

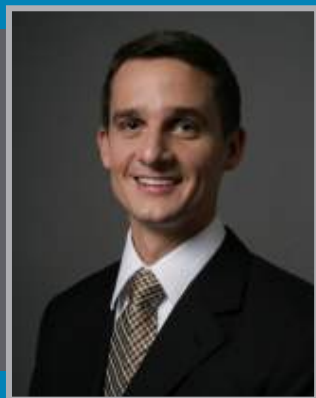


# Five Crucial Steps to Deploying a Secure Guest Network



**Cisco Mobility TV**

# Cisco Mobility TV



**Mobility TV Host**  
**Chris Kozup**

Senior Manager,  
Mobility Solutions  
Marketing,  
Cisco



**Brian Uffelman**

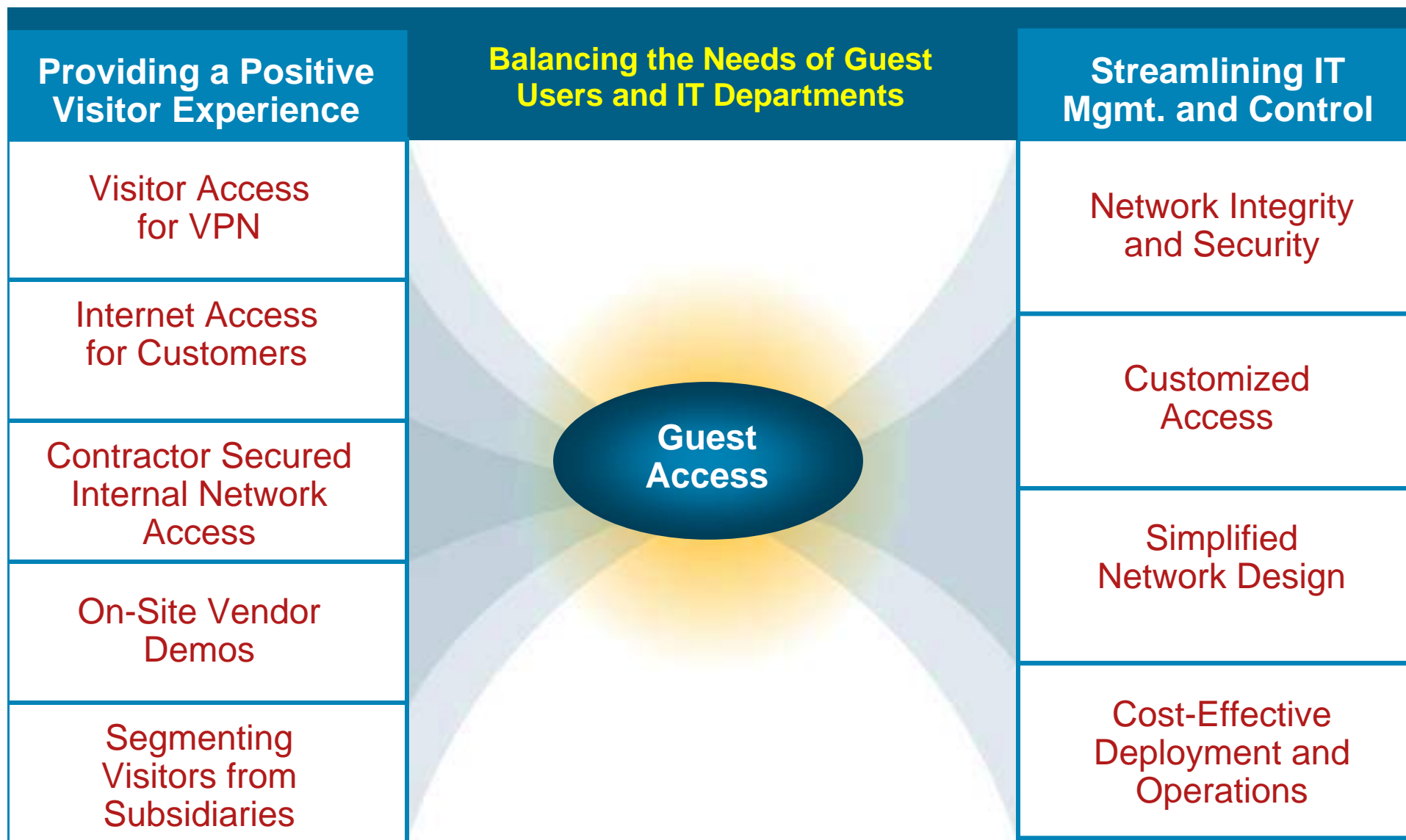
Product Manager,  
Wireless Networking BU,  
Cisco

# Agenda

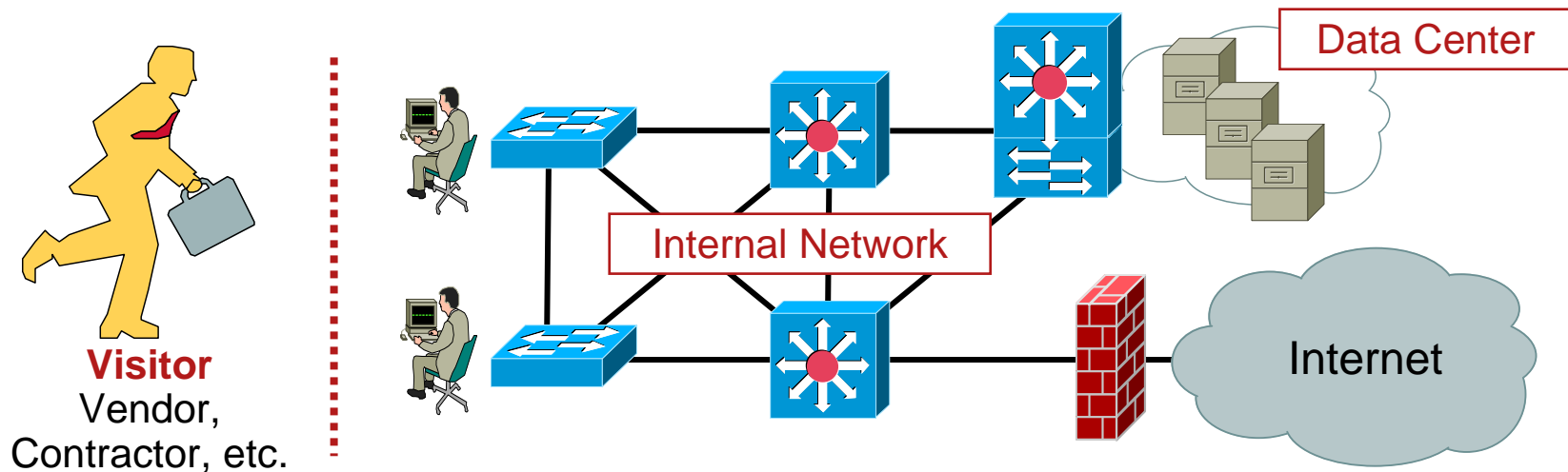
- 1 Guest Access Business Drivers
- 2 Network Segmentation
- 3 User Policy Management
- 4 Guest User Provisioning
- 5 Login Portal
- 6 Reporting and Billing
- 7 Cisco Guest Access Solutions



