What's so smart about Smart-hopping?

A closer look at some of the key technology decisions behind the IntelliVue Smart-hopping WMTS band

Introduction

The IntelliVue Smart-hopping WMTS band opens up a world of possibilities:

- **Shared wireless infrastructure** for advanced wearable patient monitoring, and mobile bedside monitoring
- **Coexistence** with 802.11 networks and UHF telemetry systems
- **Two-way communication** between wireless devices and the IntelliVue Information Center
- **Scalability**, with a wireless infrastructure designed to support up to 1,024 devices

The enabling technologies include IntelliVue Smart-hopping networking, flexible network topologies, and integration with the IntelliVue Clinical Network.

This paper describes these enabling technologies in some detail and explains key terms and concepts in wireless network design with the goal of illuminating some of our reasoning behind significant design decisions.

ISM or WMTS band. What's the difference?

The band you choose for your wireless patient monitoring will affect most of your remaining decisions about what kind of system to use, where you can use it safely, and how you will manage it in relation to the numerous non-medical wireless applications you have in your facility.

As the diagram on page 2 shows, WMTS (Wireless Medical Telemetry Service) are a small slice of the radio spectrum in the United States. It is a protected spectrum for transmission of life-critical data (physiological parameters and other patient-related information) in healthcare facilities. Equipment operating in the WMTS bands (1395-1400 MHz, and 1427-1432 MHz) is operating under primary status, and therefore, protected from interference by other devices. Prior to operation, authorized health care providers who desire to use wireless medical telemetry devices must register all devices with a designated frequency coordinator.

In contrast, the ISM band are large, unlicensed areas of spectrum for a growing variety of devices that can be used to transmit everything from ECG waveforms to multimedia news streams.

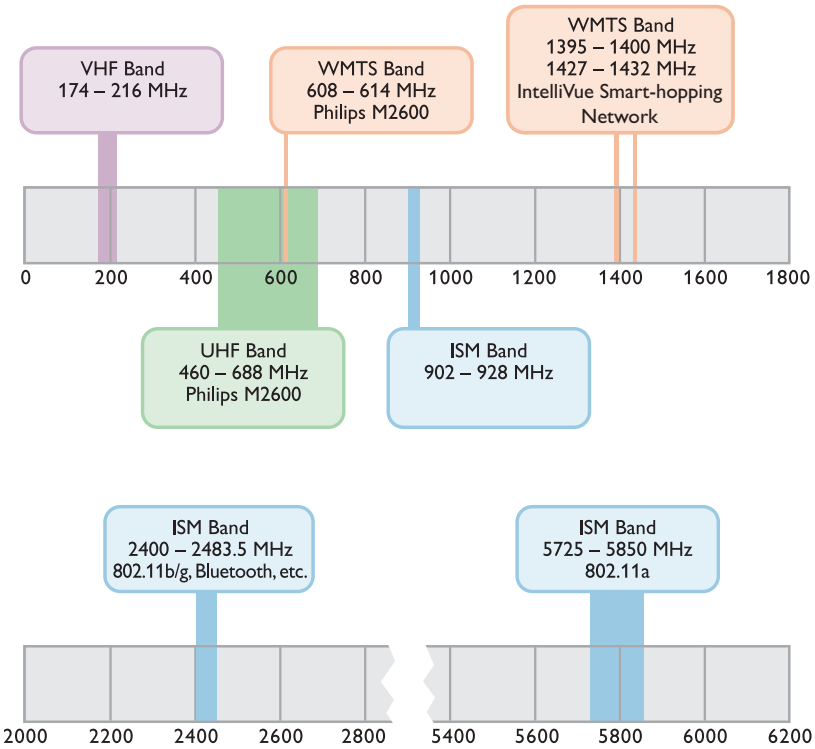
WMTS for primary wireless patient monitoring

In patient monitoring applications, many devices are sending continuous data into the infrastructure at the same time, all the time. In the United States, the best protection for those continuous data streams is the reserved, licensed spectrum in the WMTS band.

PHILIPS

sense and simplicity

Spectrum allocations for scientific, industrial and medical use



While the idea of using one 802.11 wireless infrastructure for patient monitoring and non-medical devices is appealing, especially for hospitals that already have a network in place, we believe the safety advantages of operating in protected bandwidth and the performance advantages of using an infrastructure that is optimized for wireless patient monitoring are valuable enough to warrant a dedicated monitoring infrastructure.

