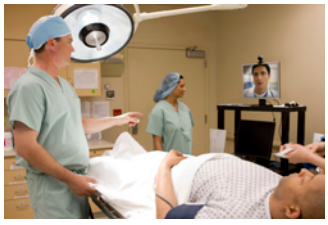
Cisco BioMed NAC Solution for Healthcare:



Flexible, Cost-Effective Provisioning for Identified Networked Biomedical Devices

Housekeeping Incident in the OR

In a real situation, hospital housekeeping staff accidentally unplugged network cables that connect workstations and medical devices to network ports in the wall of an operating room.

Following the cleaning, the devices were reconnected, but not to their original ports. The resulting port security violation caused the devices to be quarantined. It took several days for IT staff to resolve this incident, and created a major disruption in the OR.

Emergency Overflow Incident

With the critical care unit fully occupied, patients were being admitted to the critical care overflow unit. Since the overflow unit had not been used for days, only one port and workstation were operational for charting on six patients.

In this real-life incident, the issue was escalated to the hospital administration. But it was still one full day before it was resolved.

Visiting Physician Incident

A visiting physician was unable to access patient records from his personal digital assistant (PDA) while doing hospital rounds. It took the hospital administration staff two days to grant him the appropriate access and provision security so he could be more efficient and view the patient information he needed.

Executive Summary

More and more biomedical devices, from patient monitors to infusion pumps, are designed for network connection. While this enables hospitals to efficiently collect and share patient and device information, it also poses security risks. When caregivers, patients, or guests access the hospital network with a variety of communication devices, it introduces an even higher level of risk. The Cisco® BioMed Network Admission Control (NAC) solution and Network Management System solution is an effective way for hospitals to automate the process of getting certain biomedical or IT devices onto the network. It isolates biomedical devices from other hosts on an IP network and protects the devices from a variety of security threats.

Introduction

As more and more biomedical devices are IP-enabled, medical facilities face a dilemma. The trend in hospitals is to converge networks to combine administration and management tasks and control costs. Hospitals do not want to add more network infrastructure for biomedical devices, manage multiple disparate networks, or provision ports manually because of the added cost and delays.

Adding biomedical devices to a converged network can pose significant risks such as viruses, worms, or other malware, which can severely impact the overall network security and availability. It is essential to have a way to connect biomedical, guest, and IT devices to the IP network safely.

Medical facilities need a way to leverage their existing network infrastructure and provide highly secure wired or wireless network access for all devices.

The Cisco BioMed NAC solution for healthcare is an effective way for hospitals to automate the process of connecting certain biomedical, IT, and guest devices to the network, eliminating a time-consuming manual process. Cisco technology automatically distinguishes a biomedical device and provisions the network for the appropriate access capabilities and restrictions. It isolates and protects specific biomedical devices from other hosts on the IP network to protect them from malware and provide the appropriate quality of service.

In addition, the solution allows hospitals to manage guest devices on the network with appropriate security and minimal impact on IT resources.

Table 1: Key Components of the Cisco BioMed NAC Healthcare Solution

NAC Appliance	Function
Cisco NAC Appliance Manager 3310	Centrally manages and monitors servers and performs dynamic configuration to access switches
Cisco NAC Appliance Server 3310	Performs endpoint policy enforcement and access control
Cisco NAC Appliance Profiler 3350	Aggregates and classifies data from collectors and manages database of medical device information
Cisco NAC Collector (installed on NAC Appliance Server)	Gathers information about endpoints using SNMP, NetFlow, DHCP, and active profiling
Infrastructure	
Cisco Catalyst® 2950, 2960, 3550, 3560, and 3750 Series	Access switches for wired medical devices
Cisco Catalyst 6500 Series	Distribution/core switch