# Drivers for Guest Network Access



# The Challenge of the “Guest” User



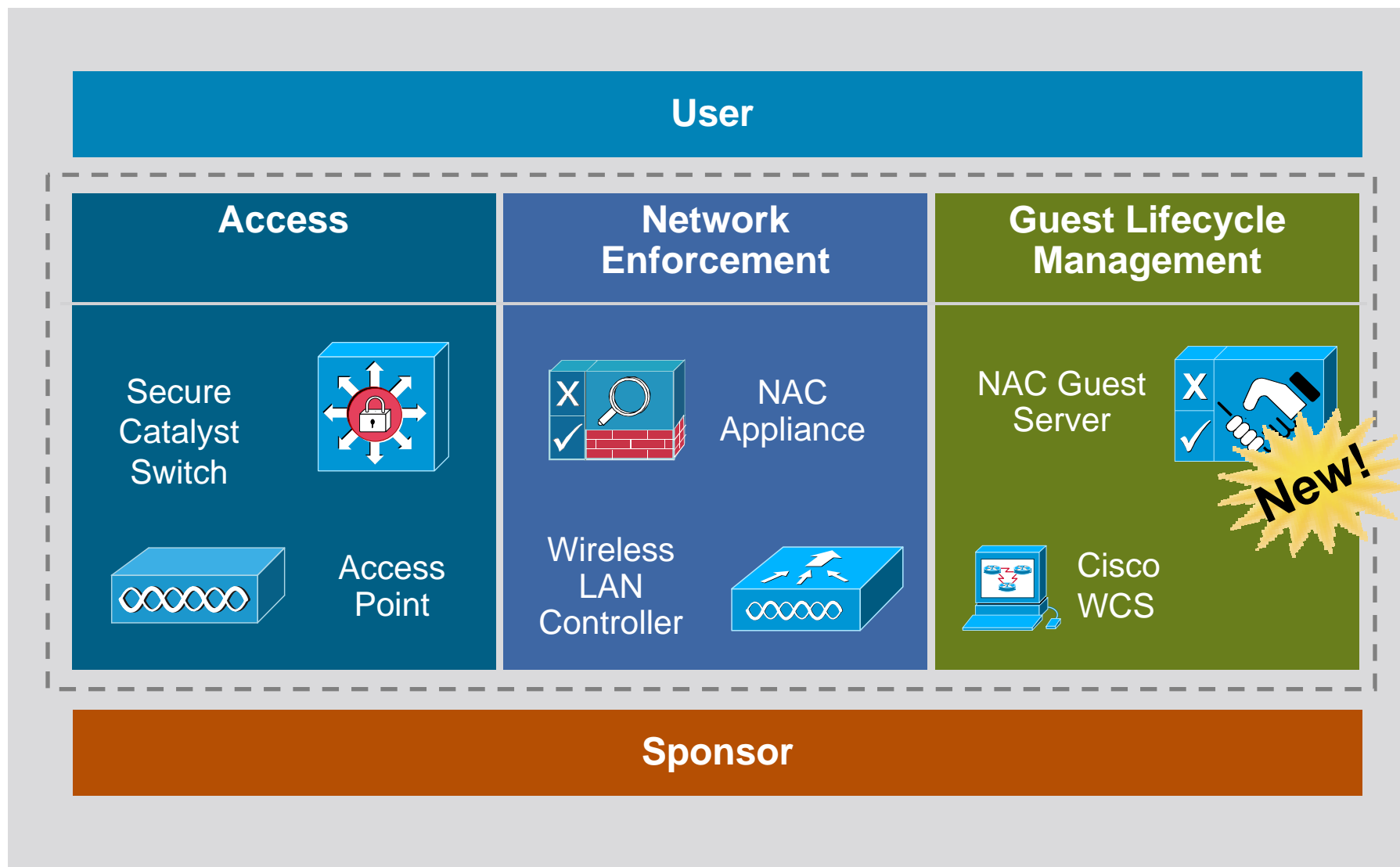
- Guest traffic should be segmented from the internal network
- Limited internal network access must be extended to guest securely
- “Guest network” must be cost-effective and non-disruptive
- Must not require guest desktop software or configuration

# Types of Network Users

Corporate Employees	Contractors/Consultants	Guests Users
<ul style="list-style-type: none"><li>▪ Need internal network access</li><li>▪ Can be role based to allow granular access if needs require</li></ul>	<ul style="list-style-type: none"><li>▪ Need restricted internal access</li><li>▪ Printers</li><li>▪ File shares</li><li>▪ Specific applications</li><li>▪ Device support</li></ul>	<ul style="list-style-type: none"><li>▪ Internet access only</li><li>▪ No need to access internal systems</li><li>▪ Segment access completely</li></ul>



# Guest Access Solution Entities



# Components of a Guest Access Solution

<b>Network Segmentation</b>	IT Admin Function
<b>User Policy Management</b>	IT Admin Function
<b>Guest User Provisioning</b>	Employee Function
<b>Login Portal</b>	Guest User Function
<b>Reporting, Billing</b>	IT Admin Function