No wireless system is immune from interference, but using a dedicated infrastructure for patient monitoring avoids many frequency management problems with 802.11 or UHF systems sharing the same airspace.

WMTS band devices[1]

- Medical telemetry devices
- Patient monitors

ISM (Industrial, Scientific, and Medical) band devices

- Patient monitors
- Cordless phones
- Laptop computers
- Peripherals such as wireless keyboards and mice
- Wireless webcams
- Bluetooth devices such as cameras and PDAs
- 802.11 a/b/g access points
- Microwave ovens

Using the ISM band for this type of application can lead to contention with the many other devices that use the same spectrum. Effective throughput could then be degraded, and latencies throughout the system would increase. Since physiologic data has "real time" requirements, excessive latency cannot be tolerated. The perceptible effect of latency for end users is gaps in the waveform display at the central station, gaps in wave review and discontinuities in arrhythmia monitoring.

The limited bandwidth of WMTS makes it very important to use that spectrum efficiently. IntelliVue Smart-hopping technology is adapted to the specific demands of patient monitoring, and Philips 1.4 GHz wireless infrastructure is designed to support up to 1,024 wireless telemetry devices and/or wireless patient monitors.

[1] In some areas of the US, utility telemetry still have primary allocation of part of the WMTS spectrum. In these areas, Philips 1.4 GHz radios can still operate with secondary status.

ISM can be used for patient monitoring, provided the risks are understood

The FCC requires devices in the ISM band to share spectrum. This means that no device can reserve bandwidth for its exclusive use. Every device has to know how to take turns and deal with collisions. Most do this by using various spread spectrum schemes and retry mechanisms. In crowded environments, data transmissions will collide more often, increasing the delay, or latency, of the network.

For a telemetry device in particular, increased latency can result in gaps in the physiologic data, which causes monitoring discontinuities. A wireless bedside or transport monitor can still generate and display alarms locally, so a spotty wireless connection to the central station does not jeopardize primary monitoring.

Key concepts in wireless network design

As wireless technologies (especially 802.11-based) have gained mass market appeal, there is a rapid evolution of hardware and protocols to meet increasing demand for bandwidth and Quality of Service (QoS). These are some of the key elements of wireless networking that we considered in building our IntelliVue Smart-hopping WMTS:

- Communication protocols
- Quality of Service (QoS)
- Roaming
- Scalability

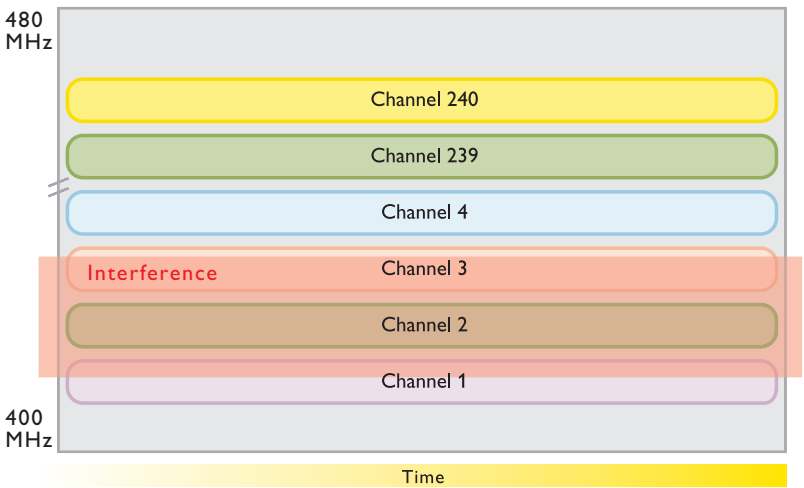
Communication protocols

The protocol specifies how wireless devices and access points will communicate on the network. In this context, the term "channel" always denotes the path between the transmitter and receiver. Depending on the type of wireless system used, that channel or path can be a frequency range, a repeating pattern, a timeslot, a code or some combination of these paths. For our IntelliVue Smart-hopping WMTS, we chose to adapt a relatively long-standing, proven in-building cellular technology. The diagrams and explanations that follow show how it compares with other well-known protocols.

(Fixed Frequency) Narrowband FM

Narrowband FM is the protocol we use in our UHF telemetry system. Each channel corresponds to a specific range of frequencies that is assigned to a particular device. In an environment without competing devices, this is a very efficient way to transmit data. A transmitter and its corresponding receiver simply tune in to each other. One disadvantage is that this type of system cannot actively avoid interference, and interference can easily take out a channel completely. Another limitation is that it doesn't support spectrum reuse. Each channel is dedicated to a single transmitter/receiver pair. It cannot be shared by other pairs, and so the total number of channels (that is, patients that can be monitored at any given time) is limited.

