Guest Networking
Cisco on Cisco
Technology Seminar

Oisin MacAlasdair, Program Manager
—Network and Data Center Services, Cisco IT

Julie Nordquist, Program Manager—Cisco on Cisco (Host)
Agenda

- Business objective
- Architecture & design
- Deployment
- Adoption & benefits
- Future
Objectives & Constraints

Build a policy and architecture in which:

Non-Cisco visitors can access the Internet
   a) Where and when Cisco deems appropriate
   b) With Cisco's permission
   c) From Cisco’s infrastructure
   d) Secure, Authenticated, Recorded
   e) Minimal administrative burden
Architecture highlights

- Redundant policy enforcement points
  - Dual Building Broadband Services Manager
  - NAC Appliance to replace BBSM

- Globally distributed egress points
  - Guest traffic routed to geographically appropriate DMZ

- Internal guest networking portal for access code creation
  - Employees create access codes for their own visitors via “hotspot.cisco.com”

- “guestnet” SSID available on all access points worldwide
  - Every Cisco building has guest networking services

- Wired guest networking at selected sites
  - Training rooms, briefing centers etc.
Current wireless hotspot architecture

Guest Data

Corporate

Policy enforcement point in DMZ

WWW

Guest traffic tunneled in GRE

“http://hotspot.cisco.com”

Employee generates access code via portal

Employee generates access code via portal

Guest

Data

Data

Guest

Employee generates access code via portal

Employee generates access code via portal

Guest

Data

Data

Guest

Employee generates access code via portal

Employee generates access code via portal

Guest

Data

Data

Guest
Wireless SSID Architecture

Common SSID configuration for all access points

Two production data SSIDs
EAP-FAST authentication
CKIP encryption on one
WPA encryption on the other
Broadcast = NO

Guest networking SSID
Open authentication
No encryption
Broadcast = SELECTED

Cisco wireless voice users
Cisco wireless data users
NON-Cisco, guest WLAN users

Wireless voice SSID
EAP-FAST authentication
WPA encryption
QoS
Broadcast = NO
Globally distributed guest networks

San Jose
Amsterdam
RTP
Hong Kong
Bangalore
Singapore
Tokyo
Sydney
Baseline User Experience for Enterprise Guest Access

1. Authorized employee registers the guest via an intranet portal

2. One-time login is generated and distributed to the Guest User

3. Guest User connects to WLAN and opens Web browser

4. Redirected to login screen

5. To access the Internet, the guest user must login to the service

6. User then free to pass traffic to the Internet, Web, E-mail, VPN...
Guest Usage Trends - Global

- Average of 19,000 users per month (and rising)
- Over 228,000 guests past 12 months
- Over 330 buildings with wired & wireless guest services
## Support Cost Analysis – FY 2007

### Support Cost of hotspot.cisco.com

<table>
<thead>
<tr>
<th>Description</th>
<th>FY 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Guest Codes (Annual)</td>
<td>228,048</td>
</tr>
<tr>
<td># IT Support Cases (Annual)</td>
<td>578</td>
</tr>
<tr>
<td>Support Case Cost ($25 per case)</td>
<td>$14,450</td>
</tr>
<tr>
<td>Tier 2/3 Support (Est. 1 FTE)</td>
<td>$144,000</td>
</tr>
<tr>
<td><strong>Total Support Cost</strong></td>
<td><strong>$158,450</strong> or $0.69 per guest</td>
</tr>
</tbody>
</table>

### Support Cost pre-hotspot.cisco.com

<table>
<thead>
<tr>
<th>Description</th>
<th>FY 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td># of helpdesk calls required (without guest service)</td>
<td>228,048</td>
</tr>
<tr>
<td>Total cost of support ($25 x 228,048)</td>
<td>$5,701,200</td>
</tr>
<tr>
<td>Cost of “Hotspot.cisco.com” (see above)</td>
<td>$158,450</td>
</tr>
<tr>
<td><strong>Cost Avoidance</strong></td>
<td><strong>$5,542,750</strong></td>
</tr>
</tbody>
</table>
## Guest network benefits

