PHILIPS

Patient monitoring

Smart-hopping

What's so smart about Smart-hopping?

A closer look at some of the key technology decisions behind the Philips Smart-hopping 2.0 1.4 GHz common wireless Infrastructure

Introduction

The Philips Smart-hopping 2.0 1.4 GHz common wireless infrastructure opens up a world of possibilities:

- **Shared wireless infrastructure** for advanced cellular telemetry and wireless bedside monitoring
- **Low risk** of interference from other wireless systems, inside or outside the hospital
- **Coexistence with 802.11** networks and UHF telemetry systems
- **Two-way communication** between wireless devices and the Philips Patient Information Center IX (PIC iX)
- **Scalability,** with a wireless infrastructure designed to support up to 1,000 devices

The enabling technologies behind these capabilities include Smart-hopping® technology in the 1.4 GHz Wireless Medical Telemetry Service (WMTS) band, flexible network topologies, and integration with the Philips 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.

* 47CFR90.259 and 47CFR95 Subpart H

ISM or WMTS. What's the difference?

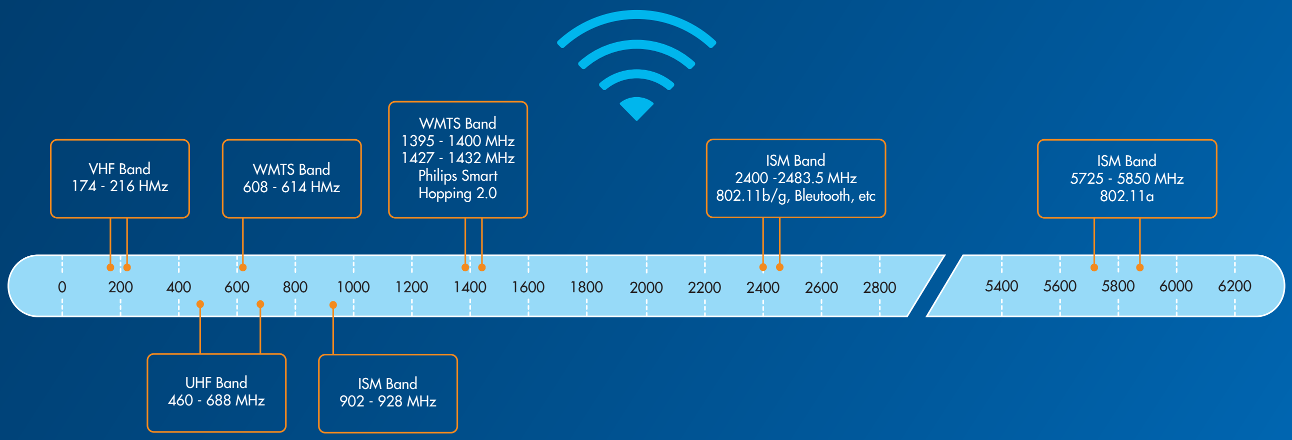
The band you choose for your wireless patient monitoring will affect most of your remaining decisions about what kind of system to use, where you can use it safely, and how you will manage it in relation to the probably numerous non-medical wireless applications you have in your facility.

As the diagram below shows, Wireless Medical Telemetry Service is a small slice of the spectrum. But it is reserved for transmission of life-critical data (physiological parameters and other patient-related information) in healthcare facilities[1]. It's also licensed spectrum, which gives hospitals that go through the licensing process the advantage of primary user status over an interfering, unlicensed system.

In contrast, the Industrial, Scientific and Medical (ISM) band is a large, unlicensed spectrum space for a growing variety of devices that can be used to transmit everything from ECG waveforms to multimedia news streams.

In the United States, WMTS is the best choice 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.



WMTS 608-614 MHz (1.5 MHz channels defined), 1395-1400 MHz (no channels defined), 1427-1432 MHz (no channels defined) = 16 MHz total available bandwidth

ISM 902-928 MHz, 2400 – 2483.5 MHz, 5725-5850 MHz = 234.5 MHz total available bandwidth – Spread spectrum required

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. Our 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 1,000 wireless telemetry devices and/or wireless patient monitors.