# Network Segmentation

Network Segmentation

User Policy Management

Guest User Provisioning

Login Portal

Reporting, Billing

**Goal:** Ensure security by segmenting guest traffic from the internal network out to the Internet/DMZ (unsecured) edge

**Requirement:** Ease of network design, configuration and operation. Compatibility with existing network architecture

## Architectural Flexibility to Ease Deployment and Operations

### VLANs

- Use of a 802.1Q trunk for switch to AP connection to carry all the defined VLANs (one VLAN per SSID)
- VLAN isolation ceases if there is a Layer 3 hop between WLAN Controller Internet edge

### Tunneling—Ethernet over IP

- Provides tunneling (encapsulation) of traffic between WLAN Controllers out to Internet/DMZ edge
- Can carry traffic for all guest SSIDs in single tunnel—simplifies configuration and network architecture
- Can traverse Layer 3 networks—simplifies network design

# Ethernet over IP Tunneling

- EoIP tunnels logically segment and transport guest traffic between access layer and Internet edge
- Original guest's Ethernet frame maintained across LWAPP and EoIP tunnels
- Eliminates need for guest VLANs across network
- EoIP supported on all Cisco WLAN Controllers

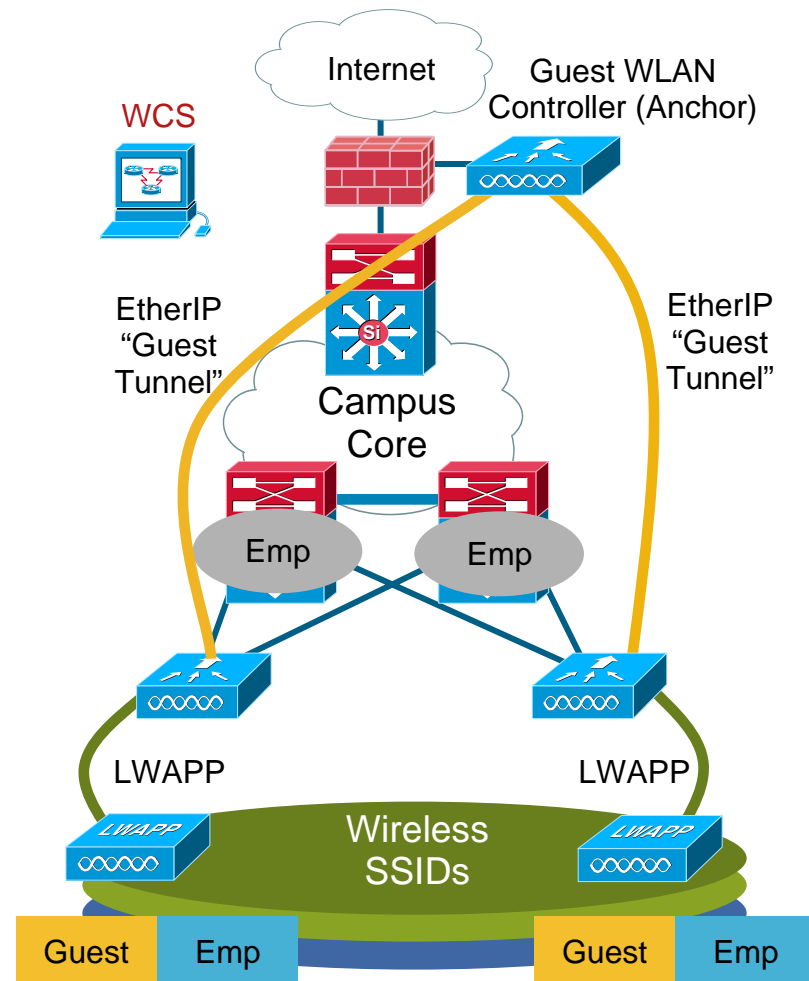
## Catalyst Wireless Services Module

## Cisco 4400 Series

## Cisco 3750 Series

Cisco 2100 Series (tunnel origination only; no termination)

## Cisco ISR WLAN Controller Module



# Enhancing Cisco Unified Wireless Guest Access with NAC

## Increased Flexibility

- **Dynamically provisioned wired guest ports**

Wired ports can be provisioned as “guest ports” at the time the guest logs in (no pre-provisioning of wired guest ports required)

- **Improves network scalability**

Centralizing authentication, posture assessment and remediation provides easier visibility to the network administrator

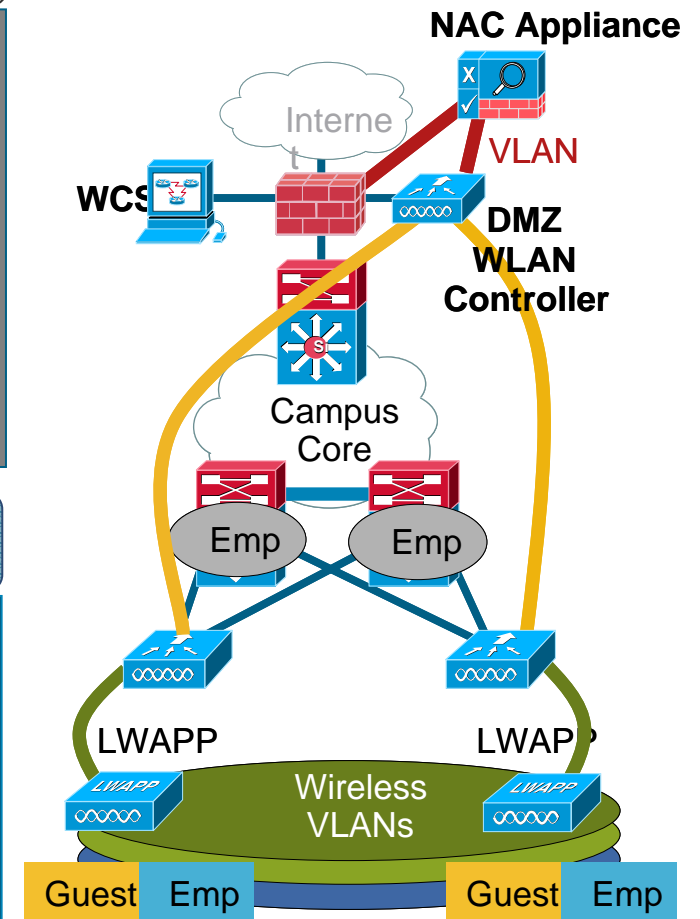
## Improved Policies

- **Provides new policy options:**

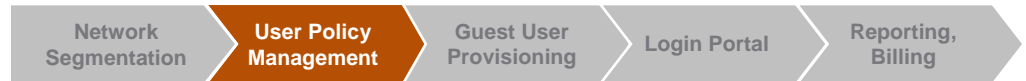
Integration with broader AAA (LDAP, AD)  
Granular access control  
Bandwidth policies

