



Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

PROJECTE FINAL DE CARRERA

AD HOC NETWORKING IN A MEDICAL ENVIRONMENT

Estudis: ENGINYERIA DE TELECOMUNICACIÓ

Autor: DIEGO BENAVENTE MIRA

Director: DR. T. J. J. DENTENEER
Principal Research Scientist
Distributed Sensor Systems
Philips Research

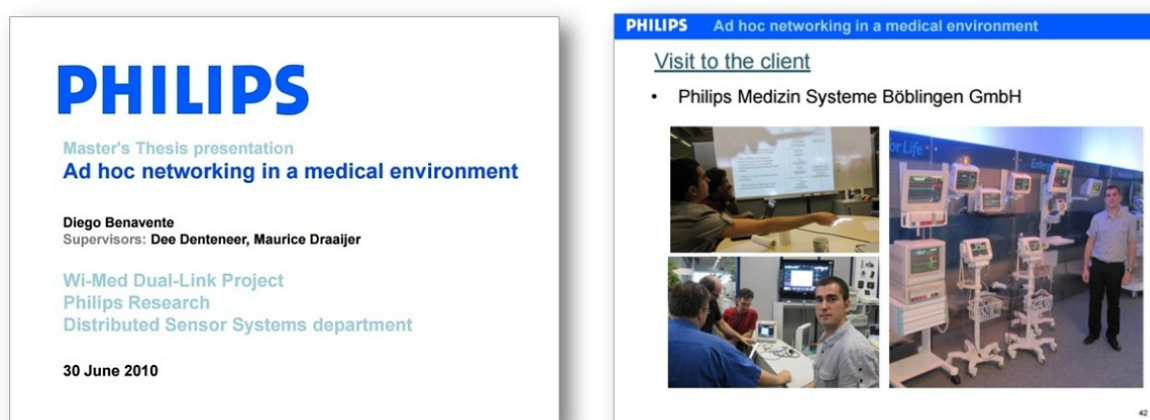
Ponent: DR. RAMÓN A. FERRÚS FERRÉ
Professor Titular
Departament de Teoria del Senyal i Comunicacions
Universitat Politècnica de Catalunya

Any de realització: 2010
Any de presentació: 2016

Collaborations

The research work for this Master of Science thesis report was done under the program “UPC-Empresa. PFC a Empreses internacionals. Tardor 2009-10” from the *Escola Tècnica Superior d’Enginyeria de Telecomunicació de Barcelona*, during an internship at the Distributed Sensor Systems department of Philips Research (Philips Electronics Nederland B.V.) in Eindhoven, The Netherlands, from september 2009 to june 2010.

At the end of the internship the results of the research and the developments were shown to the fellow researchers at the department and to the client during a visit to Philips Medizin Systeme Böblingen GmbH in Germany.



In July 2016 this work was presented as Master of Science thesis report for *Enginyeria de Telecomunicació Pla 92* degree at the *Escola Tècnica Superior d’Enginyeria de Telecomunicació de Barcelona* with Prof. Ramón Ferrús from Signal Theory and Communications Department as lecturer, Prof. Jordi Perez from Signal Theory and Communications Department as President of the tribunal and Prof. Isidro Martín from Electrical Engineering as Vocal.



Note: Although the conclusions detailed in chapter 8 together with the *further research* recommendations were contextualized at the time of publication in accordance to the current validity and maturity level of Wi-Fi technology, the comparison and selection of *Applicable technologies* was carried out according to the available technologies in 2010.

Col·laboracions

La recerca i el desenvolupament d'aquest Projecte es van dur a terme entre setembre del 2009 i juny del 2010 sota el programa "UPC-Empresa. PFC a Empreses internacionals. Tardor 2009-10" de l'Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona, a les instal·lacions del departament *Distributed Sensor Systems Philips Research* de l'empresa *Philips Electronics Nederland B.V.*, al High Tech Campus de la ciutat d'Eindhoven als Països Baixos.

Al finalitzar l'estada els resultats de la investigació es van presentar a la resta de companys investigadors del departament així com al client durant una visita a *Philips Medizin Systeme Böblingen GmbH* a Alemanya.

Al juliol de 2016 aquest projecte es va presentar com a PFC (Projecte de Fi de Carrera) dels estudis d'Enginyeria de Telecomunicació Pla 92 a l'Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona amb el Prof. Ramón Ferrús del Departament de Teoria del Senyal i Comunicacions com a Ponent, el Prof. Jordi Perez del Departament de Teoria del Senyal i Comunicacions com a President del tribunal i el Prof. Isidro Martín del Departament d'Enginyeria Electrònica com a Vocal.

Nota: Tot i que les conclusions detallades al capítol 8 juntament amb les recomanacions de línies d'investigació futures es van contextualitzar al moment de la publicació tenint en compte la vigència i nivell de maduresa de les tecnologies Wi-Fi, la comparació i tria de tecnologies aplicables es van realitzar segons les tecnologies disponibles al 2010.

Colaboraciones

La investigación y desarrollo de este Proyecto se llevó a cabo entre septiembre de 2009 y junio de 2010 bajo el programa "UPC-Empresa. PFC a Empresas internacionales. Tardor 2009-10" de la *Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona*, en las instalaciones del departamento *Distributed Sensor Systems Philips Research* de la empresa *Philips Electronics Nederland B.V.*, en el High Tech Campus de la ciudad de Eindhoven en los Países Bajos.

Al finalizar la estancia los resultados de la investigación se presentaron al resto de compañeros investigadores del departamento así como al cliente durante una visita a *Philips Medizin Systeme Böblingen GmbH* en Alemania.

En julio de 2016 este proyecto se presentó como PFC(Proyecto de Fin de Carrera) de los estudios de Ingeniería de Telecomunicaciones Plan 92 en la *Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona* con el Prof. Ramón Ferrús del Departamento de Teoría de la Señal y Comunicaciones como Ponente, el Prof. Jordi Perez del Departamento de Teoría de la Señal y Comunicaciones como Presidente del tribunal y el Prof. Isidro Martín del Departamento de Ingeniería Electrónica como Vocal.

Nota: A pesar de que las conclusiones detalladas en el capítulo 8 junto con las recomendaciones

de líneas de investigación futuras se contextualizaron al momento de la publicación teniendo en cuenta la vigencia y nivel de madurez de las tecnologías Wi-Fi, la comparación y elección de tecnologías aplicables se realizó según su disponibilidad en el año 2010.

Acknowledgements

I would like to express my gratitude to my mentor and supervisor at Philips, Dee Denteneer, for his patience and good vibes, and to Maurice Draaijer for his help and resolution.

My acknowledgements to Prof. Ferran Casadevall for encouraging me with his lectures, to Prof. Ramón Ferrús for supervising my work, to the members of the tribunal for valuing my efforts invested in this work, and to the Mobility and International Relations Office and Academic Secretary of my school for helping with bureaucracy.

I would like to thank all the people that directly or indirectly helped me to arrive to this point of my life. I dedicate this work to them.

Confidencialitat

El contingut d'aquesta publicació pot incloure coneixements tècnics secrets i informació de valor tècnic i comercial per la companyia Philips Research, department of Distributed Sensors Systems.

Segons el corresponent Acord de Confidencialitat, aquest document ha de ser classificat com a confidencial i per tant no pot ser accessible al públic per un període de 2 anys a partir de la seva data de lectura. Al final d'aquest període, l'informe podrà ser depositat a la biblioteca de la Universitat Politècnica de Catalunya per a ser accessible al públic.

Confidencialidad

El contenido de esta publicación puede incluir conocimientos técnicos secretos e información de valor técnico y comercial para la compañía Philips Research, department of Distributed Sensors Systems.

Según el correspondiente Acuerdo de Confidencialidad, este documento debe ser clasificado como confidencial y por lo tanto no ser accesible al público por un período de 2 años a partir de la fecha de su lectura. Al final de dicho período, el informe se podrá depositar en la biblioteca de la Universitat Politècnica de Catalunya para ser de acceso público.

Non Disclosure Agreement

This publications contents might include secret know-how and information of a technical and commercial value for the company Philips Research, department of Distributed Sensors Systems. According to the corresponding Non Disclosure Agreement, this thesis report should be classified as confidential and therefore not be accessible to the public for a period of 2 years starting the date of its presentation. At the end of such period, the report may be stored at the Universitat Politècnica de Catalunya corresponding library to be publicly accessible.

Abstract

Medical patient monitoring would benefit from the capability to wirelessly connect bedside fixed monitors with portable monitoring equipment. Several *ad hoc* networking techniques for Wi-Fi equipment are available and reaching maturity.

The potential benefits of applying these wireless techniques to patient monitoring in hospitals are several:

Firstly, enabling continuous patient monitoring throughout the whole hospital. Secondly, using the already deployed hospital network for IT applications, since Wi-Fi is a well-known and widespread technology in hospital facilities. Moreover, Wi-Fi is a technology that allows using open-source software, whose benefits include flexibility, reliability, stability and auditability, among others.

In this project, the potential solutions and standards (WDS, TDLS, Wi-Fi Direct, Soft AP, 802.11s mesh networking and the good old ad hoc mode, among others) were compared in terms of functionality, hardware requirements and availability of platforms, prior to take a decision on its suitability.

The decision was to select the *Soft AP* approach, which relies in the virtualization of a single wireless hardware adapter (operating simultaneously in client mode and access point mode) to allow both the connectivity with the hospital network for forwarding the real-time physiological data as well as the procedures involved in the pairing between bedside fixed monitors and portable monitoring units.

Furthermore, the design, development and testing of an open source implementation in an embedded Linux platform, based in the selected approach, was carried out to investigate the quality of the ad hoc link in the presence of other Wi-Fi equipment.

The performance test results confirmed the compliance of the implemented prototype following the Soft AP approach with the medical scenario requirements in terms of throughput (more than 5 Mbps available), link delay (under 200 ms) and delay jitter (under 200 ms), in a quiet channel as well as in a fully loaded channel environment.

Resum

La monitorització mèdica de pacients es veuria beneficiada amb la incorporació de la capacitat de connectar sense fils els monitors fixos de capçalera amb els equips de monitorització portàtil. Diverses tècniques *ad hoc* per a la connexió d'equips mitjançant xarxes Wi-Fi són disponibles avui dia i la seva maduresa tecnològica és clara.

Els potencials beneficis de l'aplicació d'aquestes tècniques sense fils per a la monitorització de pacients en hospitals són diversos: En primer lloc, permetria la monitorització contínua del pacient al llarg de tot l'hospital, amb la consegüent major mobilitat per al pacient. En segon lloc, utilitzaria les xarxes Wi-Fi habitualment ja desplegades per a altres aplicacions de TI, aprofitant que la tecnologia Wi-Fi és ben estesa a les instal·lacions hospitalàries. D'altra banda, aquesta tecnologia permet l'ús de programari de codi obert, el que comporta avantatges com flexibilitat, fiabilitat, estabilitat i capacitat d'auditoria, entre d'altres.

En aquest projecte, les possibles solucions i estàndards (WDS, TDLS, Wi-Fi Direct, Soft AP, xarxes mallades 802.11s i el mode ad hoc IBSS, entre d'altres) van ser comparats en termes de funcionalitat, requisits del maquinari i disponibilitat de plataformes, abans de prendre una decisió sobre la seva idoneïtat.

La decisió va ser la selecció de l'enfocament Soft AP, que es basa en la virtualització d'un sol adaptador de maquinari sense fils (operant simultàniament en mode client i en mode punt d'accés) per permetre alhora tant la connectivitat amb la xarxa de l'hospital per a la transmissió de les dades fisiològiques en temps real com els procediments implicats en l'associació i aparellament entre els monitors fixos de capçalera i les unitats portàtils de monitorització.

Addicionalment, es va dur a terme el disseny, desenvolupament i prova d'una implementació de codi obert en una plataforma Linux encastada, basada en l'enfocament seleccionat, amb la finalitat d'investigar la qualitat de la connexió ad hoc en presència d'altres equips Wi-Fi.

Els resultats de les proves de rendiment van confirmar el compliment del prototip implementat sota l'enfocament Soft AP amb els requisits d'escenaris mèdics en termes de rendiment de xarxa (més de 5 Mbps disponibles), retard i fluctuació del retard (ambdós per sota de 200 ms), tant en el cas ideal d'un canal sense tràfic com en un entorn de canal completament carregat.

Resumen

La monitorización médica de pacientes se vería beneficiada con la incorporación de la capacidad de conectar de forma inalámbrica los monitores fijos de cabecera con los equipos de monitorización portátil. Varias técnicas *ad hoc* para la conexión de equipos mediante redes Wi-Fi están disponibles y su madurez tecnológica está clara.

Los potenciales beneficios de la aplicación de estas técnicas inalámbricas a la monitorización de pacientes en hospitales son varios: En primer lugar, permitiría la monitorización continua del paciente a lo largo de todo el hospital, con la consecuente mayor movilidad para el paciente. En segundo lugar, utilizaría las redes ya desplegadas para otras aplicaciones de TI, aprovechando que la tecnología Wi-Fi está ampliamente extendida en las instalaciones hospitalarias. Por otro lado, la tecnología Wi-Fi permite el uso de software de código abierto, lo que conlleva ventajas como flexibilidad, fiabilidad, estabilidad y capacidad de auditoría, entre otras.

En este proyecto, las posibles soluciones y estándares (WDS, TDLS, Wi-Fi Direct, Soft AP, redes malladas 802.11s y el modo ad hoc IBSS, entre otros) fueron comparados en términos de funcionalidad, requisitos de hardware y disponibilidad de plataformas, antes de tomar una decisión sobre su idoneidad.

La decisión fue la selección del enfoque Soft AP, que se basa en la virtualización de un solo adaptador de hardware inalámbrico (operando simultáneamente en modo cliente y en modo punto de acceso) para permitir a la vez tanto la conectividad con la red del hospital para la transmisión de los datos fisiológicos en tiempo real como los procedimientos implicados en la asociación y emparejamiento entre los monitores fijos de cabecera y las unidades portátiles de monitorización.

Adicionalmente, se llevó a cabo el diseño, desarrollo y prueba de una implementación de código abierto en una plataforma Linux embebida, basada en el enfoque seleccionado, con el fin de investigar la calidad de la conexión ad hoc en presencia de otros equipos Wi-Fi.

Los resultados de la prueba de rendimiento confirmaron el cumplimiento del prototipo implementado bajo el enfoque Soft AP con los requisitos de escenarios médicos en términos de rendimiento de red (más de 5 Mbps disponibles), retardo y fluctuación del retardo (ambos por debajo de 200 ms), tanto en el caso ideal de un canal sin tráfico como en un entorno de canal completamente cargado.

Contents

Collaborations and acknowledgements	iv
Abstract	xv
Resum	xvii
Resumen	xix
Table of Contents	xxv
List of Tables	xxviii
List of Figures	xxxiv
List of Acronyms	xxxix
1 Introduction	1
1.1 Objectives	2
1.2 Document organization	3
2 Context and state of the art	5
2.1 Context	5
2.2 State of the art	13
3 Scenarios and requirements	15
3.1 Scenarios	15
3.1.1 Current scenario	15
3.1.2 Dual-link scenario	17
3.2 Requirements	19
3.2.1 Connectivity architecture requirements	19
3.2.2 MP70-X2 link requirements	20
3.2.3 Hardware requirements	21
3.2.4 Application requirements	22
4 Technology selection	25
4.1 Technology evaluation methodology	25
4.1.1 Balanced scoreboard comparison of available wireless technologies	29

4.2	IEEE 802.11-based ad hoc techniques review	35
4.2.1	Ad hoc mode (IBSS)	46
4.2.2	TDLS (802.11z)	53
4.2.3	Wireless Distribution System (WDS)	62
4.2.4	Wi-Fi Direct TM	70
4.2.5	Mesh networking (802.11s)	80
4.2.6	SoftAP	91
4.2.7	Bluetooth 3.0	97
4.3	Suitability assessment and technology selection decision summary	105
5	Solution design	109
5.1	Dual-link scenario problematic	109
5.1.1	Derived use cases	110
5.2	Pairing and device discovery	113
5.2.1	Pairing mechanisms discussion	113
5.2.2	Device Discovery mechanisms discussion	115
5.2.3	Alternative solutions considered	118
5.3	Solution design description	121
5.3.1	State diagrams	123
5.3.2	Pairing process diagram	125
6	Implemented platform	131
6.0.3	Linux-based router embedded platform	132
6.0.4	Firmware for the embedded-Linux router	133
6.0.5	Other hardware options considered	136
6.1	Open source platform implemented	138
6.1.1	Soft-AP with OpenWrt and Tomato in WRT54GL routers equipped with UI	138
7	Experimental evaluation	153
7.1	Experiment 1: Channel usage characterization	154
7.1.1	Motivation to carry out the experiment	154
7.1.2	Description of the experiment	155
7.1.3	Results of the experiment	157
7.1.4	Interpretation of the results	158
7.2	Experiment 2: Scan parameters analysis	160
7.2.1	Description of the experiment	160
7.2.2	Motivation to carry out the experiment	161
7.2.3	Results of the experiment	161
7.3	Experiment 3: Scanning performance	164
7.3.1	Description of the experiment	164
7.3.2	Motivation to carry out the experiment	165
7.3.3	Results of the experiment	165
7.3.4	Interpretation of the results	167
7.4	Experiment 4: Delay and delay jitter measurement	168
7.4.1	Description of the experiment	168
7.4.2	Motivation to carry out the experiment	168

7.4.3	Results of the experiment	168
7.4.4	Interpretation of the results	170
7.5	Experiment 5: Throughput measurement	171
7.5.1	Description of the experiment	171
7.5.2	Motivation to carry out the experiment	171
7.5.3	Results of the experiment	171
7.5.4	Interpretation of the results	172
8	Conclusions and further research	173
8.1	Conclusions	173
8.2	Further research	174
	Bibliography	179
A	Wireless patient monitoring state of the art	185
B	Hardware specifications	197
B.1	WRT54GL Linksys Linux based router by Cisco	197
B.2	AVR-P40-8535 Microcontroller Prototype Board by Olimex	200
B.3	ATmega32 40-pin DIP package microcontroller by Atmel	209
B.4	AMC2004A-B-Y6WFDY 4x20 LCD Display Module by Orient Display	215
B.5	AVR-MT-128 display and interface board	234
B.6	AVR-PG1B serial port 10 pin ICSP AVR microcontroller programmer	248
C	Preliminary WDS implementation	251
C.0.1	Preliminary WDS implementation: X2 portable monitor scripts	256
C.0.2	Preliminary WDS implementation: MP70 bedside monitor WDS link con- figuration	259
D	Implemented scripts code	261
D.1	X2 portable monitor scripts: advanced UI embedded implementation	261
D.2	MP70 bedside monitor script: SoftAP implementation	278
E	Philips Patient Monitoring products	291
E.1	IntelliVue MP2/X2 Multi-Measurement Module and transport monitor	295
E.2	IntelliVue MP70 bedside patient monitor	309
E.3	IntelliVue Information Center	318