Narrowband FM

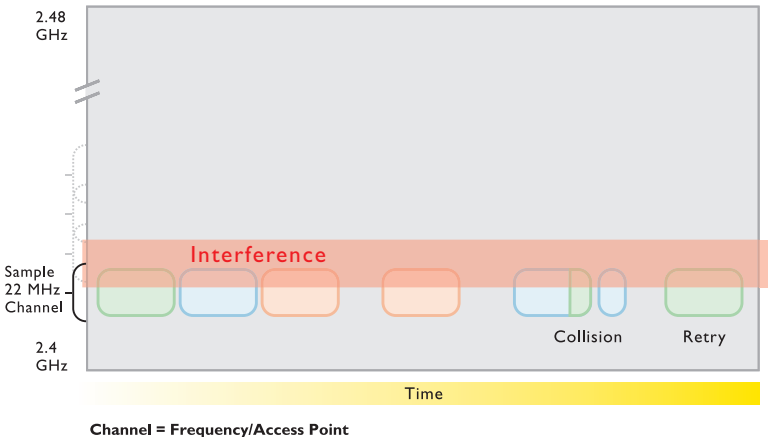


Channel = Frequency Range.

Effect of interference on narrowband FM system.

Data dropouts in sample telemetry waveform display.

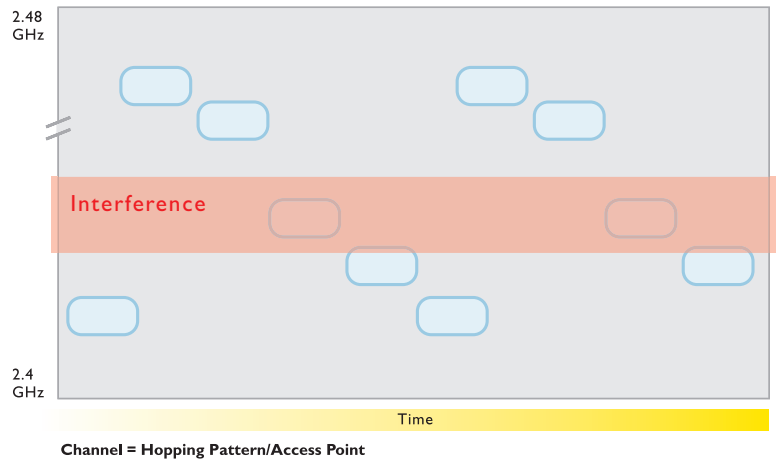
Direct sequence spread spectrum (DSSS)



Effect of interference on a DSSS system.

Direct sequence spread spectrum 802.11b/g divides the ISM spectrum at 2.4 GHz into 14 overlapping 22 MHz channels. By spreading the signal over such a relatively wide range, the system is more tolerant of interference. 802.11b/g devices are able to transmit over a range of channels (for example, channels 1-11 are used in the United States), while each 802.11b/g access point is set to just one channel. Thus, every device within range of an access point uses the same channel to communicate with it. 802.11b/g systems also use what is called Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). As a result, the end devices initially listen to the channel to identify whether or not another node is transmitting on the channel within wireless range. If the channel being used is busy, the end device will wait to transmit which can introduce delay.

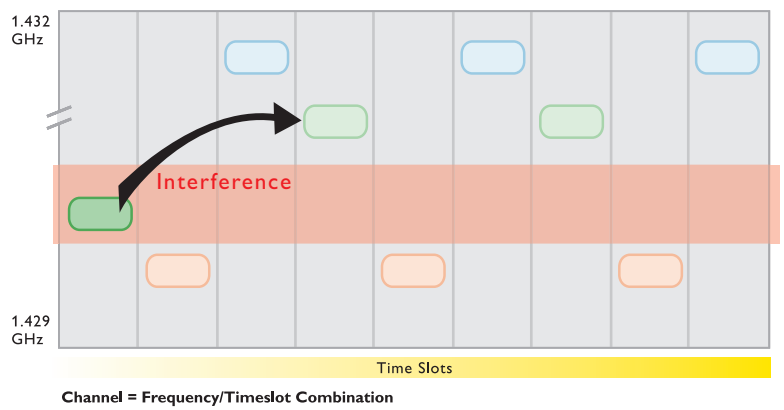
Frequency hopping



Effect of interference on frequency hopping system.