- **Added security benefits:**

Network privileges based on user roles/groups  
End-user security posture assessment, restriction and remediation



# Considerations for Guest User Policy Management



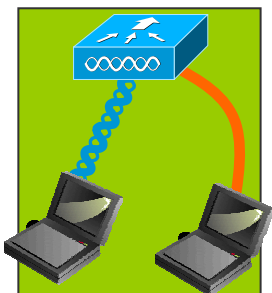
- What type of Guest Access is Required?
  - Wired?
  - Wireless?
  - Unified Wired and Wireless?
- What are the bandwidth policies for different types of guests?
- How are large numbers of guests provisioned?

# Comprehensive User Policy Management



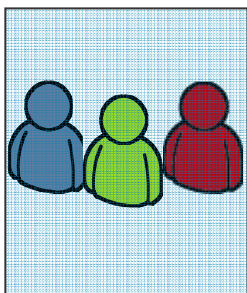
## Time Of Day Access

- Provision Guest Network Access based on when network usage is required
- Provides granular control over when guests can access network



## Technology Specific

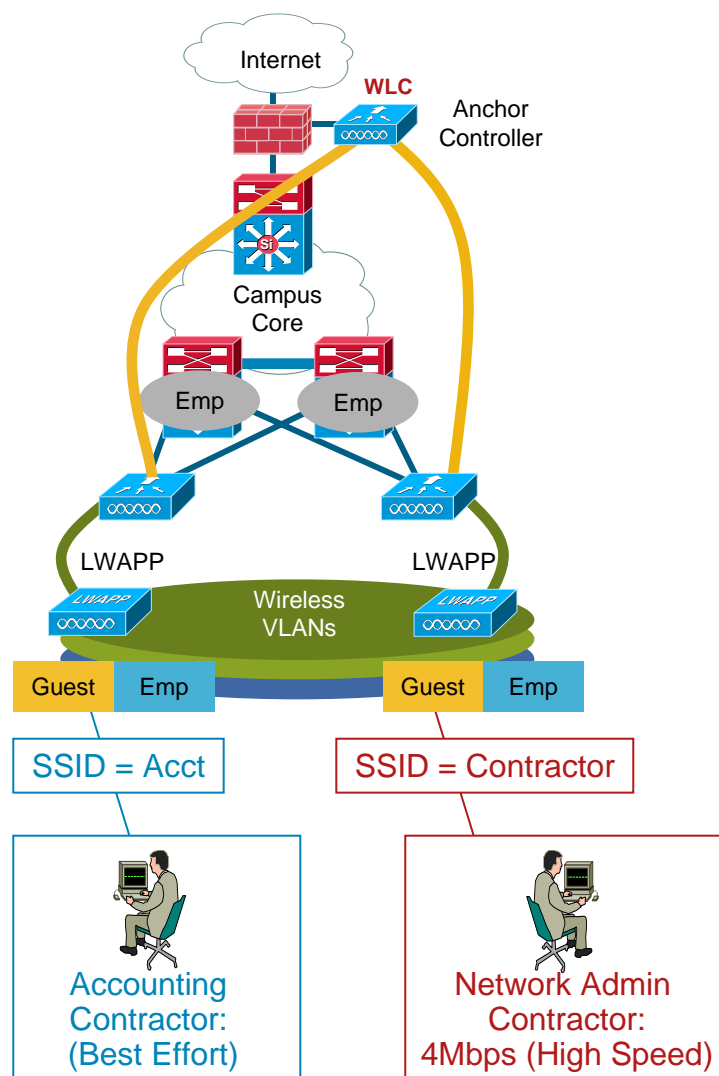
- Easily deployable universal (wired or wireless) guest access
- Deploying appropriate access per site, location, or network user population



## Per User/Role

- Extend network access based on the specific user or group
- Granular, role-based access enhances network security

# Guest Network Bandwidth Policy Controls



## Requirements

- Specify bandwidth limitations and policies by individual user or group
- Allocate resources by specific job function or throughput requirements

## Benefits

- Organization's overall network performance is enhanced
- Increased granularity and control improves network security

# Guest User Provisioning Enhancements

## Considerations Features

- Guest Provisioning Templates: Configure guests using pre-configured provisioning templates
- Bulk Guest User Provisioning: Providing the ability to configure multiple guest users at once

## Business Benefits

- Streamlines guest access provisioning
- Single-click guest provisioning reduces errors made by provisioning personnel
- Templates are defined and uploaded by the network administrator
- No “network knowledge” required to provision guests when locked-down templates are in place
- Reduces time required to provision multiple groups of users Bulk provisioning of multiple

# User Policy Management Options

## Integrated Device Management

- Web-based management GUI served from WLAN Controller
- Designed for small, single Controller deployments
- Basic user scheduling



## Cisco Wireless Control System

- Web-based multi-device management
- Designed for more feature-rich and multiple controller deployments
- Full-featured user scheduling
- Provision users by physical area



Versatile Management for Any Deployment Environment



# Deep Dive: Provisioning



Niall El-Assaad  
Product Manager  
Cisco

# Provisioning

- Who should create user accounts?
  - Receptionist/Lobby Ambassador
  - IT Security
  - Managers
  - Helpdesk
  - Anyone
- Allowing **anyone** to create accounts provides increased usage and will be just as secure



- Reduced cost
- Full audit trail

- Speed of access
- Ease of use

# Creating Guest Accounts



- What details should be captured?