List of Tables

3.1	Connectivity architecture requirements	20
3.2	MP70-X2 link requirements	21
3.3	Hardware requirements	22
3.4	Application requirements	23
4.1	Wireless specifications features comparison	31
4.2	Wireless specifications balanced scorecard	33
4.3	802.11 Frame classes and categories	42
4.4	Ad hoc mode operation options depending on devices state	48
4.5	IBSS Ad hoc mode suitability points	52
4.6	TDLS 802.11z suitability points	60
4.7	To/From DS Frame Control field value combinations in data type frames	63
4.8	Data frames address fields	64
4.9	WDS suitability points	69
4.10	Key mechanisms defined in the Wi-Fi Direct Specification	72
4.11	Wi-Fi Direct TM suitability points	78
4.12	Approximated mesh throughput in function of number of hops	89
4.13	Mesh 802.11s suitability points	90
4.14	SoftAP suitability points	95
4.15	Bluetooth 3.0 suitability points	103
4.16	Ad hoc techniques suitability balanced scorecard	106
4.17	Technology selection decision	107
5.1	Link and patient assignment status for the MP70 bedside monitor's states.	124
5.2	Link and patient assignment status for the X2 portable monitor's states.	125
6.1	Embedded Linux distributions, features and compatibility	134
6.2	Embedded Linux distributions, key features	135
6.3	JP2 pinout serial header in WRT54GL	140
7.1	Experiment 1. Measurement 1. Characterization of the environment without additional traffic load	158
7.2	Experiment 1, Measurement 2. Characterization of the environment without additional traffic load	158
7.3	Experiment 1, Measurement 3. Characterization of the environment with additional traffic load	159

7.4	Experiment 2, Measurement 1. Inter-probe and inter-scan times, varying number of probes and dwell time	162
7.5	Experiment 2, Measurement 2. Inter-scan times, varying dwell time for multiple repetitions	163
7.6	Experiment 3. Scan performance	166
7.7	Experiment 4. Delay and delay jitter measurement	170
7.8	Experiment 5. Throughput measurement	172
E.1	MP2/X2 portable patient monitors specifications	295
E.2	MP70 bedside patient monitor specifications	309

List of Figures

2.1	Dräger’s <i>Infinity Delta XL</i> (left), <i>Infinity Gamma XL</i> (center) and <i>Infinity M300</i> (right)	13
2.2	Welch Allyn’s <i>Acuity Propaq CS</i> and <i>Micropaq Wearable Monitor</i>	14
3.1	Current X2 and MP70 usage scenario using wired local connection	16
3.2	X2 and MP70 usage scenario with local wireless connections	17
3.3	Example of in-hospital dual-link scenario integration in current Wi-Fi network	18
4.1	Legacy IEEE 802.11 standard’s MAC and PHY layers mapped to the OSI reference model	36
4.2	IEEE 802.11 DCF and PCF functions architecture	37
4.3	Basic Service Set (BSS)	37
4.4	Extended Service Set (ESS)	38
4.5	Independent Basic Service Set (IBSS)	38
4.6	802.11 state machine: Relation between 802.11 station states, services and frames	41
4.7	802.11b DSSS 22MHz channel width	44
4.8	802.11b DSSS 22MHz channel width (non overlapping channels)	44
4.9	802.11g/n OFDM 20MHz channel width (16.25 MHz used by sub-carriers)	45
4.10	802.11n OFDM 40MHz channel width (33.75 MHz used by sub-carriers)	45
4.11	Independent Basic Service Set (IBSS)	46
4.12	Ad hoc mode strengths and weaknesses	52
4.13	TDLS set-up	53
4.14	TDLS setup	55
4.15	TDLS 802.11z strengths and weaknesses	61
4.16	Wireless Distribution System (WDS) setup	62
4.17	Wireless Distribution System (WDS) detail of channel configuration	64
4.18	Wireless Distribution System (WDS) chain configuration	65
4.19	Wireless Distribution System (WDS) star configuration	66
4.20	Wireless Distribution System (WDS) applied to the Philips Patient Monitoring system	67
4.21	WDS strengths and weaknesses	69
4.22	Wi-Fi Direct example setup	70
4.23	Wi-Fi Direct services architecture	74
4.24	Global Wi-Fi Direct devices distributed (2014, ABI Research)	77
4.25	Wi-Fi Direct strengths and weaknesses	78
4.26	Mesh backbone example setup	81

4.27	Mesh clients network example setup	82
4.28	Mesh hybrid network example setup	83
4.29	Mesh system architecture	86
4.30	IEEE 802.11s mesh approach applied to the Philips Patient Monitoring system	88
4.31	Approximated mesh throughput in function of number of hops	89
4.32	802.11s Mesh strengths and weaknesses	90
4.33	SoftAP example setup, connected simultaneously to an AP in STA mode and with a legacy STA connected to the virtual access point created by the SoftAP	91
4.34	SoftAP system architecture and relation between the Hardware, Kernel and User levels	92
4.35	SoftAP approach applied to the Philips Patient Monitoring system	93
4.36	SoftAP strengths and weaknesses	96
4.37	Bluetooth core stack architecture	99
4.38	Bluetooth 1 MHz and Bluetooth LE 2 MHz channels compared with 802.11b DSSS 22MHz channel width (non overlapping channels)	100
4.39	Bluetooth state machine diagram	101
4.40	Bluetooth 3.0 strengths and weaknesses	104
5.1	Use case 1. Wire replaced by wireless connection between X2-MP70	110
5.2	Use case 2. X2 connects to the hospital infrastructure APs when there is no MP70 available	111
5.3	Use case 3. X2 replacement with already assigned MP70 and PatientID	112
5.4	Use case 4. Patient info connection independent from physical wireless link	112
5.5	Device Discovery algorithm (passive)	117
5.6	Device Discovery algorithm (active)	119
5.7	SSID field schema and SSID example in a packet capture	121
5.8	X2 portable monitor and measuring cables	122
5.9	Different uses for MP70 monitor: bedside, anaesthesia and operation room configurations	122
5.10	Cardinality relations between patients, portable monitors and bedside monitors	123
5.11	MP70 bedside monitor state diagram	123
5.12	X2 portable monitor state diagram	124
5.13	Pairing process and user interaction flow diagrams legend	126
5.14	Pairing process and user interaction, part 1	127
5.15	Pairing process and user interaction, part 2	128
6.1	Linksys Linux based WRT54GL router by Cisco	132
6.2	Linksys WRT54GL board distribution	133
6.3	OpenWRT configuration web interface	135
6.4	OpenWRT command line interface	136
6.5	AVR-MT-128 display and interface integrated board	139
6.6	Detail of LCD display and UI buttons installed directly in the router cover	139
6.7	Detail of power input wired solidary to the router DC input (red and black braided wires)	140
6.8	Detail of external ICSP port wired to the AVRMT128 ICSP port (grey bus)	140
6.9	JP2 RS232 pinout for serial connection WRT54GL-AVRMT128	141
6.10	AVR-PG1B (serial port) 10 pin ICSP AVR microcontroller programmer	141

6.11	QR image link to demonstration video https://goo.gl/La5c3r	142
6.12	Overall result and internal aspect of the WRT54GL router with AVR MT128 modification	142
6.13	Hospital AP and MP70 connected through WDS link	143
6.14	Pairing, assignment and device discovery flow diagrams legend	145
6.15	Pairing process implementation flow diagram, X2, part 1	146
6.16	Pairing process implementation flow diagram, X2, part 2	147
6.17	Pairing process implementation flow diagram, MP70, part 1	148
6.18	Pairing process implementation flow diagram, MP70, part 2	149
6.19	Network topology, basic setup	150
6.20	Network topology, extended and generalized setup	151
7.1	Experimental setup	154
7.2	Wireshark - Network Protocol Analyzer	155
7.3	Wireshark - Network Protocol Analyzer - Statistics analysis	156
7.4	Experiment 1 setup: Channel characterization	157
7.5	Wireshark - Network Protocol Analyzer - Flow graph	160
7.6	Experiment 2 setup: Scan parameters analysis	161
7.7	Experiment 3 setup: Scanning performance	165
7.8	Experiment 4 setup: Delay and delay jitter measurement	169
7.9	Experiment 4 results: RTT for delay and delay jitter requirements	169
7.10	Experiment 5 setup: Throughput measurement	171
A.1	Dräger's <i>Infinity Delta XL</i>	186
A.2	Dräger's <i>Infinity Gamma XL</i>	187
A.3	Dräger's <i>Infinity M300</i>	187
A.4	Dräger's <i>Infinity OneNet architecture</i>	188
A.5	GE Dash patient monitors	190
A.6	GE Dash 5000 patient monitor	190
A.7	GE CARESCAPE Network hospital-wide deployment for wireless patient monitoring, WMTS telemetry, two-way radio and VoIP phones	191
A.8	Welch Allyn's <i>Acuity System overview</i>	195
A.9	Welch Allyn's <i>Propaq CS</i>	196
A.10	Welch Allyn's <i>Micropaq Wearable Monitor</i>	196
C.1	RS233 schematic for serial ports modification in WRT54GL	252
C.2	WDS link implementation schema	253
C.4	QR image link to demonstration video URL https://goo.gl/yDHLtU	253
C.3	WDS link setup on OpenWRT configuration web interface	254
C.5	X2 with basic UI implementation. Overall look and cardboard case assembly detail	254
C.6	X2 with basic UI implementation, LCD display module (back) and UI detail (frontal push-button)	255
C.7	Hospital AP and MP70 connected through WDS link	255
C.8	First implementation. LCD display module detail (front)	255
C.9	First implementation. GUI detail (LCD display)	256
C.10	WDS link setup on OpenWRT configuration web interface	259
C.11	MP70's DHCP server on OpenWRT configuration web interface	260

C.12 Hospital AP's DNS and gateway on OpenWRT configuration web interface . . . 260

List of Acronyms

AC	Access Category
ACK	ACKnowledgement [frame]
AP	Access Point
ATIM	Announcement Traffic Indication Messages
BSS	Basic Service Set
CF	Compact Flash card
CIS	Clinical Information Systems
CSCN	Client supplied wired network
CSMA/CA	Carrier sense multiple access/collision avoidance
CSMA/CD	Carrier sense multiple access/collision detect
DCF	Distributed Coordination Function
DLS	Direct Link Setup
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine standard
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Map
ECG	Electrocardiography
EHR	Electronic Health Record
FHSS	Frequency Hopping Spread Spectrum
GPIO	General Purpose Input/Output
GUI	Graphical User Interface
HIS	Hospital Information System
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
ICSP	In-Circuit Serial Programming
ICT	Information and communication technologies
IE	Information Element, part of IEEE 802.11 management frames
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, scientific and medical frequency band
JTAG	Joint Test Action Group interface for in-circuit programming and debugging
LAN	Local Area Network
LIS	Laboratory Information System
LLC	Logical Link Control
MAC	Medium Access Control

MIMO	Multiple-Input Multiple-Output, technology to exploit multipath propagation
MMS	Multi Measurement Server, Philips patient monitoring sensors unit
MP70	Philips bedside patient monitoring head unit
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAT	Network Address Translation
NFC	Near Field Communication
NIC	Network Interface Card
OEM	Original equipment manufacturer
OFDM	Orthogonal frequency-division multiplexing
P2P	Peer-to-peer
PACS	Picture archiving and communication system for medical imaging
PCI	Peripheral Component Interconnect bus
PDA	Personal Digital Assistant
PHY	Physical layer
PS	Power Save
PSM	Power Save Mode
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RMT	Remote patient Monitoring and Treatment
SDIO	Secure Digital Input/Output
SPI	Serial Peripheral Interface Bus
SSID	Service Set Identifier
STA	Wireless Station
STP	Spanning Tree Protocol
SoC	System-on-chip
TBTT	Target Beacon Transmission Time
TDLS	Tunneled Direct Link Set Up
TIM	Traffic Indication Map
TXOP	Transmission Opportunity
UART	Universal Asynchronous Receiver-Transmitter, serial port controller
UI	User interface
VoIP	Voice over Internet Protocol
WDS	Wireless Distribution Systems
WLAN	Wireless Local Area Networks
WMM®	Wi-Fi Multimedia™
WMM®-PS	Wi-Fi Multimedia™ Power Save
WMN	Wireless Mesh Networks
WPA2™	Wi-Fi Protected Access 2™
WPA™	Wi-Fi Protected Access™
WPAN	Wireless Personal Area Network
WPS™	Wi-Fi Protected Setup™
X2	Philips portable patient monitoring unit

Chapter 1

Introduction

The interest in wireless systems for medical applications has experienced a significant increase lately. Given the general advantages over wired alternatives, including: improved mobility, reduced patient discomfort and reduced cost of healthcare delivery, the application of wireless techniques promises exciting possibilities and new applications for the medical market.

Devices for the continuous monitoring of heart rate, blood pressure, oxygen blood saturation and electrocardiogram are essential tools in modern healthcare. Usually, the sensors for these instruments are attached to patients and monitors by wires, hence the patients sequentially become confined to their beds. In addition, if the patients have to be moved, all monitoring devices must be disconnected and reconnected again. All these time consuming tasks may be obviated and patients could be released from bed and instrumentation by wireless technology.

Moreover, the new introduced wireless devices could communicate with a gateway that connects to the network of the medical center and transmit the healthcare data to a data warehouse, in order to monitor, control and evaluate it in real time or after its storage and processing.

In that sense, the Patient Monitoring division of Philips Healthcare would like to introduce the capability to wirelessly connect bedside fixed monitors with portable monitoring equipment making use of *ad hoc* networking techniques for Wi-Fi equipment.

The potential benefits of applying the aforementioned wireless techniques to the specific case of patient monitoring are several:

- Firstly, all the parameters monitored at the hospital room with the bedside monitors could continue to be monitored during transport, enabling continuous patient monitoring wherever the patient had to be carried (surgery room, intensive care, emergency room, etc), promoting also the healing of ambulatory patients, whom would enjoy a greater freedom of movements throughout the hospital.
- Secondly, there would be no need of a dedicated network for patient monitoring apart from the already deployed hospital IT applications, since Wi-Fi is a well-known and widespread

technology in hospital environments, whose facilities are nowadays equipped with fully operational standard access points.

- Moreover, Wi-Fi is a technology that allows using open-source software, whose benefits include flexibility, reliability, stability and auditability, among others.

In this work, a reasoned decision is made on which of the available *ad hoc* networking techniques apply, and a solution is proposed to address the additional problems due to the replacement of the former cable connection between fixed and portable monitors by a wireless link. These issues arise in terms of device discovery, reliable pairing and patient identification.

1.1 Objectives

The principal objective of this report is to describe and analyse with technical rigour the research work carried out in 2010 during an internship at the Distributed Sensor Systems department of Philips Research, in the Netherlands, under the program *UPC-Empresa. PFC a Empreses internacionals. Tardor 2009-10*, and to present it as *PFC (Projecte de Fi de Carrera)* for the *Enginyeria de Telecomunicació, Pla 92* studies.

Problem statement and project objectives

This project arised from the need of Philips Healthcare to substitute the wired connection between their portable patient monitoring units and bedside fixed monitors by a wireless connection using *ad hoc* Wi-Fi technology.

After capturing the requirements in the so-called *dual-link scenario*, we decided that the objectives of this work as a *PFC (Projecte de Fi de Carrera)* would be the following:

- To study and review the applicable Wi-Fi *ad hoc* techniques to solve the problem stated, different from the well known infrastructure mode Wi-Fi schemes, taking a suitability assessment and making a technology selection on which specific technique and specification to use on the following steps.
- To design an abstract solution addressing the specific problematic of the targeted dual-link scenario, detailing use cases to illustrate the desired behaviour and user interaction with the solution.
- To implement a platform over embedded hardware in which to demonstrate the validity of our technology selection decision and solution design.
- To design a set of experiments to evaluate the performance of our implementation and the fulfilment of the initial requirements, in terms of a sub-set of the use-cases derived before.

1.2 Document organization

This thesis report is organized as follows.

A review of the global context and the state of the art in the field of *wireless patient monitoring* are approached in Chapter 2 **Context and state of the art**.

The current and target scenarios are described in Chapter 3 **Scenarios and requirements**, together with the derived requirements of the target scenario.

The potential technologies and standards (Wireless Distribution System, Tunneled Direct Link Set-up, Peer-to-peer, SoftAP, mesh networking and the good old *ad hoc* IBSS mode) are compared in terms of functionality, hardware requirements and availability of platforms, among others, in Chapter 4 **Technology selection** prior to take a decision on its suitability to solve the problem stated, following a custom designed assessment methodology.

The description of the overall solution design are presented in Chapter **Solution design 5**, together with the discussion on the alternative strategies considered.

The development and testing of an open source implementation in an embedded Linux platform, based in the selected technologies and designed solution, carried out to investigate the quality of the ad hoc link and validate the requirements fulfilment, are contained in chapters 6 **Implemented platform** and 7 **Experimental evaluation**, respectively.

Finally, the experimental results are discussed, together with a recommendation on the further research and recommendations to be taken, in Chapter 8 **Conclusions and further research**.

Chapter 2

Context and state of the art

In the current chapter, a thorough review of the current global **context of the ICTs applied to healthcare** is taken, to introduce the *Remote patient Monitoring and Treatment (RMT) market* together with a **brief summary on the state of the art of wireless patient monitoring** for the principal competitors of Philips with equivalent products in this field. This last point is extended in Appendix A with a thoroughly detailed identification of the available products of the principal companies on the market addressing the specific problem of wireless monitoring of vital signs.