Frequency hopping devices (e.g., Bluetooth), jump constantly (typically hundreds of times each second) through a range of frequencies in a repeated, "pseudo-random" pattern set by the access point. Each device's hopping pattern is its channel. In installations with multiple access points (and thus, multiple hopping patterns), devices will occasionally land on the same frequency at the same time and interfere with each other, requiring a retransmission. Typically the next hop is clear, but in dense deployments (lots of devices), collisions become more of a problem.

Smart-hopping



Effect of interference on the IntelliVue Smart-hopping Network.

IntelliVue Smart-hopping Networks synchronize all of the access points. Devices on the system are allotted time slots during which they can transmit their data over a range of frequencies. IntelliVue Smart-hopping Network devices switch frequency or time slot only to avoid interference or when they detect a significantly stronger signal. Fewer hops means fewer collisions, even on a busy system.

Quality of Service (QoS)

Quality of Service is the ability to assure a certain level of performance to given applications over a network. It has become more important on wireless networks as more users and applications share the same airspace. Multimedia streams and voice communications are particular challenges because end users perceive poor network performance in the form of poor quality video/voice-over-IP (VOIP) phone connection.

Quality of Service is absolutely essential for wireless patient monitoring applications. Unlike multimedia streams, patient monitoring data cannot be buffered to mask jitter and latency on the receiving end. If the network cannot reliably deliver continuous, real-time vital signs and alarms, patients' lives are placed at risk.

Strategies for providing QoS

Quality of service (QoS) for wireless network environments can prove challenging. There are different mechanisms to address aspects of QoS.

Signal path is an important consideration for QoS. The IntelliVue Smart-hopping Network provides QoS along the full signal path from the end monitoring device to the access point and through to the IntelliVue Information Center. The Smart-hopping network provides Qos through a combination of adaptive spectrum management and automatic transmission retry. Strategies such as isolating a system may help with application performance but don't necessarily guarantee QoS. Traffic shaping appliances address only the wired portion of the signal path, beginning at the access point. It's important to consider end to end QoS when deploying real time monitoring systems.

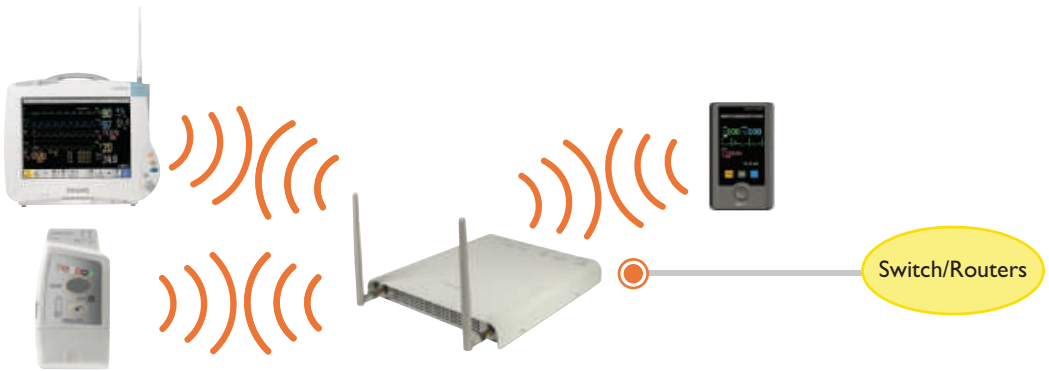
Common metrics for network performance

jitter (transmission time variability from packet to packet) – Patient monitoring traffic needs to flow steadily. Variability is imperceptible when receiving an email message that is reconstituted on the receiving end, but the display of vital signs data is continually refreshed so excessive jitter is not tolerable.

