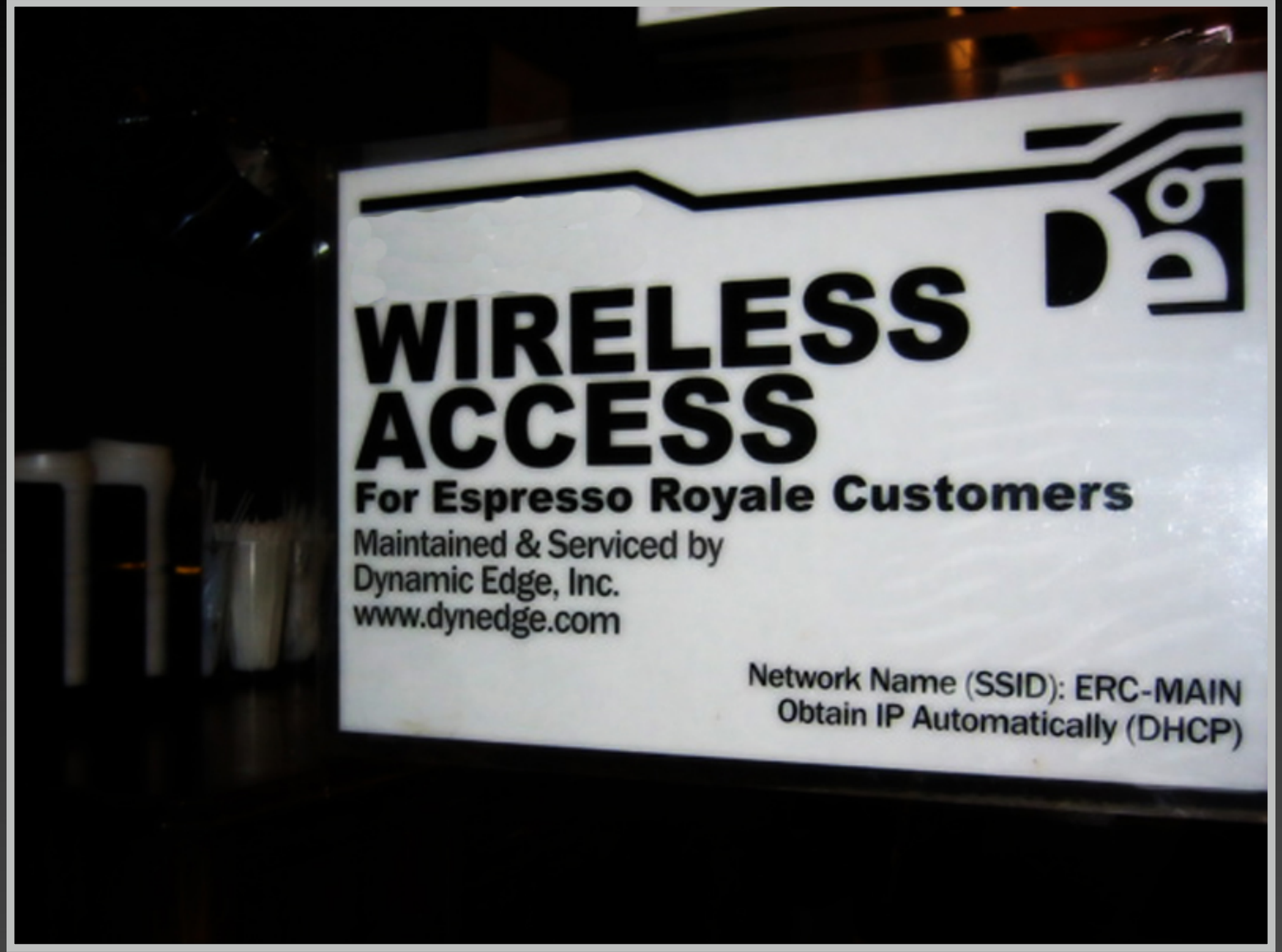
