Staying Safe in Wireless Hot Spots

Lisa Phifer

Core Competence Inc.

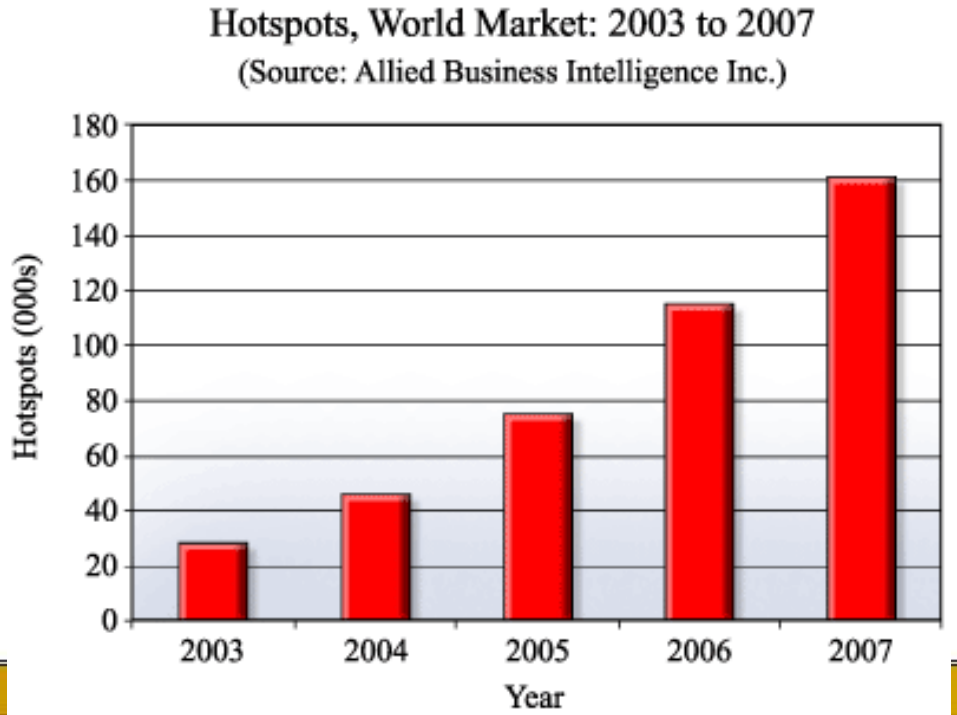
lisa@corecom.com

Agenda

- **Hot spot security threats**
- **Subscriber authentication and roaming**
- **Role of WEP, WPA and WPA2 in hot spots**
- **Using VPNs to secure hot spot traffic**
- **Overcoming hot spot security challenges**

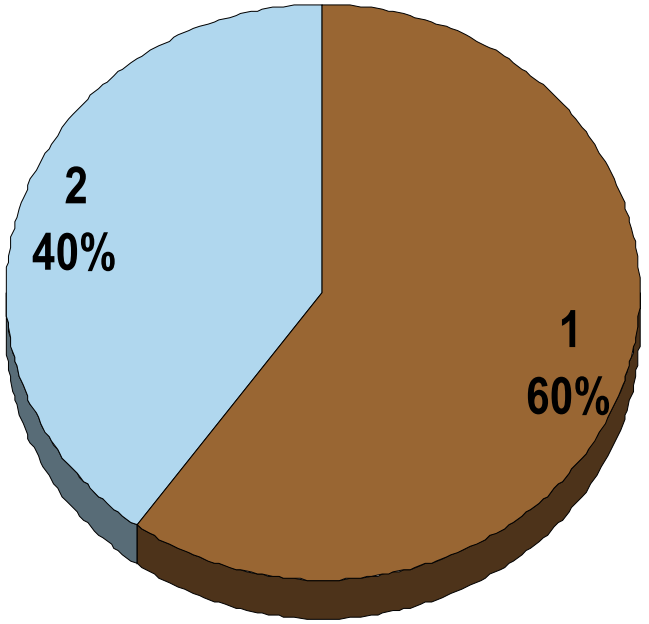
Wireless Hot Spots Are Hot

- **Business travelers dominate today's market**
  - **Most hot spots are in places frequented by business travelers: airports, hotels, train stations, cafes**
  - **71% of hot spot access cost is borne by employers**



Have you ever used a wireless (Wi-Fi) hot spot to send business-related data?

1. **Yes**
2. **No**



But Hot Spots Are Also Risky

- **Vulnerable to 802.11 security threats, including**
  - **Eavesdropping on wireless data**
  - **Unauthorized wireless network access**
  - **Attacks against wireless APs**
  - **Attacks against other stations**
  - **Denial-of-service attacks**
- **Public environments just increase the threat level**
  - **Business users make each hot spot a juicy target**
  - **Surrounded by strangers for lengthy periods**
  - **Hot spot operators' security varies**

A Few Examples

Rogue AP
pretends to be hot spot AP, modifies traffic

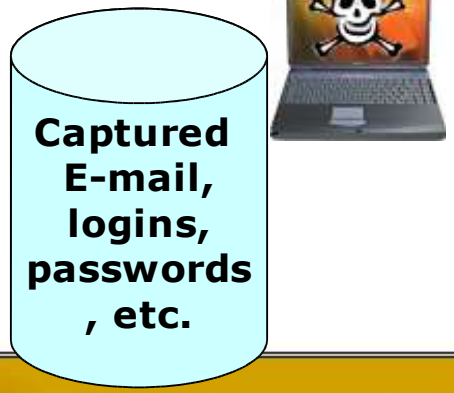
DoS attacker
floods WLAN with bogus frames

Hot spot visitor
station holds:
- User credentials
- Personal data
- Business data

Legitimate hot spot AP

Stolen files

Active attacker
scans other stations for open ports & shares, copies stored data, pushes malware



Passive attacker
uses sniffer to capture & store transmitted data

Hot Spot User Expectations

- **Ideally, must implement adequate security measures while preserving convenience and ease of use**
- **Convenience**
  - **Hot spot finders that discover known or nearby hot spots**
  - **Consistent access from any public hot spot**
  - **Strong, ubiquitous coverage in public spaces**
- **Ease of use**
  - **No reconfiguring WLAN card for every hot spot**
  - **No installing new software for every hot spot**
  - **Avoiding complex, multi-level login processes**
  - **Minimizing application timeouts, broken sessions**

