



Cisco IT Technology Tutorial Guest Networking at Cisco



Oisín Mac Alasdair, Member of Technical Staff

July 2009

Produced by the Cisco on Cisco team within Cisco IT

Agenda

- NexGen WLAN overview
- Design details
- Adoption & benefits
- Management & troubleshooting
- Guest networking

What is guest networking

Cisco's original guest networking solution

Cisco IT's NexGen Guest Networking solution

Adoption & benefits

Guest networking design considerations

The future of guest networking at Cisco

What is guest networking?



What Is Guest Networking?

- Provision of network access, typically Internet access, to **noncorporate** users
- Differing service positioning
 - Amenity
 - Service differentiator
 - Security control
 - Revenue generator
- Legal liability protection and acceptable use a primary driver

How Is It Provided?

- Most commonly guest networking is provided through the “wireless hotspot” model
- Wireless service can be delivered via parallel guest network or third-party service provider
- Some enterprises offer both wired and wireless guest networking
- Usually static
 - Fixed SSID (wireless)
 - Fixed Ethernet ports (wired)
- The future lies with dynamic network access controls and intelligence

Guest Networking Solution Components

- A robust, enterprise-class guest networking solution has three components:

Provisioning Portal

Enable enterprise users to sponsor visitors, empower employees, create access tokens, distribute operational burden, etc.

Traffic Segmentation

Ensure guest traffic is securely segmented from the corporate network (WLAN, LAN, and WAN)

Access Control

Provide welcome screen, ensure guests are approved, validate identity, etc. (e.g., policy enforcement)

Cisco's Original Guest Networking Solution



Original Objectives and 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

Original Architectural Overview

- Dual BBSMs at 8 DMZ locations globalwide
- Internal web application for provisioning guest accounts
- GRE tunnels from each site to geographically appropriate DMZ
- No URL filtering, traffic monitoring, or logging
(except guest and sponsor ID, session start/stop time, and IP address)



Original Management and Reporting

- No centralized management capabilities
- Only partial integration into EMAN
 - Alerting on BBSM status
 - No IP address depletion alarms
 - No web application status alarms
- However, robust IP2 User reporting
 - On-demand report to identify guest ID, sponsor ID, session start/stop time, and IP address
 - Used to identify source of illegitimate or prohibited traffic (malware, P2P file sharing, copyright infringement, etc.)
 - Used only on request by Information Security team

So Why NexGen Guest Networking?

- Mature service based on obsolescent hardware and custom code
- Year-on-year growth exceeds 150 percent
- Averaging more than 28,000 sessions per month
- Low SLA, high service expectation
- Strong perception of high case load despite low numbers in relation to actual usage
- But . . . any impact is **high impact**

It Is Working . . . but Fix It Anyway

- Analyze case history for trends
- Improve resilience
- Address capacity constraints
- Lay foundation for future services
- Add capabilities

What Were Causing the Problems?

- Issues comprised three categories (in order of impact):
 1. Regular user support (65 percent of cases)

How do I create codes?, How do I use the service?, Can guests get Internet access?
 2. IP address depletion (16 percent of cases)

Too many guests for existing IP addresses
 3. Service components (8 percent of cases)

Related to the BBSM or the internally developed hotspot.cisco.com portal

Interpreting the Figures

- 65 percent of cases were calls for information

How do I create codes?, Can visitors use the Internet?, How does hotspot.cisco.com work?

- Addressed issues through service management and user education

User education and communication includes email newsletter stories, internal website stories, digital signage, online discussion forums, print collateral including handouts, posters, tabletop trifolds, and improved search smart tags (Intranet search)

Interpreting the Figures (cont.)

