Dräger Medical Patient Monitoring Deployment in Cisco Unified Wireless Network Infrastructure

This document provides the design considerations and deployment guidelines for the Dräger Medical Patient Monitoring solution within the Cisco Unified Wireless Network infrastructure.

Note Support for Dräger Medical products should be obtained directly from Dräger Medical support channels. Cisco TAC is not trained to resolve problems related to Dräger Medical products.

This guide addresses the configuration parameters that are particular to Dräger Medical patient monitoring devices in a managed wireless architecture. The scope of this document does not include necessary information such as basic network design, wired multicast recommendations, or basic protocol design concepts. Therefore a fundamental understanding of network architecture and protocol design concepts is a prerequisite for understanding this document.

You should read and become familiar with the terms and concepts presented in the following Cisco documents:

- *Wireless Considerations in Healthcare Environments*: http://www.cisco.com/web/strategy/docs/healthcare/wireless_hc_environ061208.pdf
- *Wireless and Network Security Integration Solution Design Guide* http://www.cisco.com/en/US/partner/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg.html
- *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* http://www.cisco.com/en/US/docs/wireless/controller/5.2/configuration/guide/Controller52CG.html
- *Cisco IP Telephony Solution Reference Network Design Guide*: http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/models.html

These documents are available at www.cisco.com with the proper login permissions.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Executive Summary

Although this document builds on key concepts presented in Cisco IP Telephony, patient monitoring data and its priority should not be compared with that of voice data. Voice transmission quality is well defined, and its value is measured by the Mean Opinion Score (MOS). This numerical scale from 5 (Imperceptible) to 1 (Very Annoying) cannot apply to patient data, where a lost or delayed packet may have much greater consequences than with voice. For example, a lost packet in a patient monitoring application may result in delays alerting nursing staff to alarm conditions. With this understanding, a strong radio policy is critical in an 802.11 environment, where packet loss *must* be kept to a minimum.

Note The Dräger Medical Patient Monitoring solution requires Cisco Unified Wireless LAN Controller software 4.2 or later. Earlier versions of the controller software flood multicast packets to all access points, resulting in collisions and data loss.

The Dräger Medical Solution Overview

The following sections provide an overview of the Dräger Medical system devices that can be integrated into a Cisco Unified wireless network.

Infinity Bedside Patient Monitoring Solution

Infinity bedside patient monitors provide comprehensive patient monitoring that includes multiple-lead ECG, SpO_2, respiration, dual temperature, cardiac output, multiple invasive pressures, noninvasive blood pressure, and arrhythmia classification (see Figure 1).

Figure 1 Infinity Bedside Patient Monitors

A wide range of sizes and styles including the Infinity Delta, Gamma, Kappa and Vista series let a biomedical engineer tailor the system to departmental needs. These monitors bring critical information from other bedside devices to the patient monitor via the Infinity Docking Station to help the clinician make faster patient assessments. The monitor provides maximum reliability, decreased downtime, and reduced spare parts and support costs.

The Infinity Central Monitoring Solution gathers and displays information from the Infinity bedside monitors and Infinity Telemetry devices. Up to 32 patients can be simultaneously monitored and displayed on each Infinity Central Station.

The patented Pick&Go® flexibility lets Infinity monitors move with the patient (see Figure 2). When undocked, the patient monitor switches to wireless mode and continuously transmits vital signs back to the central systems. The ability to monitor patients during transport throughout the healthcare facility has become an important requirement for caregivers.

Figure 2 Infinity Monitor Moving with a Patient

Technical Aspects

The Infinity bedside monitoring solution uses standard IP multicast packets for more than 90% of its input/output (I/O). Devices are both IP Multicast transmitters and receivers, which ensures the exchange of information with all connected devices of a defined group, called a monitoring unit (MU). To prevent flooding of this traffic, both the wired and wireless portions of the network must be configured for Internet Group Management Protocol (IGMP) multicast traffic. Infinity bedside monitors constantly transmit packets at approximately 100 kb/s in both wired and wireless mode.