Differentiate Biomedical Devices on the Network

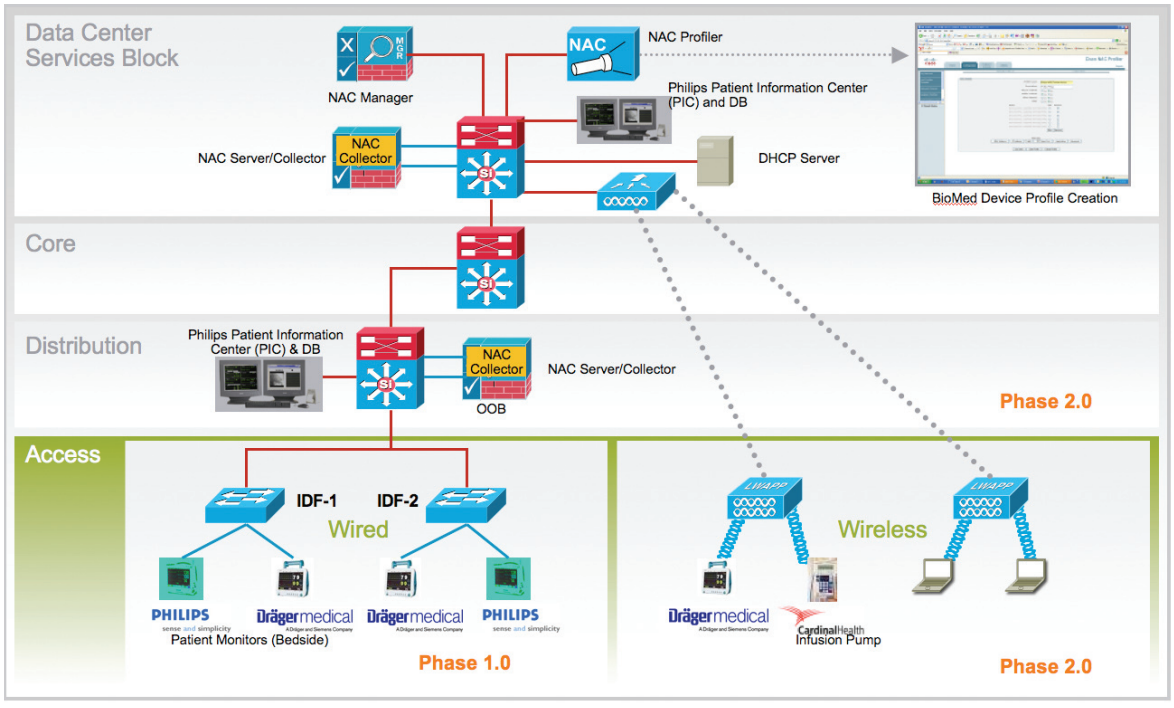
Without the ability to differentiate biomedical devices from other network devices, security, quality, and class of service are extremely difficult to manage. This can complicate collaboration and communication, or make it difficult to access patient information. Either issue could compromise patient care.

The Cisco BioMed NAC solution solves these issues as it provides the ability to:

- Isolate and protect certain biomedical devices from other hosts on the IP network
- Distinguish a biomedical device from other types of hosts
- Automatically provision certain biomedical devices for appropriate access capabilities and restrictions

Figure 1 shows the overall architecture topology of the Cisco BioMed NAC solution. The solution is based on the Cisco Medical Grade Network (MGN) to enable a flexible, scalable, highly secure, and reliable network.

Figure 1: Cisco BioMed NAC Solution Overall Architecture



Flexible and Scalable

The Cisco BioMed NAC solution allows healthcare organizations to use a single, unified, and converged IP network that supports IT equipment, biomedical devices, and guest services. The technology can quickly distinguish certain biomedical devices from other types of hosts, and automatically provision the network for appropriate access capabilities and restrictions for more flexibility and optimal patient care as it:

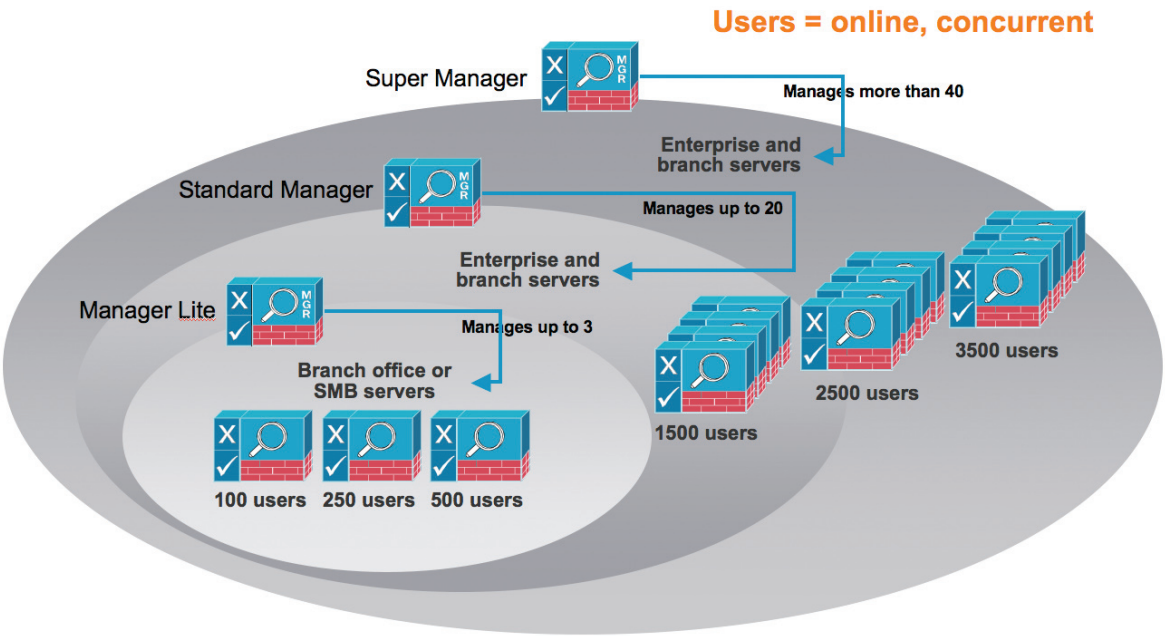
- Automates device assignments to controlled zones on the hospital network
- Allows quick setup in other areas of the hospital as caregivers simply plug in the devices they need for more flexible facility use or in an emergency
- Inventories and tracks assets to more effectively use a myriad of IP-connected endpoint devices
- Permits more mobility by bringing the device to the patient, rather than the reverse, improving patient care and overall efficiency
- Provides flexible biomedical, IT, and guest access on all ports