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 isolating the 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

- Medical telemetry devices
- Patient monitors

ISM band devices

- Patient monitors
- Cordless phones (not cell phones)
- Laptop computers
- Peripherals such as wireless keyboards and mice
- Wireless webcams
- Bluetooth devices, such as cameras
- 802.11 a/b/g access points
- Microwave ovens

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 telemetry patients in particular, increased latency can result in gaps in the physiologic data, which cause 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.

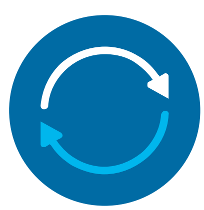
Key concepts in wireless network design

As wireless technologies (especially 802.11-based) are common, we are seeing rapid evolution of hardware and protocols to meet increasing demand for bandwidth and Quality of Service (QoS). This section is intended to give you an overview of the following key elements of wireless networking that we considered in building our 1.4 GHz common wireless infrastructure.

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 kind of wireless system you're using, though, that channel or path can be a frequency range, a repeating pattern, a timeslot, a code or some combination of these things. For our 1.4 GHz common wireless infrastructure, we have chosen to adapt a relatively long-standing, proven in-building cellular technology called DECT. The diagrams and explanations that follow show how it compares with other well-known protocols.

Communication protocols

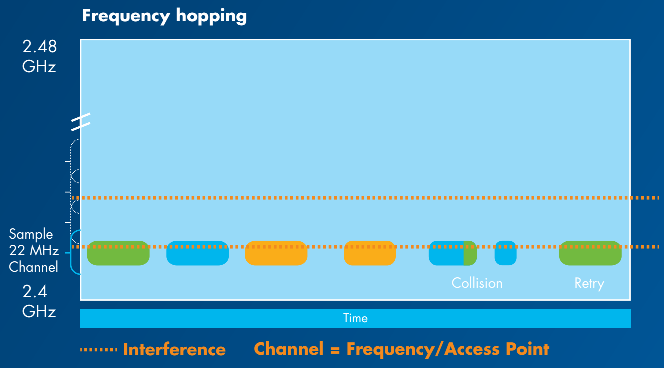
Quality of Service (QoS)



Handling handoffs (roaming)

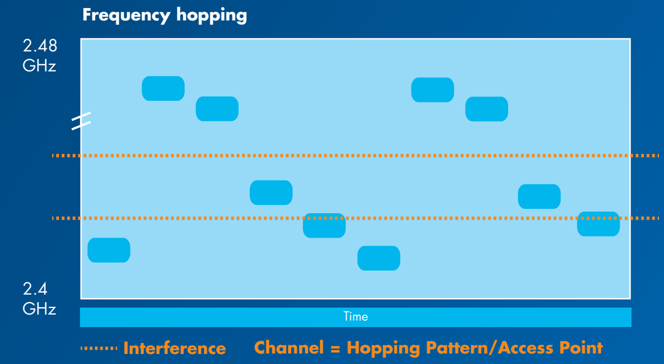
Scalability

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, we use channels 1-11 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 collision-detection multiple access (CDMA). Since every device transmits whenever it has data to send, they all have to be able to tell when their signals have collided, and then retry. The rate of collisions (and thus, latency) generally increases with the number of devices on the systems.



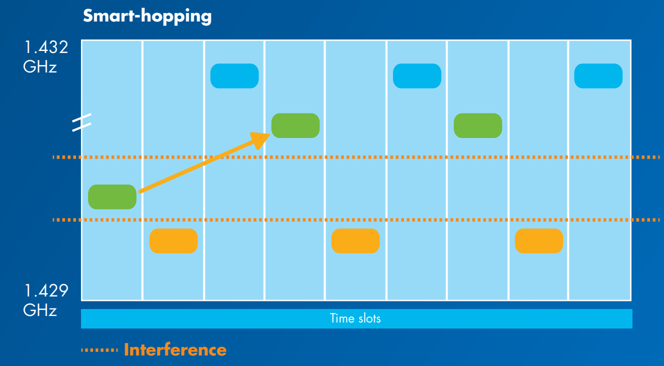
Effect of interference on a DSSS system

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.



Effect of interference on frequency hopping system

Smart-hopping/DECT systems 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. Smart-hopping 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.



Effect of interference on Smart-hopping system

Quality of Service (QoS)

Quality of Service is a measure of a network's ability to assure bandwidth for a given application. 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 readily perceive poor network performance in the form of stuttery video or a patchy 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 endangered.