Hot Spot Operator Concerns

- **To charge for services, operators may**
  - **Prevent unauthorized users**
  - **Log hot spot usage to feed billing systems**
  - **Support on-line enrollment for new visitors**
  - **Increase revenue through roaming agreements**
- **To limit legal liability, operators may**
  - **Monitor for illegal activities (e.g., spamming, cyber-stalking, copyrighted music downloads, attacks against others)**
  - **Enforce terms of service**
- **To deliver more reliable service, operators may**
  - **Detect and stop wireless-borne attacks against hot spot itself**
  - **Help customers protect themselves**

Corporate IT Needs

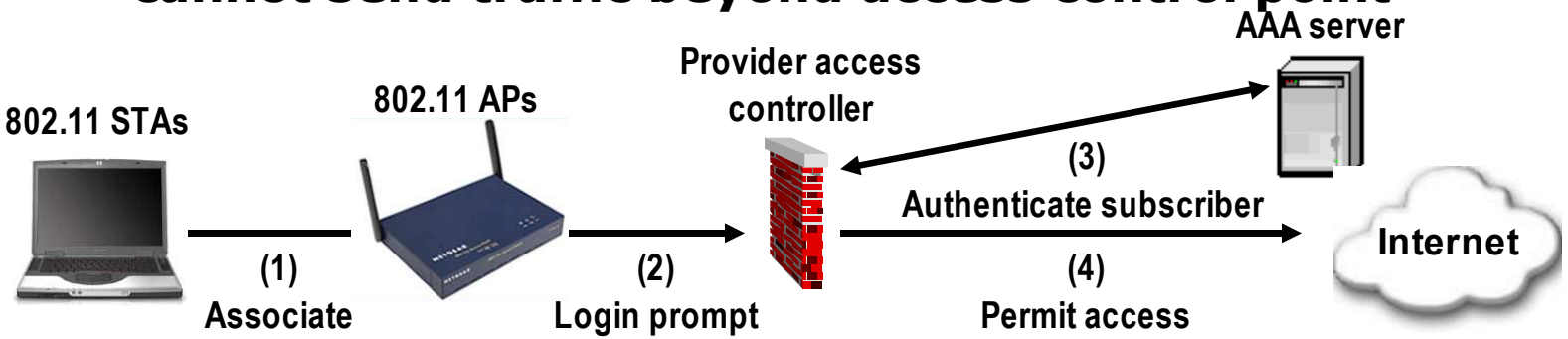
- **To control access from hot spots, IT may**
  - **Track hot spot usage for billing reconciliation**
  - **Prevent theft/abuse of company-paid hot spot service**
- **To minimize risk to corporate assets, IT may**
  - **Inhibit eavesdropping on business data, credentials**
  - **Ensure integrity of business data over wireless**
  - **Prevent theft of sensitive data on company laptops**
  - **Stop virus and malware infection over wireless**
- **IT may deny corporate network access to wireless stations that fail to comply with security policies**

Security Measures That Can Help Meet These Needs

- **Hot spot subscriber authentication**
  - **Prevents hot spot access by unauthorized users, but does not provide any data protection**
- **802.11 Link Security (WEP/WPA/WPA2)**
  - **Provides airlink authentication and encryption, but does not protect traffic crossing the Internet**
- **VPN Tunnels**
  - **End-to-end authentication and encryption from hot spot stations to corporate VPN gateways**

I. Hot Spot Subscriber Authentication

- **Web portal login is a proven method for controlling hospitality LAN visitor access to the public Internet**
  - **Redirect selected TCP ports (80,443) to secure login page**
  - **User is prompted for login/password**
  - **Credentials checked against a subscriber database**
  - **If login fails, station is still associated with AP, but cannot send traffic beyond access control point**