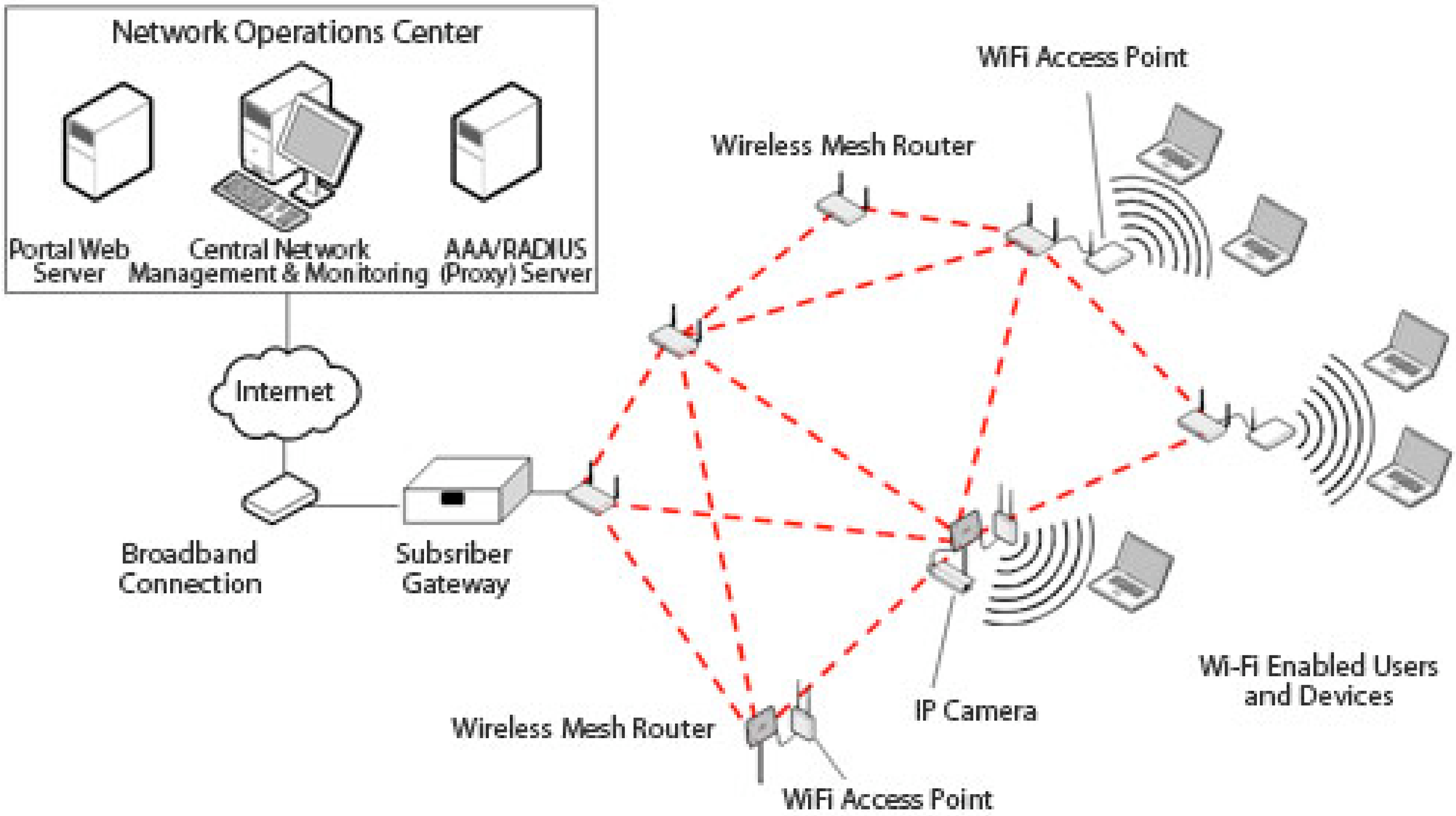
Wi-fi Hotspot Security