Name

Phone

Company

Driving license number

Email

Anything else?

- When should the account be valid?

Allow setting start/end time

Pre-defined times: 2 hours, 1 day, etc.

By usage: 120 minutes from login,  
60 minutes in a day, etc

A screenshot of a web form for creating a guest account. It includes fields for 'Account Start: Time' (00:00), 'Date' (19 Sep 2007), 'Account End: Time' (23:59), 'Date' (19 Sep 2007), and 'Timezone' (America/Los\_Angeles). A calendar pop-up is visible, showing the month of September 2007. The calendar has a grid with days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and dates. The date 19 is highlighted in red, and the date 20 is highlighted in blue. The text 'Thu. 20. Sep 2007' is at the bottom of the calendar.

- Where should it be used, and what can the guest do?

# Delivering the Guest Account Details

**CISCO** Create a Guest User Account

Username: john@mycompany.com3  
Password: WCn5anO2  
Account Start: 2007-9-19 00:00:00  
Account End: 2007-9-19 23:59:00  
Timezone: America/Los\_Angeles

Print Email SMS

Enter the guest user name and then

© Cisco 2007

Send Account Information via Print-Out, Email, or SMS

**Guest User Details**

To access the network, please use the following credentials:

Username	john@mycompany.com3
Password	WCn5anO2
Start Time	2007-9-19 00:00:00
End Time	2007-9-19 23:59:00
Timezone	America/Los_Angeles

By logging on to the network you are agreeing to the terms and conditions of the acceptable use policy.

**Wired Connections**

Please plug your computer into a network connection and open a web browser. You will be able to access the network.

**Wireless Connections**

Please connect to the network with the SSID = guestnet. Then open a web browser. You will be able to access the network.

**Further Assistance**

If you require further assistance, please contact the network operations team at 555-5555.

**Acceptable Use Policy**

1.0 Overview

InfoTech's intention in publishing an Acceptable Use Policy is not to impose restrictions on employees, partners and the company from illegal or damaging actions by individuals, but to ensure that the company's information systems, including but not limited to computer equipment and FTP, are the property of InfoTech. These systems are to be used for business purposes in accordance with the company's policies. Please review Human Resources policies for further details. Effectiveness is a team effort involving the participation and support of every employee. Computer users must know these guidelines, and conduct their activities accordingly.

**Guest User Account Details - Message (Plain Text)**

Reply Reply to All Forward

File Edit View Insert Format Tools Actions Help

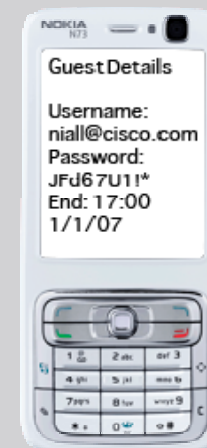
This message has extra line breaks.

From: guest-access-portal Sent: Tue 13/03/2007 14:07  
Subject: Guest User Account Details

The following guest user account has been created for you

Username: cs000013  
Password: E&CVNEXP  
Valid From: 2007-03-13 00:00:00  
Valid To: 2007-03-13 23:59:00

To access the network you must agree to the AUP



# User Login Portal

Network  
Segmentation

User Policy  
Management

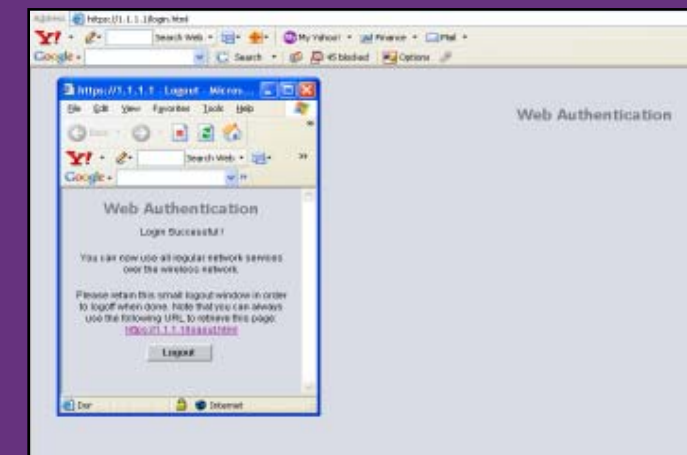
Guest User  
Provisioning

Login Portal

Reporting,  
Billing

- Login portal is the splash page guest users are directed upon associating to the guest SSID
- User will need to authenticate on this web page before browsing the Internet
- Is a fully customizable web page that typically includes:
  - Web authentication
  - Corporate branding (i.e. logo)
  - Usage agreement
  - Access to some content without authenticating (walled garden)

A screenshot of a web browser displaying a login portal. The address bar shows `https://1.1.1.1/login.html?redirect=1.1.1.1/login.html`. The page has a green header with the word "Login". Below the header, it says "Welcome to the Cisco wireless network" and "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work." There are two input fields: "User Name" with the value "guest1" and "Password" with masked characters "••••••". A green "Submit" button is at the bottom.