Biomedical devices, which are currently limited to Philips and Draeger, may include:

- Patient monitors
- Portable imaging units
- Infusion pumps
- Ventilators
- EKG monitors
- Patient-controlled analgesia
- Pulse oximeters
- PACS workstations

The Cisco BioMed NAC solution grows as your needs do—scaling to support new campus facilities, new users, and new applications. See Figure 2.

Figure 2: Cisco BioMed NAC Solution Provides Unprecedented Scalability



Highly Secure and Reliable

The Cisco BioMed NAC solution focuses on testing defined medical device endpoints for admission control, dynamic profiling, and access port provisioning.

Auto provisioning of wired access ports allows caregivers to connect certain patient monitors to different bedside wall jacks, or switch ports, within the hospital. The network automatically identifies the device type and vendor and re-provisions the associated port to the correct segment of the network.

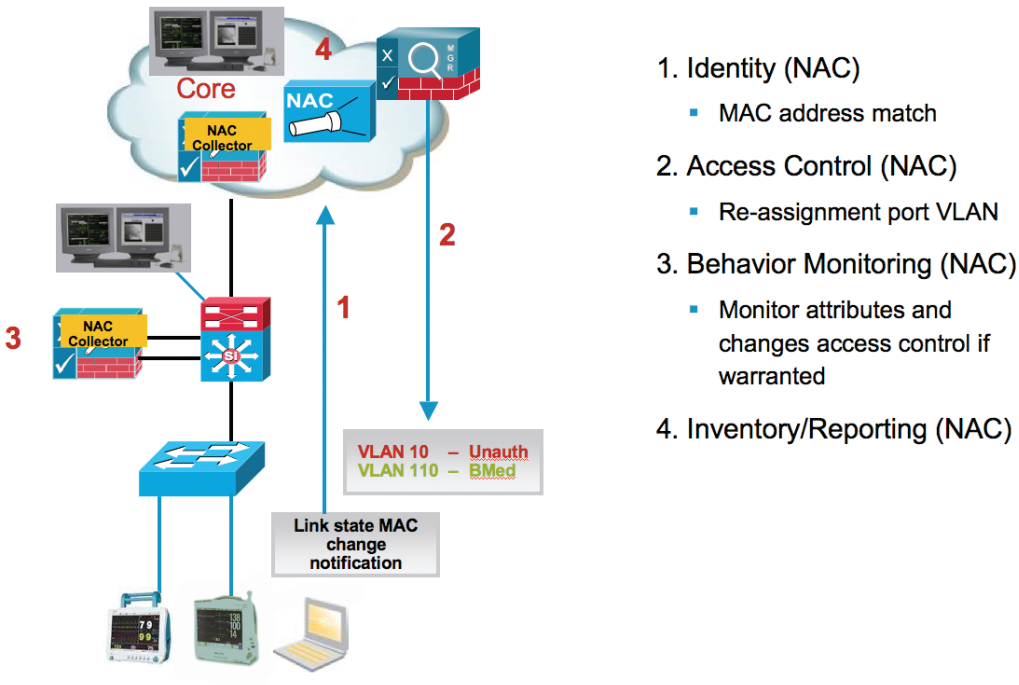
The Cisco BioMed NAC solution with Cisco Network Management System technology automates device assignments to controlled zones on the hospital network and provides port access only to approved endpoint devices through a profiling process. It also provisions devices with the appropriate security measures and continuously monitors the device behavior.

