



Securing the Empowered Branch with Cisco Network Admission Control



September 2007

Contents

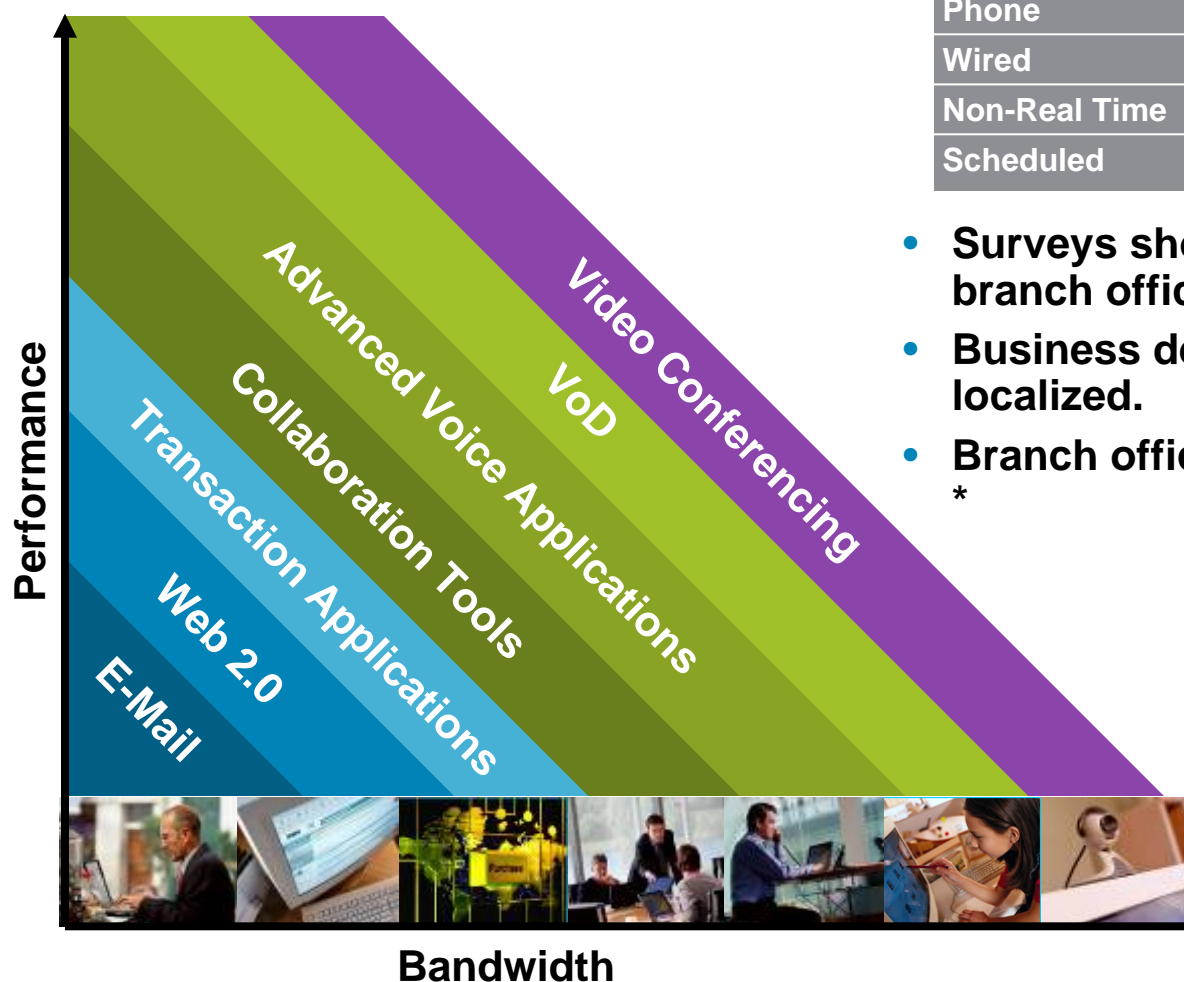
- ➔ 1 The Cisco® Empowered Branch
- 2 Security Considerations for the Branch Office
- 3 Cisco Network Admission Control (NAC) Overview
- 4 Securing the Empowered Branch with Cisco NAC



New Business Realities

Technology Innovation

Point-to-Point	↔	Multipoint
Voice Only	↔	Rich-Media
Phone	↔	PC/PDA
Wired	↔	Wireless
Non-Real Time	↔	Real Time
Scheduled	↔	Impromptu