2.1 Context

The health sector is experiencing deep changes characterized by an ageing population with growing life expectancy resulting in an increase in the proportion of elderly and a reduction of economically active individuals, thus compromising the tax base that supports the existing public health systems. According to the World Health Organization[2]:

- By 2025, increases of up to 300% of the older population are expected in many developing countries.
- It is expected that 2.000 million people will be over the age of 60 by the year 2050.
- Today's population contains 3.100 million adults aged between 20 and 64; and 390 million over 65 years.

To meet the growing demand for health services is estimated to be necessary to dedicate to health related jobs at least the 25% of the active population.

- According to the World Health Organization, the world is short of over four million health workers.

As a result there is a need to establish a new paradigm of health care: more focused on patients, health care quality and at the same time keeping or reducing costs, with special emphasis on taking advantage of new developments in Information and Communications Technologies.

Geographical differences in the application of ICTs to health

European National Health Systems generally have complex decision schemes depending on the interests of politicians, hospital managers, medical professionals and patients-voters, whose interests do not always coincide and regularly present rejection in adopting information technology advances, issues which together are hampering the penetration of remote monitoring technologies and telemedicine.

In contrast, U.S. are the main marketplace of ICTs applied to the healthcare sector because their health system is primarily private in nature, aimed at patient satisfaction and more open to the introduction of innovation that allow differentiation between competitors.

Nevertheless, these differences tend to gradually decrease, as agreements between leader regions and with other stakeholders are achieved, in the benefit of standardization and normalization. As an illustrative example, the eHealth¹ partnership between the European Commission and the U.S. Department of Health was materialized with the signing in December 2010 of a Memorandum of Understanding[4] to promote a common approach on the interoperability of future eHealth systems in order to bring opportunities for a global approach for the benefit of patients, health systems and the market. This MoU was reviewed in May 2012 during the eHealth Week in Denmark, to present and discuss current and future perspectives of EU and US cooperation on eHealth matters, specially the jointly developed roadmap for the development of internationally recognised interoperability standards and interoperability implementation specifications for electronic health information systems.

As mentioned before, the healthcare model in Europe has been traditionally focused on public provision of health services through the respective national health systems of each country, which differ widely in their institutional and organizational settings, and act as monopolies in their respective geographical areas. As a result, the introduction of changes and new technologies tend to be relatively slow and shows markedly different geographic patterns.

European Commission interest on eHealth and its presence in European strategies and policies

The huge potential and strategic value to the economy that the application of ICTs to the European health systems could bring has been stressed by the European Commission since

¹According to the World Health Organization, eHealth or E-Health is the transfer of health resources and health care by electronic means. It encompasses three main areas: 1) The delivery of health information, for health professionals and health consumers, through the Internet and telecommunications.

2) Using the power of IT and e-commerce to improve public health services.

3) The use of e-commerce and e-business practices in health systems management.

2007, as eHealth was defined as one of the six sectors of particular interest within the Lead Market Initiative for Europe[5]. According to this European policy, launched by the European Commission with the scope of creating the right framework to foster lead markets, innovation-friendly markets by creating conditions to facilitate the translation of technological and non-technological innovation into commercial products and services, eHealth can help to deliver better care for less money within citizen-centred health delivery systems, alleviating the cost pressure on the public budgets for health.

More recently, the European Commission interest on ICTs for health was pointed out within the Digital Agenda for Europe[7], one of the seven flagship initiatives that set Europe 2020, the EU's growth strategy, to catalyse advances in ICT and make them the key piece for Europe to achieve its ambitions for 2020 [8]. Based on extensive consultations, in particular the contributions of the "Competitiveness Report 2009 - COM (2009) 390" of the Commission's public consultation on the future and priorities of ICT and the "ICT Industry Partnership Contribution to the Spanish Presidency Digital Europe Strategy", the Digital Agenda for Europe established the deployment of eHealth technologies in Europe as a key objective, with a view to create sustainable healthcare, improving the quality of health care, reducing medical costs and fostering independent living.

And it is still an up-trend within the European digital strategy, as the latest Annual Progress Report of the Digital Agenda[9] details that *"eHealth and telemedicine services will be key to long term sustainability of health care systems that are increasingly challenged by the needs of an ageing population and shortage of healthcare professionals and financial resources"*.

The next step on European digital strategy policy initiatives within the framework of the Digital Agenda was the publication of an Action Plan in June 2012, setting out a vision for innovative eHealth services and addressing aspects such as user empowerment, standards uptake, interoperability, testing and certification, as well as need for legal certainty and research & innovation, according to the cited progress report. *eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century* provides a roadmap to empower patients and healthcare workers, to link up devices and technologies, and to invest in research towards the personalised medicine of the future[11].

In the past 20 years the EU has funded over 500 research projects in eHealth with more than 1.000 million euro[6]. At least 23 of these projects were clearly related to the RMT, primarily in the context of the Framework Programme 6 and 7, Eten and CIP programmes[6].

Usually the goal of these projects has been to improve medical data collection systems, in order to reduce the number of patient visits to medical facilities or allowing an exhaustive patient monitoring outside as well as inside hospitals, based on data transmission by wireless means, data processing and reception of this data by the monitoring staff to give patient a proper response.

This last point, **wireless monitoring of vital signs**, which consists of the collection, treatment and analysis of data pertaining to physiological measurements such as vital signs of pulse, respiration, temperature, and blood pressure, as well as blood sugar level, bladder and bowel output, etc. is the one addressed in this project and has a very specific and defined market supply, which is presented in the next section 2.2.

Telemedicine, Remote patient Monitoring and Treatment market

Despite the economic crisis, the market potential of eHealth is strong. The global telemedicine market grew from 7,200 million euro in 2010 to 8,500 million euro in 2011, and is expected to continue to expand to 20,100 million euro in 2016, representing a compound annual growth rate of 18.6%[11]. The well being market enabled by digital technologies (mobile applications, devices) is rapidly growing. The convergence between wireless communication technologies and healthcare devices represents an upcoming potential for economy and will bring benefits to the converging health and social care.

Wireless patient monitoring is an specific application of a more generic field in eHealth, Remote patient Monitoring and Treatment (RMT), which can be defined as the health systems that help patients by monitoring their vital signs thus improving the quality of care, their quality of life and enable the prediction of aggravations of their medical condition. Wireless patient monitoring is meant to be applied primarily in healthcare institutions and during medical transportation of patients. On the other hand RMT is consolidating a niche in Personal Health Systems, telemedicine and home monitoring systems, in its widespread application for chronic and elderly patients.

While this subsector can represent a relatively small and immature market, its huge growth potential and strategic value to the European economy has been stressed by the European Commission[5]: In terms of economic size, its market turnover was 127.9 million euro in 2007 and is estimated to grow to 292.3 million euro in 2014² divided into 40% for device manufacturers (52 million euro) and 60% for service providers (76 million euro)[6].

eHealth adoption in European hospitals

Wireless patient monitoring systems can be deployed in hospitals as stand-alone independent systems. Nevertheless, proper results will be achieved only if the deployment is complemented by other eHealth advancements in hospitals. In that sense, progress may be perceived in the deployment of eHealth technologies in Europe, as more than 90% of European hospitals are connected to broadband and 80% have electronic patient record systems, according to the results of a survey conducted for the European Commission[10].

Actually, eHealth applications have a growing role in the majority of Europe's hospitals³, but there are still wide variations in take-up, with Nordic countries taking the lead. Large, public and university hospitals are generally more advanced in eHealth terms than smaller, private ones.

In general, public, private and university hospitals in Europe are taking advantage of eHealth technologies to a greater or lesser extent:

²According to Frost&Sullivan 2008 report *European Remote Patient Monitoring Market M22C-56*

³The survey was carried out in 2010 in 906 general public, private or university hospitals from all 27 EU Member States, plus Croatia, Iceland, and Norway.

- 92% are connected to broadband and 41% of them have broadband speed of at least 50 Mbps
- 81% have one or more electronic patient records systems in place
- 71% use online eBooking systems for patients' appointments with medical staff
- 65% have a common patient record system and 61% have an IT-based archiving and communication system
- 43% exchange radiology reports electronically

Nevertheless, the survey shows that services for patients, such as ePrescription or access to patient records are not widely available in all EU hospitals:

- 30% use ePrescription for medicines
- 8% telemonitor patients at home
- 5% have some form of electronic exchange of clinical care information with healthcare providers in other EU countries
- only 4% grant patients online access to their electronic patient record.

European hospitals' Wi-Fi infrastructure

Starting with a minimal LAN infrastructure, wireless networks availability are necessary for the operation of wireless patient monitoring. Furthermore, the availability of wireless and mobile computing in hospitals is becoming an important part of the healthcare information technology, as it connects caregivers to clinical data and applications anywhere and anytime, thereby improving efficiency, specially in intensive care units where time can often be of critical importance.

- Although most of the hospitals are connected to broadband, only 54% of the total have wireless infrastructure.
- Wireless single infrastructures have yet to be widely deployed in many acute hospitals, however. One-third of the hospitals with wireless infrastructure (18% of the total) have multiple individual wireless infrastructures for discrete applications rather than having a single unified infrastructure.
- Hospitals offer Internet access wirelessly from a number of locations inside their own walls, especially for workstations (75%) and also to inpatients (47%).

Looking at the particular cases of Spain and the Netherlands, both countries present similar results with around 60% of the hospitals with some kind of wireless infrastructure. The only difference is that single, unified wireless infrastructure is more spread in Dutch hospitals, with a 48% compared with 41% in the Spanish ones.

In the other extreme, wireless is not present in any Croatian hospital surveyed, nor in the 88%

of the Greek hospitals with broadband, 71% of the Romanian hospitals with broadband, or 69% of the Polish hospitals with broadband.

Wireless patient monitoring in European hospitals

Only just over a quarter (28%) of the hospitals with a wireless infrastructure provide wireless monitoring of patients inside the hospital. In geographical terms, there are noticeable differences among hospitals wireless availability. While more than half of the Swedish and Norwegian hospitals count on that kind of advances, the proportions vary from 43% of the Italian hospitals and 39% of those in the UK to the new Member States where the percentage of affirmative answers is rather low (11% for Poland, for instance).

Finally, in several countries, none of the hospitals surveyed that have wireless systems in place provide wireless monitoring of patients: these include, among others, Croatia, Estonia, Hungary, Lithuania, Malta, Slovakia, and Slovenia. Indeed, it may be that there are restrictions in a number of Member States with regard to wireless monitoring of patients or use of wireless in proximity to patients. Belgium is an example, where it is prohibited by legislation, by concerns about health and safety.

Regarding the size of the hospitals, wireless monitoring of patients inside the hospital is more common, the larger a hospital is:

- More than 750 beds: 45%
- 251-750 beds: 26%
- 101-250 beds: 27%
- Less than 101 beds: 17%

In conclusion one can say that there is a potential niche market for wireless patient monitoring in European hospitals. Specially there exist many opportunities for new wireless monitoring products in the new Member States and in the ones without limitations for wireless signals to be utilized in proximity to patients.

Medical benefits from using patient monitoring systems in hospitals

Evaluation of hospitalised patient parameters, such as heart rate and oxygen saturation in the blood, is critical to provide quality health care.

Systems based on monitoring sensors are used, also, to monitor specific parameters and environments that can seriously affect the health of the patient. That is the case, for instance, of incubators for babies: The use of specific sensors, tracking optimum temperature and humidity inside the incubators in infants intensive care units.

Patients with serious health condition require continuous monitoring of multiple vital signs, as

their conditions may change rapidly. Moreover, clinicians who care for them must make timely decisions based on accurate clinical data.

In that sense, the benefits that electronic centralized monitoring can bring to hospital inpatients are diverse. Several medical papers⁴⁵⁶ suggest that the continuous inpatient monitoring systems bring benefits like the following:

- The ability of providing with a quicker response to patient deterioration, thanks to the automatic notifications generated in the event of abnormalities in the vital signs monitored.
- Systems that monitor patient parameters continuously provide better information than the ones that collect discrete data. This provides a greater understanding of clinical patterns and trends, allowing physicians to make better decisions.
- Clinical data from patient monitoring systems can be filled in the patient's electronic health record (EHR) and become a part of the systems to support clinical decisions.
- These systems contribute to patient safety and error prevention. Thresholds of critical parameters can be set in most of the monitoring devices, and if the patient measurements exceed these preset limits, the system can alert the clinicians in charge.
- Intelligent monitoring and early warning systems can help to intervene at an early stage in order to avoid the occurrence of critical events, which may considerably increase patient safety. Accordingly, a consequence of the use of these systems is a reduction in unexpected deaths, reducing in general morbidity and mortality rates, due to the avoidance of unmonitored periods between rounds of the classical supervision procedures based on nurse visits to every monitored patient room.
- Patient monitoring systems improve economic as well as patient outcomes. Providing optimal care and preventing errors can shorten patient's hospitalisation stays and reduce medical costs.

Moreover, many systems can be configured to monitor several patients simultaneously at a central monitoring station. This centralized electronic monitoring represents an opportunity for healthcare staff to monitor more patients at the same time, thus increasing their efficiency and reducing their fatigue. It can enhance convenience, reduces effort without sacrificing quality of care, and frees up more time for caregivers to provide direct care. Increased time at the bedside, in turn, can improve both patient care and nurses' job satisfaction.

In addition, several technical papers have already investigated the potential benefits of wireless

⁴*Integrated monitoring and analysis for early warning of patient deterioration*, L. Tarassenko, A. Hann, and D. Young, BJA Advance Access published May 2006.

⁵*Cardiorespiratory instability before and after implementing an integrated monitoring system*, Pinsky M. et. al. American Journal of Respiratory Critical Care Medicine, 2008: 177: A842. Presented at the American Thoracic Society Meeting, Toronto, May 2008.

⁶*Ability of an electronic integrated monitoring system to impact duration of patient instability on a step down unit*, Pinsky, M. et. al. American Journal of Critical Care, 2008, 17 (3), 279. Presented at the American Association of Critical Care Nurses National Teaching Institute, Chicago, May 2008.

patient monitoring systems:

- Wireless connectivity will enable new applications to improve health-care delivery in many different scenarios. WLAN and WPAN technologies are the enablers for an integrated communication infrastructure at medical environments that can improve efficiency, and reduce errors and costs[18].
- Wireless medical body sensor networks enable a new way of continuous patient monitoring, extending the reach of current healthcare solutions. They improve care giving by a flexible acquisition of relevant vital sign data, and by providing more convenience for patients[30].
- These systems allow patients a greater freedom of movement and allow doctors to identify pre-defined symptoms earlier[28].
- Continuous monitoring with early detection has likely potential to provide patients with an increased level of confidence, which in turn may improve quality of life[29].

Potential challenges and drawbacks of wireless medical applications

The use of wireless technologies in medical environments could bring major benefits, as seen, to existing health services. However, there are several challenges still to be researched:

- Prevailing over wires by switching to wireless technologies requires a careful analysis of some of the candidate technologies available in order to find out which ones are best suitable for such demanding environments[28].
- Reliability is one of the most important factors. To ensure it, adaptation of nodes when its location, connection and link quality is changed[18] have to be addressed.
- The integrity of the data distribution and fault tolerance must be given adequate consideration as well. Each device can operate differently at different times, especially sensor-based devices. One of the nodes in a system can be failure at any time by the number of reasons including natural issues, issues related to man and battery depletion. Ensure continuous service during the lifetime of the system could be a great challenge.
- In mission-critical applications, it is vital that devices do not get out of battery. As a matter of fact, most based wireless network devices are battery operated, therefore, the design of a system should minimize energy expenditure by devices. Battery longevity for the devices and its extension by using scheduling algorithms and power management systems must be considered.
- For medical usage, this system behaviour has to be transformed to a reliable and defined system set-up, working automatically but nevertheless being under explicit control of a clinician. [30]
- Life-critical nature of some medical applications imposes additional challenges that have not been considered in non medical scenarios (mainly power consumption, coexistence with other technologies, roaming support and security)[18].

2.2 State of the art

A brief summary on the state of the art is presented in this section, pointing the main conclusions on the products which could represent an alternative to the solution we propose in this work. A further identification of the main companies and their products on the market addressing the specific problem of wireless monitoring of vital signs is detailed in appendix A.

Dräger Medical AG & Co products Dräger’s portfolio comprises various vital signs monitors, both fixed, portable and to be worn by the patient[12]:

- *Infinity Delta XL* serves as both a bedside and transport monitor. The wireless operation in this 12.2” screen unit is performed by a 802.11g wireless card that offers enhanced security (WPA2).
- *Infinity Gamma XL* is a compact (8.4” screen) vital signs monitor that can operate as a standalone device or as part of the Infinity Network.
- *Infinity M300* is a patient-worn telemetry device, equipped with 802.11b/g technology and WPA2 standard encryption support.



Figure 2.1: Dräger’s *Infinity Delta XL* (left), *Infinity Gamma XL* (center) and *Infinity M300* (right)

This company’s solution is based on the *Infinity OneNet* architecture that integrates patient monitoring systems into existing hospital-wide wired and wireless networks, although requires validated network components (mainly access points) that meet Dräger’s networking requirements.

Direct communication from the monitors to the *Infinity CentralStation* through the *Infinity OneNet* facilitates wireless data exchange. Dräger monitors provide continuous standalone monitoring, even if the patient moves out of the wireless network coverage area.

Welch Allyn products Welch Allyn’s *FlexNet* technology allows to operate real-time patient monitoring (in the 802.11a 5GHz band) on a shared 802.11 a/b/g network along with other hospital applications[13]. Although Welch Allyn claims their system to be based on no proprietary infrastructure components, its functioning is limited to a list of vendor brands whose

wireless equipments are supported by the Welch Allyn's *FlexNet* solution.

Welch Allyn's *Propaq CS* is a base monitor with optional wireless connectivity to *Acuity Central Station* while the *Micropaq Wearable Monitor* is a limited monitoring device designed to wirelessly connect to Welch Allyn's *Acuity Central Monitoring System*, without the option of working as a standalone monitor.



Figure 2.2: *Welch Allyn's Acuity Propaq CS and Micropaq Wearable Monitor*

Welch Allyn's *Acuity Central Monitoring System* provides hospital managers with a full solution, including patient admission and discharge management, wireless and wired monitoring management, patient-monitor assignment by room/location, patient-specific alarms and waveform remote monitoring.