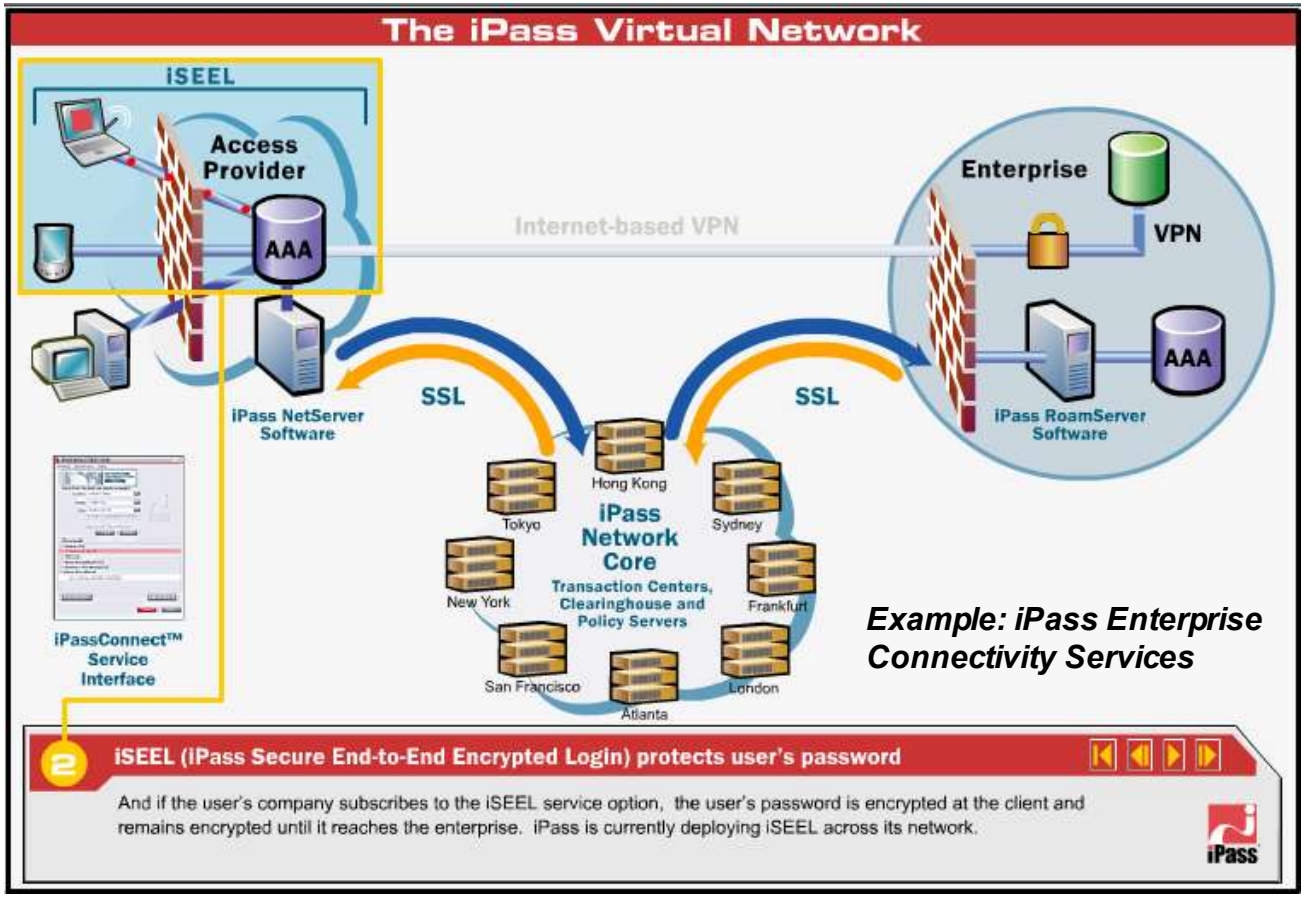
Focused on Operator's Needs

- **Benefits**
  - **Subscriber login (and enrollment) protected by SSL**
  - **No station reconfiguration or added software**
  - **Redirection is transparent to Web users**
  - **Integrates easily with RADIUS, existing user databases**
  - **AAA server records can feed existing billing systems**
- **Limitations**
  - **Confidentiality is limited to login/enrollment process**
  - **Subscribers that require VPN tunnels for ALL traffic (even Web traffic) can be a problem**
  - **No operator control over AP, DHCP resource consumption**
  - **No IT control over hot spot account creation, accounting**

Extending Corporate Control

- **Enterprise hot spot clients (e.g., iPass) may**
  - **Support hot spot finding and roaming**
  - **Secure login process end-to-end (user-to-enterprise)**
  - **Integrate with VPN for data protection, unified login**
  - **Enforce desktop security**
  - **Let IT control enrollment, authentication, billing**
- **But there are still limitations**
  - **Requires installed client and server software**
  - **Limited support for uncommon systems (e.g., PDAs)**
  - **Solution only covers operator's (roaming) footprint**
  - **Roaming infrastructure adds cost**

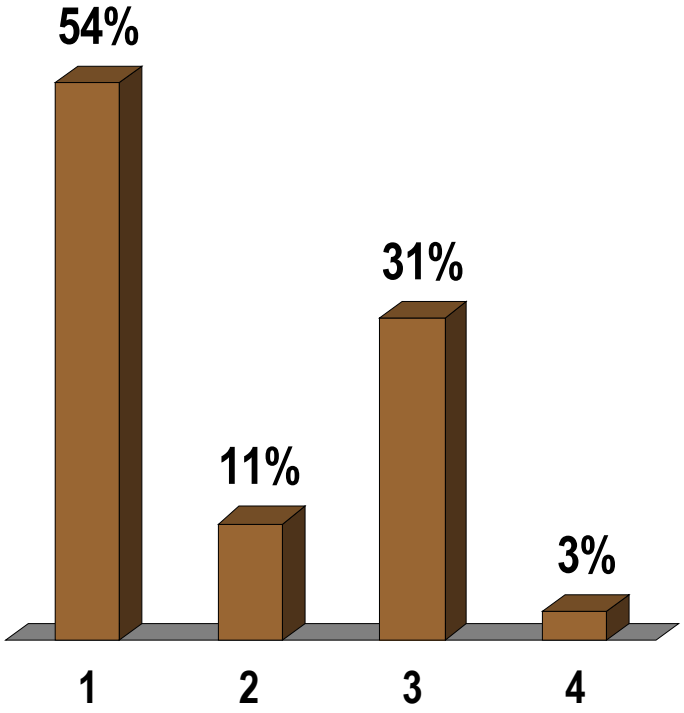
Roaming Authentication with Enterprise Servers



Example: iPass Enterprise Connectivity Services

When using a Wi-Fi hot spot to conduct company business, how do you pay for access?

1. **I don't use hot spots for business.**
2. **I pay for hot spot usage myself.**
3. **I expense hot spot fees to my employer.**
4. **My employer provides me with a corporate-paid hot spot account.**



II. 802.11 Link Security (WEP/WPA/WPA2)

- **Originally based on Wired Equivalent Privacy (WEP)**
  - **Uses RC4 to encrypt data over air between station and AP**
  - **Detects corruption, but does not prevent modification**
  - **Same shared key used for authentication and encryption**
- **Crippled by significant well-known vulnerabilities**
- **Issues for hot spots**
  - **Shared keys don't authenticate individual subscribers**
  - **Subscribers can decrypt each other's data with shared keys**
  - **How do you deliver/configure shared WEP keys?**