- Surveys show >35% of all employees are in branch offices, and the number is growing.
- Business decisions are increasingly localized.
- Branch offices consume 70–90% of resources *

Most Employees **Cannot** Take Full Advantage of These Today, Unless Network Infrastructure Keeps Up

New Branch-Office Realities

Today's Branch: WAN



Aging, Disparate Data and Voice Networks



Saturated WAN; Poor Response Time



Blended Security Threats, Compliance



Limited Mobility; Limited Disaster Recovery



Inconsistent Branches and Branch-Headquarters Solutions

Empowered Branch: WAN

Unified Voice, Data, and Video Network Platform

Optimized WAN; Accelerated Applications

Self-Defending Networks

High Availability, Unified Wireless–Wireline Business

Consistent Branches and Branch-Headquarters Services

Cisco Integrated Services Routers

**Secure, Concurrent Services
Leading Solution for Branch Offices**

**Increased
Performance, Service
Density, and Memory
for Enhanced
Efficiency**

**Built-In, Self-
Defending Security:**

- Firewalls
- Intrusion prevention systems
- Antivirus
- Application inspection
- Transaction privacy
- Network admission control



**Embedded Wireless
Access Points for
Improved Mobility**

**Voice-Ready
Capabilities for
Improved
Responsiveness**

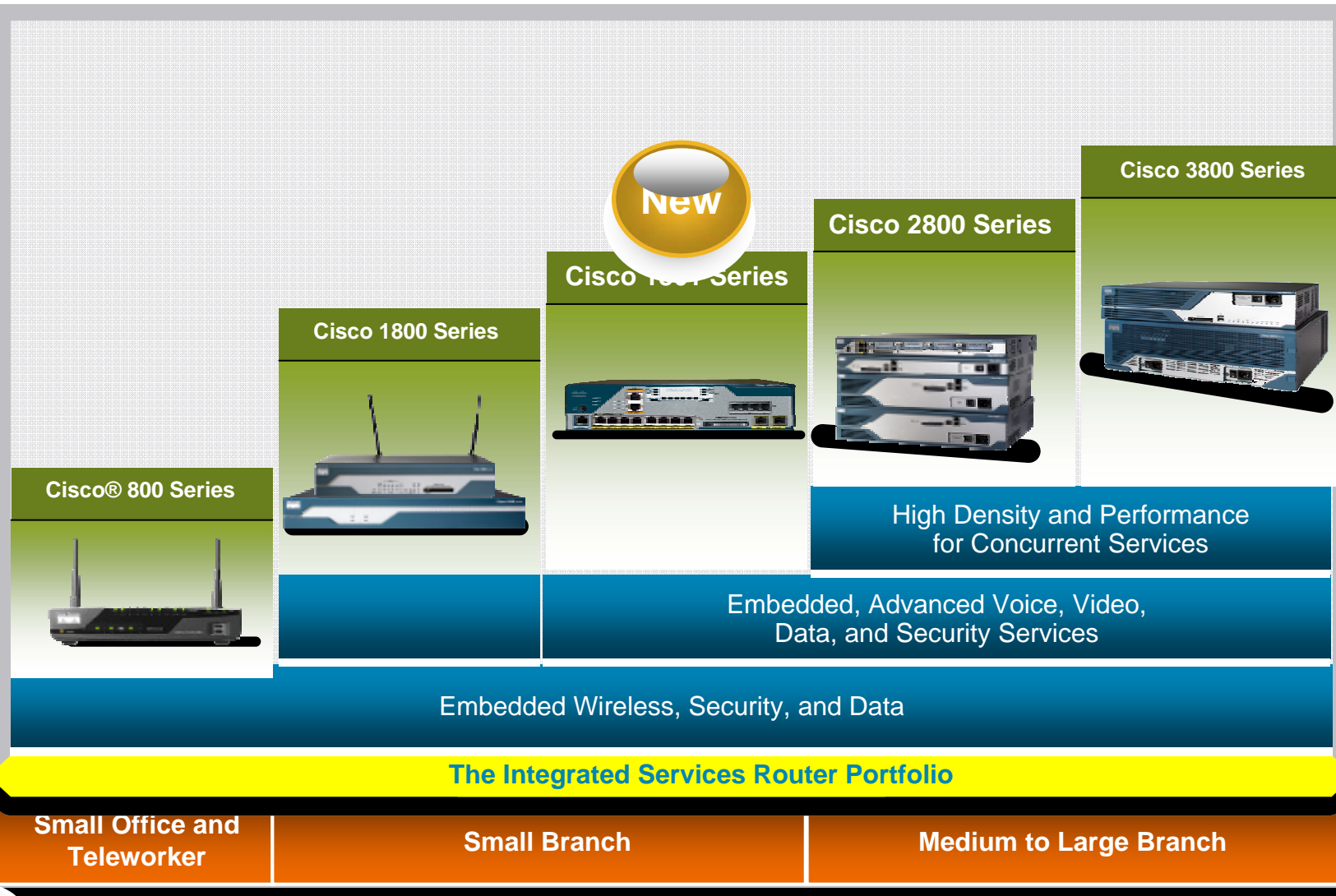
**Easy-to-Deploy
Device Management:**

- Cisco® Router and Security Device Manager (SDM)

**Remote Management (e.g., Cisco
IOS® Software and CiscoWorks)**