Conclusions on the analysed wireless patient monitoring products

- The analysed solutions do not contemplate direct connection between the portable, or patient-worn, devices and the bedside monitoring devices.
- These solutions are available in the market since around 2008, and including the provision of QoS management.
- The analysed solutions, in spite of sharing the wireless network with common hospital applications data, depend on the adoption of their respective architectures in the whole hospital network and the use of compatible Wi-Fi infrastructure equipment from specific vendors.

Chapter 3

Scenarios and requirements

The **current and target scenarios** are described in this chapter, together with the **requirements of the target scenario** for which the following analysis and developments will be made.

3.1 Scenarios

As it was introduced in the previous chapter 1, the Patient Monitoring division of Philips Healthcare would like to introduce the capability to wirelessly connect bedside fixed monitors with portable monitoring equipment making use of *ad hoc* networking techniques for Wi-Fi equipment.

In this section the current and desired scenarios are described. Both are located in a hospital room and consist of a portable monitor (X2), a bedside monitor (MP70) and an infrastructure Wi-Fi wireless access point.

3.1.1 Current scenario

The **MP70** is a high-end bedside monitor which can receive data from a multi measurement server (MMS) or a portable monitor X2. See Appendix E.2 for detailed illustrations and descriptions of the MP70 bedside monitor.

It has a display and it is usually placed at a fixed place in a room, for example, mounted on a wall. An MP70 establishes connectivity with the central server in normal mode of operation. An MP70 has both wired (Ethernet) and wireless (Wi-Fi) network connectivity capability. When a wired connection is detected it is preferably used to connect to the central and in absence of wired connection, wireless connection to the central server is established, if possible. There is one wireless card per MP70 which is based on the Atheros AR5K series chipset with an small

embedded host processor. The wireless drivers are based on the VxWorks real-time operating system.

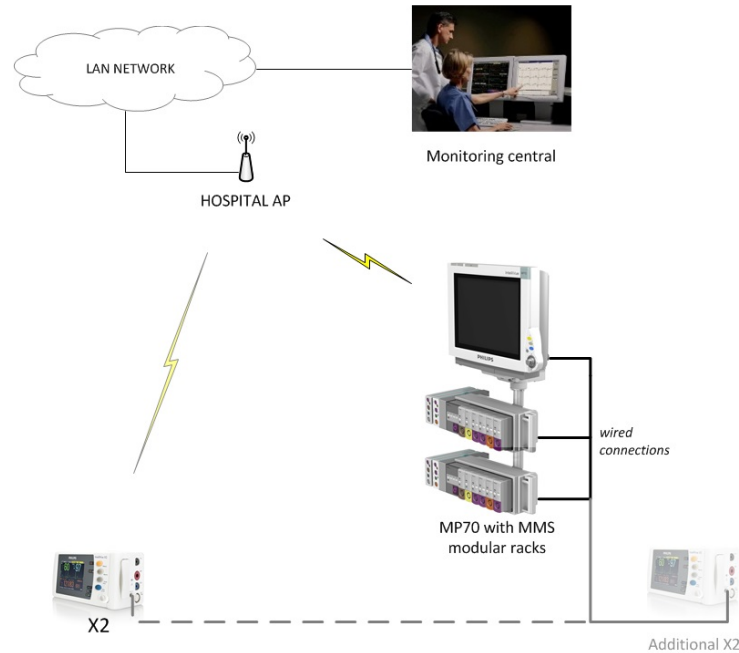


Figure 3.1: Current X2 and MP70 usage scenario using wired local connection

An **X2** is a portable monitor with rack-less measurement modules. See Appendix E.1 for detailed illustrations and descriptions of the X2 portable monitor.

The X2 has a local display, as it can work as a stand-alone monitor or it could connect to the monitoring central (see Appendix E for detailed illustrations and descriptions of the complete patient monitoring solution, specifically the monitoring central in E.3) wirelessly using Wi-Fi capability through a hospital infrastructure AP (see figure 3.1). When on transport, the X2 connects to the hospital AP, if available. The data are used by applications running on the MP70 and running on the central. When brought into vicinity of the MP70, the X2 can be directly connected to the MP70 using a cable. It then releases its wireless connection to the infrastructure AP (if present) and transmits the required data via the cable to the MP70. The MP70 provides own bed overview and acts as a display for the X2. Additionally, it forwards part of the data to the central. This forwarding is done by the application and does not involve, for example, bridging or multi-hop communication.

The wired X2-to-MP70 and the wireless X2-to-AP links are mutually exclusive, that is, only one link is active at a time. The MP2/X2 platform uses the WiVue (AR6K) series chipsets which has SDIO/SPI interface. AR6K series has full MAC protocol embedded in the chipset. Currently, it is not possible to do ad-hoc to infrastructure mode switch while operating, that is, both modes cannot be used simultaneously.

The **MMS** has measurement modules but no display and is connected by cable to the MP70. Currently, the MP70 supports up to two MMS modules and up to two X2s, although usually, only one X2 needs to be supported.

The current usage scenario using wired local connection is shown in figure 3.1.

3.1.2 Dual-link scenario

The target scenario when X2 connects wirelessly to MP70 without going through hospital infrastructure AP is referred to as *dual-link* scenario, since the capability of the MP70 to connect simultaneously to the hospital infrastructure AP and to the X2 portable monitor would require any sort of *ad hoc dual link* Wi-Fi capability.

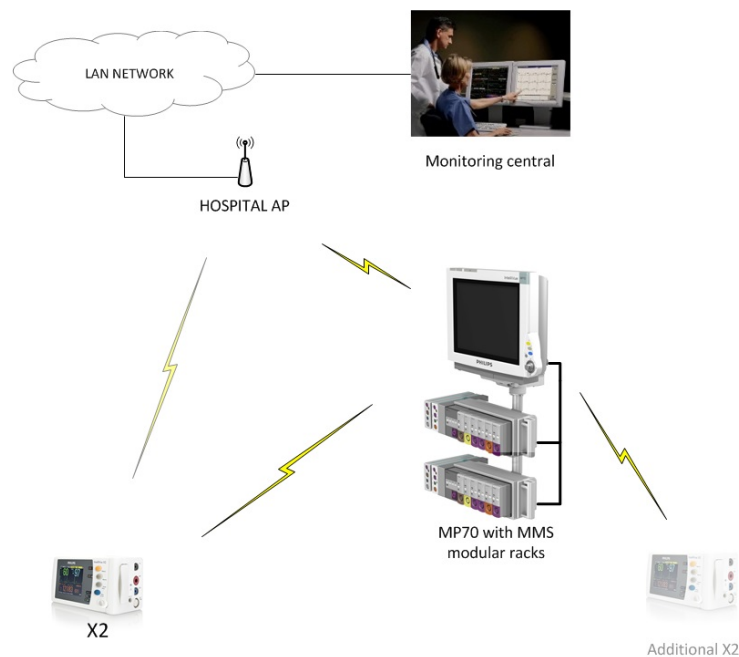


Figure 3.2: X2 and MP70 usage scenario with local wireless connections

As the X2 monitor moves in the vicinity of MP70 monitor which is associated with the same patient it is desired that the X2 monitor detects the presence of such MP70 and associates with it providing wireless connectivity. The previous wireless connection to the hospital Wi-Fi infrastructure is dropped. The new X2-MP70 wireless connection should provide equivalent capabilities which are available in the wired connection currently. These include for MP70 acting as a display for X2, providing application-level connection with the central either through wired (Ethernet backend) or wirelessly, if possible. Note that it is not expected that the MP70 have both wired and wireless connection with the infrastructure to connect with the central; only one connection is required. Also, in the case both routes are possible, wired connections are preferred as they are more reliable.

The targeted *dual-link* scenario is shown in figure 3.2.

It is a marketing requirement that the local X2-MP70 wireless connection be achieved even in the case when MP70 or X2 is not able to communicate with the hospital infrastructure AP. For

example, this could be the case when either X2 or MP70 or both are not in the coverage of hospital infrastructure AP.

It is also desired that in the case that X2 is not able to locate an MP70 belonging to the same patient that it could connect to any other MP70 when not in the range of hospital infrastructure AP. In addition to X2, an MP70 would have up to 2 MMS's and, if possible, an additional X2 wirelessly connected to it.

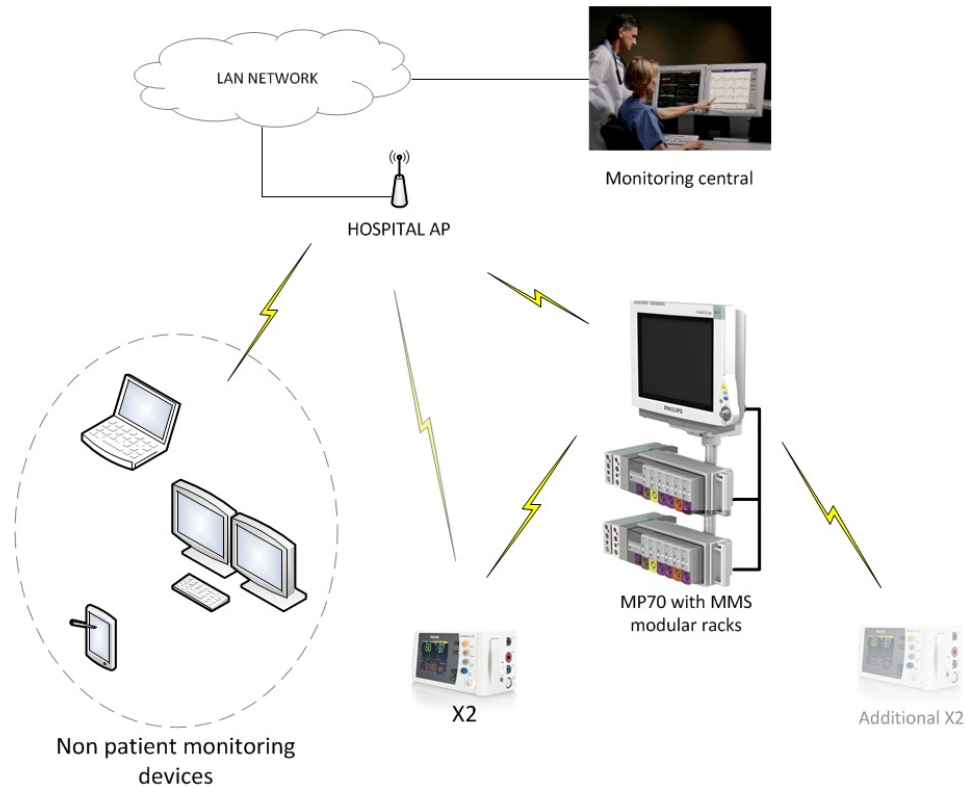


Figure 3.3: *Example of in-hospital dual-link scenario integration in current Wi-Fi network*

3.2 Requirements

To sum up and collect the constraints and desired behaviours of the targeted scenario, this section gathers together the target scenario requirements.

The requirements for the Dual-link Wi-Fi solution can be sub-divided into four distinct categories:

1. **Connectivity architecture requirements**
2. **MP70-X2 link requirements**
3. **Application requirements**
4. **Hardware requirements**

At the same time, each requirement is classified into three categories, depending on its severity:

Must have: The *Must have* requirements must be addressed by the proposed solution; a solution which does not address the requirement will not be considered a viable solution. A requirement which results in a **numeric constraint**, for example *maximum allowable jitter*, would be stated as such and it shall be considered a *Must have* requirement.

Nice to have: A solution which addresses a *Nice to have* requirement will be preferred over the one which does not address the requirement, if both solutions meet all the *Must have* requirements.

Do not care: A solution which addresses a *Do not care* requirement would not have preference over a solution which does not meet those requirements.

3.2.1 Connectivity architecture requirements

The requirements on the connectivity architecture are collected in table 3.1.

Requirement description	Category
Minimum number of MMS simultaneously supported	2 units
Minimum X2's simultaneously supported	1 unit
Dual-link operation without MP70 having hospital infrastructure AP coverage	Must have
Dual-link operation without X2 having hospital infrastructure AP coverage	Must have
X2 and MP70 operating in different subnets	Do not care
For MP70: simultaneous operation of wired (Ethernet) and hospital infrastructure AP connection	Do not care
Runtime MP70 connection switch between infrastructure wired (Ethernet) and hospital infrastructure AP and vice versa	Nice to have

Table 3.1: *Connectivity architecture requirements*

Runtime MP70 connection switch between wired (Ethernet) and hospital infrastructure AP and vice versa: Generally it is possible that the MP70-HospitalAP link may be switched from wired to wireless connection. This is less important for a usage scenario with the MP70 which is a big wall mounted monitor, but could be more important for smaller monitors. It would be a *nice to have* feature if this operation could be carried out without impacting the wireless MP70-X2 link.

3.2.2 MP70-X2 link requirements

The applications running on the MP70 and the X2 demand a certain quality from the wireless link between them, in terms of delay, jitter, and throughput. Hence, a set of requirements on this link are collected in table 3.2.

Description	Requirement
Minimum peak data throughput	5 Mb/s
Maximum link delay	200 ms
Maximum allowable jitter	200 ms
User perceived data loss	No user perception of loss
MP70-HospitalAP and MP70-X2 link co-existence (if applicable)	Must have

Table 3.2: *MP70-X2 link requirements*

Throughput: The current cable is based on twisted pair 10 Mbps Ethernet, and loaded up to 50%, so 5 Mbps (as a first guess) is required as peak throughput. The up to three simultaneous connections are served via a scheme with 32ms tokens. The delay in transporting a frame is thus roughly 100ms. Around 200ms delay seems acceptable for these kind of applications. The link is bidirectional, but most data would flow from X2 to MP70.

Delay: The delay of the link, i.e. from the instant that the packet becomes available until it arrives at the MP70. The wired solution provides a delay which is bounded by 32ms. What is strictly needed here is a delay that does not interfere with the real-time character of the display, so the end-to-end delay should be below around 200 ms.

Jitter: No exact requirements are known but should neither impact the real-time character of the display nor lead to visible artifacts. The current solution provides a delay jitter which is bounded by 32ms. What is strictly needed here is a delay jitter that does not interfere with the aforementioned real-time character of the display, so the jitter should be below around 200 ms.

Packet loss: No exact requirements are known but should neither impact the real-time of the display nor lead to visible artifacts.

Link coexistence: Additionally, the link must possibly co-exist with the MP70-HospitalAP wireless link if it is present.

3.2.3 Hardware requirements

The proposed dual-link Wi-Fi solution would need to run on an MP70 bedside monitor and X2 monitors need to be compatible with the solution. The current and the planned future hardware on the two platforms are described in this section. Limits or constraints on any potential deviations from this hardware in order to implement the proposed solution are also captured here.

X2 hardware: Patient Monitoring has already decided on the WiVue series to use the Atheros AR6K chipset which has a SDIO/SPI interface. This AR6K series has a full MAC protocol embedded in the chipset. Because of this limitations or efforts involved in changing the firmware of the chipset, it is desirable to have a solution which works with the firmware on the chipset provided by the manufacturer.

MP70 hardware: The preferred solution for the cable replacement should target the wireless platform in the MP70. Currently, the MP70 uses the Wistron CM9 802.11 a/b/g miniPCI radio card, based on the Atheros AR5213A chipset. An alternative solution could be based on an upgrade of the MP70 to the WiVue platform that is also used in the X2. If this is not feasible to provide a solution with one of those hardware, then the addition of an USB wireless adapter based on Atheros chips for the MP70 could be acceptable, although it is not preferred.

The requirements in these terms are collected in table 3.3.

Requirement description	Category
The proposed solution works with one wireless adapter based platform on MP70	Must have
The proposed solution works with the WiVue platform on X2	Nice to have
The proposed solution works with the WiVue platform on MP70	Nice to have
The proposed solution works with an additional USB-based wireless adapter on MP70	Acceptable (not preferred)

Table 3.3: Hardware requirements

3.2.4 Application requirements

The application requirements mainly target how the top application will switch from the X2 to infrastructure link to the X2 to MP70 direct link, and are captured in the table 3.4.

Requirement description	Category
The time required to switch the X2-HospitalAP link to the X2-MP70 direct link	Few seconds
The time required to switch the X2-MP70 link to the X2-HospitalAP link	Few seconds
X2 automatically detects and selects the right MP70 with the patient context	Nice to have

Table 3.4: *Application requirements*

Switch time: the time required to switch the X2-to-infrastructure link to the X2-to-MP70 direct link. This criterion is expressed in seconds. A switch time comparable to the time needed to position the cable (a few seconds) would suffice.

Auto-discovery: indicates whether the possibility for a direct link between the X2 and the MP70 is detected automatically or on a user issued command such as a push button.

Auto-discovery and very short switch times (e.g. around 1 sec.) would enable a seamless switch between the applications acting on the data provided via the infrastructure and the application acting on the data provided by the direct link between the MP70 and the X2. Although this would be an attractive feature, it is not considered as vital.

Chapter 4

Technology selection

In the current chapter the potential wireless technologies and Wi-Fi standards, and the applicable IEEE 802.11-based *ad hoc* techniques are described and compared in terms of functionality, hardware requirements and availability of platforms, among others, prior to take a decision on its suitability.

To carry out the suitability assessment we designed our own custom *technology evaluation methodology* as detailed in first place in section 4.1, assigning scores to each *ad hoc* technique following a common criteria for each characteristic and comparing all them objectively in a balanced scorecard in section 4.3.

4.1 Technology evaluation methodology

Before reviewing and describing the multiple considered *ad hoc* techniques we designed our own *technology evaluation methodology*, based on previous references [26] on how to address technology selection processes, assessing each technology individually in terms of its characteristics and suitability for our application, to finally compare them in a homogeneous scale.

1. We granted scores to each of the characteristics that we understood would be of importance when implementing, installing, deploying and using our wireless patient monitoring solution.
2. We assigned the same weight to each of the characteristics analysed. In a general case though, different weights could be assigned to each characteristic depending on its relative importance to the overall solution.
3. We added up all the scores for each technique. For that task, a balanced scorecard helped us to compare the resulting scores and select the preferred technique.

