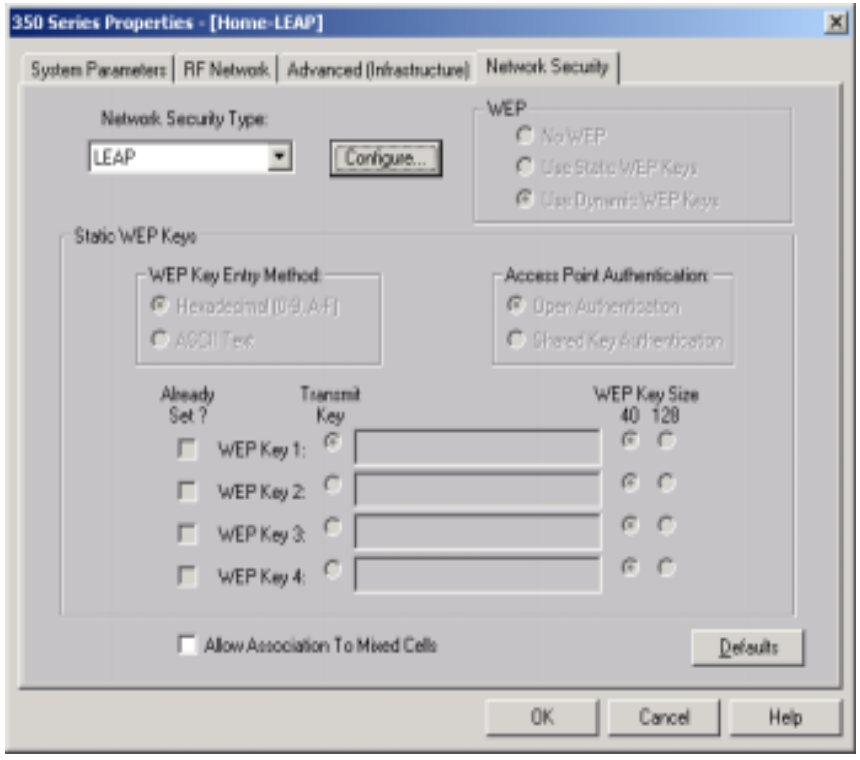


符合TKIP协议的802.1X—拓扑结构



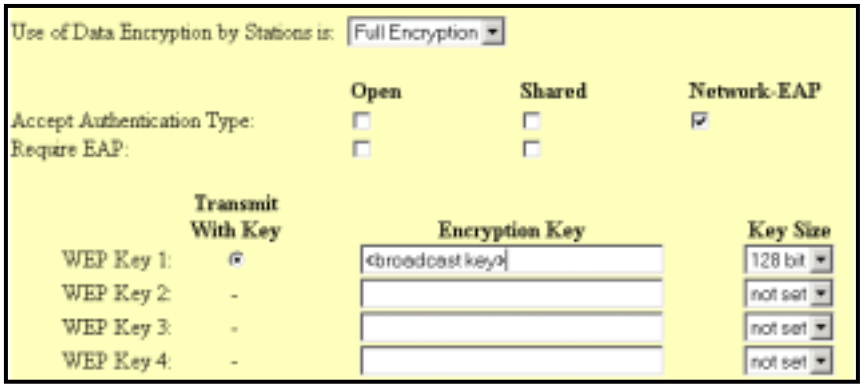
符合TKIP协议的EAP-Cisco—客户机

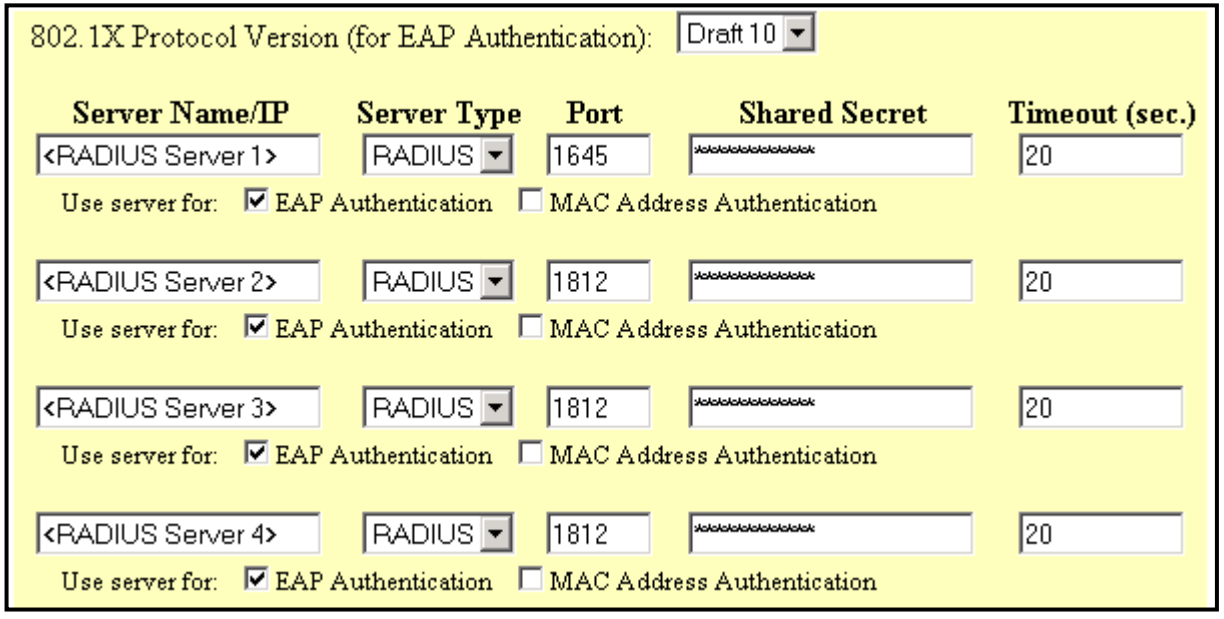
- 要求Cisco 340/350 系列客户机
- Cisco EAP-Cisco (LEAP) 配置
- 单一登录Windows客户机