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 really 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.

Strategies for providing QoS

How to provide QOS in the wireless network environment is still a fairly open question. In the ISM band, QoS is well understood for Wi-Fi devices: IEEE802.11e standard, which addresses QoS, has been ratified in 2005, and the corresponding industry certification, Wi-Fi Alliance WMM (Wi-Fi Multimedia) has been introduced in 2004. Nowadays all Wi-Fi Access Points (AP) and client devices support QoS.. Other vendors have developed proprietary protocols that aim to address QoS in the ISM band.

Isolating a system is one way to ensure QoS, though this is difficult to do with systems that use highly desirable bandwidth. WMTS systems benefit from the relative isolation of their reserved airspace.

Another important factor to consider for QoS is the signal path. Philips Smart-hopping technology provides QoS along the full signal path – wired and wireless – from the transceiver to the access point and through to the central station.

Other technologies designed to provide QoS, such as traffic shaping appliances, address only the wired portion of the signal path beginning at the access point.

Signal path addresses with Philips 1.4 GHz infrastructure

Quality of Service all the way to the end user device with Philips Smart-hopping technology.

Seamless handoff: When moving from one access point to another, a DECT/Smart-hopping portable device temporarily maintains 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.

Handling handoffs

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 you use, handoffs may be managed by the access point, the device or both. Moreover, handoff methods may be optimized for speed, reliability or simplicity.

With DECT and Philips Smart-hopping technology, 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, a Smart-hopping portable 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. The protocol is designed for sporadic connections in different places (such as a home network, coffee shop and airport), not continuous operation in motion.

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 Philips Smart-hopping 2.0 infrastructure can support up to 1,000 wireless patient monitoring devices. An ISM network that combined medical and non-medical wireless uses could potentially have to scale much higher than that.

The Philips wired/wireless clinical network: It all works together

The Philips 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 Philips Smart-hopping 2.0 1.4 GHz wireless infrastructure with capacity to support wireless patient monitoring needs throughout a facility. For large facilities with multiple telemetry units and flexibly monitored beds, we use routers to manage all of the network interconnections.

Smaller facilities might choose a direct (non-routed) installation, in which the 1.4 GHz wireless infrastructure is associated with only one Philips Patient Information Center iX (PIC iX) or Database Server.

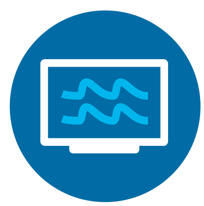
Making the most of two-way communications

Our wireless infrastructure permits two-way communications between wireless devices and the PIC iX. And Philips Smart-hopping 2.0 makes good use of that capability in several ways.