We assigned these scores to each ad hoc technique following a common criteria for each characteristic. Following, we detail the criteria utilized:

Functionality — Capability to provide necessary degree of functionality, specially in terms of *pairing procedure*¹ and *device discovery*. Depending on the default range of functions included in the normal operation of the given technique, and its applicability to our implementation, we assigned the following scores:

- 1 point.** Very few functions included in the technique are applicable to the system.
- 2 points.** A minority of the functions included in the technique are applicable and cover a few functionality needs of the system.
- 3 points.** Some of the functions included in the technique are applicable and cover some functionality needs of the system.
- 4 points.** The majority of the functions included in the technique are applicable and cover a part of the functionality needs of the system.
- 5 points.** All the functions included in the technique are applicable and cover almost all the functionality needs of the system.

Hardware requirements and availability — Necessity for an specific hardware in case of choosing the given technique, in terms of specific or non-standard hardware, manufacturing brand, specific chipset, wireless card version or needed modifications. Depending on the hardware-related constraints of the technique and whether commercial devices based on the given technique are available on the market we assigned the following scores:

- 1 point.** The technique requires custom hardware.
- 2 points.** Major modifications or a very specific hardware are needed to support the given technique.
- 3 points.** Significant modifications on standard hardware or a variety of available hardware are needed to support the given technique.
- 4 points.** Minor modifications on standard hardware or a wide variety of hardware support the given technique.
- 5 points.** The technique does not require a specific hardware or any modification on standard hardware.

Simplicity — Grade of complexity of the solution if it was implemented with the selected approach, evaluated from the point of view of the differences implied by the use of one or another wireless technique. Depending on the overall simplicity of the wireless technique and the solution to be implemented on it, we assigned the following scores:

¹Understanding the *pairing procedure* as the logical connection between the portable and the bedside monitors over the given wireless technique.

- 1 point. High complexity.
- 2 points. Complex solution.
- 3 points. Moderate complexity.
- 4 points. Simple solution.
- 5 points. The simplest solution.

Flexibility — Flexibility of the system, understood as its capability to adapt to changing conditions and its scalability in size. Depending on the overall flexibility of the system, we assigned the following scores:

- 1 point. Rigid system.
- 2 points. Low flexibility.
- 3 points. Moderate flexibility (some aspects).
- 4 points. Flexible system.
- 5 points. High flexibility.

Throughput — Depending on the expected throughput of the solution, we assigned the following scores:

- 1 point. Too low throughput, under the requirements.
- 2 points. Low throughput, too tight for the requirements.
- 3 points. Moderate throughput, around the requirements.
- 4 points. Sufficient throughput, satisfying the requirements.
- 5 points. High throughput, over the requirements.

Implementation — Evaluation of the obstacles and difficulty that could be faced after selecting a given technique, in the next steps of development of the solution, prototyping and implementation. Depending on the expected difficulty of the system implementation, we assigned the following scores:

- 1 point. Very difficult to implement the solution with very specific tools/knowledge.
- 2 points. Difficult to implement the solution with specific tools/knowledge and in a given time.
- 3 points. Difficult to implement the solution with standard tools/knowledge in a given short time.

4 points. Easy to implement the solution with specific tools/knowledge and in a given time.

5 points. Easy to implement the solution with standard tools/knowledge and in a given short time.

Installation — Evaluation of the obstacles and difficulties that could be faced during the system deployment in the hospital facilities, its installation, configuration and integration. Depending on the expected difficulty of the installation over a given technique, we assigned the following scores:

1 point. Very difficult and time-consuming installation. Each node requires specific configuration.

2 points. Difficult or time-consuming installation. Some nodes require particular configuration.

3 points. Moderate difficulty. Nodes work on a generic configuration.

4 points. Relative ease to install the system. Nodes work on a standard configuration.

5 points. Easy to install the system. Nodes are auto-configurable or do not require any configuration.

4.1.1 Balanced scoreboard comparison of available wireless technologies

Together with the ad hoc technique suitability assessment following the described methodology, we started **comparing the available wireless technologies** on which to develop and implement our solution using the ad hoc techniques which will be reviewed in the next section, [4.2 IEEE 802.11-based ad hoc techniques review](#).

Previous attempts of wireless patient monitoring systems have used non-IEEE 802.11 based techniques, like **WSN in the unlicensed 900 MHz band**² in the ISM (industrial/scientific/medical) band, an unlicensed frequency band of 902 to 928 MHz. The 900-MHz band claims to have long broadcast range because of its relatively longer wavelength and its correspondingly longer battery life. However, lower frequency means the use of a larger antenna than higher frequencies. Besides, in order to be able to have the system available in the global market, there would be a lack of standardization in the 900-MHz range as in Europe 900 MHz band is part of the GSM (Global System for Mobile communications) network for cell-phone communication and, thus, is unavailable.

Other options could be based on the **802.15.4 standard**, but taking into account that Zigbee presents severe limitations, it is more applicable to ultralow-power purposes rather than continuous high-bandwidth applications like the one in study.

Taking into account the *Dual-link scenario requirements* related to hardware as in [3.2.3](#), non-IEEE 802.11 solutions to the dual-link scenario should be avoided, due to the *one wireless chip based on the current MP70 Wi-Fi platform* requirement cited as *high desired*.

Nevertheless, Bluetooth 3.0 + HS was still considered due to its interesting pairing functionalities and reasonably high throughput specifications announced, thanks to the **smart use of an alternate MAC/PHY substituting its radio by 802.11 for enhanced data rates** when on data transmission. For that last reason **we included Bluetooth 3.0 in the suitability assessment** carried out in this chapter in section [4.3](#).

Table [4.1](#) details the available considered wireless technologies comparison, in full-page landscape configuration for a better visualization. It reviews features that are of a significant importance for our application, such as expected data rates, communication range in indoor environments or the frequency band in usage.

It also includes other features that are not explicitly related to any requirement, but can help to decide between two different technologies with similar performance. Among these are power consumption, the lower the better, for guaranteeing long operation times when running on battery; spectral efficiency, the higher the better; or chip price, the cheaper the better, obviously. Other features as the access method, the signal bandwidth and the release year are indicative.

For the price figures, extensive search was conducted with the use of chip price search engines:

1. Findchips, that performs a search over many distributors: <http://www.findchips.com>.

²N. O'Donoghue, S. Kulkarni, D. Marzella, *Design and implementation of a framework for monitoring patients in hospitals using wireless sensors in ad hoc configuration*, Conf. Proc. IEEE Eng. Med. Biol. Soc. 1:6449-6452, 2006

2. Octoparts that conducts the searches over distributors as well as semiconductor manufacturers for the price listings, <http://octopart.com/categories>.

The average chip prices indicated in the table were calculated after averaging and rounding the results found in May 2010, to provide with comparative relative costs of every technology rather than providing with absolute figures. In order to assess the economical viability of a final product, up-to-date prices should be considered.

Feature	ZigBee 802.15.4	Bluetooth 2.0-2.1 EDR	Bluetooth 3.0 + HS	802.11b	802.11g	802.11a	802.11n	UWB 802.15.3a
Data rate [Mbps]	0.03	1 - 3	1 / 24	11	54	54	144.4	200
Max. Indoor Range [m]	25	10	10	40	40	35	50	10
Power [mW]	30	100	100 / 1000	750	1000	1500	2000	400
Bandwidth [MHz]	0.6	1	1 / 20	22	20	20	40	500
Frequency Band [GHz]	868 MHz 915 MHz 2.4 GHz	2.4	2.4	2.4	2.4	5	2.4 / 5	3.1 - 10.6
Spectral efficiency [(b/s)/Hz]	0.05	1 - 3	1 / 1.2	0.5	2.7	2.7	5	0.4
Access Method	DSSS	FHSS	FHSS 802.11 Alt. MAC/PHY	DSSS CCK	OFDM DSSS	OFDM	MIMO OFDM	DS-UWB OFDM
Average chip price	2.00 eur	3.00 eur	-	5.00 eur	9.00 eur	12.00 eur	20.00 eur	7.00 eur
Release year	2007	1994 (1.1) 2004 (2.0) 2007 (2.1)	2009	1999	2003	1999	2009	2004

Table 4.1: Wireless specifications features comparison

In order to carry out an objective comparison of the different applicable wireless specifications, we developed a method for extracting a score in a fair way for each considered specification according to the key features. For that task, a balanced scorecard helped us to extract a more objective total score.

We extracted the *best* values, the maximum or minimum values depending on the feature, and we filled the scorecard with proportional scores for each specification, in relation with the best value for each feature.

$$score_{i,j} = \frac{value_{i,j}}{best_i\{value_{i,j}\}} = \frac{value_{i,j}}{max_i\{value_{i,j}\}}$$

Where i is the index referring to the different specifications and j refers to the different features for each specification, respectively. And $best_i$ is the best value for a given j feature, calculated as the maximum value for that feature along i for all the specifications j values.

In the cases of power consumption and price, the best value is calculated as the minimum value for that feature along all the specifications' values, instead of the maximum.

$$score_{i,j} = \frac{value_{i,j}}{best_i\{value_{i,j}\}} = \frac{value_{i,j}}{min_i\{value_{i,j}\}}$$

We adjusted the scores in the cases where the difference between the maximum and the minimum values was too high³, making the proportions not linear but proportional to the square root of the ratio between the given value and the best value for that feature.

$$score_{i,j}^{adj} = \sqrt{\frac{value_{i,j}}{best_i\{value_{i,j}\}}} \quad \text{if} \quad \frac{max_i\{value_{i,j}\}}{min_i\{value_{i,j}\}} \gg 10$$

Finally we scaled the scores, that were normalized to 1 given its construction, to a maximum of 10 for having each feature's score ranging from 0 to 10 points.

$$total\ score_{i,j} = \begin{cases} 10 \cdot score_{i,j} \\ 10 \cdot score_{i,j}^{adj} \end{cases} \quad \text{if} \quad \frac{max_i\{value_{i,j}\}}{min_i\{value_{i,j}\}} \gg 10$$

Table 4.2 details the wireless specifications balanced scorecard, with the adjusted and scaled scores for each feature and specification.

³The scores of *Data rate*, *Power consumption* and *Spectral efficiency* had to be adjusted.



Feature	ZigBee 802.15.4	Bluetooth 2.0-2.1 EDR	Bluetooth 3.0 + HS	802.11b	802.11g	802.11a	802.11n	UWB 802.15.3a
Data Rate	0.1	1.2	3.5	2.3	5.2	5.2	8.5	10.0
Indoor Range	5.0	2.0	2.0	8.0	8.0	7.0	10.0	2.0
Power consumption (10=lowest)	10.0	5.5	1.7	2.0	1.7	1.4	1.2	2.7
Spectral efficiency	1.0	4.5	4.9	3.2	7.3	7.3	10.0	2.8
Chip price (10=lowest)	10.0	6.7	-	4.0	2.2	1.7	1.0	2.9
Total score	26.1	19.8	12.1	19.5	24.5	22.6	30.7	20.4

Table 4.2: Wireless specifications balanced scorecard

Taking into account the *Dual-link scenario requirements* related to hardware, as in subsection 3.2.3, we discarded the UWB and legacy Bluetooth options. We also had to discard the ZigBee for the hardware requirements as well as for obvious throughput reasons, regardless of the overall score, which turned out to be the second highest. Nevertheless we maintained in this chapter the suitability analysis of the Bluetooth 3.0 for its interest (see its detailed review in section 4.2.7), since is the only hybrid technique using the good features of both easy-to-setup PAN networks and powerful and fast WLAN networks.

Discarded options are shadowed in dark gray in Table 4.2.

Regarding the wireless networks availability in European hospitals, as discussed in section 2.1, the consulted surveys[10] do not focus on which specific protocols are present in hospitals, but only provide with general availability figures for wireless infrastructure and the presence of wireless patient monitoring systems.

We assumed that in medical environments as in businesses and general public facilities, where there was more reticence toward early adoption of advanced Wi-Fi protocols⁴, 802.11n adoption had still to be low, so the majority of hospital facilities' wireless infrastructures were supposed to be based on 802.11g networks at best.

Moreover, it was a requirement agreed with the customer[34], to **stay in the 2.4 GHz frequency band and avoid the 5 GHz** to stick with the 802.11g current hospitals' wireless network deployments and current patient monitoring hardware platforms, like the Philips IntelliVue 802.11 a/b/g Clinical Network, for cost reasons.

After discarding 802.11n for the aforementioned availability reasons, in spite of having been provided with the highest score, we chose **IEEE 802.11 as the most appropriate wireless technology and 802.11g as the most appropriate specification** over which to continue our design and development of a wireless patient monitoring solution.

⁴N. Graychase, Wi-Fi Planet.com, "802.11n: Ratified at Last", <http://www.wi-fiplanet.com/news/article.php/3838991>, Sept. 2009

4.2 IEEE 802.11-based ad hoc techniques review

Several *ad hoc* networking techniques are already available or are reaching maturity, especially IEEE 802.11 based techniques. Among these are:

Ad hoc: IEEE *ad hoc mode* forming an IBSS (Independent Basic Service Set). Reviewed in section 4.2.1.

TDLS: 802.11z Tunneled Direct Link Setup. Reviewed in section 4.2.2.

WDS: Wireless Distribution System. Reviewed in section 4.2.3.

P2P: Wi-Fi Direct™, formerly *Wi-Fi Peer-to-Peer* or *Wi-Fi P2P*. Reviewed in section 4.2.4.

Mesh: 802.11s mesh networking. Reviewed in section 4.2.5.

SoftAP: Software Access Point, with a simultaneous AP and STA. Reviewed in section 4.2.6.

As introduced before, taking into account the *Dual-link scenario requirements* related to hardware in 3.2.3, non-IEEE 802.11 solutions for the dual-link scenario should be avoided, due to the *one wireless chip based on the current MP70 Wi-Fi platform* requirement cited as *high desired*.

Nevertheless, Bluetooth 3.0 + HS was still considered due to its interesting pairing functionalities and reasonably high throughput specifications announced, thanks to the **smart use of an alternate MAC/PHY substituting its radio by 802.11 for enhanced data rates** when on data transmission. For that last reason **we included Bluetooth 3.0 in the suitability assessment** carried out in this chapter in section 4.3:

Bluetooth 3.0: Bluetooth 3.0 + HS (High Speed) with IEEE 802.11 alternate MAC/PHY. Reviewed in section 4.2.7.

The 802.11 standard

As a basis for the description of the reviewed techniques and their operation details, the 802.11 standard is described at first instance, making emphasis on the most relevant aspects.

The IEEE Working Group adopted in 1997[15] the first wireless LAN (WLAN) standard, IEEE Std. 802.11-1997. This specification defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless connectivity.

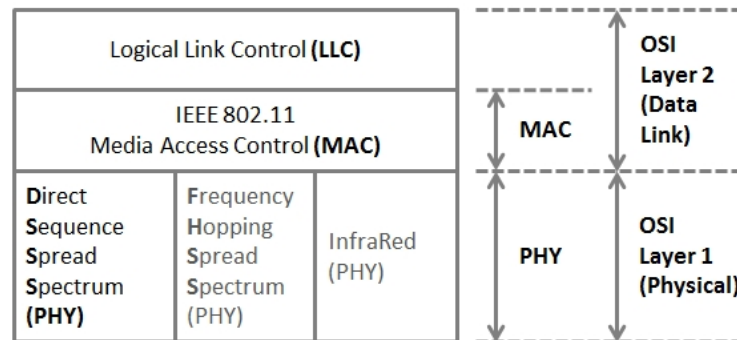


Figure 4.1: Legacy IEEE 802.11 standard's MAC and PHY layers mapped to the OSI reference model

The IEEE 802.11 MAC layer corresponds to the data link layer in the OSI model, see figure 4.1. The main objective of the OSI data link layer is to provide error-free transmission of data across a physical link. IEEE 802.11 protocols' version of this scheme consists of two sublayers: Logical Link Control (LLC) and Medium Access Control (MAC).

The most important services offered by the LLC are error and flow control. The MAC interfaces directly with the physical layer, and provides services such as addressing, framing, and medium access control.

The 802.11 MAC must coordinate an access mechanism to allow fair access to the medium. 802.11 stations do not have the ability to sense collisions that the carrier sense multiple access/collision detect (CSMA/CD) based wired Ethernet stations do have, since most of the wireless transceivers are half-duplex (are not able to listen to the media while transmitting and vice versa). As a consequence, a more robust MAC with minimized overhead is required for wireless medium access, compared to the common wired Ethernet local network standard IEEE 802.3.

The 802.11 MAC layer offers two different types of service, see figure 4.2: a contention service provided by the Distributed Coordination Function (DCF), and a contention-free service implemented by the Point Coordination Function (PCF).

The DCF provides the basic access method of the 802.11 MAC protocol and is based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. The PCF is implemented on top of the DCF and is based on a centralised polling scheme that obviously can not be adopted in distributed configurations.

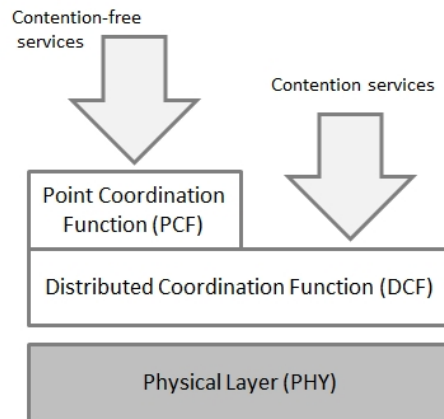


Figure 4.2: IEEE 802.11 DCF and PCF functions architecture

802.11 network topologies

Regarding 802.11 network topologies, in “infrastructure” mode wireless devices communicate via base stations known as access points (hereafter referred to as APs). Each AP and its wireless devices, stations (hereafter referred to as STAs) are known as a **Basic Service Set (BSS)**.

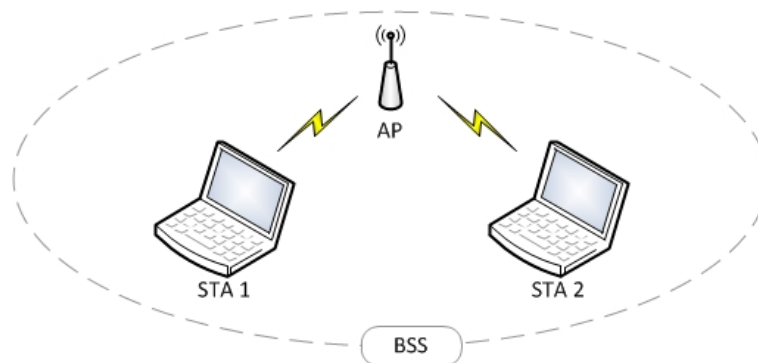


Figure 4.3: Basic Service Set (BSS)

An **Extended Service Set (ESS)** is a set of infrastructure BSS’s, as in figure 4.4, where the access points communicate amongst themselves to forward traffic from one BSS to another to facilitate movement of stations between BSS’s. Access points perform this communication through distribution systems. The distribution system (DS) is the backbone of a wireless LAN, connecting APs to form ESS; it is the means by which two different APs can exchange frames for stations in their respective BSSs, forward frames to follow mobile stations as they move from one BSS to another, and exchange frames with a wired network.