Cisco Integrated Services Router Portfolio

Performance and Services Density



Contents

- 1 The Cisco® Empowered Branch
- ➔ 2 Security Considerations for the Branch Office
- 3 Cisco Network Admission Control (NAC) Overview
- 4 Securing the Empowered Branch with Cisco NAC

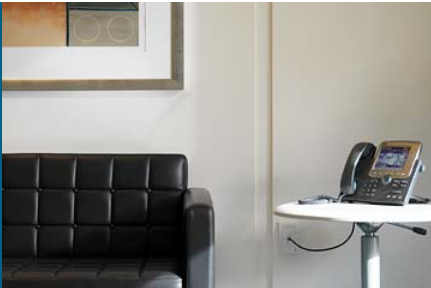


Today: Branch-Office Security Concerns



Extended Network Boundaries

- Need protection at the edge before threats enter corporate network
- Need to control guest and unmanaged devices



Effect of Compliance on IT

- IT resources leaner at branch than at headquarters
- Regulations such as PCI call for enhanced security between remote offices and headquarters



“Inherited” Security Applications and Infrastructure

- May differ from or lag behind security at headquarters
- Security policies must accommodate without increasing inconsistencies

Cost of Risk as Measured by Downtime

- Costs for downtime are high
One day cost of lost productivity
= \$1,640 per employee
- More than just a data network outage
- More than just revenue affected:
 - o Revenue loss
 - o Productivity loss
 - o Impaired financial performance
 - o Damaged reputation
 - o Recovery expenses

Industry Sector	Revenue/Hour	Revenue/ Employee- Hour
Energy	\$2,817,846	\$ 569
Telecommunications	\$2,066,245	\$ 186
Manufacturing	\$1,610,654	\$ 134
Financial Institution	\$1,495,134	\$1,079
Insurance	\$1,202,444	\$ 370
Retail	\$1,107,274	\$ 244
Transportation	\$ 668,586	\$ 107
Average	\$1,010,536	\$ 205