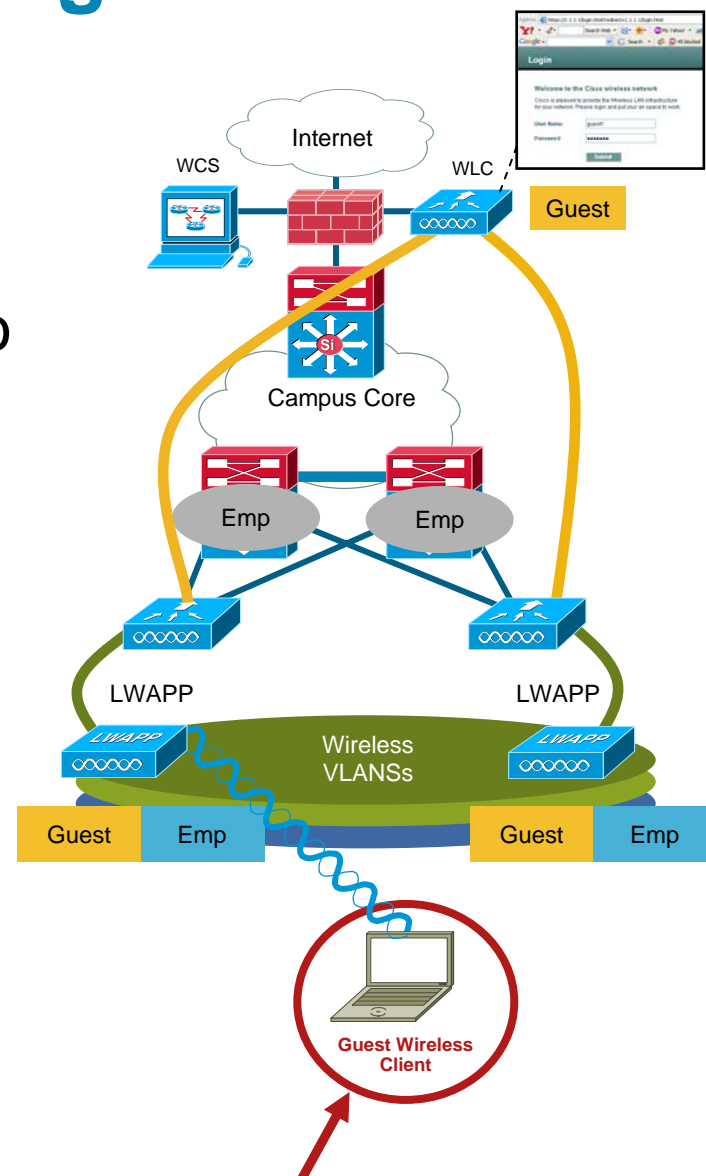
# How to Implement User Login Portal

## Simple and Customizable

- Upload an HTML file from the Wireless Control System (WCS) to the WLAN Controller
- The login portal is then served from WLAN Controller or external server

## Additional Considerations

- To help reduce help desk calls:
  - Login failure message portal
  - Logout verification message portal