As IEEE 802.11 describes it, the distribution system is not necessarily a network nor does the standard place any restrictions on how the distribution system is implemented, only on the services it must provide.

The same applies to portals, which can be implemented by a router, a bridge or simply an AP, and serve as a gateway from the DS to the rest of networks. A portal is just a transference point between the ESS and other wired LANs, where frames logically enter and exit the ESS.

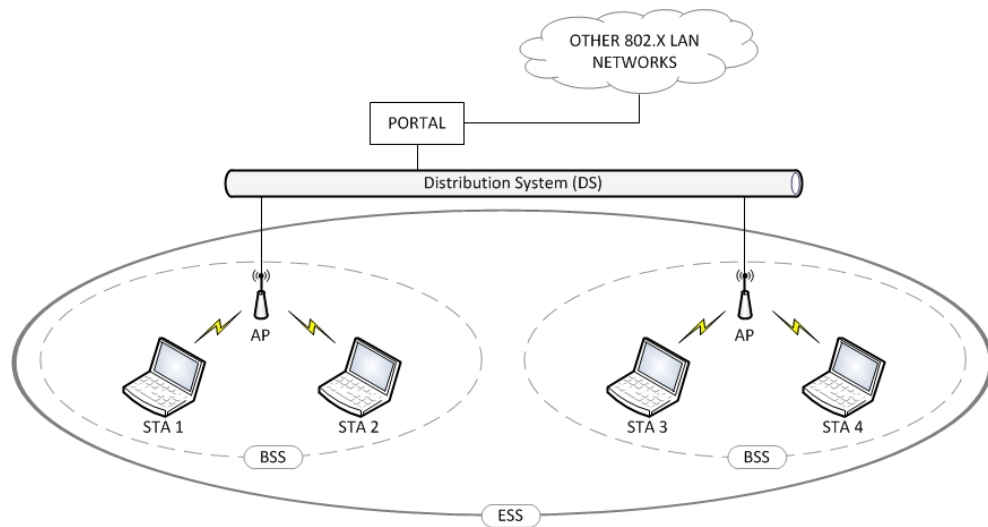


Figure 4.4: *Extended Service Set (ESS)*

Network equipment outside of the Extended Service Set view the ESS and all of its mobile stations as a single MAC-layer network where all stations are physically stationary, allowing existing network protocols that have no concept of mobility to operate correctly with a wireless LAN where there is an inherent station mobility.

In *ad hoc mode*, which will be described in depth in subsection 4.2.1, wireless devices communicate with each other directly without an access point, forming an **Independent Basic Service Set (IBSS)**, see figure 4.5.

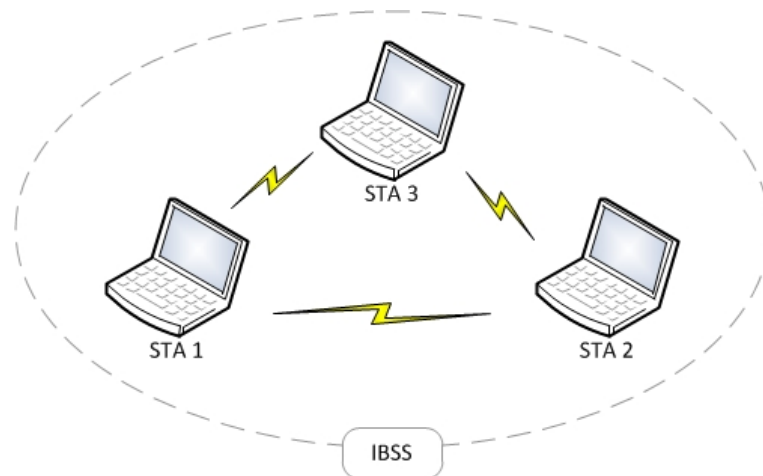


Figure 4.5: *Independent Basic Service Set (IBSS)*

802.11 services

The 802.11 standard defines services for providing essential functions for the network operation, some of them implemented by stations and others by distribution systems[16].

Station services are implemented within all stations on an 802.11 WLAN, including access points. The main thrust behind station services is to provide security and data delivery services

for the WLAN:

Authentication: 802.11 defines authentication services to control access to the WLAN, to prevent unauthorized access, because wireless LANs have limited physical security. The authentication service provides a mechanism for one station to identify another station. Without this proof of identity, the station is not allowed to use the WLAN for data delivery. All 802.11 stations, whether they are part of an independent BSS or ESS network, must use the authentication service prior to communicating with another station.

Open system authentication is the default authentication method, which is a simple, two-step process. First the station that wants to authenticate with another station sends an authentication management frame containing its identity. The receiving station then sends back a frame acknowledging whether it recognizes the identity of the authenticating station or not.

Shared key authentication assumes that each station has received a secret shared key through a secure channel independent of the 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of that kind of authentication requires implementation of encryption via the Wired Equivalent Privacy (WEP) algorithm.

De-authentication: The de-authentication service is used to avoid a previously authorized user from any further use of the network. Once a station is de-authenticated, that station is no longer able to access the WLAN without performing the authentication process again. De-authentication is a notification and thus, cannot be refused. For instance, when a station wishes to be removed from a BSS, it can send a de-authentication management frame to the associated access point to notify it of the removal from the network. An access point can also de-authenticate a given station by sending a de-authentication frame to that station.

Privacy: The privacy service of IEEE 802.11 is designed to provide an equivalent level of protection for data on the WLAN as that provided by a wired network with its inherent restricted physical access. Note that this service protects that data only as it traverses the wireless medium.

Data delivery: Similarly to that provided by all other IEEE 802 LANs, provides reliable delivery of data frames from the MAC in one station to the MAC in one or more other stations, with minimal duplication and reordering of frames. Also known as *MAC Service Data Unit (MSDU) delivery service*.

Distribution services provide functionality across a distribution system, and thus only apply on infrastructure mode networks. Typically, access points provide distribution services:

Association: The association service is used to make the logical connection between a mobile station and an access point. Each station must become associated with an access point before it is allowed to send data through it onto the distribution system. The connection is necessary in order for the distribution system to know where and how to deliver data to mobile stations.

Mobile stations invoke the association service only once, typically when entering the BSS. Each station can associate with one access point, however an access point can be associated

with multiple stations.

Disassociation: The disassociation service is used either to force a mobile station to cancel a previous association with an access point or for a mobile station to inform an access point that it no longer requires its services. When a station becomes disassociated, it must begin a new association to communicate with an access point again.

An access point may force a station or stations to disassociate because of resource restraints, the access point shutting down or being removed from the network.

Stations should disassociate when they plan to leave a network, although there is nothing in the specification of 802.11 devices to assure this happens. Disassociation is a notification and can be invoked by either associated party. Neither party can refuse the termination of the association.

Re-association: Re-association enables a station to change its current association with an access point; it is always initiated by the mobile station. The re-association service is similar to the association service, with the exception that it includes information about the access point with which a mobile station has been previously associated. A mobile station will use the re-association service repeatedly as it moves throughout an ESS, loses contact with the access point with which it is associated, and needs to become associated with a new access point.

This allows the newly associated access point to contact the previously associated access point to obtain frames that may be waiting there for delivery to the mobile station as well as other information that may be relevant to the new association.

Distribution: Distribution is the primary service used by an 802.11 station every time it sends MAC frames across the distribution system. The distribution service provides distribution systems with the necessary information to properly determine the destination for MAC frames along an ESS.

Integration: The integration service connects the 802.11 WLAN to other Local Area Networks, including wired LANs or 802.11 WLANs. A portal, an abstract architectural concept, performs the integration service. Portals typically reside in access points although they could entirely be part of separate network components.

Relation between 802.11 station states, services and frames

802.11 stations can be in one of three possible states, depending on its authentication and association status. Changes between states depend on the sending of certain frames, and allowed frame types vary with the association and authentication statuses, thus forming the state machine displayed in figure 4.6.

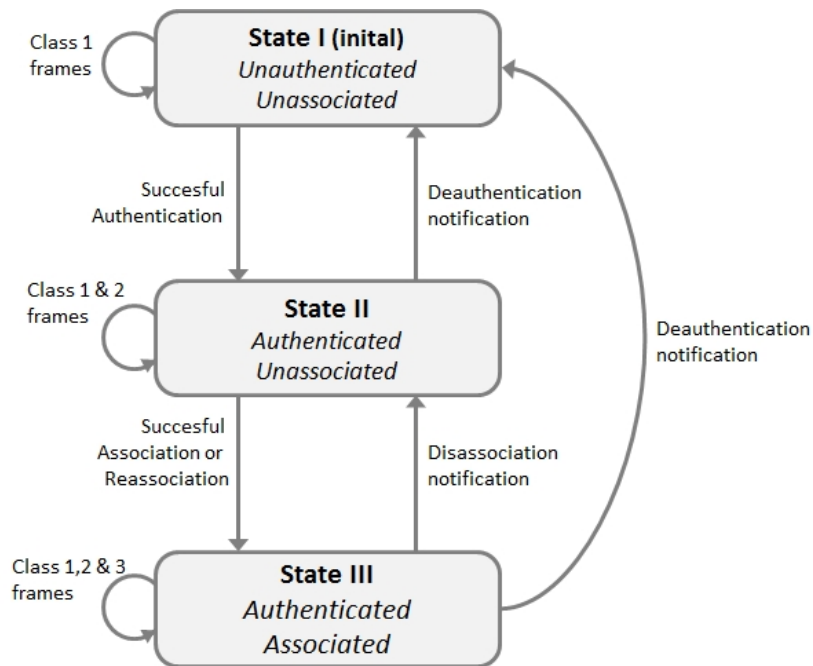


Figure 4.6: 802.11 state machine: Relation between 802.11 station states, services and frames

Starting in State I, each one is a successively more advanced stage in the development of an 802.11 connection.

1. In the first state, only Class 1 frames (see table 4.3) can be transmitted, the ones to provide basic operations used by 802.11 stations Control frames (Request to Send, Clear to send, Acknowledgement, Contention-free End and CF-End Acknowledgements) and Management frames (Probe Request, Probe Response, Beacons, Authentication, De-authentication and Announcement Traffic Indication Message). Moreover, data frames within an IBSS or a BSS are allowed, with frame control bits “To DS” and “From DS” both false. After an authentication failure, stations remain in State I.
2. After a successful Authentication, the state machine moves to State II in which Class 1 and Class 2 frames can be sent. In addition to basic operation frames, in the second state frames related with the association process are allowed (Association, Re-Association and Dis-Association requests and responses). Since IBSSs do not have access points nor associations, connections on *ad hoc mode* networks only reach State II after stations authenticate each other. After an association failure, stations remain in State II.
3. An association or re-association process carried out correctly conducts to the third and last, more advanced state. In State III all-Class frames can be sent: basic ones, frames related to association and the more advanced ones; i.e. Power-Save Poll frames and data frames including those either “To DS” or “From DS”. Data can be transmitted through a distribution system only in State III. If an AP receives frames from an authenticated but not associated station, the AP responds

with a disassociation frame to reject the station back to State II. But in the case the station is not even authenticated, the AP responds with a Deauthentication frame to force the station back to State I, as shown in the state machine figure 4.6.

Frames are classified into 3 different categories, as in table 4.3: Control Frames, Management Frames and Data Frames.

- **Control Frames** assist in the delivery of IEEE 802.11 Data frames and Management frames.
- **Management Frames** help implementing 802.11 defined functions / services.
- **Data Frames** carry higher level/layer data in the frame body.

	Control Frames	Management Frames	Data Frames
Class 1	RTS CTS ACK CF-End CF-End-ACK	Probe Req./Resp. Beacon Auth. De-auth. ATIM	Data (IBSS/BSS)
Class 2		Assoc. Req./Resp. Re-Assoc. Req./Resp. Dis-Assoc. Req./Resp.	
Class 3	PS-Poll	De-auth.	Data (all)

Table 4.3: 802.11 Frame classes and categories

802.11 Power management

IEEE 802.11 supports the necessary operations to manage and save power in stations since, no matter the application, battery it is always a limited resource.

In infrastructure mode:

- Stations may operate in Power-Save mode (also referred as Sleep mode) or Awake mode.
- The AP does not transmit normal frames to stations in Power-Save mode. It does keep buffering that frames, instead.
- Within the Beacon frames is inserted a Traffic Indication Map (TIM), reflecting which stations have pending frames in the AP.
- Stations in PS mode wake up periodically in order to listen to Beacon frames.
- In the case a station finds out that there are pending frames for it, it sends the AP a PS-Poll frame asking for retrieval. The AP replies with the stored frame. The process repeats until there are no more frames stored for the station.
- When a station awakes to go out from PS mode, it indicates the AP with a bit within a

control field of the frames to send. The station will not change its status until receiving the corresponding response.

- The AP buffers broadcast and multicast packets if any of the associated stations enter into the Power-Save mode.
- A Delivery Traffic Indication Map (DTIM) is transmitted by the AP every some Beacon intervals (depending on the BSS configuration), after which buffered broadcast and multicast frames are transmitted, with priority over unicast PS-Poll demanded buffered frames.

Power management in *ad hoc mode* will be reviewed in subsection 4.2.1

802.11 standards and amendments

IEEE Std. 802.11-1997 was the original first one of a subsequent standards (and their amendments) of which there have been several major upgrades, relating primarily to data rates and differentiated by letter suffixes:

802.11-1997 Standard: The 802.11 specification defined originally three PHY types of WLANs, all operating at a data transmission rate of 1 or 2 Mbps: 802.11 DSSS and 802.11 FHSS, that use radiofrequency radiation as the transmission medium in the unlicensed ISM (Industrial, Scientific and Medical) band at 2.4 GHz, and a third specification based on diffuse infra-red transmission, obsolete nowadays.

The idea behind FHSS is that the transmitter hops from frequency to frequency hundreds of times per second. The hop pattern is known to both the sender and receiver, and to other receivers not aware of the pattern, the transmission is hard to detect. DSSS, on the other hand, does not hop from one frequency to another, but distributes the signal over the entire frequency band at once, based on a sequence of short chips.

FHSS and InfraRed were abandoned by the Wi-Fi Alliance and further developments focused on DSSS and OFDM transmission schemes. 1 Mbps DSSS methods are still used by current, modern access points for the basic operations (e.g. beaconing, association, etc.) to guarantee backward compatibility with legacy stations.

802.11b Amendment (1999): Using DSSS transmission scheme and the same 2.4 GHz band as defined in the original standard, 802.11b boosted data rate up to 11 Mbps while keeping slower DSSS modes to function in noisy environments. It was the first major WLAN standard, with a great worldwide adoption and operates at data rates of 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps. However, practical figures for the maximum net throughput at 11 Mbps data rates are around 5.9 Mbps using TCP and 7.1 Mbps for UDP transmissions due to the CSMA/CA overhead[35].

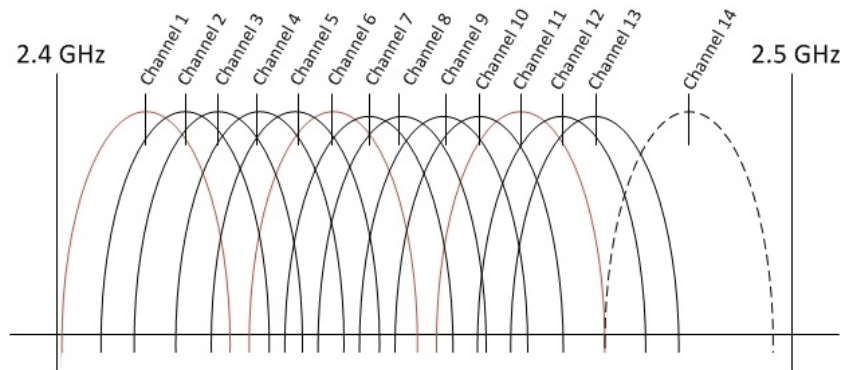


Figure 4.7: 802.11b DSSS 22MHz channel width

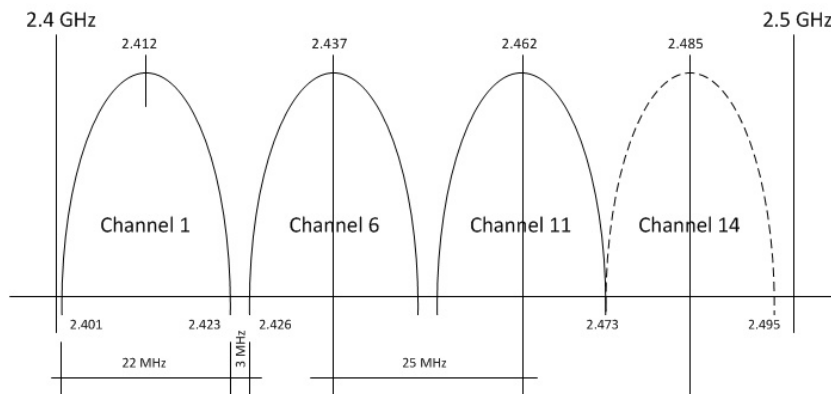


Figure 4.8: 802.11b DSSS 22MHz channel width (non overlapping channels)

802.11a Amendment (1999): Using orthogonal frequency-division multiplexing (OFDM), a different and more complex modulation technique that carries data over multiple orthogonal sub-carrier frequencies, operates in the 5 GHz band, thus is not backward compatible with the slower 11b equipment. The higher frequency used by 802.11a typically shortens the communication range and its ability to penetrate through obstructions, however it has the advantages of higher data rates (up to 54 Mbps) and also does not interfere with the comparatively larger amounts of 2.4 GHz equipment on the market, as the 5 GHz band is, in general, much less crowded. Supports multiple data rates, from 6 Mbps (when using BPSK modulation with basic coding rate), 9, 12, 18, 24, 36, 48 and 54 Mbps (when using 64QAM modulation with the highest coding rate).