符合TKIP协议的EAP-Cisco—接入点

- 简单鉴权配置
- 建议802.1X 10版





符合TKIP协议的EAP-Cisco——RADIUS

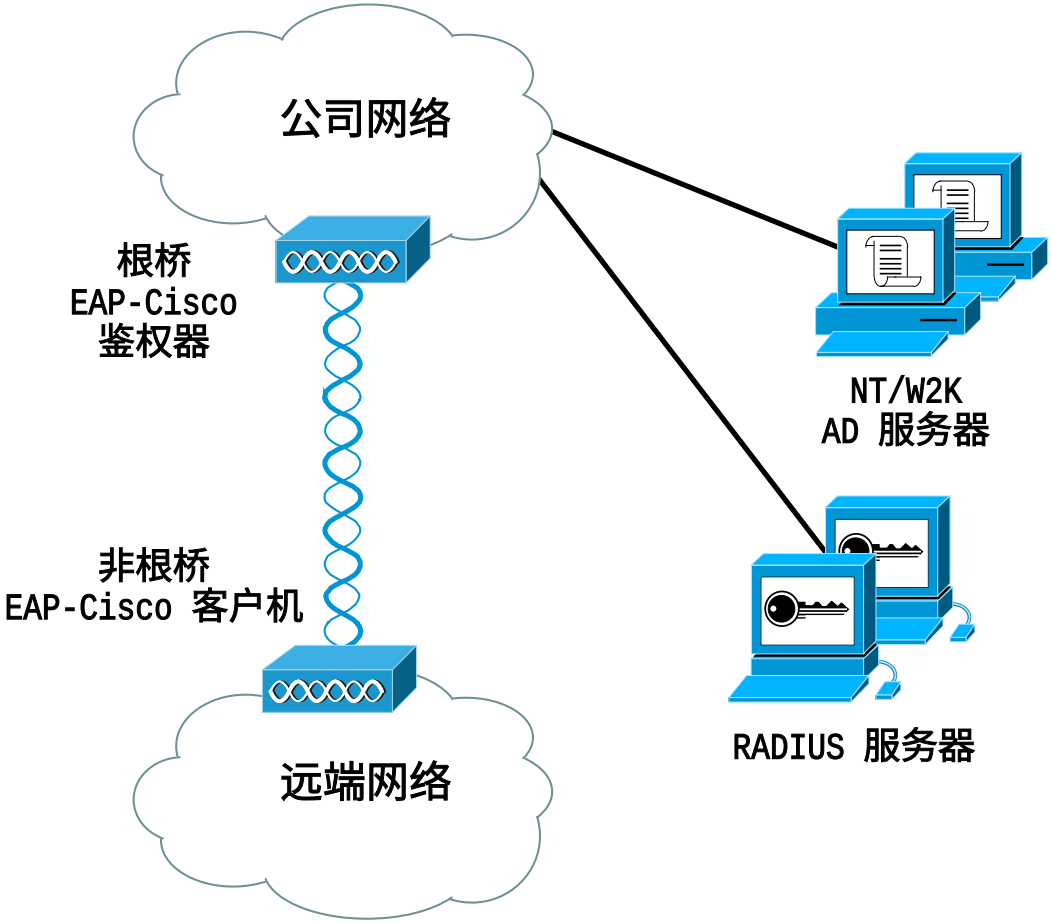
- 支持本地鉴权或 NT域/W2K Active Directory

符合TKIP协议的EAP-Cisco—非根桥

- 非根桥可以是EAP-Cisco 客户机
- 要求桥接固件 v11.10T1

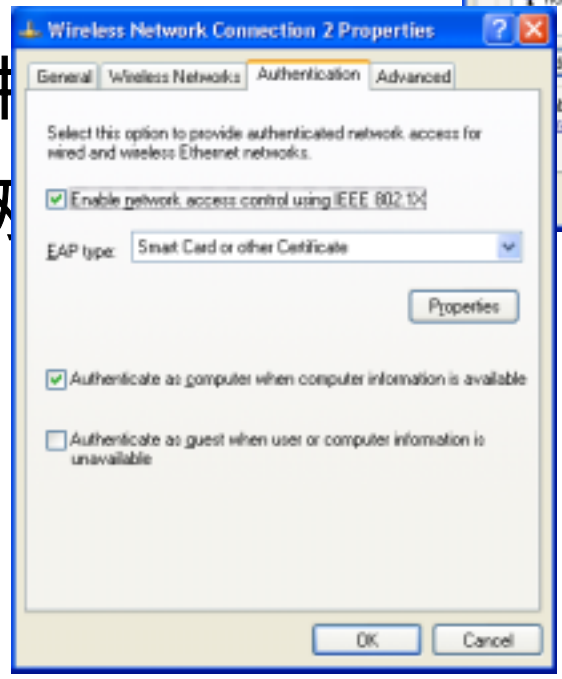
Service Set ID (SSID):	<SSID>