Source: Meta Group

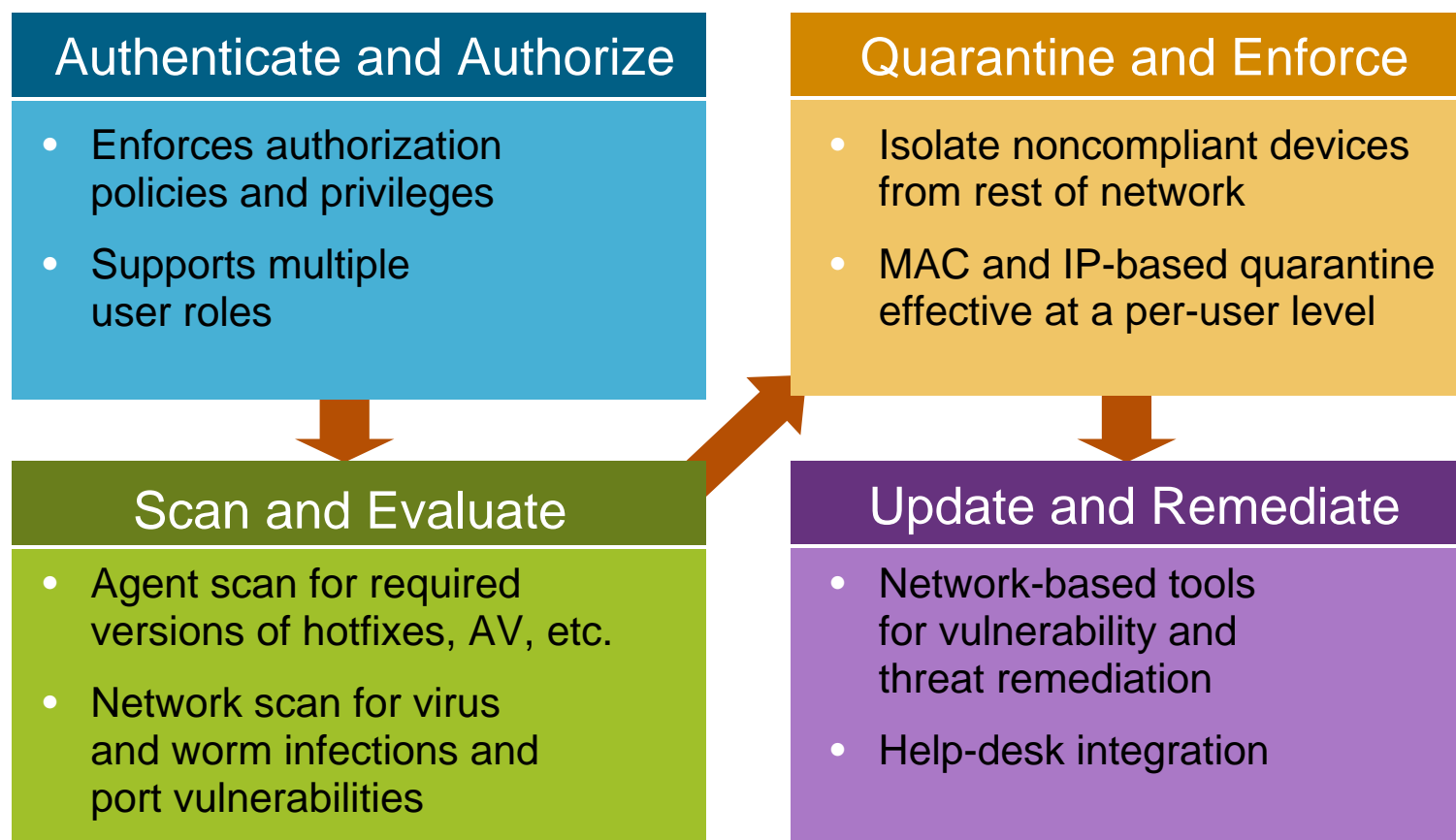
Contents

- 1 The Cisco® Empowered Branch
- 2 Security Considerations for the Branch Office
- ➔ 3 Cisco Network Admission Control (NAC) Overview
- 4 Securing the Empowered Branch with Cisco NAC



Cisco Network Admission Control

Using the *Network* to Enforce Policies Helps Ensure that Incoming Devices Are Compliant.




Cisco NAC Addresses Top Pain Points



How to Implement Role-Based Access Control

Cisco® NAC applies access and posture policies based on roles.



How to Handle Guest and Unmanaged Users

Cisco NAC authenticates and controls guest and unmanaged assets.



How to Enforce Endpoint Policy Requirements

Cisco NAC assesses, quarantines, and remediates noncompliant endpoints.