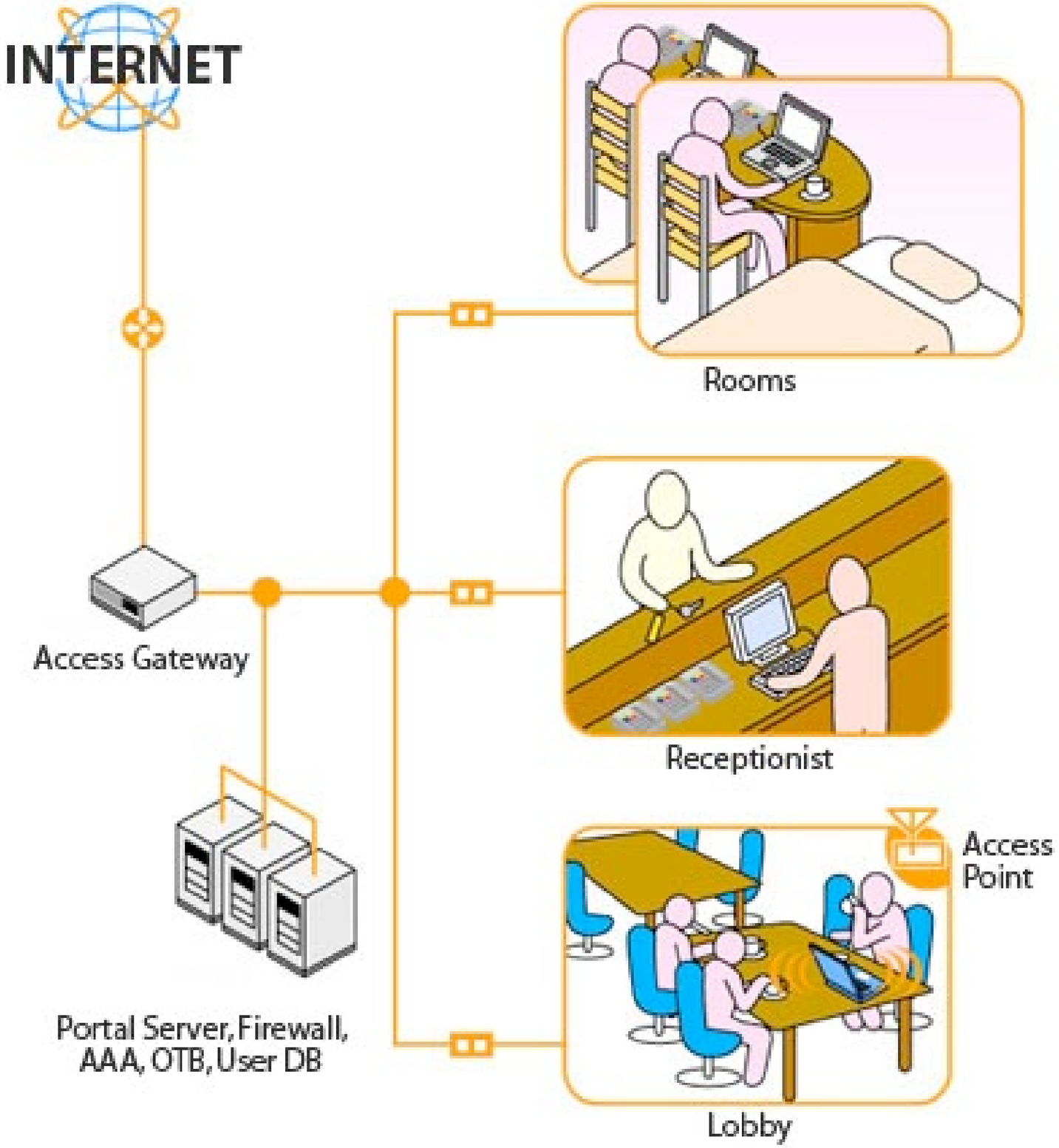
Jim Geovedi <jim@geovedi.com>

Information

- The printable version of this presentation is less cooler than the original version and also it’s already modified.


WIRELESS
ACCESS
For Espresso Royale Customers
Maintained & Serviced by
Dynamic Edge, Inc.
www.dynedge.com
Network Name (SSID): ERC-MAIN
Obtain IP Automatically (DHCP)


Network Operations Center
Portal Web Server
Central Network Management & Monitoring
AAA/RADIUS (Proxy) Server
Internet
Broadband Connection
Subsriber Gateway
WiFi Access Point
Wireless Mesh Router
Wireless Mesh Router
IP Camera
Wi-Fi Enabled Users and Devices
WiFi Access Point


INTERNET
Rooms
Access Gateway
Receptionist
Access
Point
Portal Server, Firewall,
AAA, OTB, User DB
Lobby

How To Use Hotspot

- Getting access
- Visit hotspot with wireless device
- Associate and get network configuration
- Open web browser and get redirected to login page
- Authenticate
- ... welcome to the Internet!

Getting Access

- Buy prepaid card
- Registration with Credit card
- Use now pay later (e.g. charge in your hotel room at **INCREDIBLE** price)
- Send text message (SMS) and get login information
- Social engineering
- Hacking (sniffing, bruteforcing, etc.)

Hacking The Hotspot

Motivations

- If you are **bored**
- If you want to do something bad (e.g. spamming, hacking, etc.)
- If you don’t have money or lazy to pay but need Internet connection

  will hack **for** bandwidth

Critical Points

- Network configuration
- Authentication methods
- 3rd party interfaces
- Misunderstanding the trust