LEAP User Name:	<EAP-Cisco Username>
LEAP Password:	**********
Firmware Version:	4.25.22
Boot Block Version:	1.50

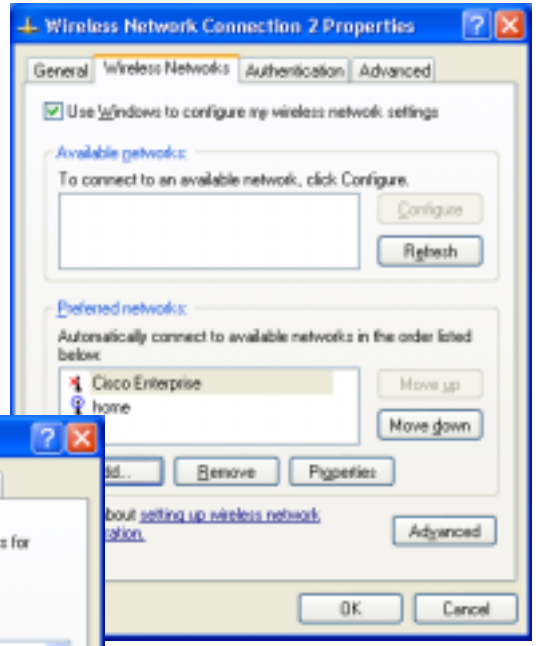
符合TKIP协议的EAP-Cisco—桥接方案



符合TKIP协议的EAP-TLS—客户机

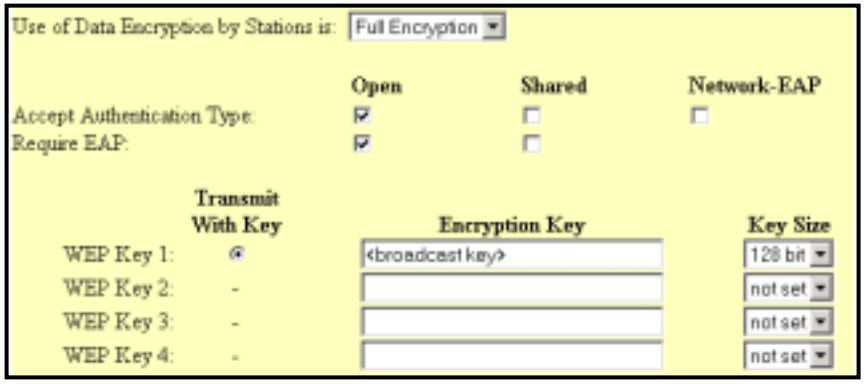
- 包括在 WinXP 和Win2K SP3 OS 版本中
- 配置多个网络配置文件
- 客户机显示所有已知网络，并激活了广播 SSID

