



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 certain biomedical, IT, and guest 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. It isolates and protects identified biomedical devices from other hosts on the IP network to protect the devices from malware and provide the appropriate quality of service.

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

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. But hospitals 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

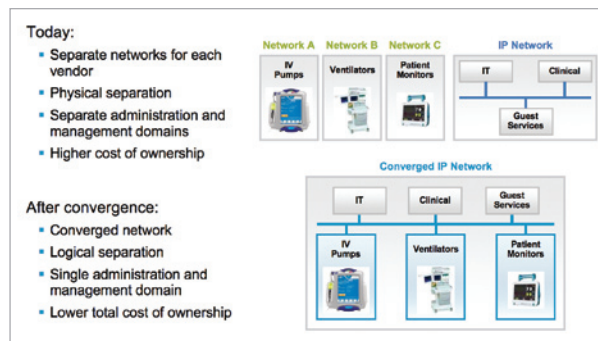
Without the ability to differentiate biomedical devices from other network devices, security, quality, and class of service are extremely difficult to manage. This can lead to challenges with collaboration and communication, or in accessing patient information, which could compromise care.

Cisco BioMed NAC

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

- Automates device assignments to controlled zones on the hospital network
- Monitors device behavior, alerting the appropriate party of rules violations that could lead to either segregation or remediation of the device

Figure 1: Converging Biomedical Networks



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 NAC Appliance and NAC Profiler components into an existing healthcare campus network to accomplish a number of tasks.

- **Autoprovisioning of wired access ports:** Allows caregivers to connect identified biomedical devices to different bedside wall jacks (switch ports) within the hospital. The network is able to automatically identify the device type and vendor and re-provision the associated port to the correct segment of the network.
- **Device security:** 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 identified devices with the appropriate security measures and continuously monitors the device behavior.
- **Reporting and visibility:** A graphical interface of profiling events that occur on the network provides visibility and offers the ability to send event changes such as profile matches to a central network management plane.

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 healthcare network infrastructure to allow hospitals to:

- Distinguish certain biomedical device 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 and monitoring

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.

Based on proven Cisco NAC 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 identified biomedical medical device endpoints and specific features designed for healthcare environments.

Figure 2: Automated, Secure Communication Flow