802.11g Amendment (2003): Using orthogonal FDM (OFDM) transmission, 11g increased data rates from 11 to 54 Mbps. Both 11b and 11g use the 2.4 GHz band and are compatible, which is why equipment is often designated as 802.11b/g. If 11b and 11g devices communicate, it is done at the slower 11b speed for compatibility reasons, in what is known as mixed mode. The practical figure for maximum net throughput in 802.11g is around 27.9 Mbps due to protocols overhead[35] over 54 Mbps data rate.

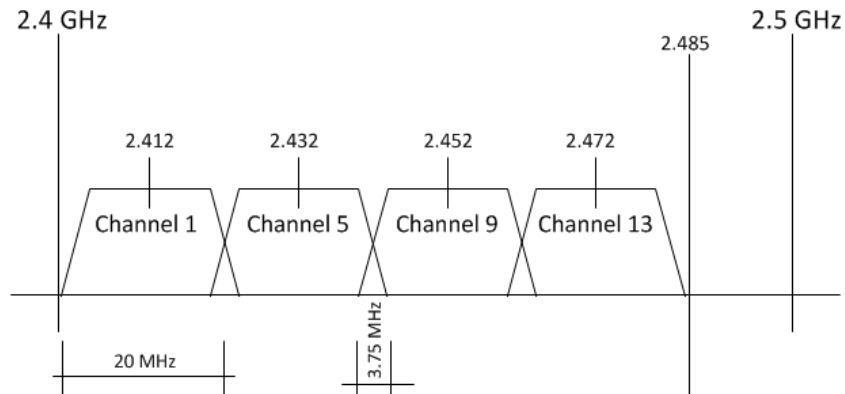


Figure 4.9: 802.11g/n OFDM 20MHz channel width (16.25 MHz used by sub-carriers)

802.11n Amendment (2009): The 802.11n standard uses multiple-input and multiple-output (MIMO) and 40 MHz channels for speeds up to 150 Mbps. Thanks to the use of multiple antennas and multiple wireless connections this technology is much more resistant to interference without requiring a significant increase in power used to transmit the data. MIMO also presents the ability to use multipath (a radiation peculiarity thanks to which a single signal takes different paths and arrives at the receiver at slightly different times, what is exploited for good with this technique but used to cause a negative factor on performance when using older standards). Since 11n can operate in both spectrum bands, it is compatible with previous 11b/g and 11a standards, although there are concerns that 802.11n devices may interfere with the operation of nearby 802.11b and 802.11g devices due to the use of wider channels.

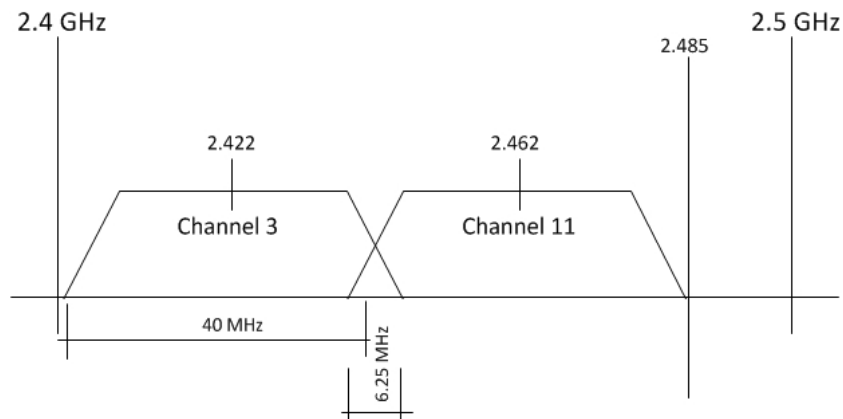


Figure 4.10: 802.11n OFDM 40MHz channel width (33.75 MHz used by sub-carriers)

These different IEEE 802.11 specifications will be reviewed again in the Suitability Assessment section 4.3.

4.2.1 Ad hoc mode (IBSS)

An *ad hoc mode* network is a WLAN network, described in the IEEE 802.11 standard as Independent Basic Service Set (IBSS), where two or more peer stations communicate directly without any access point.

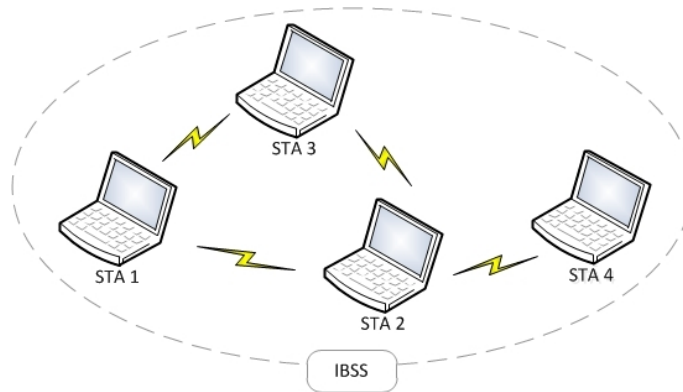


Figure 4.11: *Independent Basic Service Set (IBSS)*

The main characteristics of an 802.11 ad hoc network are the following:

- These networks do not involve any pre-planning or site survey, so they are usually small and only last long enough for a brief communication to address a specific need.
- In an IBSS all stations directly communicate to each other within the IBSS.
- In *ad hoc mode* there is no master device, the connectivity is among IBSS members as equals (not multiple paired station links like in an Infrastructure BSS or ESS)
- Stations may come and go at any time, since there is no process of association. When there are more than two stations in a IBSS network, the departure of any device will not impact the ability of other devices to continue communicating between them.
- *Ad hoc mode* does not provide routing, relaying or repeating of packets (as a mesh technique might provide).
- Not every mobile station may be able to communicate with all other stations due to range limitations.
- Moreover, *ad hoc mode* networks are subjecto to *hidden node problem*⁵ and *exposed node problem*⁶, although its effects can be alleviated by extending the DCF basic mechanism by

⁵Devices A and C are both in range to communicate with B, but are unaware of each other, so their communications can collide at B.

⁶Devices A and C are both in range to communicate with B, but A can not hear transmissions from C. Assuming that B is transmitting to A and C wants to transmit to D, according to the DCF protocol, C senses the medium and finds it busy because of B's transmission. Therefore, C refrains from transmitting to D although this transmission would not cause a collision at A nor B.

a virtual carrier sensing mechanism based on two control frames: Request To Send (RTS) and Clear To Send (CTS).

The most basic *ad hoc mode* topology is a set of two stations, which are inside each other's communication range, have acknowledge each other and thus, are able to connect wirelessly in a peer-to-peer fashion, forming the simplest IBSS.

Operation details

In IBSS, the BSSID is random and locally administered by the starting station. To maximize the probability of creating a unique address, it is formed of 46 random generated bits for the BSSID.

A device configured in IBSS mode will start looking for other devices with matching SSID on all frequency channels. It will scan all channels in random order for a device that sends beacon messages, containing the target SSID.

When an acceptable partner has been found (with target SSID), the channel on which the partner was transmitting will be accepted as the channel that the newly started station will use. Unlike in the infrastructure mode, when a station connects to another station in the IBSS no association requests are issued and only channel establishment occurs.

If the station did not find a partner to join or associate with (that is, no beacons with matching SSID were found) the station establishes its own IBSS with the SSID it was unsuccessfully looking for, by transmitting beacon messages, which are needed to maintain synchronization among the stations in a distributed manner. In infrastructure mode, unlikely, only the access point sends beacons.

The station that starts the IBSS sets the beacon interval to create a set of Target Beacon Transmission Times (TBTT) in order to guarantee the maintenance of the beacon timing. To do so, each station in an IBSS proceeds with the following steps:

- Suspend any pending backoff timers from the previous TBTT
- Determine a new random delay for the timer
- If a beacon arrives before the end of the random delay, resume the suspended backoff timers. If no beacon arrives prior to the end of the random delay, send a beacon and resume the suspended backoff timers

In that way, if a station does not hear a beacon within a random period, then this station assumes that no other stations are active and a beacon needs to be sent. The random delay minimizes the transmission of beacons from multiple stations by effectively reducing the number of stations that will send a beacon.

Included within the beacon frame there is a Timer Synchronization Function (TSF). Each station

compares the TSF in the beacon to its local timer and, if the received value is greater, meaning the clock in the transmitting station is running faster, it updates its timer to the received value. This has the long-term effect of updating the timing throughout the ad hoc network to the station with the fastest timer. Along a large ad hoc network where many clients cannot directly communicate, it might take some time for the timing to distribute.

Other ad hoc stations can join the network after receiving a beacon and accepting the IBSS parameters (e.g., beacon interval) found in the beacon frame.

If any device has a broadcast message to send, it just transmits and all the others listen. If any device wants to send a frame to another particular device, it just transmits it with the target device's MAC address as the destination.

Table 4.4 shows the *ad hoc mode* operation options depending on devices state assuming two IBSS capable devices A and B.

Device A State	Device B State	Action
Not IBSS member	Not IBSS member	Form new IBSS with A and B as members
Not IBSS member	IBSS2 member	A joins IBSS2 with B
IBSS1 member	Not IBSS member	B joins IBSS1 with A
IBSS1 member	IBSS1 member	Do nothing, already connected
IBSS1 member	IBSS2 member	Do nothing without additional user input

Table 4.4: *Ad hoc mode operation options depending on devices state*

Much of the 802.11 standard defines a common operation both using ad hoc or infrastructure mode. The use of *ad hoc mode* only affects the protocols, so there is no impact on the Physical Layers (e.g., 802.11a, 802.11b or 802.11g). Within the MAC Layer, all of the carrier sensing and most of the frame types and corresponding usage are the same regardless of the operation mode. The absence of an access point, however, means that stations in an ad hoc wireless LAN must take on more of the MAC Layer responsibilities.

Set up and operation of an ad hoc IBSS is independent (from an ownership viewpoint and connectivity viewpoint) from infrastructure ESS WLAN operation. Ad hoc IBSS networks can coexist with Wi-Fi infrastructure ESS networks without any inconvenience.

Power management in IBSSs

Power management in *ad hoc mode* networks is implemented in a distributed manner, accordingly, as there is no central coordination. Thus, it is not as efficient as power management in infrastructure networks, since receivers must be more available and cannot sleep for the same lengths of time as in infrastructure networks. This feature in IBSS is based on the use

of Announcement Traffic Indication Messages (ATIM), also known as *ad hoc traffic indication messages* or *ad hoc traffic indication maps*, to avoid other stations to go to sleep mode.

As with infrastructure networks, an ad hoc sleeping station (i.e., with power management *on*) indicates that is entering sleep state by setting to “1” the power management bit in the control field of any frame. All other stations learn of this by monitoring the frame control fields of all frames. Stations will then hold off transmitting to the sleeping station and buffer the corresponding packets locally.

Regularly, all sleeping stations wake up simultaneously during the ATIM window (every some beacon transmissions, as it is an IBSS configurable parameter). If a station is holding packets for a sleeping destination, the station will send an ATIM frame to the sleeping station indicating that packets are awaiting transmission. The station that had been asleep then knows that it has to stay awake during the next beacon interval, in which the station buffering the packet will send it. After receiving and acknowledging reception of the packet, the receiving station can go back to sleep. Buffering retains frames for at least one beacon period, but the standard does not define for how long more.

Initialization of power management within an IBSS:

- A station creating a new IBSS network sets the value of the ATIM window parameter. The ATIM window is indicated within the IBSS Parameter set element of the beacon.
- Joining stations have to set its ATIM window value to the IBSS creator’s ATIM window value.
- The start of ATIM window is defined as Target Beacon Transmission Time (TBTT), while the end of ATIM window have to be defined as TSF timer MOD Beacon Interval, i.e. the ATIM window.
- An ATIM window value of zero indicates that power management is not in use within the IBSS network.
- The value of ATIM window is static all along the lifetime of a given IBSS network.

Power-Save mode transitions:

- Stations can enter into PS-mode only if ATIM window is set to non-zero value.
- When a station is in PS-mode it has to set PS bit to “1” in MSDU that it transmits.
- The standard does not define the mechanisms which stations have to employ to announce their PS status.
- Stations can announce their PS status using PS bit in Beacon frames.
- Stations can employ RTS/CTS mechanism to know the PS status of counterpart stations before transmitting MSDU data frames. MSDU frames and other management frames

have to be transmitted outside the ATIM window

- RTS, CTS, ATIM, Beacon and ACK frames are allowed to transmit during the ATIM window
- If a station is in PS-mode it has to enter into the Awake state prior to the start of each TBTT, i.e. sleeping stations have to come into active mode just before the transmission of the beacon and remain in the active state until the end of the ATIM window.
- If a station receives unicast or multicast ATIM frames during the ATIM window it has to remain in the active state until the end of the next ATIM window.
- If a station transmits a Beacon or ATIM frame it has to remain in the Awake state until the end of the next ATIM window regardless whether it has received an ACK packet for the ATIM frame or not.
- A station can enter into the PS-mode only if it has not transmitted a Beacon neither transmitted nor received an ATIM.

Suitability

IEEE 802.11 *ad hoc mode* is a good technique to implement single-hop, specific-use and duration-limited ad hoc networks because of its extreme simplicity and widespread availability.

Following, an assessment of the IEEE *ad hoc mode* is done, focusing on the different relevant aspects regarding its suitability for the application under study.

For each of the aspects, a numerical integer score is given, ranging from 1 point (the worst) to 5 points (the best), in order to form a *balanced scorecard* with the aggregation of all the analysed techniques' scores. Some aspects' score can be high (close to 5) even if the aspect itself is low; for instance *hardware requirements*, the lower the better.

For detail on the *balanced scorecard* scoring method, check section 4.3.

Functionality: 1 point. IEEE 802.11 *ad hoc mode* is the most basic ad hoc technique. It provides just the essential functions to transmit data between stations without the need of an infrastructure, just the ones needed to form an ad hoc network.

The “pairing” in *ad hoc mode*, based on channel establishment and IBSS parameters (e.g. beacon interval) is both too simple to guarantee the system solution robustness, and too complex to implement simple pairing between devices and more complex functionalities as patient assignment.

Hardware requirements and availability: 5 points. The IEEE 802.11 original standard published in 1997[15] already defined the *ad hoc mode*, and every Wi-Fi certified device since then supports the ability to create and join IBSS.

Currently, the widespread use of IEEE 802.11 cards makes this technology the most avail-

able off-the-shelf technology for ad hoc networks. However, the later standardization efforts concentrated on solutions for infrastructure-based WLANs, while little or no attention was given to the old *ad hoc mode*.

Simplicity: 5 points. IEEE 802.11 *ad hoc mode* is the overall simplest ad hoc technique. The basics to be able to establish a Wi-Fi connection between two or more stations without involving an infrastructure network.

Flexibility: 3 points. The implicit flexibility of *ad hoc mode*, very useful to rapidly set up a direct communication between stations to fulfil a temporary need, would not benefit a definitive solution implementation based on that technique. In that sense, the technique's simplicity and flexibility do not pose an implicit advantage.

Throughput: 5 points. Throughput performance can be relatively high with *ad hoc mode* because of no need for packets to travel through any intermediate access point to go from the sender station to the recipient station⁷. This assuming a relatively small number of users, however. In an scenario with lots of users, better performance would be achieved by using multiple access points to separate users onto non-overlapping channels to reduce medium access contention and collisions.

Previous references[17] assessed, by means of experimental analysis, that less than half of the nominal bandwidth can be really used for data transmission over IEEE *ad hoc mode*, almost reaching the analytically computed figure of 5.120 Mbps with *ad hoc mode* over an 802.11b at a 11 Mbps rate with RTS/CTS mechanisms disabled with large packet size (1024 bytes) configured and 3.337 Mbps with 512 bytes packets and UDP as the transport protocol. That would extrapolate in below 27 Mbps of net throughput for a 54 Mbps data rate.

Implementation: 1 point. Due to its simplicity and scarce functionality, it would be very difficult to implement the solution, the complete system, just using the *ad hoc mode*.

Installation: 3 points. The installation and deployment process of the solution over a large healthcare facility, based on the *ad hoc mode* would be time-consuming. Each node would require specific configuration, assuming it would be possible to implement the system over such a limited technique.

Figure 4.12 shows all the scores given to the *ad hoc mode* technique in a spider-graph. In that kind of graph, the greater the blue surface covered by the features' scores, the more suitable a technique is.

⁷Assuming the packet goes from one STA to another. In our case, packet are originated in a STA and have to reach the AP going through a second station, so net throughput would be reduced by half at least respect the indicated figures, since 2 wireless hops would be needed

IBSS Ad hoc mode suitability	Characteristic's points
Functionality	1
Hardware requirements and availability	5
Simplicity	5
Flexibility	3
Throughput	5
Implementation	1
Installation	3
Total score	23

Table 4.5: IBSS Ad hoc mode suitability points

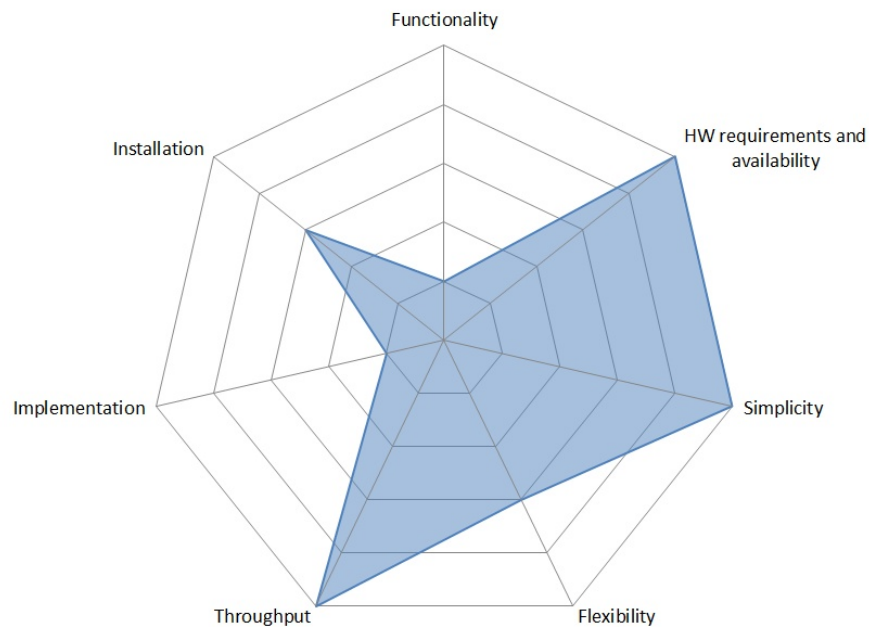


Figure 4.12: Ad hoc mode strengths and weaknesses

In conclusion, the *ad hoc mode* with a total of **23 points** thanks to its **simplicity** and **wide availability**, mostly **applies to smaller, spontaneous networks** when there is not a strong need for interfacing with a wired infrastructure network, that is **not our case**.