Within an MU, four common multicast streams are created which are shared by all Infinity devices in the MU, both as transmitters and as group members. In addition, each bedside monitor transmits its own unique multicast stream of waveform pixel and vital-signs data that an Infinity Central Station uses for active display. That stream can be requested on another bedside monitor in the same MU by a clinician using the remote view feature. The waveform display occupies the lower portion of the local monitor's screen. In this case the multicast data flows directly between the two bedside monitors and is not routed through the Infinity Central Station.

Table 1 shows an example of the Multicast addresses generated in a single Monitoring unit with four bedside devices. It is highly recommended that you create an overview of utilized Multicast addresses when deploying a patient monitoring installation.

Table 1 Example of Multicast Addresses for Patient Monitoring

Multicast Addresses for Monitoring Unit 5	
Name service	224.127.5.255
Alarm group service	224.127.5.254
Time service	224.127.5.253

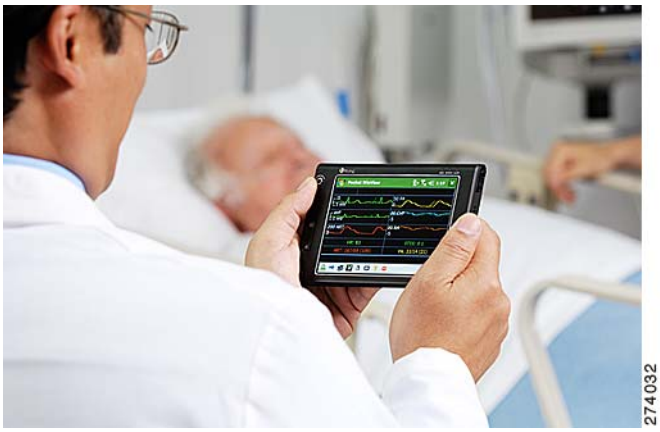
Table 1 Example of Multicast Addresses for Patient Monitoring (continued)

Alarm group service for ventilators	224.127.5.252
Patient data stream (1st Infinity Bedside Monitor)	224.0.5.1
Patient data stream (2nd Infinity Bedside Monitor)	224.0.5.2
Patient data stream (3rd Infinity Bedside Monitor)	224.0.5.3
Patient data stream (4th Infinity Bedside Monitor)	224.0.5.4

Infinity Remote Access Solution

Dräger Medical offers a software solution called Infinity WinView/WebView which enables doctors and nurses to display and access "near-real-time" data on a desktop PC, or while on the move with Microsoft Pocket PC devices (see Figure 3). This flexibility combined with the Cisco Lightweight Access Point Protocol (LWAPP) wireless infrastructure puts doctors and nurses closer to the needs of their patients.

Figure 3 Infinity WinView/WebView Displayed on a Pocket PC Device



Technical Aspects

Mobile smart clients or laptops used as part of the remote access solution are controlled and maintained by the hospital's IT department. They may not require the same strict network deployment limitations required by medical devices. Dräger Medical does not specify network requirements for remote access clients. From a deployment perspective, the mobile devices are separated by VLAN and SSID from the bedside monitors and telemetry devices. Vital signs are delivered to clients through the Infinity Network by the Infinity Gateway server.

Wireless Specifications

Table 2 lists the specifications for Dräger Medical products within a Cisco wireless network.

Note Specifications are version-specific and subject to change with new releases. Check with Dräger Medical for the latest data at www.draegermedical.com.