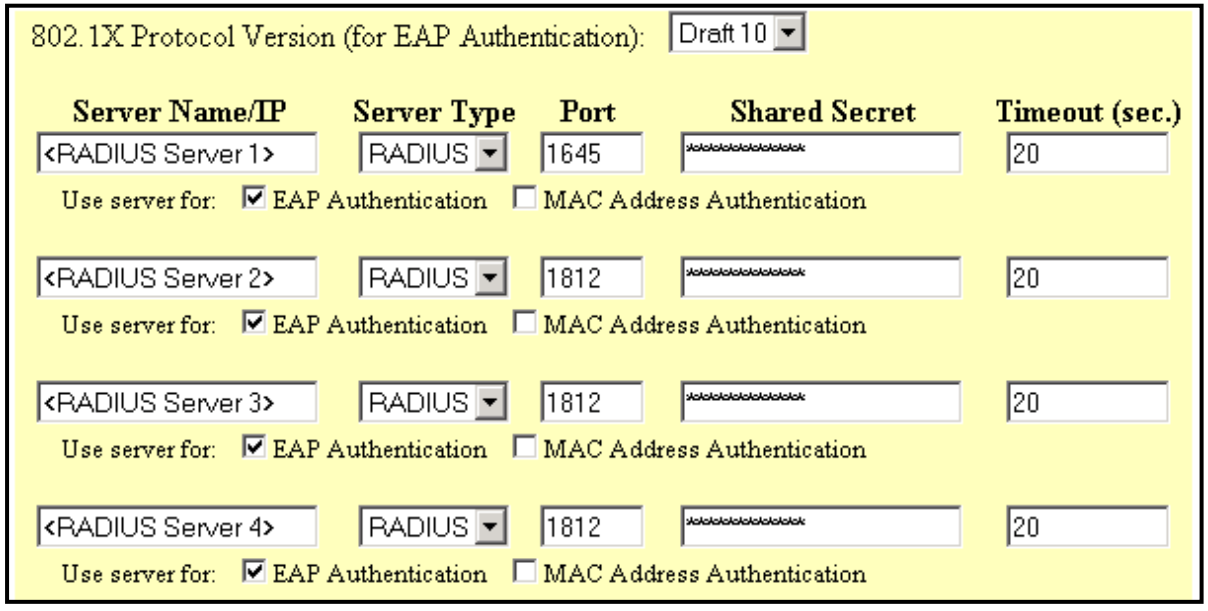




符合TKIP协议的EAP-TLS—接入点

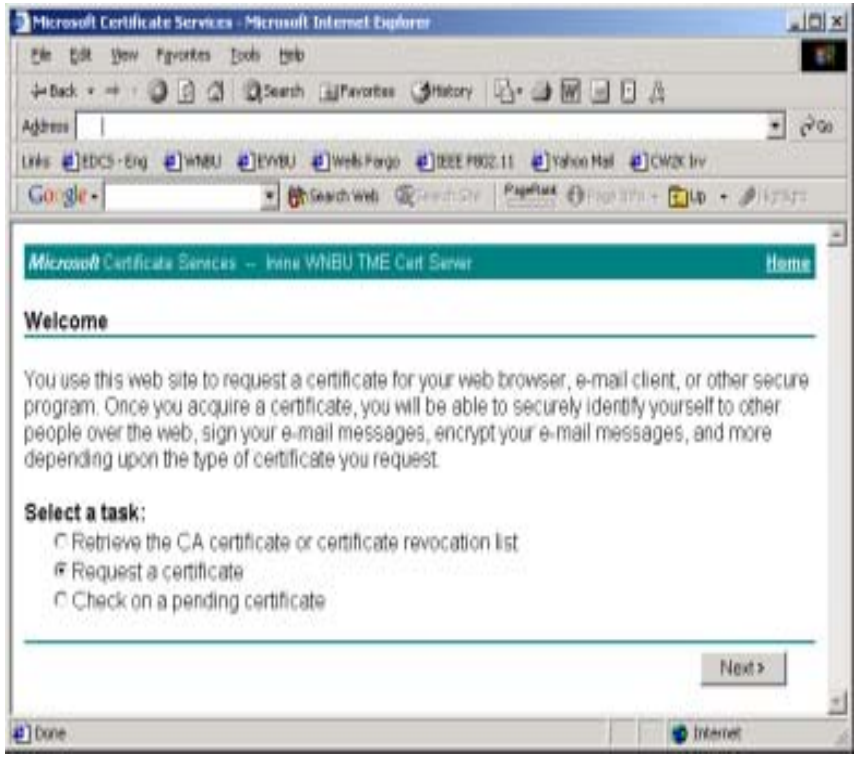
- 简单鉴权配置