<table>
<thead>
<tr>
<th>Category</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost Avoidance</strong></td>
<td>• Over $5M in potential support/administrative overhead avoided</td>
</tr>
<tr>
<td><strong>Improved Security</strong></td>
<td>• Controlled network access</td>
</tr>
<tr>
<td></td>
<td>• Uncontrolled, non-corporate clients segmented from enterprise network</td>
</tr>
<tr>
<td><strong>Improved Turnaround</strong></td>
<td>• Access codes can be generated within 15 seconds</td>
</tr>
<tr>
<td></td>
<td>• Batch codes can be generated for large groups</td>
</tr>
<tr>
<td></td>
<td>• IT administrative overhead avoided</td>
</tr>
<tr>
<td><strong>Staff Empowerment</strong></td>
<td>• Visitor sponsors responsible for generating code – no IT support needed</td>
</tr>
<tr>
<td><strong>Guest Experience</strong></td>
<td>• Branded network experience – Cisco viewed as technology leader</td>
</tr>
<tr>
<td></td>
<td>• “No hassle” network access</td>
</tr>
<tr>
<td><strong>Legal Protection</strong></td>
<td>• Users must digitally sign acceptable use policy with legal disclaimer</td>
</tr>
</tbody>
</table>
Future of guest networking in Cisco

- Adopting Advanced Services GuestNet Manager Turnkey solution
- BBSM to be replaced by NAC Appliance
- Additional features to Web front-end ([http://hotspot.cisco.com](http://hotspot.cisco.com))
  - Intelligent Access Code Allocation (limit access codes to sites with bandwidth constraints)
  - Proxy access code generation and other features.
- Improved redundancy for Hotspots (component of NexGen WLAN program)
- More End User & Administration enhancements
  - GuestNet Manager look and feel
  - Management software, improved admin, reporting, logging, etc.
Screen shots
Guest access code instructions
Printed and/or emailed to visitor

Name: John Doe
Company: Acme Enterprises
Site of Visit: San Jose, CA - Bldg 10
Start Valid Time: 2007-APR-02, 7:00 am
End Valid Time: 2007-APR-03, 7:00 pm
Access Code: ENTS659K
SSID: guestnet
WEP: none

NOTE: In your access code, there are no vowels. Any 0’s are zeros, versus the letter 0.

Requirements:

- A laptop or PDA with WLAN capabilities (802.11b). This functionality may be built into your device, or is supplemented with a wireless PCMCIA card.
- Latest wireless card drivers loaded to avoid association issues with Cisco’s advanced network.
- After enabling your wireless device, you may need to set your SSID to guestnet with no WEP (WindowsXP and Pocket PC should autodetect this setting).
- Your wireless device must be configured to obtain an IP address automatically (DHCP).
- Web Browser software. You can use any standard internet browser such as Netscape or Internet Explorer, on any operating system.

Instructions:

- Launch your web browser in any of our wireless enabled areas and you will be redirected to the Cisco Wireless Guest Access webpage.
- Simply enter the required information, scroll down and click ‘Agree’ to accept the terms and conditions. On the next page, enter your Access Code and click submit.
- You’re Connected!

NOTE: Please note that the Cisco Guest Hotspot service provides unencrypted access to the public Internet. You may wish to use VPN or encryption software for sensitive traffic and/or remote connectivity to your own enterprise network.

Legal disclaimer:

Access to the Cisco Guest Wireless Local Area Network (WLAN) service is provided for the use of authorized users only.
Authorized users must read, agree with and accept all of the terms and conditions contained in this notice before using the WLAN.

1. Cisco is providing you access to our Guest WLAN as a complimentary service for your convenience during your visit at Cisco. You acknowledge that (i) the WLAN service provides unencrypted wireless access to the Internet, and agrees you are responsible for the security of your system and any transmission you make or receive; and (ii) you understand the risks of unencrypted access to the Internet, and will take any necessary security precautions, including encrypting confidential transmissions, backing up any data, and protecting your system with a firewall and robust user authentication.