Table 2 Wireless Specifications for Dräger Medical Products

Infinity Network Wireless Specifications	Infinity Delta Series	Infinity Gamma Series
Wireless Layer 1 protocol	802.11b 802.11g[1]	802.11b 802.11g[1]
Power level of access points	15 dBm (31.6 mW)	15 dBm (31.6 mW)
Minimum received signal strength indicator	-70 dBm	-70 dBm
Maximum noise floor	-85dBm	-85dBm
Minimum signal-to-noise ratio	21 dB	21 dB
Maximum Infinity wireless devices per access point	6	6
Network security protocol	WEP 128-bit WPA2[1]	WEP 128-bit WPA2[1]
Average network traffic generated per device	100 Kbits/sec.	75 Kbits/sec.
Communication protocol	Multicast UDP, TCP	Multicast UDP, TCP
Dedicated SSIDs required	1	1
VLAN	Dräger multicast VLAN	Dräger multicast VLAN
Client cards	Cisco Aironet 350 Wireless LAN Client Adapter Ambicom WL54[1] client adapter	Cisco Aironet 350 Wireless LAN Client Adapter Ambicom WL54[1] client adapter

1. Requires Delta VF8 software or Gamma VF7 software and new Ambicom wireless client adapter.

Infrastructure Planning for Infinity Delta and Gamma Series Patient Monitors

Scaling of the patient monitoring devices is important within the RF spectrum and more importantly, within the network. The number of patient monitors directly affects the number of multicast addresses required. Each patient monitor sends to a different multicast address, so this traffic can put a heavy demand on your network if your multicast capability does not match your requirements.

In a typical environment, patient monitors should be limited to six per access point, although the actual device maximums will vary with the capacity of your wireless network. Six monitors per access point generally assures more than enough capacity for patient data and other wireless applications. If your

wireless design has no other applications beyond patient monitoring, you may be able to support more monitors per access point, although this configuration has not been tested. In addition, it may be prudent to provide for potential future wireless applications in the current design.

Again, patient monitoring data are far more critical than typical voice data. Although an occasional packet drop can be tolerated, a strong radio frequency policy, security policy, and software change control combined with a solid network design is essential.

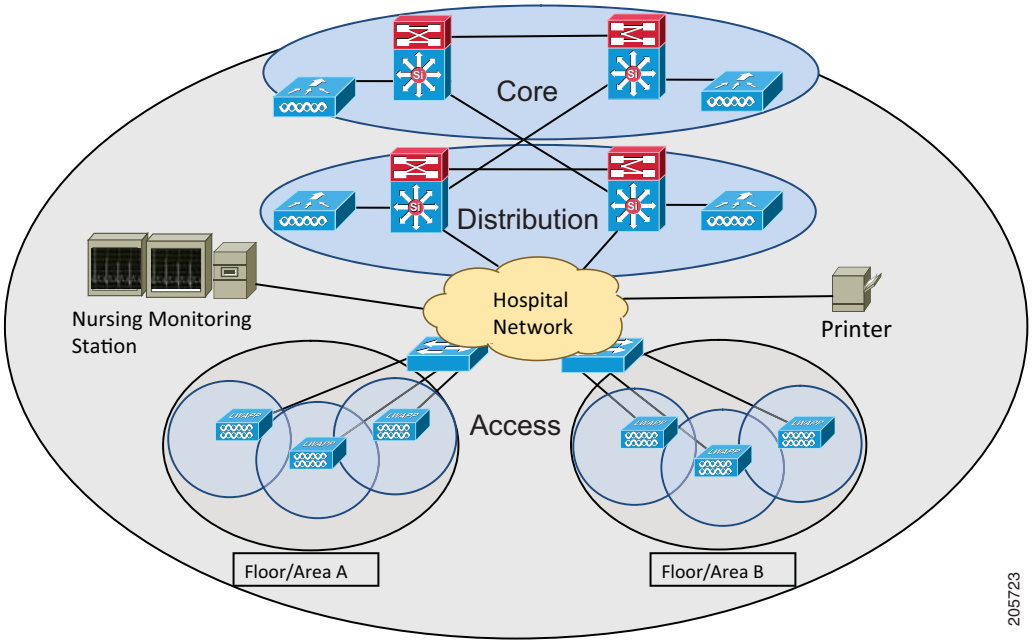
Architecture Overview

Note This overview does not include necessary information such as basic network design, wired multicast recommendations, or basic protocol design concepts. Therefore a fundamental understanding of network architecture and protocol design concepts is a prerequisite for understanding this section.