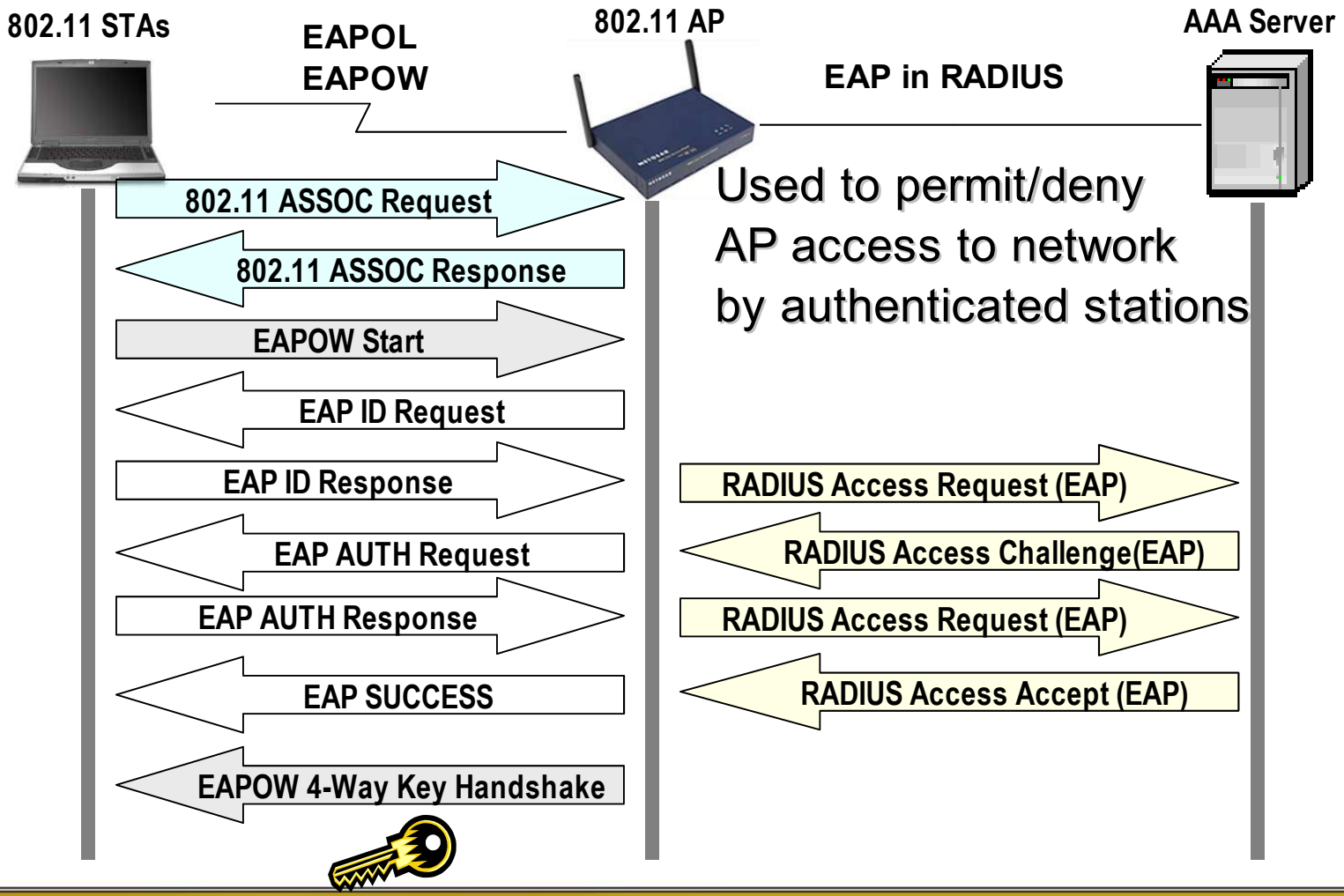
SO…most hot spots don't use WEP

Wi-Fi Protected Access (WPA)

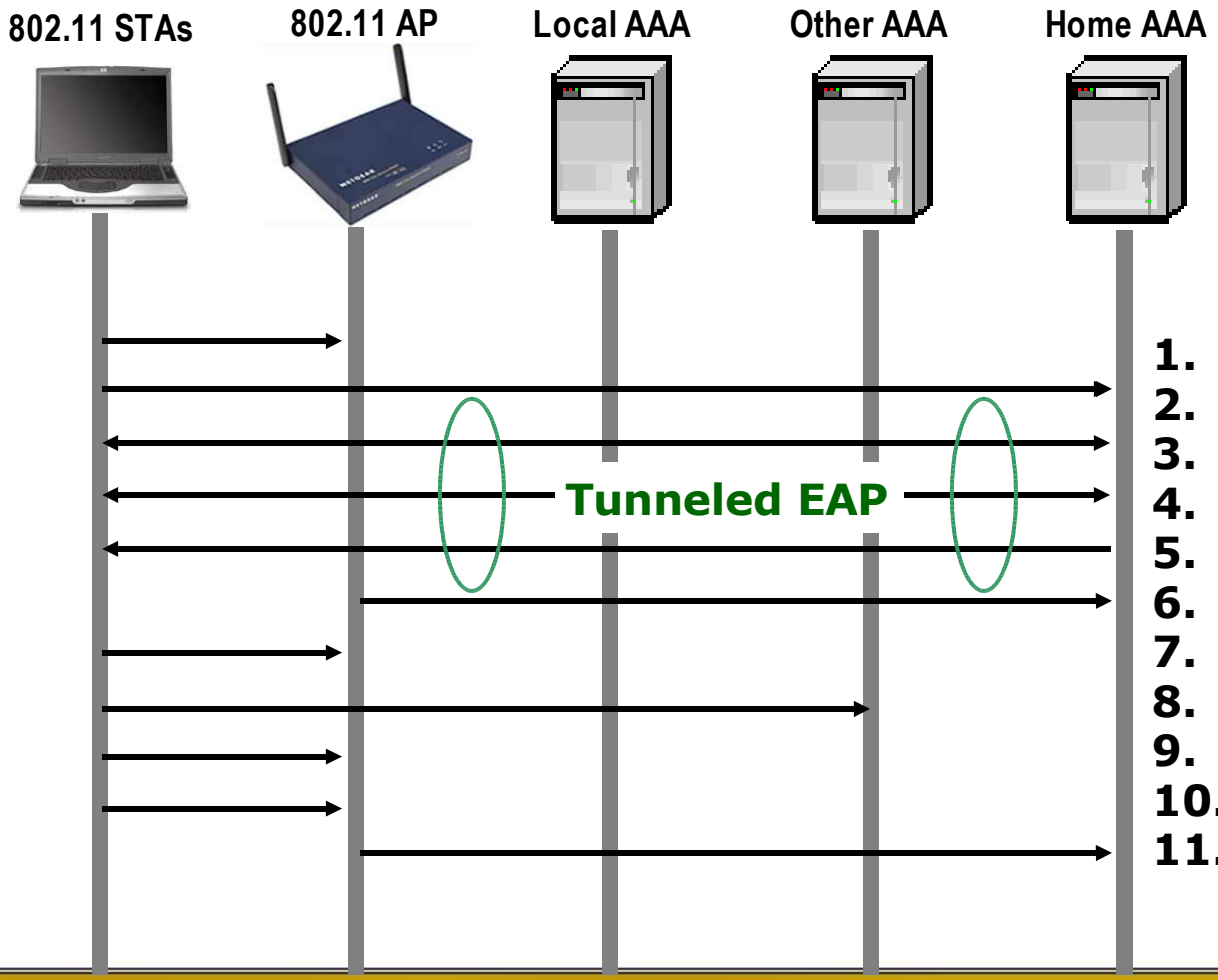
- **Wi-Fi Protected Access (WPA) avoids WEP flaws**
  - **All new Wi-Fi certified products must support WPA**
- **WPA2 is based on final 802.11i standard**
  - **First WPA2 products certified in September 2004**
- **WPA/WPA2 components include**
  - **Stronger encryption: RC4-TKIP, AES-CCMP**
  - **Stronger authentication: PSK, 802.1X Port Access Control**
- **Issues for hot spots**
  - **PSK still cannot authenticate individual users**

But what about WPA with 802.1X?