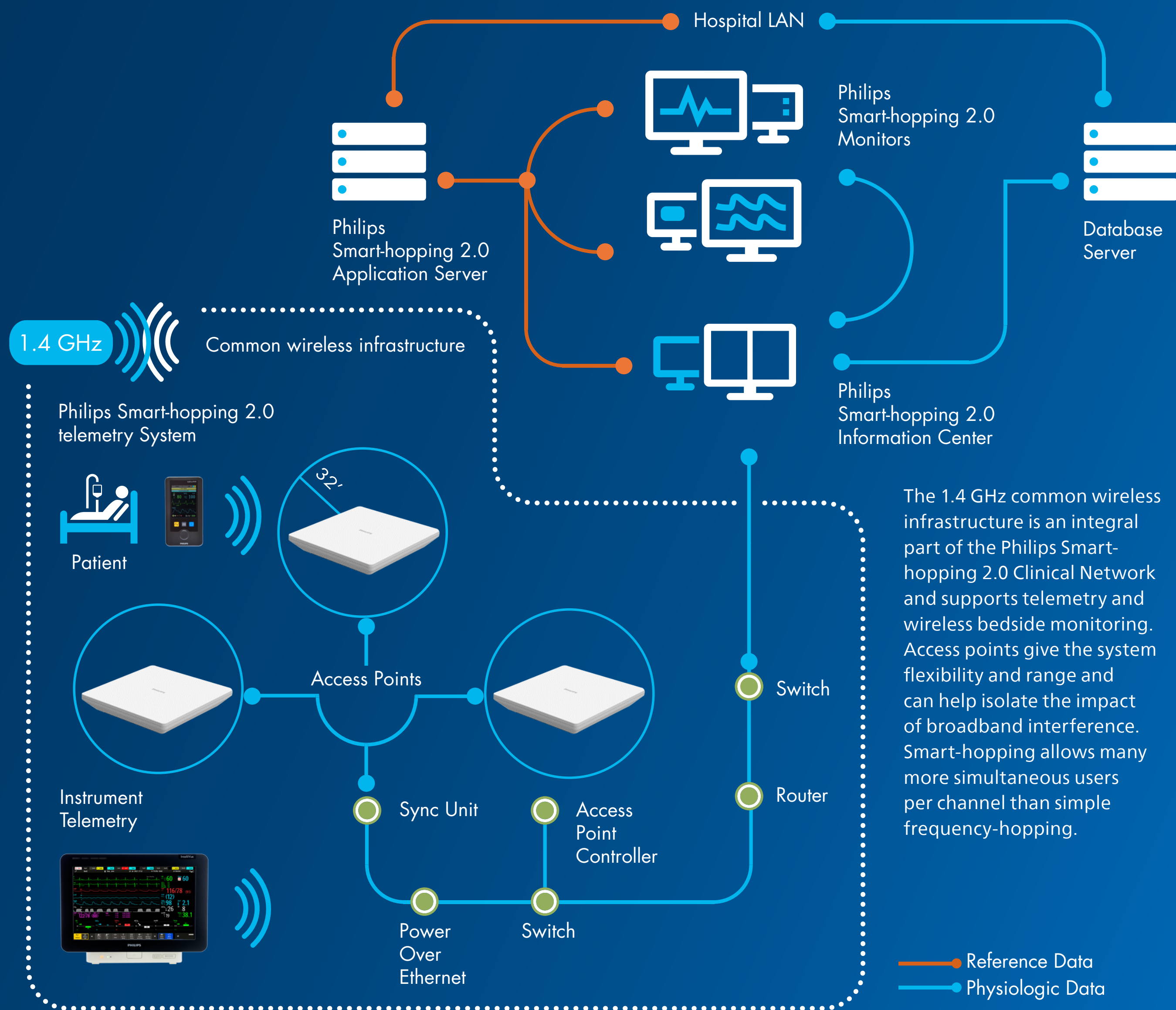
Device location
When a patient-worn Telemetry monitor goes missing (as they often do), a user on any PIC IX location connected to the wireless network can activate a beeper on the device. As long as the Telemetry Monitor is within network range and has a good battery, it will keep beeping until it's retrieved.

SpO_2 spot checks
Users can also initiate SpO_2 spot checks from the PIC iX, as well on the device itself.

Auto-resume
When a wireless monitor or Telemetry device leaves the network, it sounds a warning. An out-of-range message also appears at the PIC iX. And, when a device comes back in range, when a patient returns from Radiology, for example, it automatically resumes communication with the PIC iX.



Telemetry overview
The PIC iX is able to pair a patient's Telemetry Monitor with his or her bedside monitor. Linking the two signals allows for a single combined display at the central station and at the bedside.



The 1.4 GHz common wireless infrastructure is an integral part of the Philips Smart-hopping 2.0 Clinical Network and supports telemetry and wireless bedside monitoring. Access points give the system flexibility and range and can help isolate the impact of broadband interference. Smart-hopping allows many more simultaneous users per channel than simple frequency-hopping.

Conclusion

As healthcare technology providers, we are committed above all to patient safety. Our 1.4 GHz common wireless infrastructure, is designed specifically to optimize performance in the patient monitoring environment. Philips Smart-hopping 2.0 technology limits contention between devices.

Isolation of the network reduces competing traffic. And, operating in protected WMTS spectrum essentially eliminates the possibility of interference from non-medical wireless devices.

In the United States, we have the advantage of reserved WMTS spectrum, which provides a relatively interference-free environment for patient monitoring. To give our customers the economies of shared infrastructure, we have designed the Philips Smart-hopping 2.0 1.4 GHz Wireless Infrastructure to support up to 1,000 telemetry devices and wireless bedside monitors, leaving the 802.11 airspace free and clear.

www.philips.com

00000069-00-00 * JUL 2023