The Cisco BioMed NAC Solution for Healthcare

FLEXIBLE, COST-EFFECTIVE PROVISIONING FOR IDENTIFIED NETWORKED BIOMEDICAL DEVICES

At-A-Glance 1

Flexible, Cost-Effective Provisioning for Identified Networked Biomedical Devices

The Cisco® BioMed Network Admission Control (NAC) solution is an effective way for hospitals to automate the process of connecting biomedical devices to the network, eliminating a time-consuming manual process. Cisco technology can automatically distinguish certain biomedical devices and provision the network for the appropriate access capabilities and restrictions. Identified biomedical devices can then be logically isolated from other hosts on the IP network. The solution provides a unified access control policy for all biomedical devices, IT devices, and guest services on a hospital converged network.

A Need to Balance Flexibility, Scalability, and Security

As more and more biomedical devices are IP-enabled, medical facilities want to be able to leverage their existing network infrastructures to provide wired or wireless network access for these devices. Hospitals often don't want to manage multiple disparate networks, nor do they want to provision ports manually because of the added cost and delays.

These disparate devices can pose significant risks such as viruses, worms, and other malware, which can severely impact the network security and availability.

Connecting biomedical devices, plus guest and IT devices, to the IP network safely requires the ability to:

- Isolate and protect the biomedical devices from other hosts on the IP network
- Distinguish a biomedical device from other types of hosts, and automatically provision them to their appropriate access capabilities and restrictions
- Provide flexible biomedical, IT, and guest access on all ports where necessary
- Allow Internet connections to guest users
- Manage devices on the network that are not part of the healthcare system, with the appropriate security and minimal impact on hospital resources

Without the ability to differentiate biomedical devices from other network devices, security, quality, and class of service are extremely difficult to manage. This can lead to challenges with collaboration and communication, or in accessing patient information, which could compromise care.

Cisco BioMed NAC

Cisco BioMed NAC allows healthcare organizations to use a single, unified, and converged IP network that supports IT, identified biomedical devices, and guest services. The solution provides speed, flexibility, and cost savings by providing:

- Automated device identification for wired and wireless medical devices

The Cisco BioMed NAC Solution for Healthcare

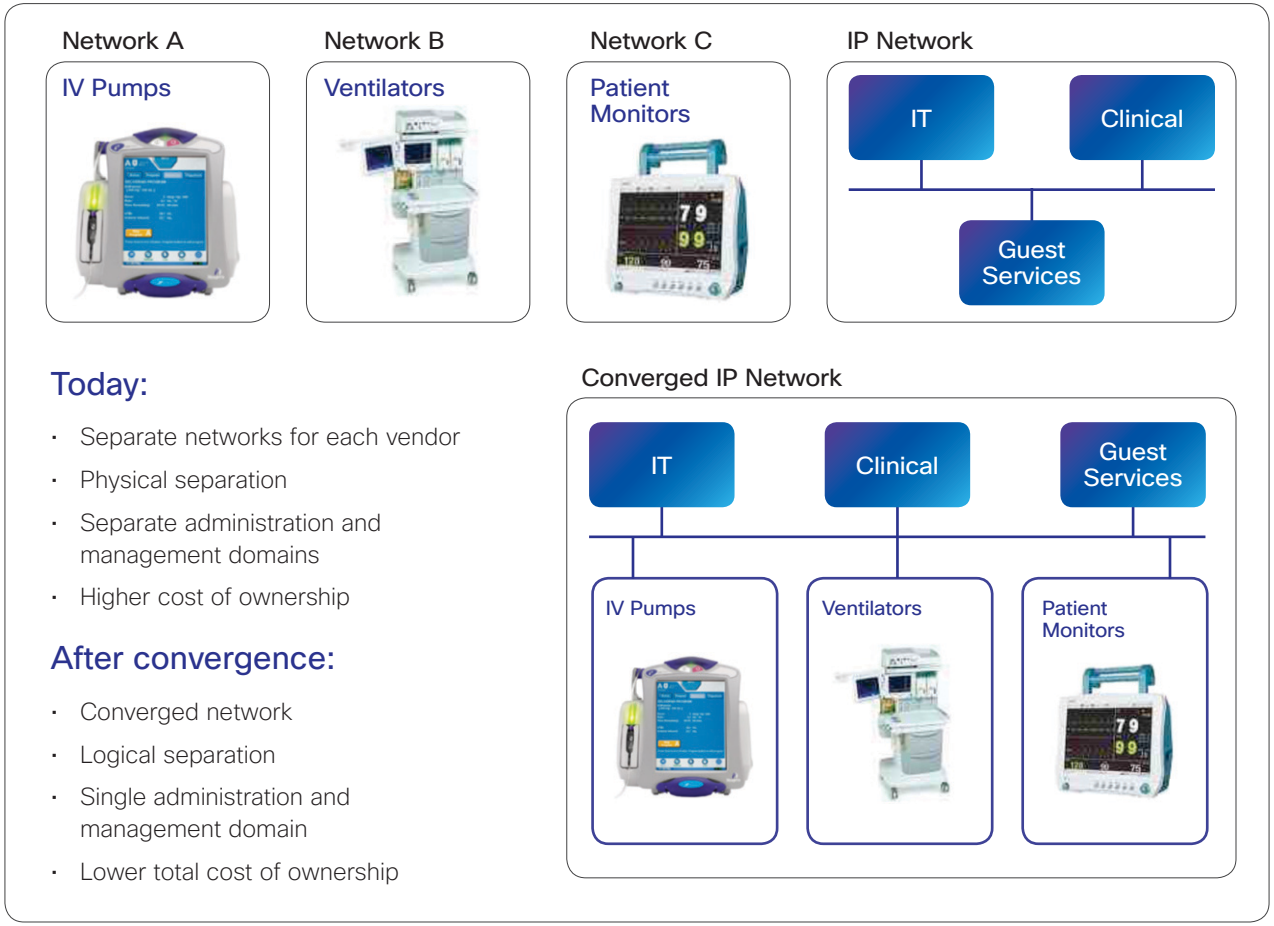
FLEXIBLE, COST-EFFECTIVE PROVISIONING FOR IDENTIFIED NETWORKED BIOMEDICAL DEVICES