802.1X Port Access Control



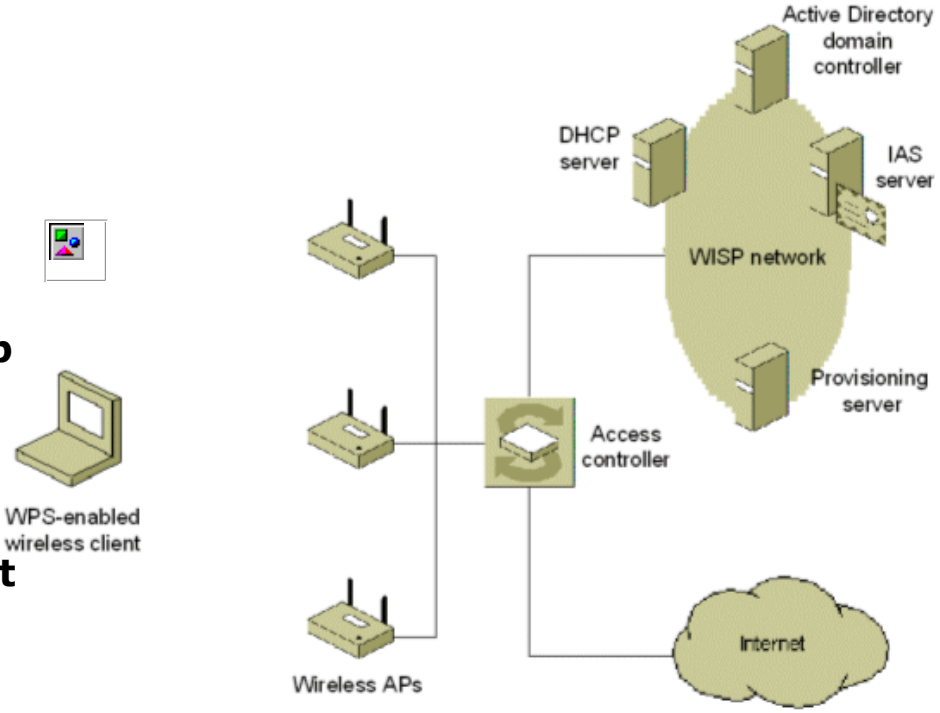
802.1X Roaming Authentication



1. 802.11 associate
2. Start 802.1X
3. Start TLS
4. Authenticate in tunnel
5. Home AAA okays use
6. RADIUS Start-Session
7. Get local IP address
8. Display welcome page
9. ...time passes...
10. 802.11 disassociate
11. RADIUS End-Session

Hot Spot Account Provisioning with 802.1X

- **MS Wireless Provisioning Services (WPS)**
  - **Supported by Win XP SP2 and 2003 Server SP1**
  - **Uses 802.1X/Protected EAP to automate hot spot sign-up**
- **Steps**
  - **Client discovers hot spot**
  - **Client authenticates as guest with 802.1X/PEAP-TLV**
  - **Client is provisioned and a new account is created**
  - **Client reauthenticated with 802.1X/PEAP-MSCHAPv2**



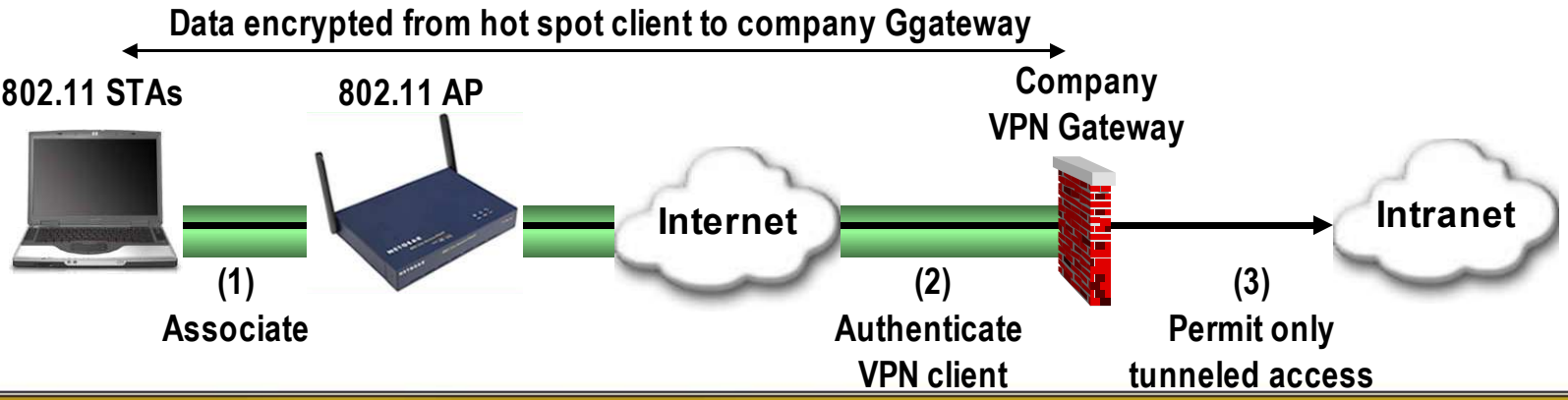
Source: Microsoft, December 2003 Wireless Provisioning Services Overview

802.1X in Hot Spots?

- **Potential benefits**
  - **Helps operator reduce resource exhaustion and attacks**
  - **802.1X can be transparent to authorized WLAN users**
  - **Authentication can be protected by TLS**
  - **Credential reuse and DB integration is possible**
  - **Access decisions made by operator or enterprise AAA**
  - **RADIUS messages can feed billing systems**
- **Potential obstacles**
  - **Lack of ubiquitous support for all OSes and WLAN cards**
  - **Lack of industry convergence on EAP types**
  - **WPA/WPA2 still wouldn't protect data over Internet...**

III. VPN Tunneling

- **Hot spot subscribers can (re)use VPN tunnels for**
  - **Confidentiality: Encrypt data across Internet**
  - **Data integrity: Detect packet modification in transit**
  - **Data source authentication: Prevent packet injection**
  - **System and/or user authentication**
- **Access controlled by VPN gateway at destination network, based on VPN client's identity**



PPTP VPN in Hot Spots?