- 16 percent of cases related to IP address depletion

Issues are being addressed by the Secure Services Client (new wireless client software), disabling SSID broadcast and assigning new IP addresses acquired as part of ARIN submission

- 8 percent of cases related to solution components

BBSM and hotspot.cisco.com failures

These are being addressed by Phase 1 of NexGen project

- During the two-month period analyzed, there were more than 60,000 guest networking sessions for 159 cases

1 case per 377 users/sessions (0.003 cases per session)

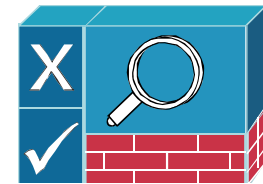
Cisco IT NexGen Guest Networking (NGGN) Solution



NGGN Components

- Cisco NAC Server (CAS)

The enforcement point. Located in the DMZ, functionally equivalent to the BBSM (except for authentication)



- Cisco NAC Manager (CAM)

Centralized management platform. Located in San Jose data center, manages all CASs. Also is the authenticator of guests

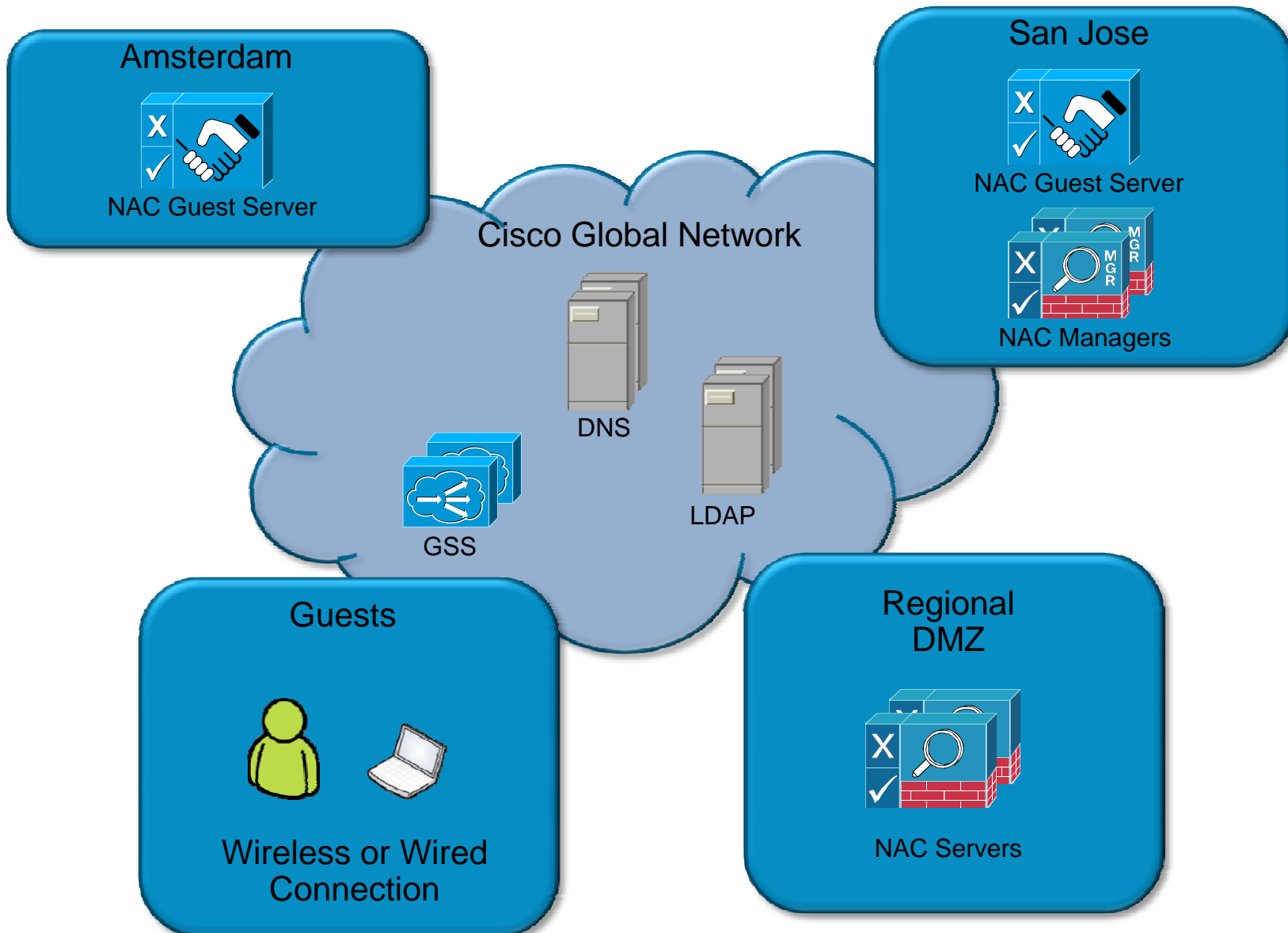


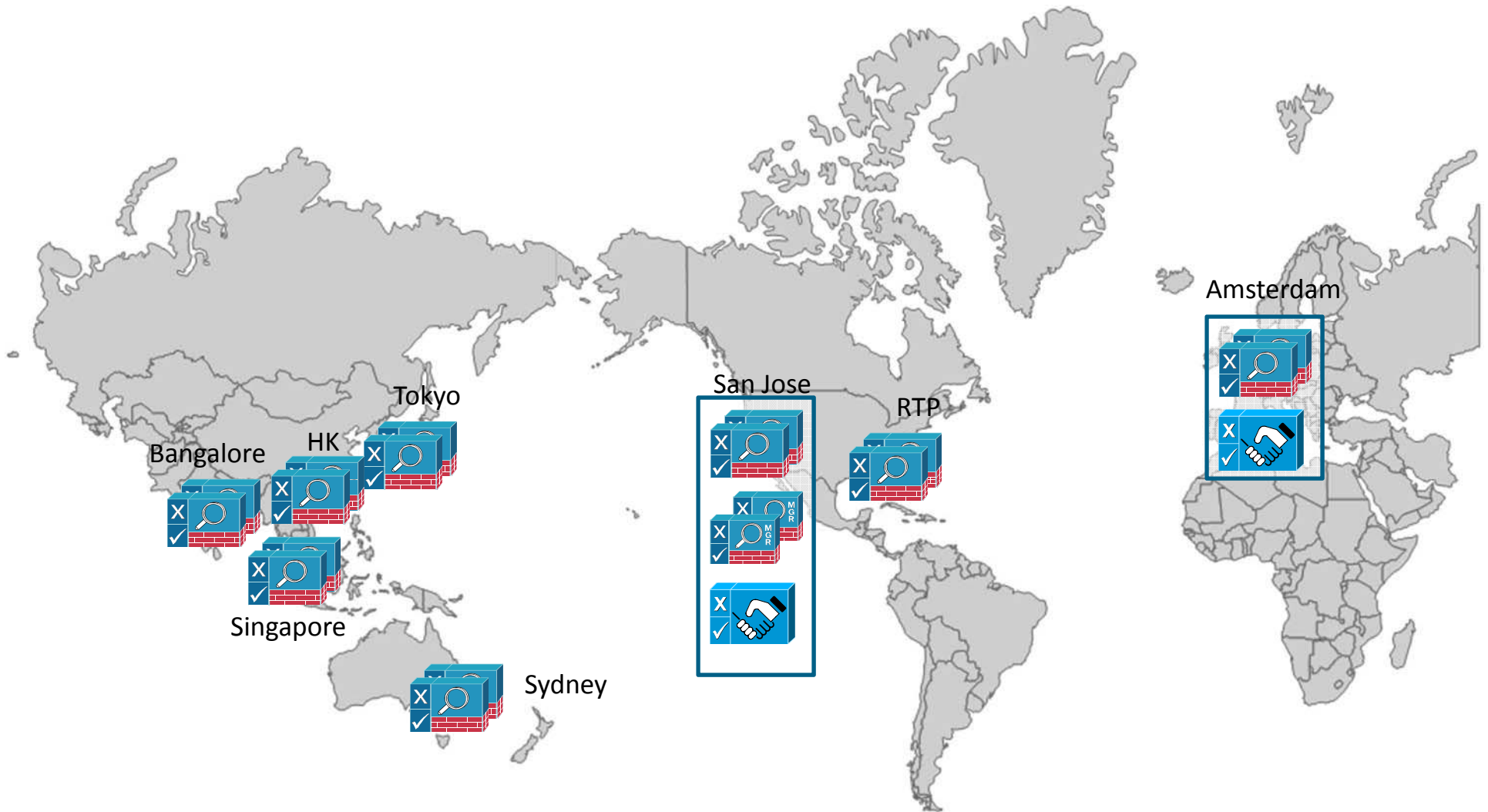
- NAC Guest Server (NGS)




Sponsor portal (hotspot.cisco.com). Located in Amsterdam and San Jose data centers, responsible for creating guest accounts and synchronizing accounts with CAM



NGGN Components (cont.)