Source: Current Analysis, July 2006

Cisco NAC by the Numbers

2000+
Customers

47%
Market
Share¹

No.1 NAC Vendor
Based on Network
World Reader Survey³

75%
of Infonetics Survey
Respondents
Ranked Cisco
No. 1 Among NAC
Vendors¹



SearchNetworking.com

Gold Award:
Determined by
Reader Survey²

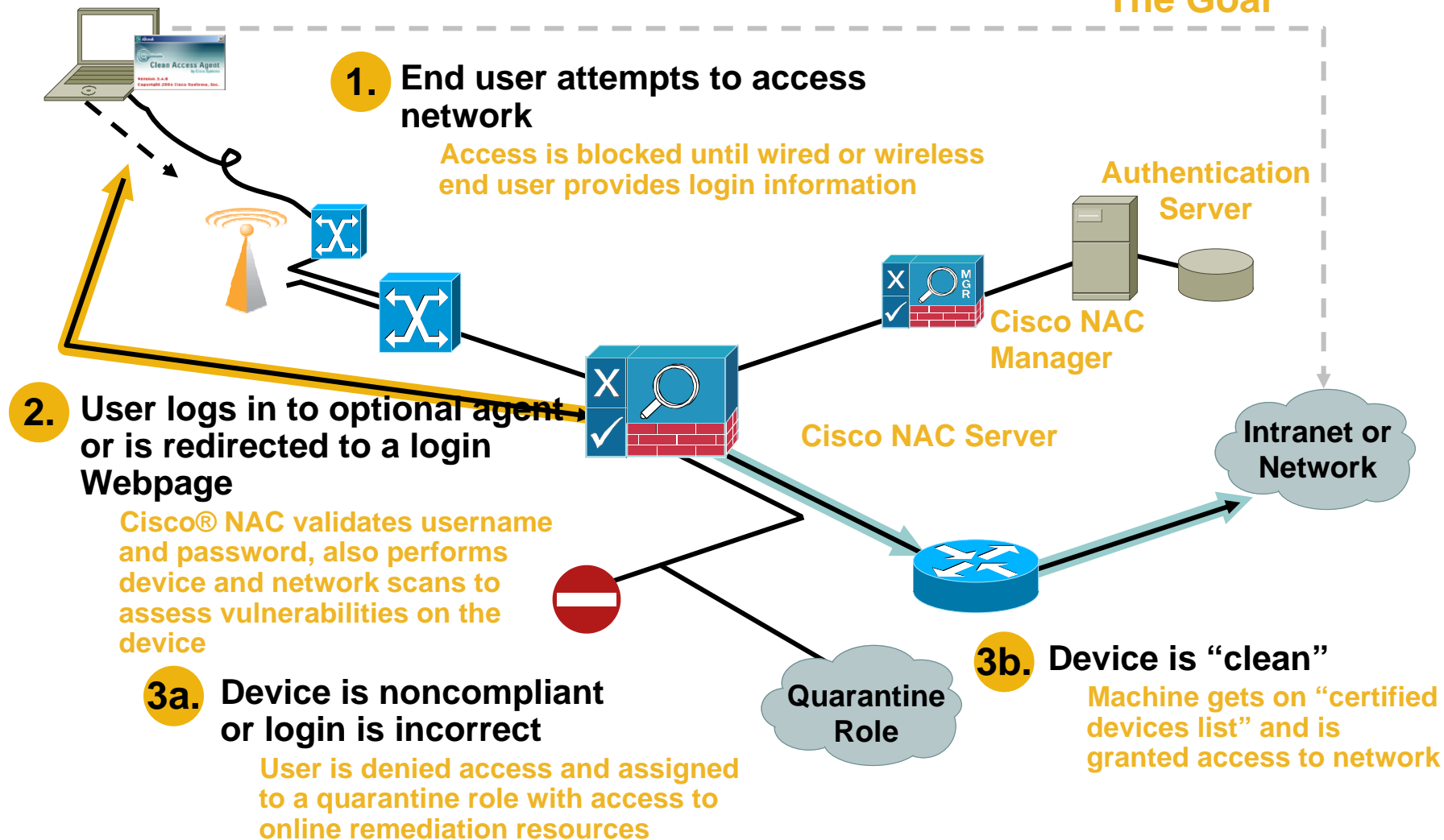
¹ Infonetics, May 2007

² March 2007 <http://searchnetworking.techtarget.com/productsOfTheYear/>

³ May 2007 <http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=199204304>

Cisco NAC Appliance Flow

The Goal



Cisco Business Benefits



Maintain Network Accessibility

Cisco NAC Addresses the Two Primary Sources of Downtime.

	Network Security Attacks	Human or Configuration Errors
Monetary loss as a percentage of total revenue	3%	3.6%

“In recent years, lost productivity has started to eclipse data theft as the primary concern when it comes to network security attacks.” (*Infonetics, The Costs of Network Security Attacks, 2007*)

“Human error plays a much larger part in application downtime than in any other area; human error is responsible for 35% of outage time and 31% of service degradation time.” (*Infonetics, The Costs of Downtime, 2006*)

Part of the Cisco Self-Defending Network

Interoperates with Many Other Cisco® Products, Such as VPN, Wireless Products, Routers, and Switches to Increase Network Resiliency and Productivity