- **Some SOHOs use PPTP VPNs because**
  - **PPTP client embedded in Win32, Pocket PC, Mac OS X, etc.**
  - **PPTP gateway can be Win32 server, SOHO firewall/router**
  - **Configuration is extremely simple**
  - **Supports common password authentication methods**
- **But PPTP has significant known vulnerabilities**
  - **Dictionary attacks, DoS attacks, buffer overflows**
  - **PPTPv2 fixed the worst flaws, but not all of them**
- **Used mostly in low risk/no-budget scenarios**
  - **E.g., HotspotVPN or Boingo Personal VPN for individuals**

IPsec VPN in Hot Spots?

- **Popular in site-to-site and remote access VPNs**
  - **Robust confidentiality, integrity, mutual authentication**
  - **Remote access VPNs usually have vendor extensions**
    - **User subauthentication, dynamic IP assignment, NAT traversal, policy updates, host security checkers**
- **IPsec VPN products are widely available**
  - **Gateway can be nearly any firewall or security appliance**
  - **Client is embedded in newer OSes (e.g., W2K/XP, MacOS X)**
  - **Clients supplied with VPN remote access concentrators**
- **Extending IPsec VPN to hot spots is common**
  - **Common challenges: Client install, complex config, NAT**
  - **Hot spot-specific challenges: Subscriber login, subnet mobility**

SSL VPN in Hot Spots?

- **SSL/TLS-based VPN market is growing**
  - **Station's existing browser serves as "SSL VPN" client**
  - **Natural fit for Web-enabled apps (e.g., Webmail)**
  - **Java/ActiveX or thin clients used to support non-Web apps**
- **Security properties vary by product, but most SSL VPNs**
  - **Authenticate gateway by certificate, user by password, token, etc.**
  - **Provide confidentiality and integrity from browser to gateway**
  - **Permit access to authorized servers, applications, objects**
- **Attractive to avoid VPN client config/software**
  - **Common challenges: Breadth of applications, maturity**
  - **Hot spot-specific challenges: Subnet mobility, securing data sent to sites on public Internet (inherent split tunneling)**

Mobile VPN in Hot Spots?

- **Some example "Mobile VPN" products:**
  - **AppGate (SSH)**
  - **Columbitech (WTLS)**
  - **Ecutel (Mobile IP)**
  - **NetMotion (proprietary UDP)**
- **Secure tunneling to VPN gateway, plus**
  - **Roaming across networks (e.g., 802.11<-> GPRS/EDGE, 1xRTT)**
  - **TCP session persistence when (briefly) disconnected**
  - **Interface selection based on bandwidth, cost, policy, etc.**
- **Attractive to mobile workers who frequently use both WWAN and WLAN and want fastest link w/o disruption**
  - **Common challenges: Client install, performance**
  - **Hot spot-specific challenges: Subscriber login, atypical ports**

One More Possibility...

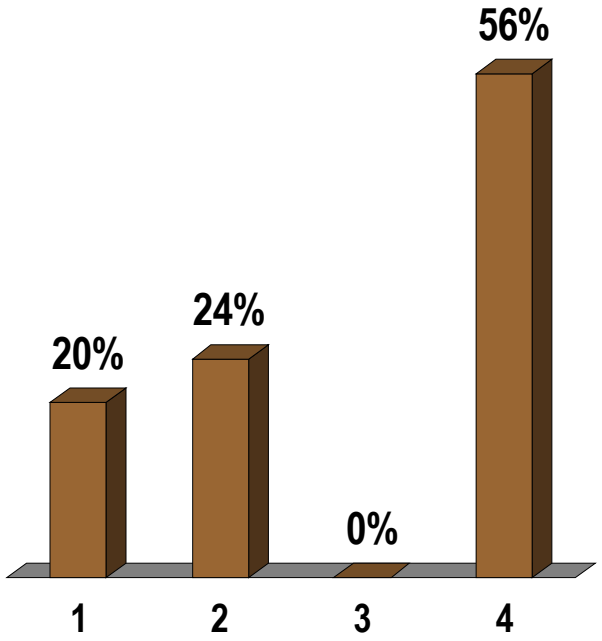
- **Do you really need a VPN for secure hot spot access to just one or two enterprise applications?**
- **Don't overlook application-specific security measures! Here are just a few examples:**
  - **Secure file transfer: SFTP, FTP over TLS**
  - **Secure desktop access: GoToMyPC, VNC over SSH**
  - **Secure e-mail: POP/SMTP over TLS, secure mail portals**
- **Consider when business needs can be met by a single application and don't already have a VPN**
  - **But it may be hard to stop unsecure public Web browsing**

VPNs Focus on Corporate Needs

- **Can help IT control hot spot-based remote access**
  - **Can often re-use VPN software, credentials, configs**
  - **VPNs alone don't control theft/abuse of hot spot accounts**
    - **See subscriber authentication discussion**
- **VPNs can reduce risk to corporate assets by protecting both wireless and Internet traffic**
  - **Scope and level of protection depends upon VPN type**
    - **Under IT control, no dependency on hot spot operator**
  - **VPNs alone don't stop stored data theft, virus infections**
    - **Treat hot spots as hostile environment**
  - **Consider hot spot clients that integrate with your VPN**

Have you ever used an IPsec, SSL, PPTP, or other VPN when visiting a Wi-Fi hot spot?

1. Yes, no problem
2. Yes, but the VPN doesn't always work
3. No, my company doesn't have a VPN
4. I don't use hot spots for business



Overcoming VPN Hot Spot Challenges

- **Some VPN obstacles encountered in hot spots**
  - **If your VPN requires an unusual protocol or port**
    - **Your VPN control or data traffic may be blocked**
  - **If your VPN client is mandatory**
    - **You may not be able to log into the hot spot Web portal**
  - **If your VPN client is incompatible with NAT**
    - **You may establish your tunnel but not send data**
  - **If your station roams while connected to the hot spot**
    - **Your VPN tunnel (and sessions) may be disconnected**
- **Fortunately, there are solutions…**