-  Dual NAC Servers at 8 iPOPs
-  Dual NAC Managers at San Jose for global service management
-  Single NAC Guest Servers at San Jose and Amsterdam, in redundant pair configuration

IP Addressing

- Routable public IP addresses

No RFC 1918 due to:

- NAT reporting
- Lack of NAT infrastructure resilience
- Client compatibility

Easier IP2 User reporting

- Subnet pool size

Increased IP address pools by ~50 percent

Guest network details

- Globally distributed guest virtual LAN
- Pervasive guest wireless network
 - SSID: `guestnet`
- Selected wired ports mapped to guest virtual LAN
 - Reception areas
 - Permanently assigned training rooms
 - Customer Briefing Centres

Improved Management

- Single management portal (NAC Manager) for all enforcement point infrastructure (NAC Servers)
- IP address depletion alerts
- Wiki graphs and status
- EMAN integration
- Improved reporting for both admins and sponsors

Resilience

- Resilient infrastructure

 - Dual NAC Servers in each DMZ in high availability mode

 - Dual NAC Managers in San Jose in high availability mode

 - Dual NAC Guest Servers in replicated mode (active/active)

 - GSS front end to the NAC Guest Servers to connect sponsors with the geographically closest operational NAC Guest Server

Adoption and Benefits



Managed Guest Networking Solution Benefits

1 support call for every 322 sessions!

Guest Networking Support Cost	FY 2008
Number of guest codes (annual)	326,431
Number of IT support cases (annual)	1012
Support case cost (\$15 per case)	\$15,180
Tier 2/3 support (est. 1 FTE)	\$160,000
Total Support Cost	\$175,180 or \$0.53 per guest

Potential Support Cost pre Guest Networking	FY 2008
# of helpdesk calls required (without guest service)	326,431
Total cost of support (\$15 x 326,431)	\$4,896,465
Cost of hotspot.cisco.com (see above)	\$175,180
Cost Avoidance	\$5,071,645

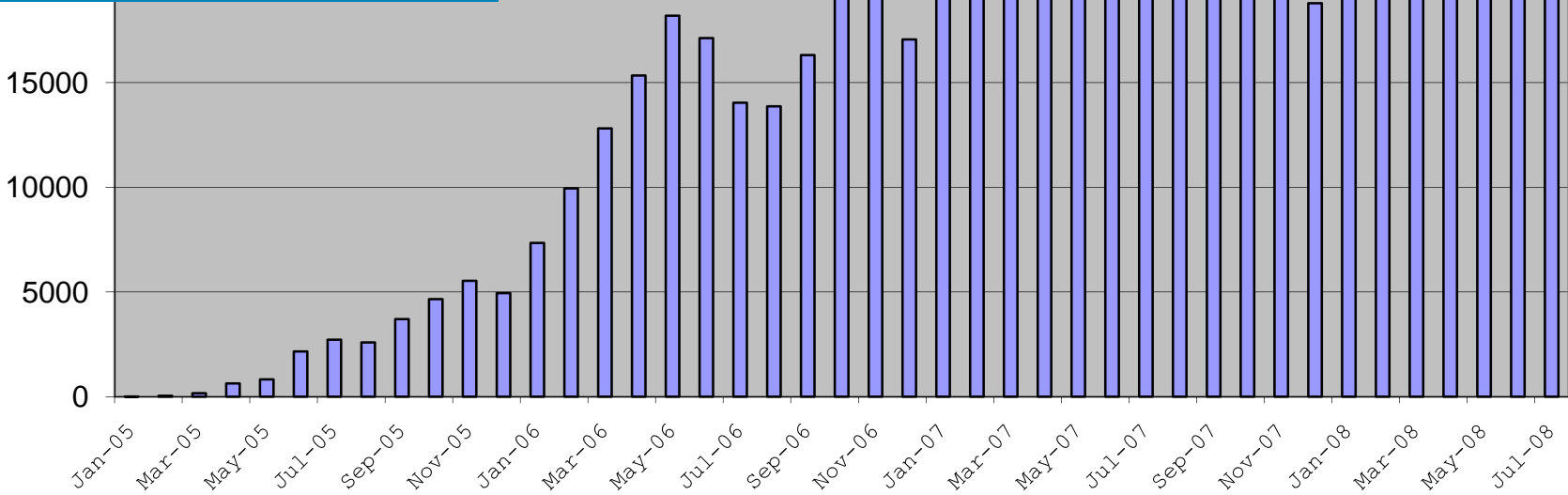
Cisco on Cisco Global Guest Usage Trends