- Switches and routers
 - All switches and routers (in band)
 - Cisco Catalyst® 2900, 2940, 2950, 2960, 3500, 3550, 3560, 3750, 3760, 4000, 4500, and 6500 models (out of band)
- VPN products
 - Cisco VPN 3000 Series Concentrators
 - Cisco ASA VPN
 - Cisco Integrated Services Router and Cisco IOS® Software VPN
- Wireless access points
 - Wireless LAN services module (WLSM) (Cisco Aironet® access points)
 - Wireless LAN Controller (WiSM/WLC)
- Cisco Security Agent for day-zero endpoint security
- Cisco Security Monitoring, Analysis and Response System (MARS) for security correlation

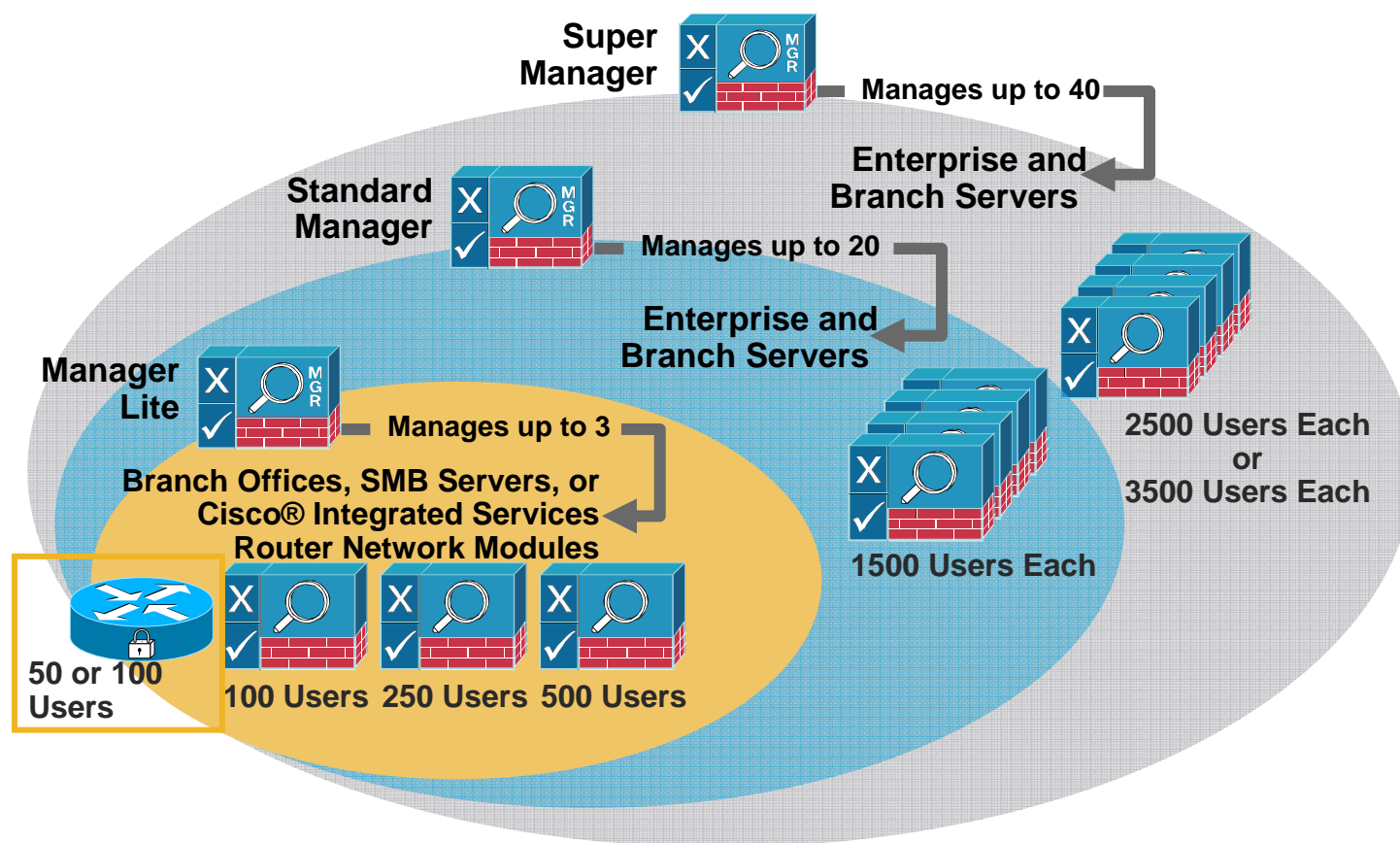
Contents

- 1 The Cisco® Empowered Branch
- 2 Security Considerations for the Branch Office
- 3 Cisco Network Admission Control (NAC) Overview
- ➔ 4 Securing the Empowered Branch with Cisco NAC