Figure 4 illustrates a typical patient monitoring architecture that uses a standard Core-Distribution-Access layer topology. Your monitoring solution can be locally connected or several Layer 3 hops away. However, if your solution requires the nurses' station to be on a different broadcast domain than the wireless network, then use a more robust Layer 3 multicast design. Whether this is a sparse or dense mode solution is up to the network architect.

Note Some of the Dräger Medical patient monitors (such as Infinity Gamma) are not capable of routing and therefore require a flat VLAN connection to the Infinity Central Station. Take these products into account when designing a network for patient monitoring use.

Figure 4 Typical Patient Monitoring Architecture



Multicast Traffic in an LWAPP Deployment

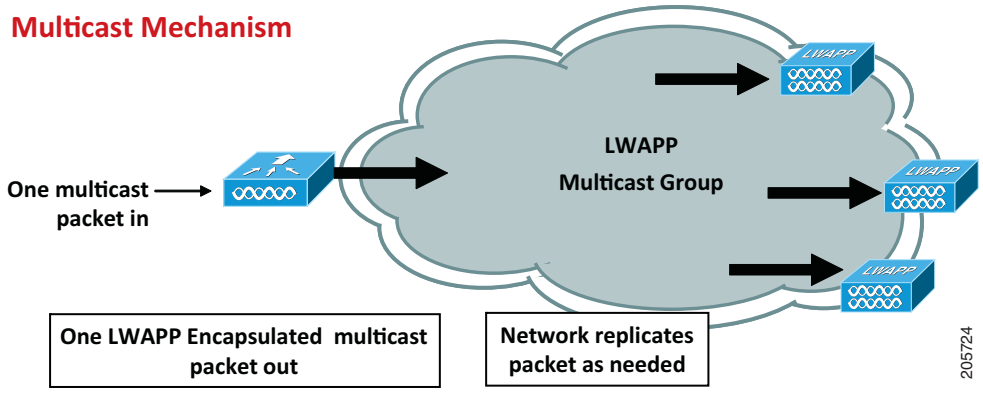
Understanding multicast traffic within an LWAPP deployment is necessary to deploy the Dräger patient monitoring solution. A Cisco LWAPP controller can be configured to deliver multicast traffic through either unicast-multicast or multicast-multicast delivery methods, but for this type of deployment, only multicast-multicast delivery options are appropriate.

Note See the "Router and Switch Multicast Configuration" section on page 8 for essential steps for enabling multicast traffic on a Cisco Unified Wireless Network controller.

Multicast-Multicast Delivery Method

The multicast-multicast delivery method does not require the controller to replicate each multicast packet received (see Figure 5). Each controller is configured for a different Internet Assigned Numbers Authority (IANA) locally scoped multicast group address (239.255.0.0 through 239.255.255.255), which each access point joins.

Figure 5 Multicast-Multicast Delivery Method



When a client sends a multicast join request to the wireless LAN, the access point encapsulates the request with an LWAPP header and forwards it to the controller. With controller software 4.2 or later (*required*), the controller proxies this link-layer protocol onto its local area network connection in the VLAN assigned to the SSID of the client and creates a client-to-multicast table entry. The controller sends an LWAPP control packet to the access point of this client and creates an identical entry table entry for this client-to-multicast group. The router that is local to the controller also adds this multicast group address to that interface for forwarding and records the controller as the last IGMP reporter.

When traffic comes through a client's multicast group, it arrives on the controller VLAN interface. The controller, using its local table of clients-to-multicast groups, sees that it has at least one listener still associated to one of its access points. It encapsulates this multicast packet with an LWAPP header and addresses it to the controller's configured multicast group, which includes the WLAN/SSID. Each access point receives this multicast. If the controller finds a recipient in its local client-to-multicast group table, it removes the LWAPP header and broadcasts the multicast packet using the WLAN/SSID broadcast key.

Router and Switch Multicast Configuration

This section outlines some basic information for enabling Multicast within your network environment. This information is intended only as a starting point for complete implementation planning and deployment.