Hot Spot Firewalls vs. VPN

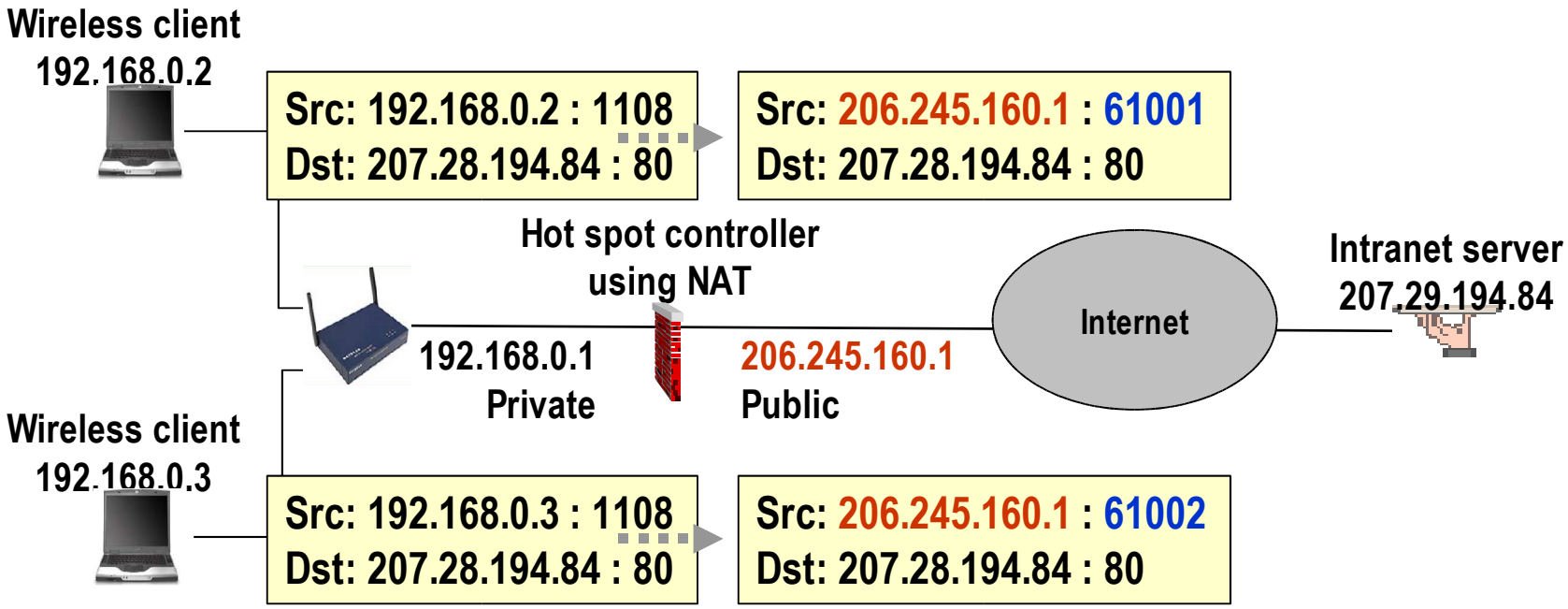
- **All hot spots allow HTTP/SSL on standard ports**
  - **So SSL VPNs have no trouble**
- **Most allow IPsec ESP (pr 50) and IKE (UDP 500)**
  - **Hot spots cater to business users, so IPsec is common**
- **Many don't filter outbound TCP/UDP ports at all**
  - **Layer 4 VPNs and secure apps often work just fine**
- **In other cases, you may be out of luck**
  - **Workaround: Send your VPN tunnel thru 80/443/etc.**
  - **Caveat: Not always practical or effective**

Hot Spot Login vs. VPN

- **Web portal logins often require station to exchange HTTP/SSL outside VPN tunnel**
  - **Workaround 1: User launches VPN client after login**
    - **Leaky and error-prone**
  - **Workaround 2: VPN client policy with split tunneling**
    - **Difficult to set selector that allows login only**
  - **Workaround 3: Use 802.1X instead of portal login**
    - **Feasible only if hot spot supports 802.1X login**
  - **Workaround 4: Hot spot client with automated VPN login**
    - **Feasible for some hot spot client/auth method combos**
  - **Workaround 5: VPN client with login pass-through/scripts**
    - **Better yet, but even less widely available**

Address Translation vs. VPN

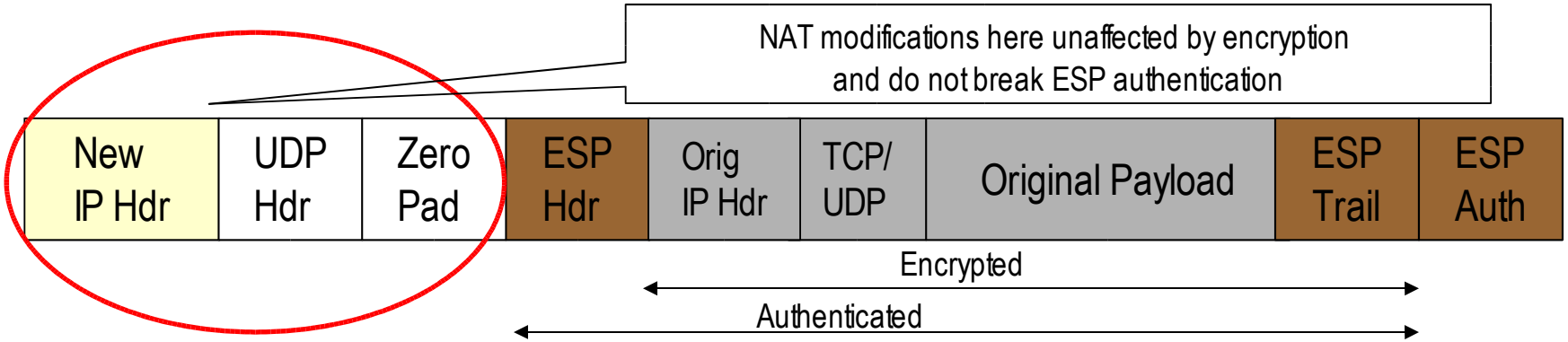
- **NAT* can "break" IPsec when applied mid-tunnel**
  - **Unfortunately, that's true in most public hot spots**



* Network and Port Address Translation (NAT/PAT)

NAT Traversal (NAT-T)

- **IETF-defined UDP Encapsulation work-around**



- **NAT-T helps a lot but it does not solve everything**
  - **Internet Key Exchange (IKE) multiplexing issues often remain**
  - **NAT still can't modify encrypted application payload (embedded IPs in FTP, IRC, SNMP, LDAP, H.323…)**

Wireless Roaming vs. VPN

- **Many VPNs bind tunnel endpoints to IP addresses**
  - **When WLAN station roams from network to network, it may get new physical IP addresses**
  - **Can disconnect VPN tunnel and application sessions**
- **Some wireless VPN products enable mobility**
  - **Some wireless gateways and switches share IPsec state or avoid changing station's IP to facilitate VPN roaming**
    - **More likely to encounter these inside enterprise WLANs**
  - **Mobile VPNs provide tunnel AND session persistence for roaming between networks (including WLAN-WWAN)**
    - **More relevant for hot spots, so I will focus on these**