Average 27,800+ users per month

More than 325,000 guests past 12 months

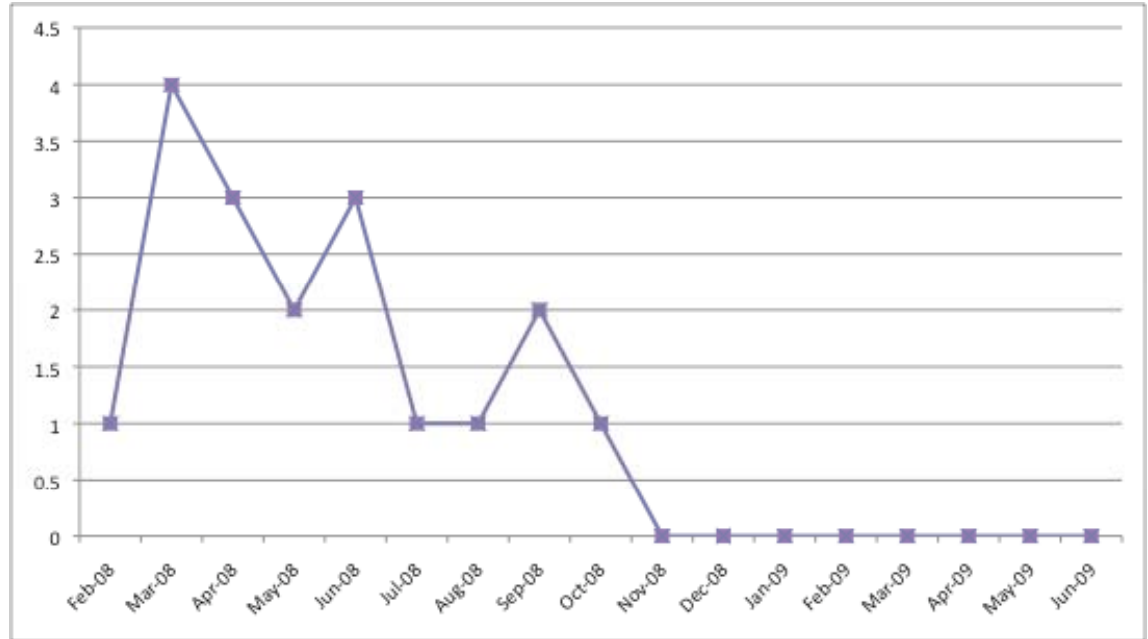
34,500 in April 2008 alone (highest ever)