A graphical interface shows profiling events that occur on the network to provide visibility, and sends event changes such as profile matches to a central network management plane for reporting purposes.

The automated system leverages the existing healthcare network infrastructure to allow hospitals to:

- Automatically isolate and protect the biomedical devices from other hosts on the IP network to meet security standards and protect network performance
- Manage devices on the network that are not part of the healthcare system, with the appropriate security and minimal impact on hospital resources
- Monitor device behavior, alerting the appropriate party of rules violations that could lead to either segregation or remediation of the device

Figure 3: Features of a Wired Implementation

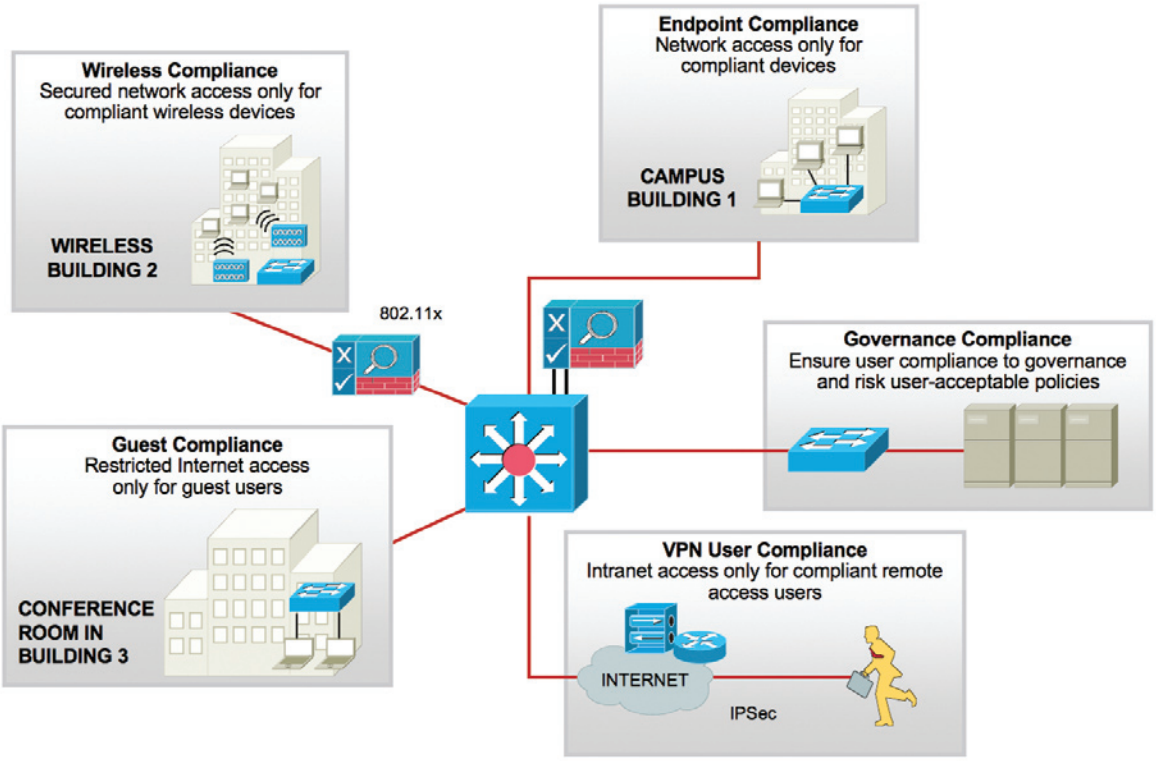


Cost-Effective

As an addition to existing hospital networks, the Cisco BioMed NAC solution provides policy-based network security for certain types of network-connected devices. This solution integrates the Cisco NAC Appliance solution and NAC Profiler components into an existing healthcare campus network to accomplish a number of tasks that improve operational efficiencies and reduce overall operational expenses by automating device access control, monitoring, and enforcement.

Figure 4 illustrates how healthcare organizations can make the most of a converged network by deploying the Cisco BioMed NAC solution for a wide variety of different uses.

Figure 4: Cisco BioMed NAC Solution Can Be Used Broadly



Why Cisco?

The Cisco BioMed NAC solution takes advantage of Cisco Medical-Grade Network technology to enable a flexible, scalable, highly secure, and reliable network.

Based on proven Cisco network access control technology and products, the solution allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and certain devices prior to network access. Architected to coexist with traditional NAC features, the solution provides an additional focus on testing of certain biomedical medical device endpoints and specific features designed for healthcare environments.

For more information about Cisco healthcare solutions, visit www.cisco.com/go/healthcare.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

DDM08CS1801 01/09