Network Configuration

- IP address
- Transparent SMTP
- Network segregation

Authentication Methods

- Web Hacking Kungfu
  - SQL injection
  - Cross site scripting
- Piggyjacking

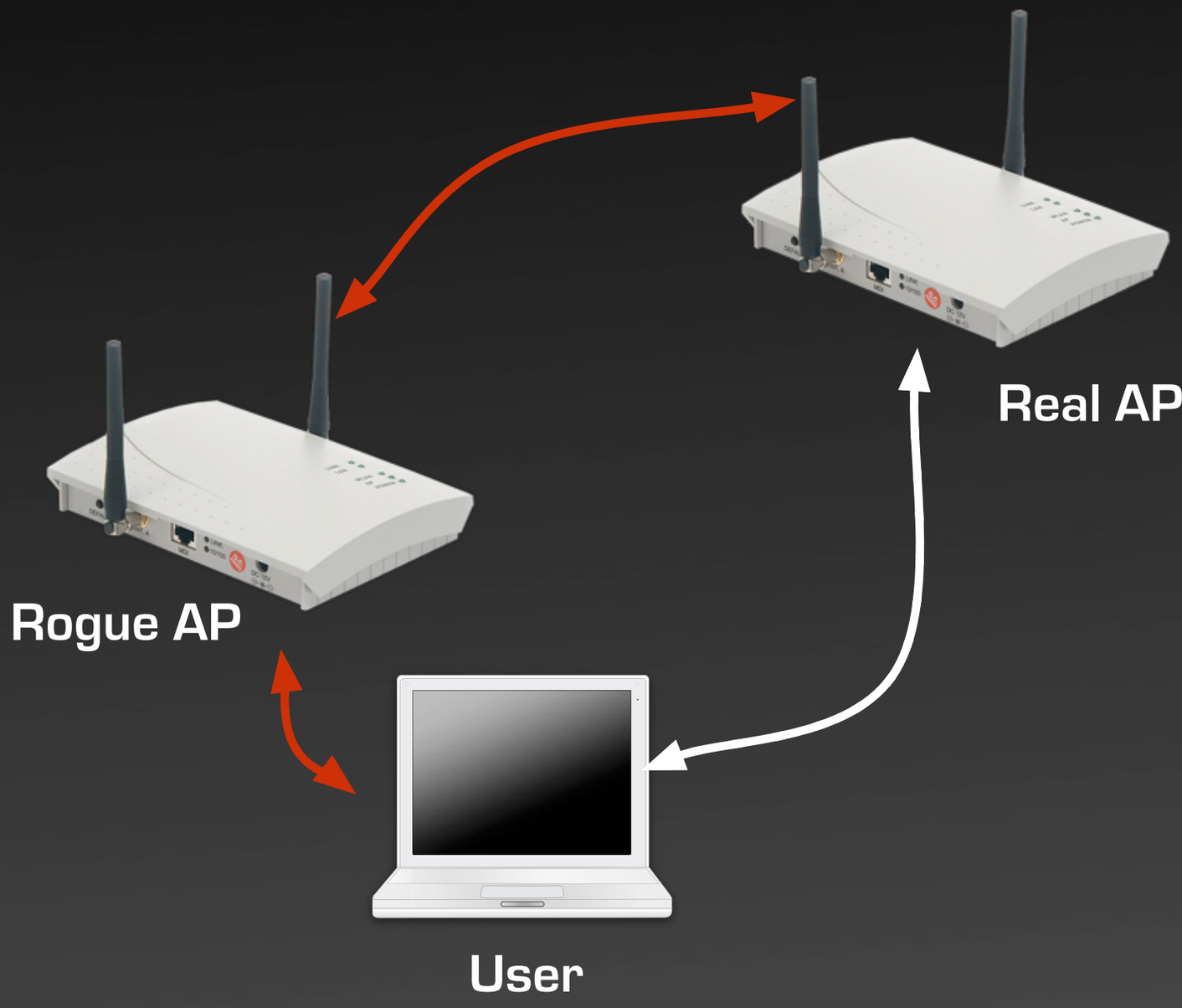
3rd Party Interfaces

- Integrated with other system:
  - Payment Management System
  - ISP's billing system

Misunderstanding Trust

- Unfiltered protocol or port tunneling
  - DNS (e.g. nstx, ozyman-dns, tunnelx)
  - UDP
  - ICMP
- Demo account (e.g. free access for 30min]
- Rogue 802.11 APs

Rogue 802.11 APs



Once you're in the middle...

- Capture (sniff) and manipulate the traffic
- Hack the client
- Automated attack tools
- FISHNet — where we can control client in a fishbowl environment

fISHNet

- Taking advantage of suspected client behavior
  - zero configuration
  - automatic update system
  - network services
- Fake services traps, exploiting clients, and create backdoor

Analysis On Some Hotspot Gateway Products

Product N

- Widely deployed at big hotels
- Vulnerabilities:
  - Can bill the Internet access to someone's room
  - Disclose the list of hotel guests to the Internet
  - Heavily depend on MAC address for identification. Easy to do piggyjacking

Product I

- Vulnerabilities:
  - Easy to bypass login by changing billing_method_id equal to 1 (one) — used by PMS
  - Only filter port 80... you can SSH to outside host and setup tunnel
  - Administration page is vulnerable to SQL Injection attacks

Product A

- Vulnerabilities:
  - You can do SQL injection in login page
  - You can manipulate the cookies
  - No network segregation

Defense Strategies

- Local AP awareness
- Customer education
- One-time authentication mechanism
- Do regular security assessment

- Write better code
- Don’t charge for hotspot access!