# Deep Dive: Reporting and Billing



Niall El-Assaad  
Product Manager  
Cisco



# Audit and Reports

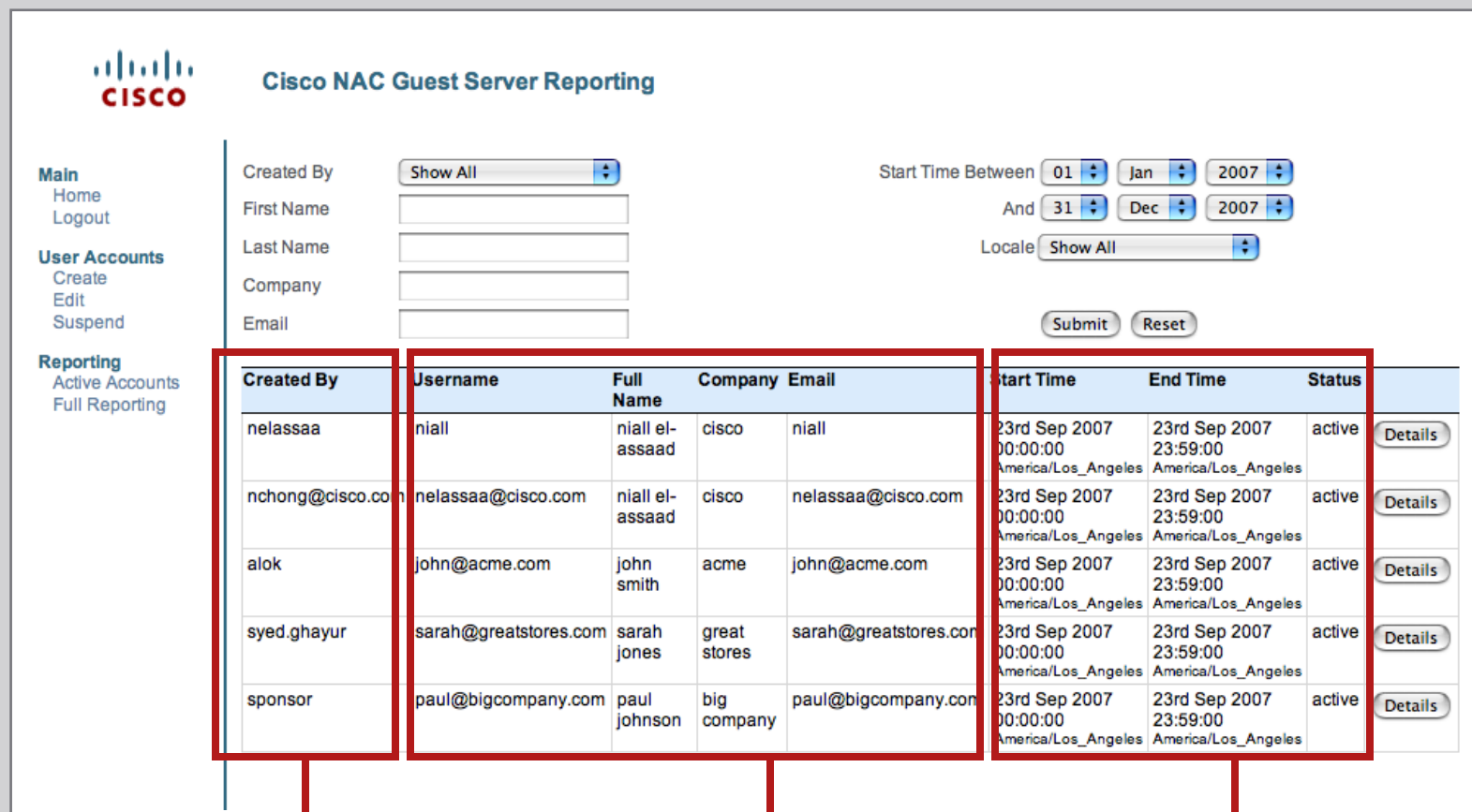
Network  
Segmentation

User Policy  
Management

Guest User  
Provisioning

Login Portal

Reporting,  
Billing



The screenshot shows the Cisco NAC Guest Server Reporting interface. On the left is a navigation menu with links: Main, Home, Logout, User Accounts (Create, Edit, Suspend), and Reporting (Active Accounts, Full Reporting). The main content area has a header with the Cisco logo and the title 'Cisco NAC Guest Server Reporting'. Below the header are search filters: 'Created By' with a 'Show All' dropdown, and 'Start Time Between' with date pickers for '01 Jan 2007' and '31 Dec 2007', plus a 'Locale' dropdown set to 'Show All'. There are 'Submit' and 'Reset' buttons. Below the filters is a table with columns: Created By, Username, Full Name, Company, Email, Start Time, End Time, Status, and a Details button. The table contains five rows of data. Red boxes highlight the 'Created By' column, the 'Username', 'Full Name', 'Company', and 'Email' columns, and the 'Start Time', 'End Time', and 'Status' columns. Red lines connect these highlighted areas to labels at the bottom: 'Sponsor Information' for the 'Created By' column, 'Guest Information' for the user-related columns, and 'Account Information' for the time and status columns.

Created By	Username	Full Name	Company	Email	Start Time	End Time	Status	
nelassaa	niall	niall el-assaad	cisco	niall	23rd Sep 2007 00:00:00 America/Los_Angeles	23rd Sep 2007 23:59:00 America/Los_Angeles	active	Details
nchong@cisco.com	nelassaa@cisco.com	niall el-assaad	cisco	nelassaa@cisco.com	23rd Sep 2007 00:00:00 America/Los_Angeles	23rd Sep 2007 23:59:00 America/Los_Angeles	active	Details
alok	john@acme.com	john smith	acme	john@acme.com	23rd Sep 2007 00:00:00 America/Los_Angeles	23rd Sep 2007 23:59:00 America/Los_Angeles	active	Details
syed.ghayur	sarah@greatstores.com	sarah jones	great stores	sarah@greatstores.com	23rd Sep 2007 00:00:00 America/Los_Angeles	23rd Sep 2007 23:59:00 America/Los_Angeles	active	Details
sponsor	paul@bigcompany.com	paul johnson	big company	paul@bigcompany.com	23rd Sep 2007 00:00:00 America/Los_Angeles	23rd Sep 2007 23:59:00 America/Los_Angeles	active	Details

**Sponsor  
Information**

**Guest  
Information**

**Account  
Information**



# Detailed Information

t [Reset](#)

	End Time	Status	
17	23rd Sep 2007 23:59:00	active	<a href="#">Details</a>
angeles	America/Los_Angeles		
17	23rd Sep 2007 23:59:00	active	<a href="#">Details</a>



### Cisco NAC Guest Server Detailed Report

**Main**  
[Home](#)  
[Logout](#)

**User Accounts**  
[Create](#)  
[Edit](#)  
[Suspend](#)

**Reporting**  
[Active Accounts](#)  
[Full Reporting](#)

Detailed Login Report for: paul@bigcompany.com

NAS IP Address	Users IP Address	Logged In	Logged Out	Duration
192.168.137.3	10.10.10.2	23rd Sep 2007 12:00:00 America/Los_Angeles	23rd Sep 2007 13:00:00 America/Los_Angeles	1:00:00

[Back to Reports](#)

# Paying for Internet Access

## Enterprise

- Internal chargeback
- Customer reporting
- Data export
- Integration with internal systems

## Hospitality

- Credit card payments
- Pre-paid accounts
- Virtual operator support
- Payment management systems

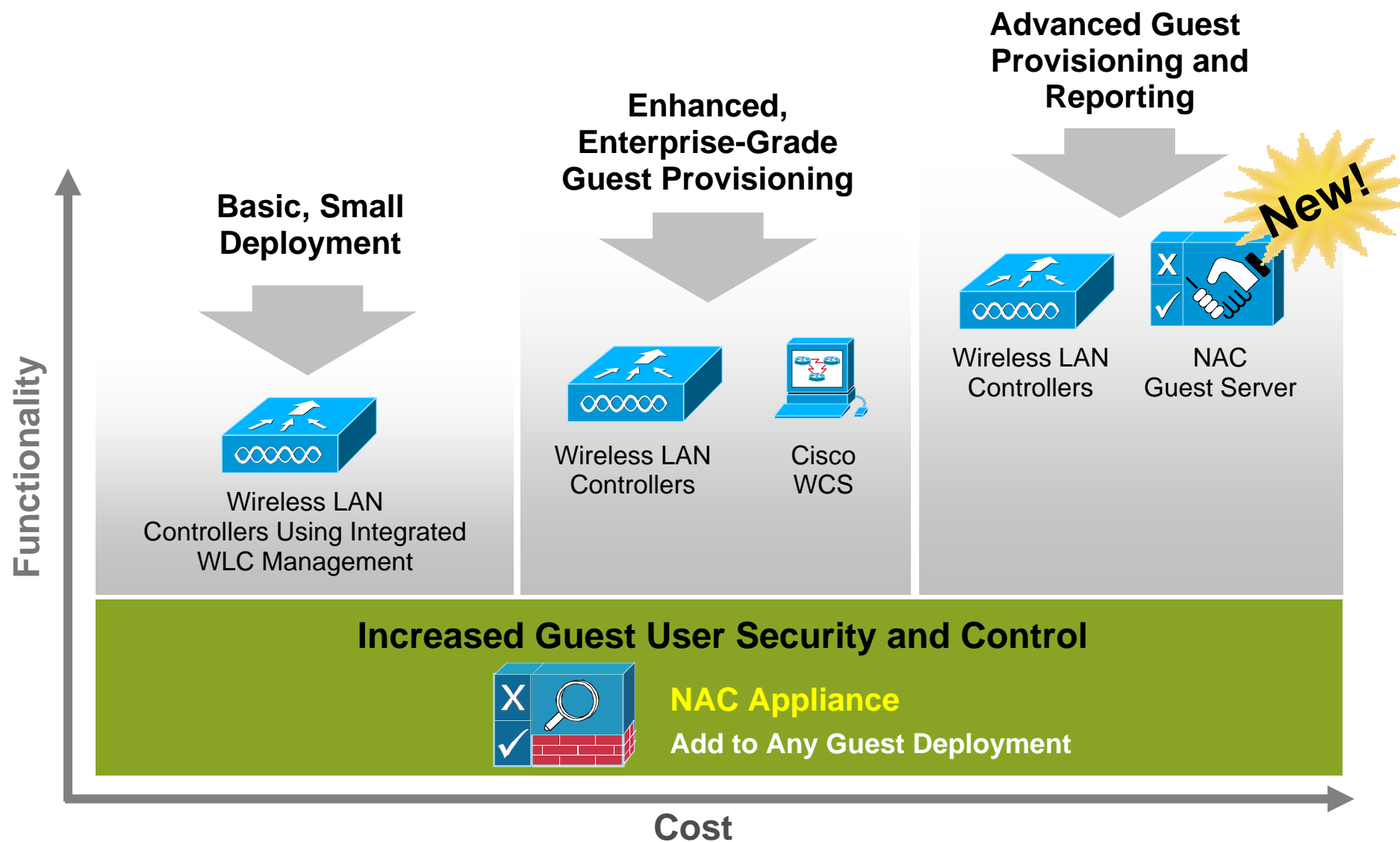
# Tracking Provisioning Personnel Activities