符合TKIP协议的EAP-TLS—CA 服务器

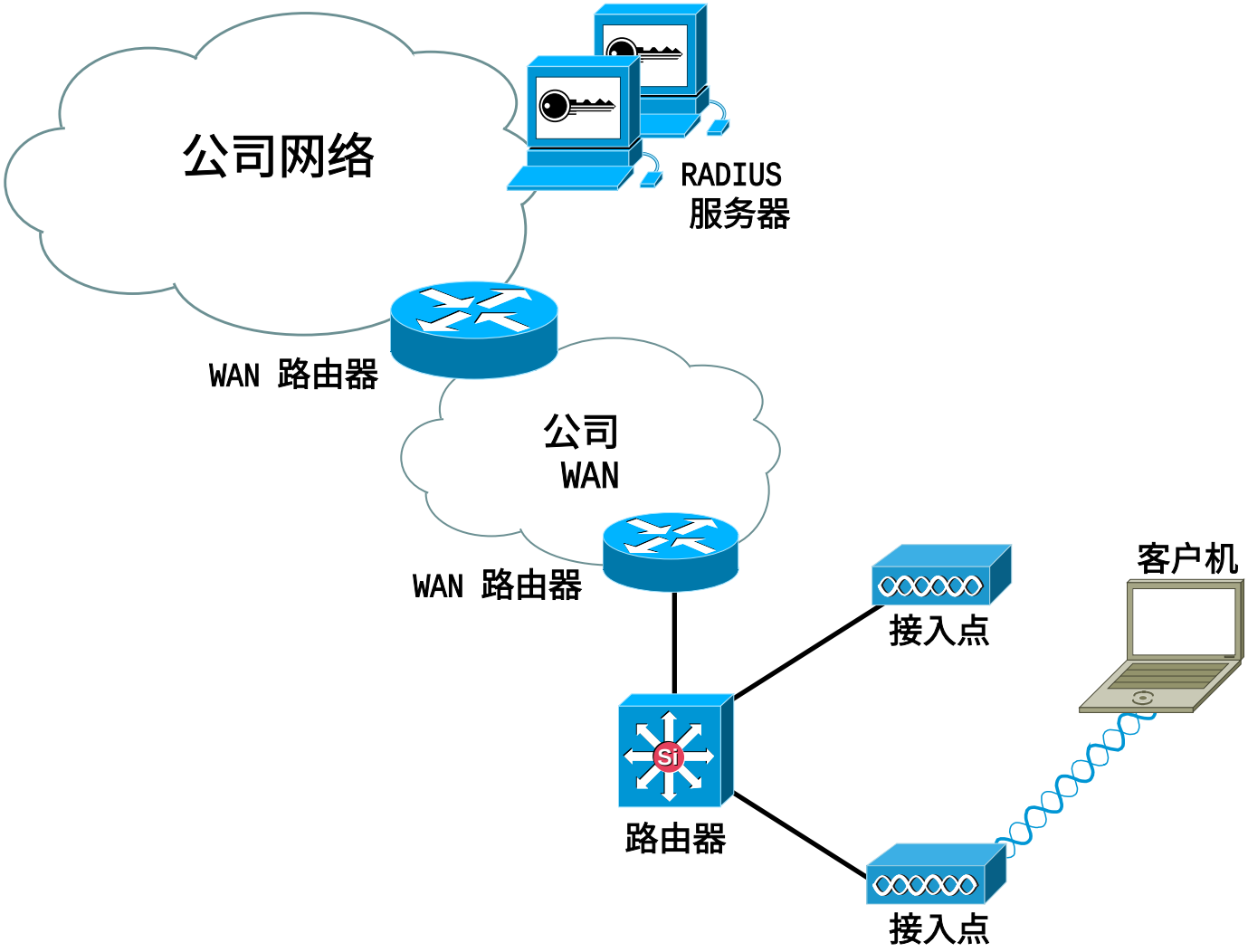
- MS 位专用CA提供 Win2K 服务器
- 支持用户、机器和服务器证书等
- 客户机证书请求需要获得管理员的准许