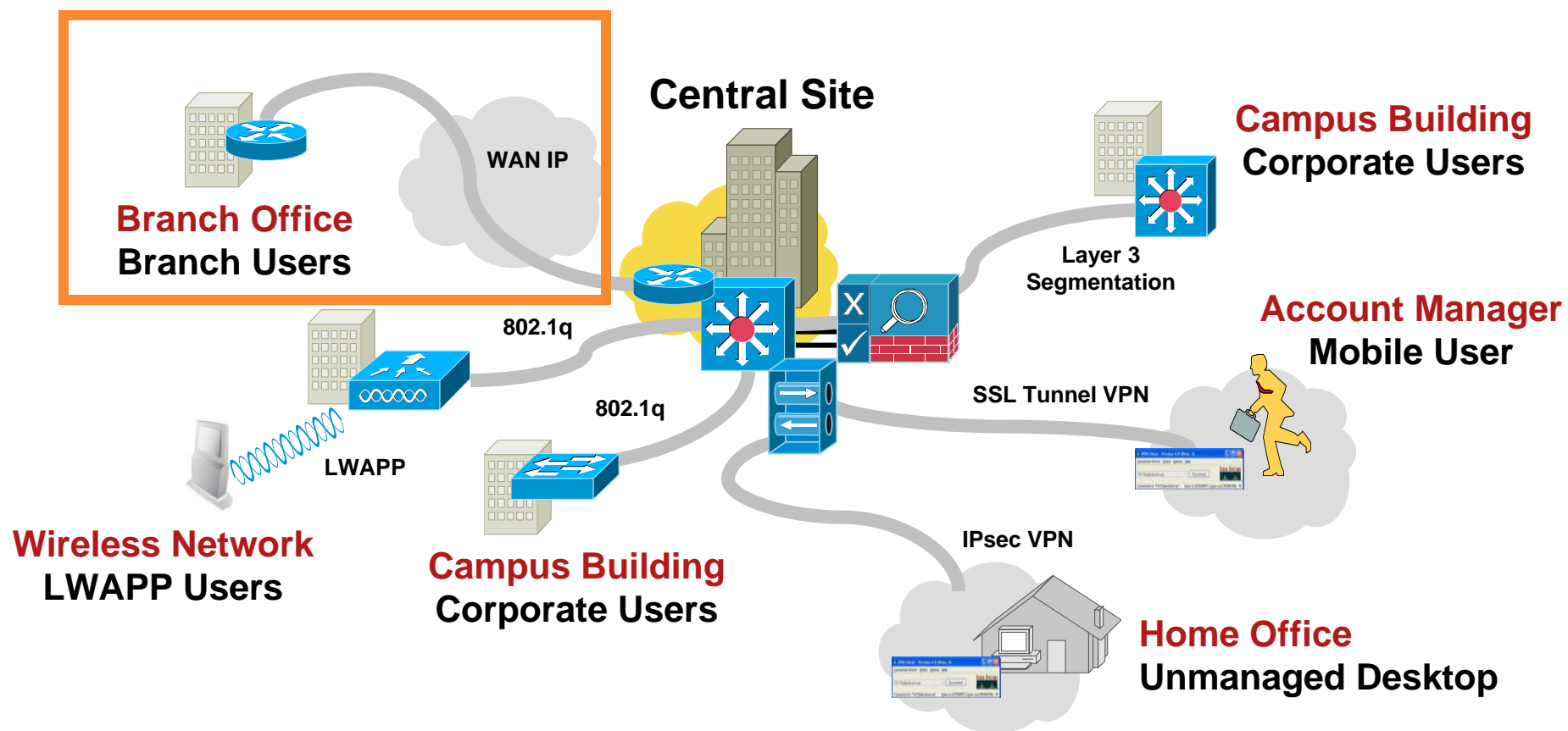
Cisco NAC Appliance Portfolio

Now Extending to Cisco Integrated Services Router



- NME-NAC for 50 and 100 users; integrates CAS functions
- Supports Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers

Cisco NAC Deployments



Extending Cisco NAC with Cisco Integrated Services Router Network Module

Network Admission Control
Better Criteria for Network Access
Beyond “Who Is It?”