2. You agree that your activities on the WLAN shall not:
   a) Introduce any viruses, Trojan horses, worms, time bombs, cancelbots, other computer programming routines that may damage, disrupt or otherwise adversely interfere with, or permit unauthorized access to or execution of any system, data or personal information;
   b) Create any liability for us or cause us to lose (in whole or in part) the services of our suppliers;
   c) Interfere in any way with the integrity or performance of any network or any services provided by Cisco or connected thereto;
   d) Interfere in any way with the use and enjoyment of the WLAN by another;
   e) Use the WLAN for any illegal purpose;
   f) Infringe any third party’s copyright, patent, trademark, trade secret or other proprietary rights;
   g) Access any data or system which you are not authorized to access;

3. Cisco reserves the right to suspend or terminate services to any network for security, performance, and other purposes. Thus, you acknowledge and agree that Cisco may access, monitor, audit, intercept and disclose any such communications, data or information.

4. You agree that Cisco may not make certain Internet services available, and may revoke your access to this WLAN at any time for any reason with or without notice.

5. THIS WLAN IS PROVIDED "AS-IS" AND "WHERE-IS," WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED.

6. OUR LIABILITY, AND THE LIABILITY OF OUR SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AND SUPPLIERS, TO YOU IS LIMITED TO U.S. $100.00.
Guest picks up Broadcast SSID “guestnet”

Guest launches browser

Guest enters real user name

Cisco Wireless Guest Internet Access

Welcome to Cisco’s High Speed Internet Access

This service allows you to access the Internet from Cisco’s office when you are visiting Cisco. If you are a participant in a Cisco conference and you need to use the Internet, you can use your VPN client to access your home office.

Please enter your name below, then click Accept.

Full Name: [John Smith]

Access to the Cisco Guest/Wireless Local Area Network (WLAN) service is provided for the use of authorized users only.

If Cisco has not authorized you to access this service, you must logout immediately.

Authorized users must read, agree with and accept all of the terms and conditions contained in this notice before using the WLAN

1. Cisco is providing you access to our Guest WLAN as a complimentary service for your convenience during your visit at Cisco. You acknowledge that (i) the WLAN service provides unencrypted wireless access to the Internet, and agree you are responsible for the security of your system and any transmissions you make or receive; and (ii) that you understand the risks of unencrypted access to the Internet, and will take any necessary security precautions, including encrypting confidential transmissions, backing up any data and protecting your system with a firewall and robust user authentication.

2. You agree that your activities on the WLAN shall not:
   a) introduce any viruses, Trojan horses, worms, time bombs, cancelbots, other computer programming routines that may damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or personal information;
b) create any liability for us or cause us to lose (in whole or in part) the services of our suppliers;

c) violate any law, statute, ordinance or regulation (including, but not limited to, those governing export control, consumer protection, unfair competition, antidiscrimination or false advertising);

d) be defamatory, trade libelous, unlawfully threatening or harassing;

e) be obscene or certain child pornography;

f) infringe any third party’s copyright, patent, trademark, trade secret or other proprietary rights; or

g) involve any attempt to access any data or system which you are not authorized to access.

3. Cisco routinely monitors and logs communications over its networks for security, performance, and other purposes. Thus, you acknowledge and agree that Cisco may access, monitor, audit, intercept and disclose any such communications, data or information.

4. You agree that Cisco may not make certain Internet services available, and may revoke your access to this WLAN at any time for any reason with or without notice.

5. AS A COMPLIMENTARY SERVICE, THIS WLAN IS PROVIDED “AS-IS” AND “WHERE-IS,” WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED.

6. OUR LIABILITY, AND THE LIABILITY OF OUR SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AND SUPPLIERS, TO YOU IS LIMITED TO U.S. $100.00.

Clicking Disagree will close the window.

Guest reads legal banner and clicks “Agree”
Guest enters Access Code

Cisco Wireless Guest Internet Access

Welcome to Cisco's High Speed Internet Access

Please enter your access code.

Full Name: John Smith
Access Code: kdn870
Submit

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices Privacy Statement and Trademarks of Cisco Systems, Inc.
Guest is granted Internet access

No wireless encryption
Guest should use VPN
www.hotspot.cisco screenshot

Sponsor (Cisco employee) can create access code for guest
To learn more about Cisco IT experience with Cisco technologies and solutions, visit

Cisco on Cisco: Inside Cisco IT

www.cisco.com/go/ciscoit