符合TKIP协议的EAP-TLS—鉴权

- RADIUS 服务器
  - Cisco ACS
  - Microsoft IAS
- 证书授权
  - Microsoft Win2k CA服务器

符合TKIP协议的802.1X—远端站点



WAN中的802.1X 鉴权

- 网络拥塞会造成鉴权延迟
- 对漫游的潜在影响

WAN中的802.1X 鉴权

- 端到端QoS缓解了WAN拥塞的影响
- 划分802.1X RADIUS消息的优先级
  - DSCP AF31/IP 优先级3
  - 建议的LLQ 或 CBWFQ
- RADIUS消息的大小约为 1.5 KB
  - 8 Kbps的带宽要求每秒支持5次鉴权

符合TKIP协议的802.1X——一般问题

- 新的加密技术

  在IEEE中已经得到证明，但需要时间的考验...

- 802.11标准还在不断发展

  需要进行改变

  802.11 任务组E, F, H, 和 I

符合TKIP协议的802.1X—性能

- 在硬件中进行WEP加密
- 在软件中进行MIC和每数据包加密
- 依赖于流量类型，吞吐量可高达5% 到15%，并实施了增强功能

符合TKIP协议的802.1X——一般问题

- 鉴权类型不普遍（但...）

  没有一种模式能够满足所有方案或要求

- 漫游

  RADIUS请求使漫游时间增加了约 300到600 ms
  需要预鉴权机制来加速漫游过程

其他安全性功能

- RADIUS 计费
- 公众网络数据包安全转发 (PSPF)

RADIUS 计费

- AP通过RFC2866 RADIUS 计费来记录客户机的关联和分离
- 无需客户机升级；只增强AP
- 供应商中立

RADIUS 计费一览

- 在关联客户机之后，AP将给计费服务器发送开始消息
- AP以配置的时间间隔发送更新消息
- 当客户机分离后，AP将发送终止消息

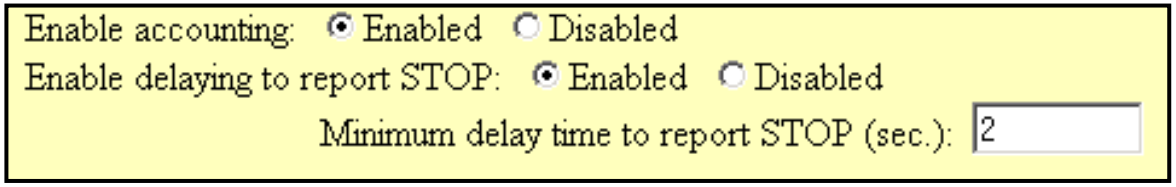
RADIUS 计费一览

- 可以为 EAP 客户机、非EAP 客户机，或这两种配置计费
- 非EAP指标准开放/共享密钥鉴权和/或MAC鉴权

RADIUS 计费一览

- RADIUS计费提供哪些消息？
  - 输入/输出字节
  - 输入/输出数据报
  - 会话时长
  - 关联ID
  - NAS（接入点）IP 地址
- 这些值与每个客户机相关