- Dynamic provisioning by applying the correct access control policy to the identified device
- Network visibility to provide device identity, location, and access history, which can be used for compliance and reporting

The Cisco BioMed NAC solution focuses on testing defined medical device endpoints for admission control, dynamic profiling, and access port provisioning. The solution integrates the Cisco Identity Services Engine (ISE) platform into an existing healthcare campus network to accomplish a number of tasks.

- **Dynamic Network Autoprovisioning:** Automatically applies correct provisioning and access policy upon identification of the device. This feature enables caregivers to seamlessly connect identified biomedical devices in either a wired or wireless mode.
- **Device security:** Cisco's consolidated policy-based access control system automates device assignments to controlled zones on the hospital network and provides access only to approved endpoint devices through a profiling process. It also provisions identified devices with the appropriate access control policy and security measures.
- **Asset Awareness:** A graphical interface that enables the organization to track real-time inventory of devices. The central reporting system provides network location of devices and usage.

Figure 1: Converging Biomedical Networks



The Cisco BioMed NAC Solution for Healthcare

FLEXIBLE, COST-EFFECTIVE PROVISIONING FOR IDENTIFIED NETWORKED BIOMEDICAL DEVICES

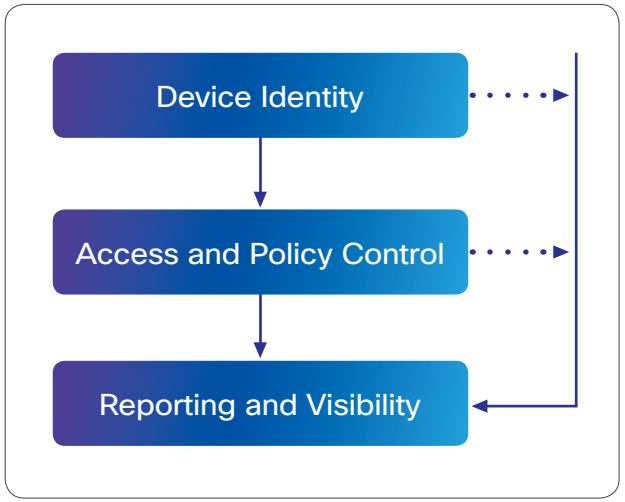
- **Regulatory Compliance:** The Cisco BioMed NAC solution enables organizations to meet compliance requirements such as HIPAA and IEC-80001.

Flexible, Scalable, Highly Secure, and Reliable

As an addition to existing hospital networks, the Cisco BioMed NAC solution provides policy-based network security for certain types of network-connected devices. The automated system works with the healthcare network infrastructure to allow hospitals to:

- Distinguish certain biomedical devices from other types of hosts, and automatically provision the network for appropriate access capabilities and restrictions to boost security and flexibility
- Automatically isolate and protect identified biomedical devices from other hosts on the IP network to meet security standards and protect network performance
- Deliver real-time inventory and asset-tracking capabilities for a myriad of endpoint devices
- Allow more mobility for devices to be brought to the patient, rather than the reverse, improving patient care and overall efficiency
- Improve operational efficiencies to reduce overall operational expenses by automating the device access control

Figure 2: Automated, Secure Communication Flow



Why Cisco?

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

The solution allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and certain devices prior to network access. The solution also provides an additional focus on testing of identified biomedical medical device endpoints and specific features designed for healthcare environments.

DDM11CS3230 08/2011 EDCS-962071