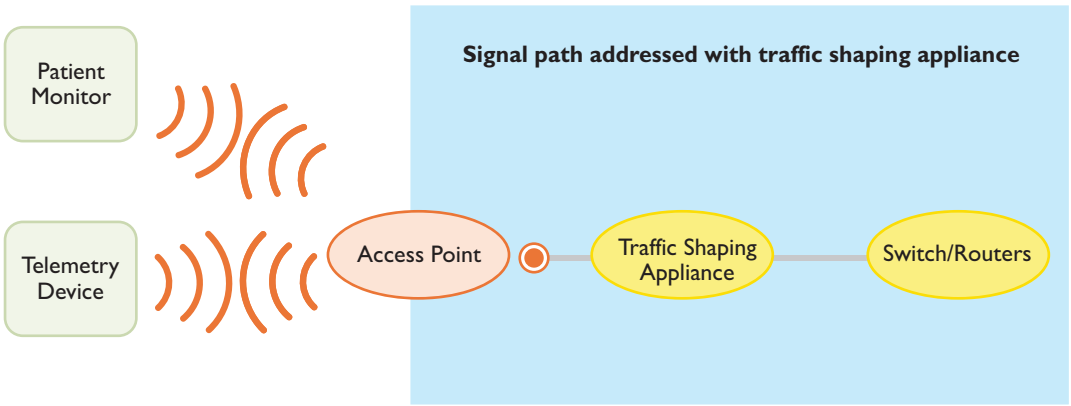
Latency (transmission delay) – Transmission delay comes from network overhead (time spent encoding and decoding packets, etc.) and from traffic loads. Since patient status can change in a heartbeat, patient monitoring networks cannot tolerate excessive latency.

Loss (dropped packets) – On wireless networks, packets are most likely to be dropped during hand-offs between access points and when too many devices attempt to communicate with the access point at the same time. The reliability of hand-offs depends heavily on the protocol being used. Data loss is highly undesirable on a patient monitoring network because dropped vital signs information could delay or prevent an alarm from reaching the central station.

Signal path addressed with IntelliVue Smart-hopping 1.4 GHz WMTS



Quality of Service all the way to the end user device with the IntelliVue Smart-hopping Network.



Traffic shaping appliances cannot provide Quality of Service along the full signal path.

Roaming

One of trickiest things to do in wireless networks is to hand off communications with a portable device between access points. Conceptually, it's much like a trapeze act, where the release and catch have to be coordinated on the fly.

Depending on the protocol used, handoffs may be managed by the access point, the device, or both. Moreover, handoff methods may be optimized for speed, reliability, or simplicity.

With the IntelliVue Smart-hopping Network, handoffs are controlled by the portable device. Our "make before break" method is optimized for speed and reliability. When moving from one access point to another, an IntelliVue Smart-hopping device temporarily maintains parallel communications with both access points. Once the new connection is established, the access points check with each other to be sure no packets have been dropped.

Contrast this with 802.11 roaming, which is a "break before make" method, optimized for simplicity. An 802.11 device will not even attempt to roam until it has already begun experiencing data loss. It then cuts off its connection with one access point before trying to associate with another. When evaluating a device for use on a Wi-Fi network, it's important to understand the mobility performance requirements of the device and whether tolerance to packet loss in a mobile environment is acceptable. The Smart-hopping network alleviates any concerns around roaming handoffs and mobile performance by leveraging the 'make before break method'.

Scalability

Wireless network performance is closely tied to the density of devices and/or applications on the system.

For this reason, it is very important to plan ahead for the growth of your system over time. The IntelliVue Smart-hopping WMTS network can support up to 1024 wireless patient monitoring devices. An ISM network that combined medical and non-medical wireless uses could potentially have to scale much higher than that.

Seamless handoff: When moving from one access point to another, IntelliVue Smart-hopping devices temporarily maintain parallel communications with both access points while it analyzes the quality of the links. Once the device figures out which link is stronger, it closes its connection with the weaker one.

The IntelliVue Wired/Wireless Clinical Network: It all works together

The IntelliVue Clinical Network manages all of the wired and wireless data flows within the patient monitoring network as well as all data exchanges between the isolated patient monitoring network and the hospital LAN.

We have designed the IntelliVue Smart-hopping Network with the capacity to support wireless patient monitoring needs throughout a hospital.

For large installations with multiple care units, we use routers to manage all of the network interconnections. Smaller facilities might choose a direct (non-routed) installation, in which the IntelliVue Smart-hopping Network connects to only one IntelliVue Information Center or Database Server.