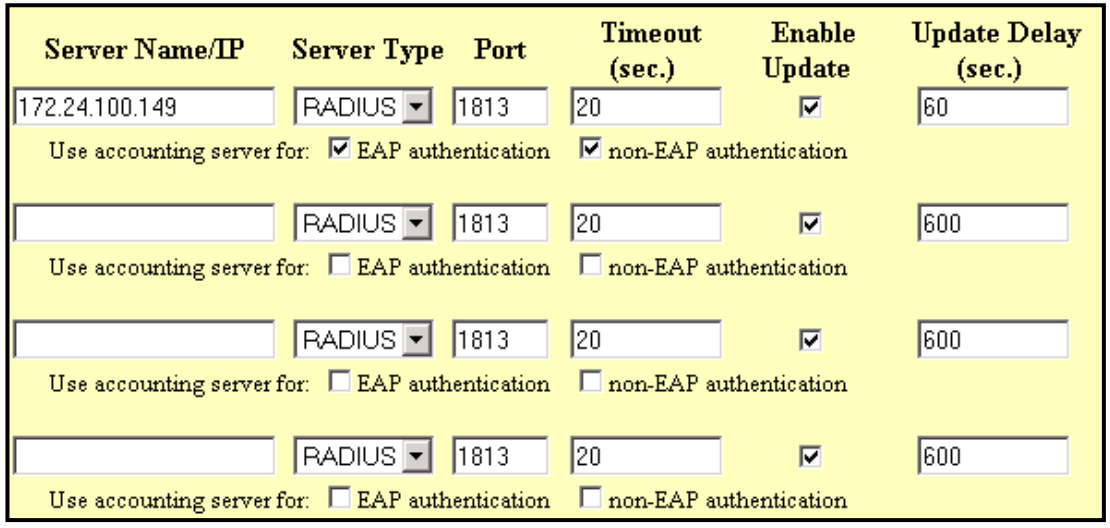
配置RADIUS 计费



- 安装 ->计费显示
- 激活/抑制计费
- 激活/抑制帐户终止延迟

  如果用户暂时漫游到服务范围之外，将延迟“ 终止 ”消息
- 计费“ 终止 ”延迟时间

配置RADIUS 计费



- 更新激活/抑制

  为服务器发送周期性计费更新

- 更新延迟

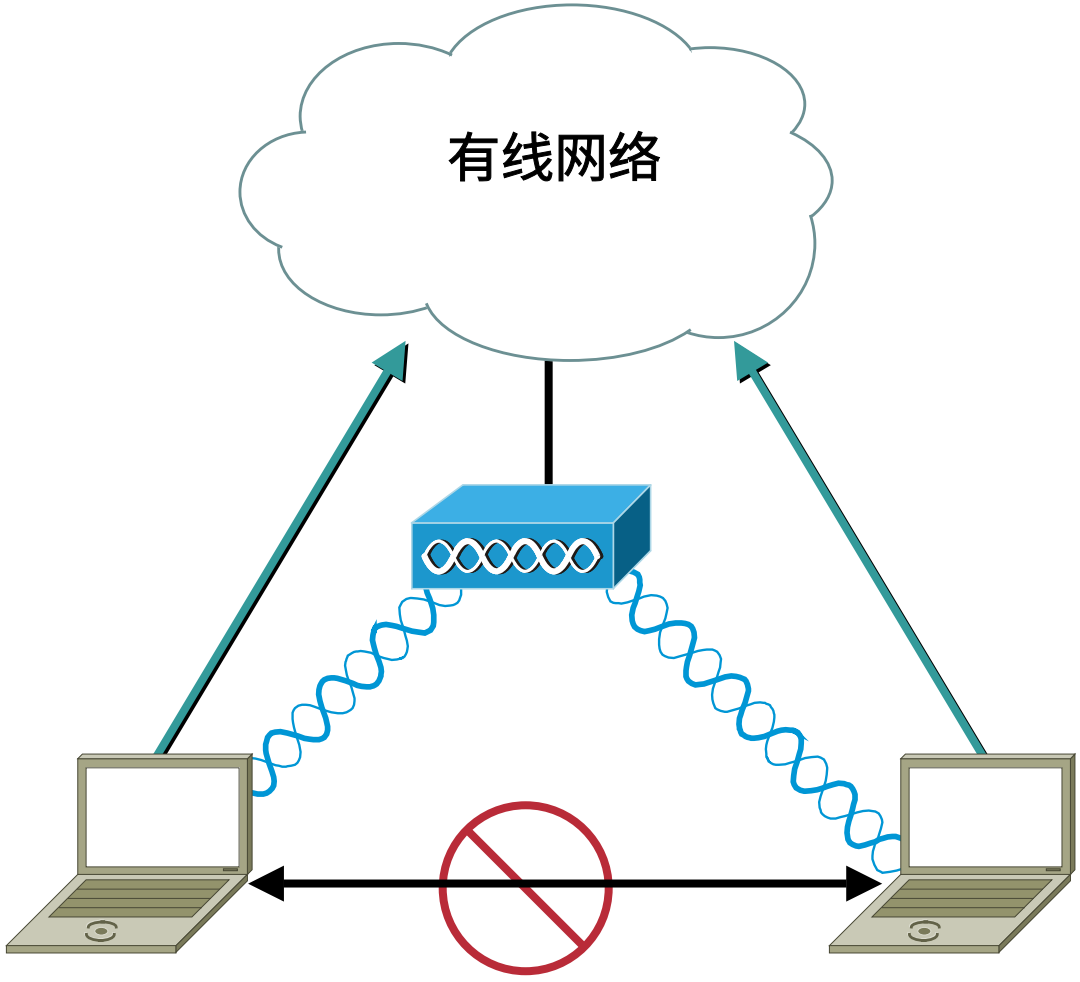
  更新消息间隔

- EAP、 非 EAP或两者

公众网络数据报安全转发

- 防止WLAN的客户机间通信
- 客户机可以与 AP通信
- 客户机无法与BSS中的其他站通信

PSPF—阻塞客户机间通信



议程

- 无线安全性驱动因素
- 802.11网络的无线安全性
- 802.11无线安全性中的薄弱环节
- 保护无线LAN的技术
- 部署安全性的无线LAN
- 前景如何

前景如何

- IEEE 802.11i的批准
- 采用TKIP加密

  保证供应商互操作性 (WiFi)
- AES加密

AES加密

- 高级加密标准
  - 3DES 成功或
  - 由NIST倡导
- Rijndael算法
  - 分组密码
  - 128,192, 和256位密钥支持

AES加密

- 要求回退模式
- 当前考虑两种方法

  抵消代码簿（OCB模式）

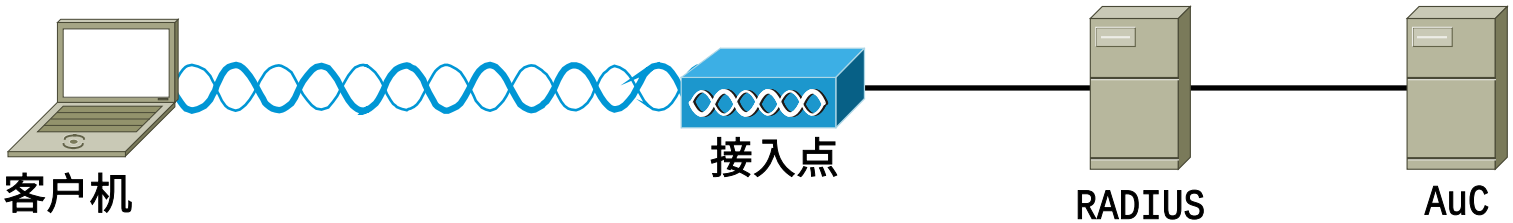
  密码分组连接以及密码分组连接消息鉴权检查（CCM 模式）
- 两种模式都提供安全的加密和消息完整性


CISCO SYSTEMS
EMPOWERING THE
INTERNET GENERATION

增强安全性总结

	符合TKIP协议的802.1X	IPSec	Static WEP