- Provisioning Personnel Audit Trail

Tracking the name of the provisioning personnel who created, deleted, or modified guest user profiles or guest user credentials

- Information assists organizations in more accurately tracking guest user provisioning
- Limiting provisioning personnel to a specific WLC or access point (SSID)
- Constraining provisioning personnel to specific wireless LAN controllers or access point SSIDs enhances network security

# Cisco **Wireless** Guest Access Solutions



# Cisco Unified Wireless Network Guest Access

## *Summary & Benefits*

### Summary

- Delivers all components of guest access within wireless infrastructure
- Guest access part of base WLAN Controller feature set
- Integrated network segmentation and flexible access control
- Non-disruptive to existing network
- Flexible management options suitable for single site SMB through largest enterprise deployments
- Streamlined provisioning and guest user portals

### Benefits

- Simplifies network design, no overlay network
- No additional cost
- Secure
- Reduces deployment time, simplifies operations
- Ease of operations
- Reduces IT burden

# Appendix



# Choosing the Right Deployment

	No DMZ Controller	DMZ Controller	DMZ Controller + NGS	DMZ Controller + NGS + NAC Appliance
Network Segmentation	VLANs	EoIP or VLANs	EoIP or VLANs	EoIP or VLANs
User Policy Management	Yes	Yes	Yes	Yes
User Provisioning	Yes	Yes	Enhanced	Enhanced
Number of Sponsors	Limited	Limited	Many	Many
User Login Portal	Yes	Yes	Yes	Yes
Reporting	Yes	Yes	Enhanced	Enhanced
User Security Posture Assessment	No	No	No	Yes
Increased Access Control Granularity	No	No	No	Yes
Bandwidth Policing	No	No	No	Yes
Support for 3 <sup>rd</sup> Party Portals, Cisco GuestNet	No	No	No	Yes
Overall Functionality	Medium	High	High	Very High
Design Complexity	Medium	Low	Low	Low

# Wired and Wireless Guest Access How it Works

1. Visitor starts Web browser and authenticates to guest portal via wired port (i.e., switch port 11)

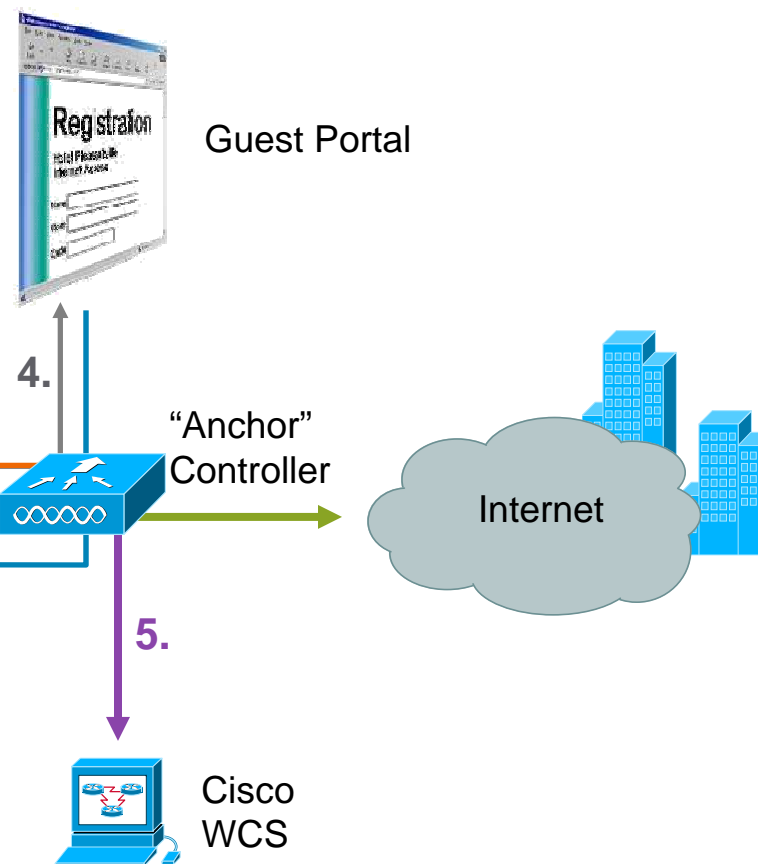
2. WLC identifies the port as a guest port and assigns the user to a “guest” VLAN (i.e., VLAN 49)



3. WLC segments guest traffic from employee

4. WLC serves up the captive portal (same as used for wireless)

5. WCS provides guest user provisioning, monitoring and logging (same as used for wireless)





# Dynamic Unified Guest Access with Cisco NAC Appliance

1. Visitor starts Web browser

2. NAC Appliance redirects to location-based connect screen

3. Visitor enters visitor access code

4. NAC Appliance provides authentication and accounting

5. NAC Appliance assigns a per user filter or changes VLAN based on whether user authenticated as a visitor or a guest