Four Critical Functions

Authenticate
and Authorize

Scan and
Evaluate

Quarantine
and Enforce

Update and
Remediate



What do you
have?

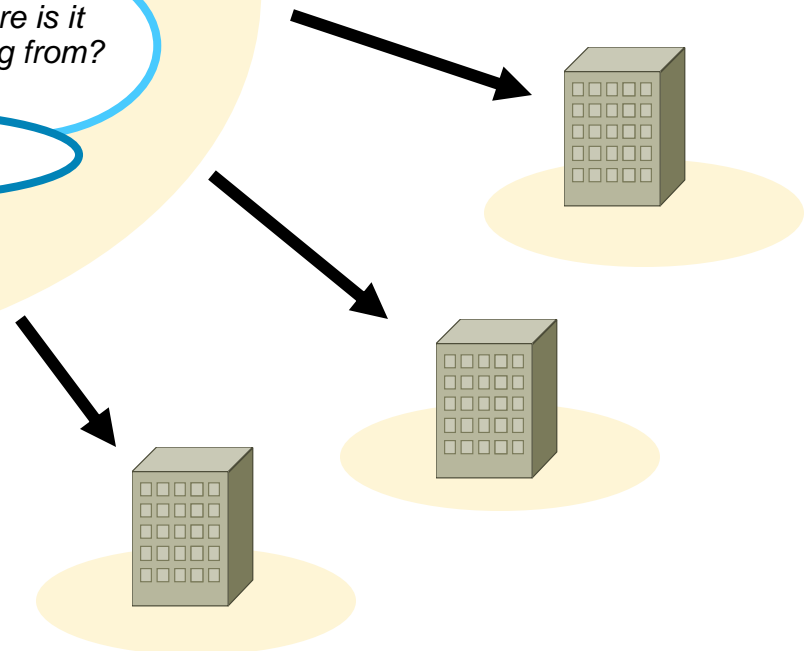
What's on it?
What is it doing?

What's the
preferred
way to check or
fix it?

Who owns it?

Where is it
coming from?

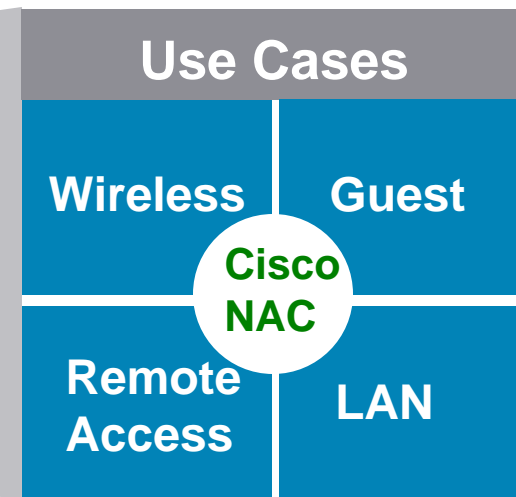
**Industry's *First* Full
NAC Network Module**



Cisco NAC Network Module on Cisco Integrated Services Router



- Authentication and identity
- Security posture
- Enforcement
- Remediation



Benefits:

- **Pervasive security**
One product for all use cases and locations
- **Consistent policy**
One policy store for consistent application across entire organization
- **Transparent deployment**
Integrated for easier deployment, troubleshooting, and management

Cisco NAC for Customer Choice

Appliances (Overlay)



Or

Cisco Integrated Services Router Network Module (Modular)



Service Interoperability

- Consistency
- Interoperability
- Tested

System Support

- Vendor accountability:
Network partner
- Fewer maintenance contracts

Operational Efficiency

- Fewer devices, management systems, and user interfaces
- Simplified troubleshooting

Investment Protection

- Flexibility to evolve through system modularity

Any Combination Works

	Appliances (Overlay)	Cisco Integrated Services Router Network Module (Modular)
Primary use cases	Campus: Wired, wireless, remote, and guest access	Branch: Wired, wireless, remote, and guest access
Number of users	Increments of 100, 250, 500, 1500, and 2500 users per server	Increments of 50 or 100 per module
Policy store or management point	Cisco NAC Appliance Manager (manages both options)	
Deployment methods	Same deployment flexibility with Layer 2 or Layer 3, in-band or out-of-band, agent or agentless	
Form factor	Separate appliance	Fits into Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers
High availability	Supported	Not supported