Layer 2 Wireless Roaming

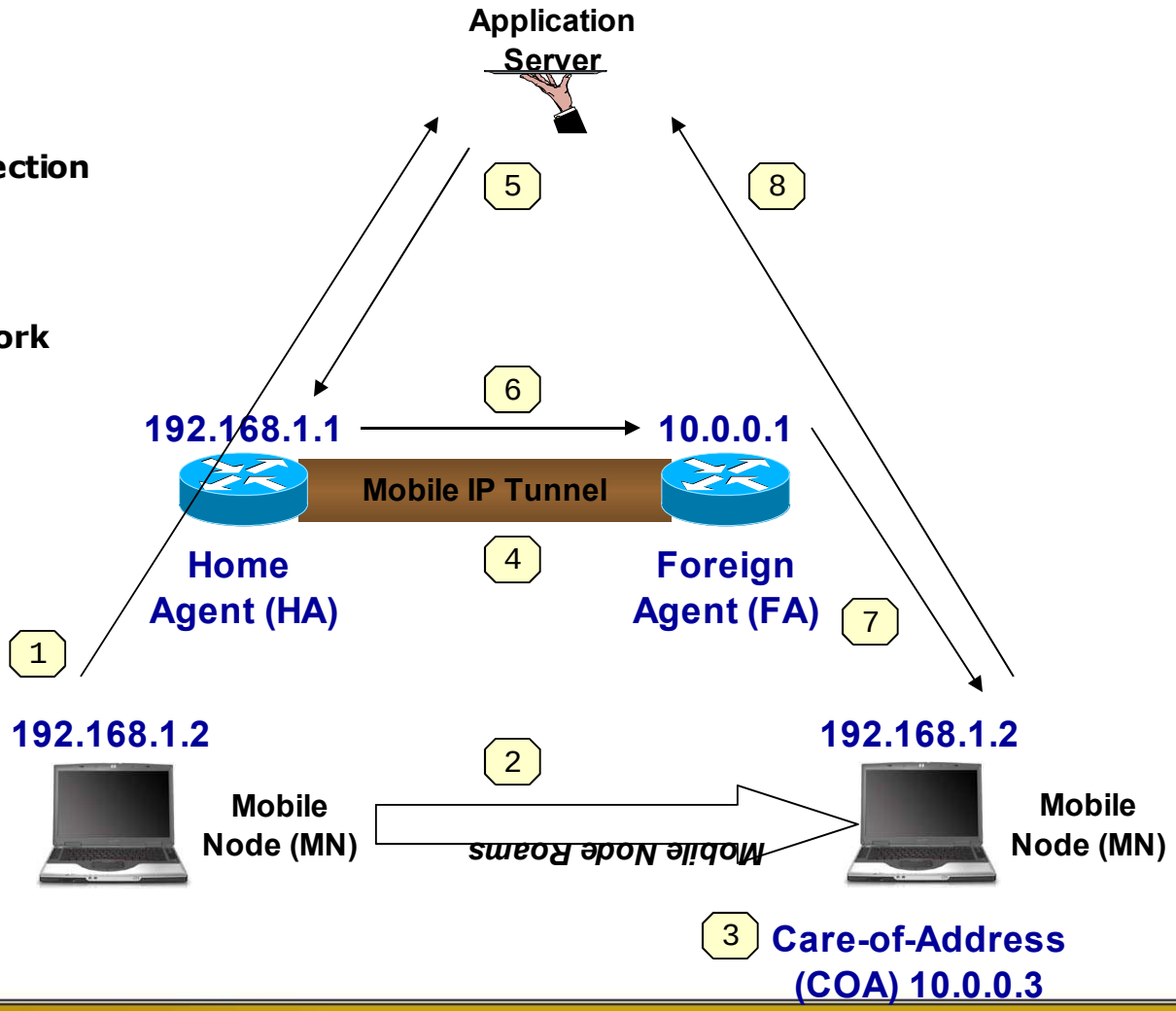
- **Stations listen to all channels to decide "best" AP**
  - **Criteria can include SSID, signal strength, errors, etc.**
- **When station decides to roam, it (re)associates**
  - **You don't have to physically move for roaming to happen**
- **L2 roaming is usually transparent, except when**
  - **802.1X requires interactive/long re-authentication**
  - **DHCP-enabled station fails to renew same IP**
- **L2 solutions to speed inter-AP roaming**
  - **IEEE 802.1f Inter-AP Protocol (IAPP)**
  - **IEEE 802.11i Key Caching, Pre-Authentication**
  - **IEEE 802.11r Fast Roaming Fast Handoff (new workgroup)**

Layer 3 Wireless Roaming

- **L3 roaming can occur when**
  - **802.11 station roams @ L2, but APs are in different subnets**
  - **802.11 station leaves AP coverage, roams to another network**
- **Hot spots may keep single-site APs in same L2 domain**
  - **But roaming from site to site, or operator to operator, almost always means roaming between L3 domains**
- **When a wireless station roams across subnets**
  - **Interface status and physical IP address change**
  - **For IPsec VPNs, authenticated peer no longer exists**
  - **VPN tunnel and sessions must be re-established**
  - **May take seconds, minutes, or longer, depending on coverage**
- **Mobile VPNs can solve one or both problems...**

One Workaround: Mobile IP

- **Mobile Node (MN)**
  - End user station
  - Can change network connection point without changing IP
- **Home Agent (HA)**
  - Router in MN's home network
  - Tracks location of MN, tunnels IP traffic to COA
- **Foreign Agent (FA)**
  - Router in network that MN is visiting at this moment
- **Care-Of-Address (CoA)**
  - MN's IP @ current location
  - Can be DHCP-assigned
  - Can be on FA or MN (CCoA)



Conclusion

- **Hot spot operators focus their security budget on subscriber authentication and access control**
  - **Using SSL portals or (in future) 802.1X**
- **Corporate IT should focus on controlling end-to-end authentication, confidentiality, integrity**
  - **Using VPN tunnels and host security measures**
- **These are complementary, not mutually exclusive**
  - **Expect WISP and enterprise WLAN vendor partnerships**
- **Individuals don't need to be unsecure**
  - **Use SSL-protected Web sites or hot spot VPNs**