More than 400 buildings with wired and wireless guest services



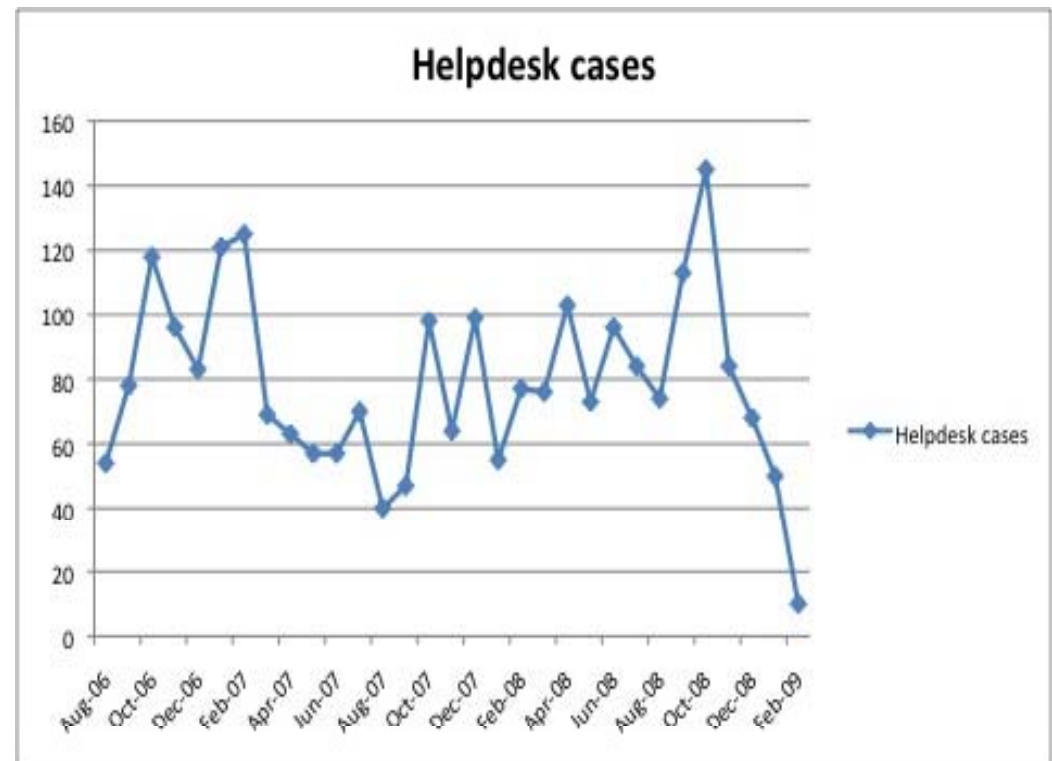
TCO Reduction

- High priority cases have fallen 100 percent
- Zero P1/P2 cases since service launched



TCO Reduction (cont.)

- Overall cases have fallen by more than forty five percent
- Average 89 cases per month in previous 12 months
- 30 cases per month in 2009
- Frontline cost savings of \$10k per annum



100 percent reduction in P1/P2 cases more impactful

NexGen Guest Networking Benefits

Cost Avoidance	<ul style="list-style-type: none">▪ More than \$5M in potential support/administrative overhead avoided
Improved Stability and Availability	<ul style="list-style-type: none">▪ 100 percent reduction in P1/P2 cases▪ 45 percent reduction in support load & costs overall
Improved Security	<ul style="list-style-type: none">▪ Controlled network access▪ Uncontrolled, noncorporate clients segmented from enterprise network
Improved Turnaround	<ul style="list-style-type: none">▪ Access codes can be generated within 15 seconds▪ Batch codes can be generated for large groups▪ IT administrative overhead avoided
Staff Empowerment	<ul style="list-style-type: none">▪ Visitor sponsors responsible for generating code – no IT support needed
Guest Experience	<ul style="list-style-type: none">▪ Branded network experience – Cisco viewed as technology leader▪ Localized portals for guests and sponsors (Phase 2)▪ SMS distribution of guest accounts (Phase 2)
Legal Protection	<ul style="list-style-type: none">▪ Users must digitally sign acceptable use policy with legal disclaimer

Benefits of Moving to NAC

- Enterprise-class solution
 - High availability, resilience
 - Feature richness
 - NAC Guest Server
- Active product
 - Well-defined roadmap
 - Integral to SDN/IBNS/NPF/IEN and more
 - TAC support
- Complimentary product suite
 - NAC Servers, Managers, and Guest Managers
 - Future integration improvements

The Future of Guest Networking at Cisco



NexGen Guest Networking: Phase 2

- Improved resilience
 - DMVPN for traffic segmentation
 - Dual active DMZ headend routers
 - CNRs for DHCP (removes SPoF)
- Improved scalability / manageability
 - DMVPN for traffic segmentation
 - Improved integration with EMAN
- Enhanced features
 - Multilanguage support
 - SMS of guest accounts
 - PDA optimized portal

The Future

- NAC products foundational to future security strategy
- Identity-enabled networking program will control access to the network based on **identity** and eventually **posture**

- Phased introduction of identity-enabled networking

Cisco Virtual Office (15,000+ sites)

NexGen Very Small Office (NGVSO)

Customer facing areas (CFA)

Meeting rooms

Heightened risk locations

Pervasive access control

Q and A



To learn more about real-world
Cisco IT deployments, visit
www.cisco.com/go/ciscoit