密钥长度（Bits）	128	168	128
加密算法	RC4	3 DES	RC4
数据包完整性	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
设备鉴权	无	预共享机密或证书	无
用户鉴权	用户名/口令和/或证书	用户名/口令或OTP	无
用户差分	否	是	否
透明用户体验	是	否	是
ACL 要求	无	大量	无
附加硬件	鉴权 服务器 和/或CA	鉴权 服务器 和 VPN 网关	否
每用户加密	是	是	否
协议支持	任意	IP单点发送	任意
客户机支持	PC和高端PAD；支持广泛的思科OS	PC和高端PAD；支持思科和第三方供应商的广泛OS	支持所有客户机
开放式标准	是	是	是
基于时间的密钥旋转	可配置	可配置	否
客户机硬件加密	是	有，软件是最普遍的方法	是
附加软件	否	IPSec 客户机	否
每流QoS策略管理	接入客户机	在VPN网关之后	接入客户机

EAP-SIM 鉴权



开始

请求识别符

AP阻塞所有请求，直到鉴权完成。

1IMSI@realm

1IMSI@realm

GetAuthInfo

SIM-开始

SIM-开始

三次

随机

随机

通过MAC_RAND ？

服务器 Authenticated

SIM-挑战

SIM-挑战

通过MAC_SRES ？

派生 密钥

挑战-Resp

挑战-Resp

EAP-成功

接受

派生 密钥

客户机鉴权

广播密钥

密钥长度

AP 发送客户机广播密钥，通过会话密钥加密

保护 802.11无线网络

Session ACC-232

请填写评估表

Session ACC-232


CISCO SYSTEMS
EMPOWERING THE
INTERNET GENERATION