Making the Most of Two-Way Communications

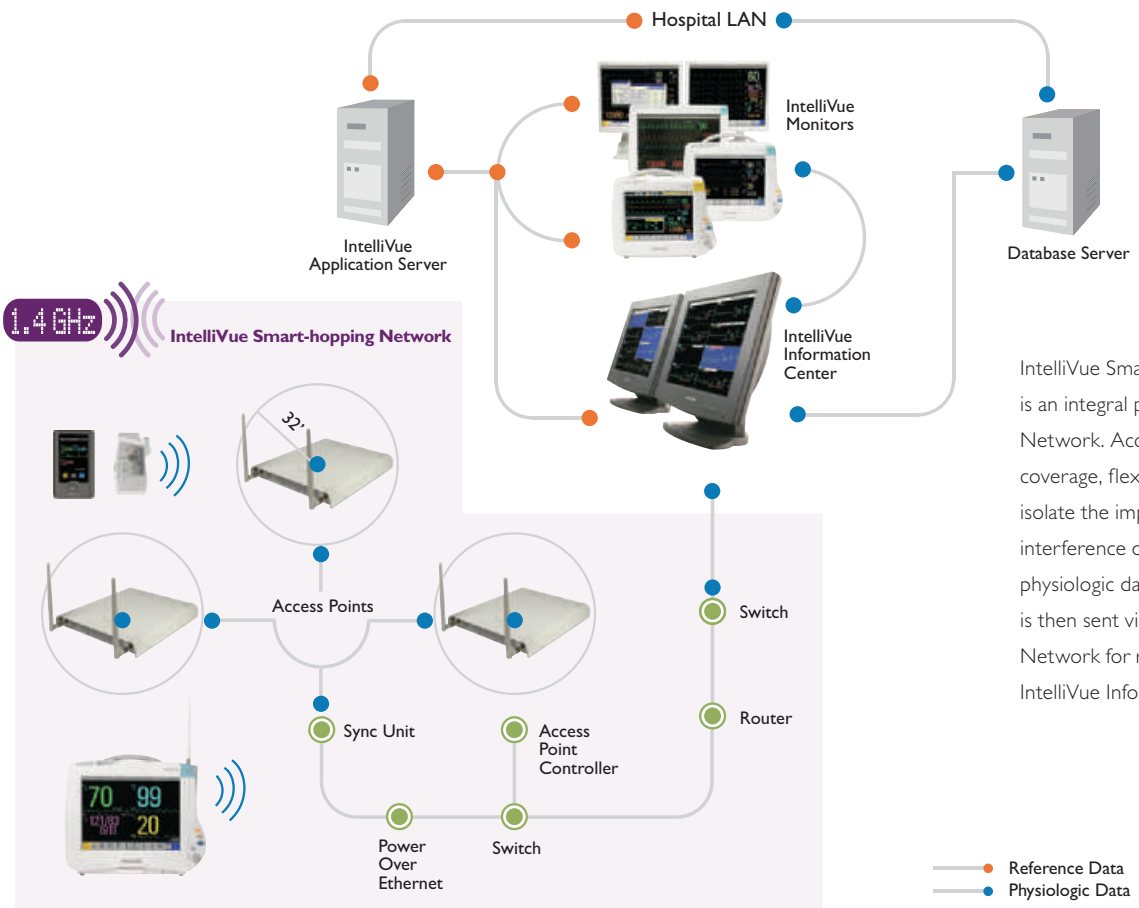
The IntelliVue Smart-hopping Network permits two-way communications between wireless devices and the IntelliVue Information Center. And the IntelliVue patient monitoring system makes good use of that capability in several ways.

Device location – When a mobile patient monitor goes missing (as they often do), a user on any IntelliVue Information Center connected to the IntelliVue Smart-hopping Network can activate a beeper on the device. As long as the device is within network range and has a good battery, it will keep beeping until it's retrieved.

SpO_2 spot checks – Users can also initiate SpO_2 spot checks from the IntelliVue Information Center, as well on the device itself.

Auto-resume – When a mobile patient monitor leaves the IntelliVue Smart-hopping Network coverage area, it sounds a warning. An out-of-range message also appears at the IntelliVue Information Center. And, when a device comes back in range, as when a patient returns from Radiology, for example, it automatically resumes communication with the IntelliVue Information Center.

Pairing – The IntelliVue Information Center is able to pair the signal from a wearable patient monitor with a bedside monitor. Linking the two signals allows for a single combined display at the central station and at the bedside.



IntelliVue Smart-hopping WMTS is an integral part of the IntelliVue Network. Access points provide coverage, flexibility and help to isolate the impact of broadband interference on continuous physiologic data. Reference data is then sent via the IntelliVue Network for review at the IntelliVue Information Center.

Conclusion

As healthcare technology providers, we are committed above all to patient safety. IntelliVue Smart-hopping WMTS is designed specifically to optimize performance of a patient monitoring environment. IntelliVue Smart-hopping technology limits contention between devices.

Please visit www.philips.com/WirelessSolutions

Philips Healthcare is part of Royal Philips Electronics

www.philips.com/healthcare
healthcare@philips.com

Printed in The Netherlands
4522 962 74731 * AUG 2011