Note For some good background information on multicast routing, refer to the "Configuring IP Multicast Routing" section of the *Cisco IOS IP Configuration Guide, Release 12.2* at http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfmulti.html.

IGMP v2 Required for Wired Clients

The Cisco wireless LAN controller acts as an IGMP proxy, sending out IGMP membership reports on its behalf. The controller supports IGMP v1, IGMP v2, and IGMP v3 reports from wireless clients. However, the controller itself generates only IGMP v2 reports on the wired network. If the IGMP querier (such as a Cisco Catalyst 6000 series switch) uses IGMP v1, it drops the IGMP v2 membership reports from the controller, and the devices will not go online because they never become members of their required multicast groups. Therefore, it is critical that the querier be configured to use IGMP v2.

Enabling IP Multicast Routing

An essential step in the correct deployment of Dräger Medical devices in a Cisco network is to enable multicast routing.

The following global configuration command-line interface (CLI) command is required to allow multicast to function in any multicast enabled network:

```
Router(config)# ip multicast-routing
```

This command should be entered to enable multicast routing on all routers within your network between the wireless LAN controller(s) and their respective access points. This allows the Cisco IOS software to forward multicast packets.

Note For more information on entering CLI commands on a Cisco wireless controller, refer to your controller configuration guide and command reference guide.

Enabling PIM on an Interface

Protocol-Independent Multicast (PIM) mode enables the routing interface for IGMP operation. The PIM mode determines how the router will populate its multicast routing table.

The following interface configuration CLI command is an example of a PIM mode configuration:

```
Router(config-if)# ip pim sparse-dense-mode
```

This method of enabling PIM in sparse-dense-mode is the most inclusive option in a multicast environment, because the command does not require the router to know the multicast group rendezvous point (RP). There are other PIM options, but the Layer 3 interface directly connected to your controller must be PIM-enabled for multicast to function.

Note All interfaces between your wireless LAN controller(s) and their respective access points *must* be enabled when you use multicast routing.

Caution Do not disable IGMP snooping in a Dräger Medical deployment, as this will cause excessive packet flooding. Disabling IGMP snooping greatly reduces the number of wireless patient monitors you can have on your network, and may still result in packet loss.

Multicast Enhancements of the Cisco Wireless LAN Controller

The following Cisco wireless LAN controller software releases contain important enhancements to multicast network environments.

Software Release 4.0.206.0

With the release of 4.0.206.0, Cisco introduces an IGMP query, which enables users to roam at Layer 2 by sending a general IGMP query when roaming is detected. The client then responds to the query with the IGMP groups to which it is a member, and this information is bridged to the wired network.

Synchronous routing was added for multicast source packets. When a client completing a Layer 3 roam sends a multicast packet from the wireless network, the foreign controller encapsulates this packet in an Ethernet over IP (EoIP) tunnel to the anchor controller. The anchor controller then forwards that packet to any wireless clients locally associated to it and bridges it back to the wired network, where it is routed using normal multicast routing methods.

Note For more information on these features, refer to your controller configuration guide and the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.0.206.0* at http://www.cisco.com/en/US/docs/wireless/controller/release/notes/cont402060rn.html.

Software Release 4.2.61.0

The latest update to multicast on the Cisco wireless LAN controller was the introduction of IGMP snooping capabilities. With the introduction of release 4.2.61.0, the controller now recognizes IGMP packets, allowing multicast packet forwarding and pruning for enhanced performance. With this recognition, it can forward multicast traffic to clients which are associated to SSIDs configured with the AP Groups feature. Prior to the 4.2 software release, multicast streams were flooded to all access points, and the resulting bandwidth congestion did not allow the Dräger Medical patient monitors to communicate reliably. Wireless LAN controller software 4.2 ensures that multicast traffic is delivered only to access points within each group.

Note For more information on IGMP snooping, refer to your controller configuration guide and the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.2.61.0* at http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn4200.html.