4.2.2 TDLS (802.11z)

Tunneled Direct Link Setup (TDLS) is a Wi-Fi Alliance 802.11 standard amendment, named as 802.11z protocol, that uses a specific frame encapsulation to tunnel frames to setup a link directly through an standard AP, in order to establish a TDLS direct link between two stations, as shown in figure 4.13. Hence two or more Wi-Fi TDLS stations can set up direct links providing, in many scenarios, an improved user experience with respect to speed of connection and overall bandwidth efficiency.

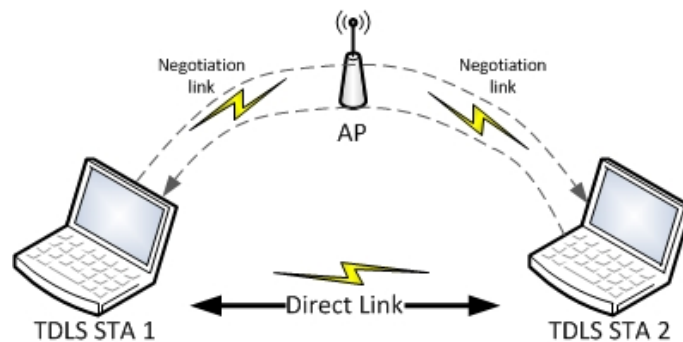


Figure 4.13: TDLS set-up

TDLS is an amendment to the original DLS (Direct Link Setup) protocol, already defined in the first 802.11 standard. DLS was meant to allow direct transmission between stations within a BSS, as in general, STAs are not allowed to transmit frames directly to other STAs in a BSS and should always rely on the AP for the delivery of the frames. However, STAs with QoS facility may transmit frames directly to another STA by setting up such data transfer using DLS.

The need for this protocol was motivated by the fact that the intended recipient may be in PS mode, in which case it can be awakened only by the AP. DLS prohibits the STAs going into PS mode for the duration of the direct stream as long as there is an active Direct Link between the two STAs.

TDLS does not apply in IBSSs, where frames are always sent directly from one STA to another.

The TDLS amendment defines a new DLS mechanism which:

- Does not require access point upgrades (i.e. supports Direct Link operation with non-DLS capable access points).
- Supports power save mode (when associated with either DLS or non-DLS capable access points).

Wi-Fi TDLS devices are able to create a direct link between two stations; improving throughput, reducing latency, and avoiding interference, all of which provide for a superior network performance without any intervention required by the user. TDLS enables improved Wi-Fi performance for uses such as streaming data resulting in improved user satisfaction.

The key benefits of TDLS are:

- Improved network bandwidth, reduced latency and increased network efficiency. With a TDLS link, data does not have to pass through an Access Point.
- Use of special features: TDLS enables two devices to take advantage of performance-enhancing features that may not be available on the infrastructure network.
- Power-saving mechanisms: TDLS enables two devices to take advantage of a power-saving feature that may not be available on the infrastructure network.
- Avoidance of interference: Wi-Fi TDLS devices can connect on a different frequency band than the main network.
- Increased data rate and reduced power consumption for TDLS clients that are operating in relatively close proximity.
- No setup required⁸: A Wi-Fi TDLS connection can be negotiated between devices without user intervention.

Operation details

TDLS is characterized by encapsulating setup frames in Data frames, which allows them to be transmitted through an AP transparently. Therefore, the AP does not need to be direct link capable, nor does it have to support the same set of capabilities that will be used on the direct link between the two TDLS peer STAs[41].

STAs that set up a TDLS direct link remain associated with their BSS, but have the option of transmitting frames directly to the other TDLS peer STA.

TDLS setup

To establish a TDLS direct link, the TDLS initiator STA sends a TDLS Setup Request frame to the intended TDLS responder STA which replies with a TDLS Set Up Response frame.

Upon receipt of a TDLS Setup Request frame, the following options exist at the TDLS responder STA:

- The TDLS responder STA can accept the TDLS Setup Request frame, responding with a TDLS Setup Response frame with status code 0 “Successful”.
- The TDLS responder STA can decline the TDLS Setup Request frame, responding with a TDLS Setup Response frame with status code 37 “Declined”.
- In the case a STA receives a TDLS Setup Request frame just after sending a TDLS Setup

⁸Even if TDLS capable devices are able to automatically create a direct link between them after accessing the same Wi-Fi infrastructure network (BSS), there has to be an upper level triggering to start the direct communication between devices, a goal that justifies the establishment of the direct link, such as a synchronization request coming from a higher layer, from an application or the explicit user command to stream data from one device to another.

Request frame but before receiving the corresponding TDLS Setup Response, TDLS defines two different behaviours depending on the STAs unique MAC addresses: 1) if the source address of the received TDLS Setup Request frame is higher than its own MAC address, the TDLS responder STA discards the received Request and continue with its own initiated TDLS setup. 2) if the the source address of the received TDLS Setup Request frame is lower than its own MAC address, the TDLS responder STA has to terminate the TDLS setup it initiated and accept or decline the received request as in the previous points.

- If a TDLS Setup Request frame is received from a TDLS STA with which currently exists an active TDLS session, then the receiving STA discards the received TDLS Setup Request.

If no TDLS Setup Response frame is received within a specific TDLS response timeout, or if a TDLS Setup Response frame is received declining, the TDLS initiator STA terminates the setup procedure. Otherwise, the TDLS initiator STA sends a TDLS Setup Confirm frame to the TDLS responder STA to confirm the receipt of the TDLS Setup Response frame.

Finally, the TDLS initiator STA sends a TDLS Setup Acknowledgement frame to the TDLS responder STA, completing the 4-step TDLS Setup handshake process.

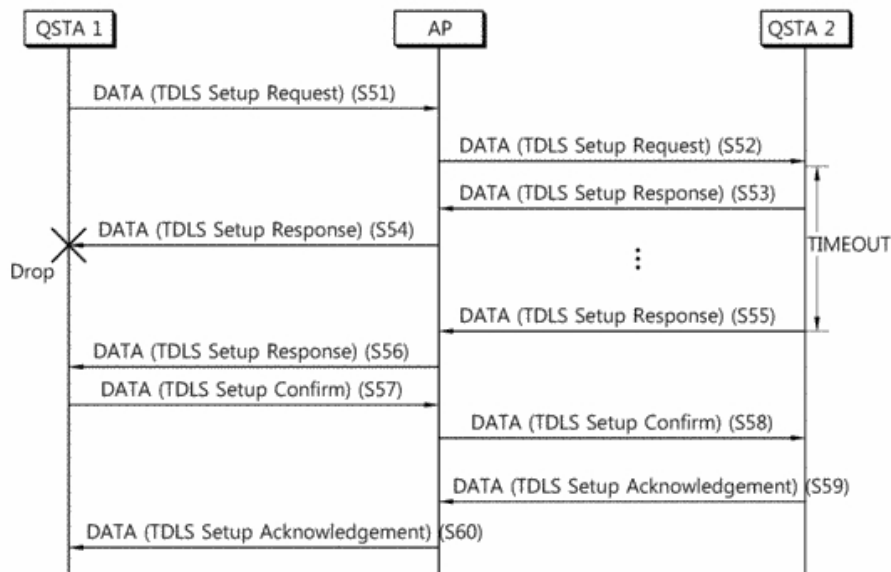


Figure 4.14: TDLS setup

TDLS Setup Request frames, TDLS Setup Response frames, TDLS Setup Confirm frames and TDLS Setup ACK frames have to be transmitted through the AP.

To set up and maintain a direct link, both TDLS peer STAs need to be associated with the same infrastructure BSS.

Further on, the TDLS initiator STA and the TDLS responder STA are TDLS peer STAs. A TDLS peer STA has to accept data frames received from the respective TDLS peer STA directly and Data frames destined for the respective TDLS peer STA may be transmitted over the direct

link.

The frame exchange in a successful TDLS Setup is shown in figure 4.14, including the case of a dropped TDLS Setup Response that does not arrive to the TDLS initiator STA, so no TDLS Setup Confirm is triggered. After a TDLS confirm timeout, the TDLS responder STA retries with a second TDLS Setup Response, which in this case is correctly received and confirmed.

To discover TDLS capable STAs in the same BSS, a STA sends a TDLS Discovery frame to the Broadcast address, through the AP. A TDLS capable STA that receives a TDLS Discovery frame with a matching BSSID in the BSSID element sends a TDLS Discovery Response frame to the requesting STA, via the direct link.

An AP may discard TDLS Setup Request frames to prevent direct links from being set up in its BSS. In this case, the AP sends a TDLS Setup Response frame with status code 4 “Direct links not allowed by the BSS” to the sender of the TDLS Setup Request frame. The AP inserts into the Address field of the TDLS Setup Response frame the TDLS responder STA Address from the TDLS Setup Request frame.

A TDLS Setup Request frame received at a STA that does not support TDLS should be ignored.

Power management in TDLS

TDLS also includes power saving, in the form of two modes, scheduled and unscheduled: TDLS Peer PSM (scheduled) and Peer U-APSD (unscheduled)[41].

TDLS Peer PSM: A power save mode that is based on periodically scheduled service periods, which may be used between two STAs that have established a TDLS direct link.

A station supporting TDLS Peer PSM is capable of acting in both initiator and responder role.

A STA that intends to enter TDLS Peer PSM (the initiator) sends a TDLS Peer PSM Request frame to the TDLS peer STA (the responder), including a proposed periodic Wakeup Schedule.

Then the responder can accept or decline the proposed Wakeup Schedule, with a TDLS Peer PSM Response frame, or even provide a new alternative wakeup schedule, which can be used by the initiator to generate a new TDLS Peer PSM Request frame and start again the process with the new proposed schedule.

Once the initiator and responder have agreed with a successful TDLS Peer PSM Response frame, both have established a periodic wakeup schedule between them. The wakeup schedule remains valid until either the TDLS direct link is ended up; the STAs explicitly update the existing wakeup schedule; or no MPDUs (802.11z protocol frames) containing data have been exchanged for an specific number of consecutive Awake Windows.

A STA transmitting a TDLS Peer PSM Request frame has to remain in the wake state until it received the corresponding TDLS Peer PSM Response frame. A TDLS Peer PSM Request frame may be transmitted via the AP or via the direct link (which is up to the implementer to decide). TDLS Peer PSM Response frames have to be transmitted over the direct path.

To keep track of the connectivity over the direct link and to maintain the wakeup schedule, TDLS peer STAs may start an acknowledged frame exchange periodically.

A TDLS Peer PSM service period is a contiguous period of time during which one or more unicast frames are transmitted between two TDLS peer STAs when at least one STA employs TDLS Peer PSM. A TDLS Peer PSM service period may be initiated during an Awake Window. A TDLS peer STA in power save mode may enter a sleeping state when it has successfully transmitted to and received from the corresponding TDLS peer STA in power save mode.

TDLS Peer U-APSD: A power save mode based on unscheduled service periods that may be used between two STAs that have established a TDLS direct link.

A station supporting this capability, called Peer-Unscheduled or in short “PU”, is capable of buffering frames destined to a PU sleeping STA, and to deliver them during unscheduled service periods.

To operate as the PU Sleep STA in Peer U-APSD, a STA configures its Peer U-APSD capable TDLS peer STA by setting some specific fields inside a TDLS Setup Response frame.

A STA that configured Peer U-APSD enters power save mode on a TDLS direct link after the successful transmission to the TDLS peer STA over the direct link of an acknowledged MPDU with the Power Management field set.

The STA that **transmitted** the frame with the Power Management field set to 1 is then referred to as a *PU sleep STA*. The STA that **received** the frame with the Power Management field set to 1 is referred to as a *PU buffer STA*. A PU sleep STA may be a PU buffer STA at the same time and on the same link.

The power save status on one direct link is independent of the power save status on other links (direct or with the AP) the STA may have.

Since the connection with the BSS-AP has to be maintained, and the sleeping STAs wake up periodically within the legacy Power Save Mode behaviour with the AP, TDLS Peer U-APSD utilizes TDLS Peer Traffic Indication frames sent through the AP: A PU buffer STA transmits a unicast TDLS Peer Traffic Indication frame to a PU sleep STA, through the AP, and the PU sleep STA then initiates a service period with the PU buffer STA to retrieve the buffered traffic. In that way, **the PU buffer STA takes the role of an AP in PSM**, while the PU sleep STA takes the role of the non-AP STA, **in a similar way as the legacy Power Save Mode**, as in subsection 4.2.

TDLS channel switching

TDLS contemplates that STAs switch to another channel, different from the one in which the infrastructure BSS is operating, by exchanging TDLS Channel Switch Request and Response frames over the TDLS direct link, with the aim of operating the direct link in a less occupied channel[41].

If channel switching is supported, the off-channel is determined by the initiator STA at the time of the direct link setup, based on the supported regulatory classes by both peer STAs. The off-channel is included in the TDLS Setup Confirm frame. The Country and Coverage Class on the off-channel are the same as in the BSS to which both peer STAs are currently associated. Both STAs are entitled to request for a channel switch. Each station may make its own determination as to when to switch channels. Prior to switching to the off-channel, the stations have to be in PS mode with the AP. To this end, a STA which receives a TDLS Channel Switch Request may enter PS mode with the AP prior to sending the TDLS Channel Switch Response. Switching

back to the base channel has always to be accepted, because the base channel is the channel at which communications with the AP can take place.

TDLS Teardown

To stop using a direct link, a TDLS peer STA sends a TDLS Teardown frame to the respective TDLS peer STA. A TDLS peer STA sending or receiving a TDLS Teardown frame has to disable the direct link and destroy the related security parameters

Suitability

TDLS is an infrastructure scheme that can be used as a performance enhancer for *ad hoc mode*-like communication when under infrastructure networks, whereas other ad hoc alternatives are essentially ad hoc schemes. The major difference is that TDLS differs from other ad hoc alternatives in that devices are already part of an infrastructure network and associated to an AP. Once TDLS devices are associated with an infrastructure network, the use of the TDLS feature is automatic, with no user intervention⁹ as long as the devices are members of the same BSS. There are other ad hoc alternatives which do not require user intervention, but TDLS has the added feature of device discovery, which enables the devices to operate at the highest level of performance and security common to both devices along with the possibility of two compliant devices to measure the signal strength between them, and determine if a direct link would be better than the traditional BSS Wi-Fi operation transmitting data through the AP.

When devices are part of an infrastructure network, TDLS can be used to advantage with no user intervention required, but still devices would be considered as members of the BSS. That is interesting for example to keep third-party connections (e.g. to the Internet) while benefiting from a direct link with another TDLS devices.

TDLS can be used to benefit ad hoc networks in such a way that the user does not notice that devices are using TDLS instead of other ad hoc networks forming strategies, like the Group Owner initiation in the case of Wi-Fi DirectTM(see subsection 4.2.4) to directly communicate.

Considering the enterprise environment where mechanisms for management and devices identification are interesting to have, TDLS shows a weak point, as the management of TDLS is constrained to turning features “off” and “on” in the enterprise AP.

While *ad hoc mode* networks among other ad hoc alternatives can be instantiated without the presence of an AP, TDLS requires an AP to be present. In addition TDLS has the ability to be disabled, if the AP is so configured, whereas *IBSS ad hoc mode* cannot be disabled. *Ad hoc mode* is also most likely to be a provisory configured capability whereas TDLS can be a transparent technique to be used as long as the candidate devices meet the TDLS requirements.

Functionality: 2 points. TDLS capable devices include “in principle” interesting functions as Device Discovery or Channel Switching. Nevertheless, the TDLS Device Discovery function is aimed just to facilitate the identification of TDLS capable devices inside a BSS

⁹As reviewed before, TDLS does not need explicit user intervention to manage the direct link establishment. Nevertheless an upper layer demand is needed to trigger the direct link formation.

for a TDLS device, including the use of the TDLS discovery procedure to measure the signal strengths from candidate TDLS devices, which can aid in deciding whether to set up a TDLS link or not. Summing up, these are not enough points to consider TDLS the better candidate technique in terms of functionality.

Whereas to form an specific TDLS link setup between two devices there is no user intervention required, these two devices should be already members of the same BSS. Although devices negotiate and establish TDLS links automatically, we consider that TDLS link setup would not suffice for our system pairing procedure considering it to be both too simple to guarantee the system solution robustness, and too complex to implement simple pairing between devices and more complex functionalities as patient assignment.

HW requirements and availability: 1 point. Two client devices that are Wi-Fi Certified™ TDLS can set up a direct connection after linking to the Wi-Fi network, regardless of the technology found in the AP. The two devices will negotiate to operate at the highest level of performance and security common to both devices. Although TDLS links enable devices to perform at the highest level of their shared capabilities, regardless of the capabilities of the AP, Wi-Fi Certified™ TDLS enabled devices are needed to enjoy the TDLS benefits. Moreover to benefit from the Channel Switching function, devices must be dual band capable, this is to be able to maintain two different links at different frequency channels at the same time.

As Wi-Fi Certified™ TDLS chipsets would be needed for the bedside monitors and portable monitors, and this conflicts with the Hardware Requirements presented in section 3.2 regarding the desired compatibility with the current platforms for the Portable and Bed-side Monitors, TDLS gets the minimum score in terms of Hardware Requirements and availability of platforms¹⁰.

Simplicity: 4 points. TDLS is an ad hoc technique focused on avoiding the limitations caused by packets having to go through the AP during transmission between BSS STAs. As simple as this.

Flexibility: 3 points. The Channel Switching functionality is a proof of TDLS technique's flexibility as it would allow to keep channel congestion low in a fully loaded Wi-Fi environment in hospital facilities. But it would require dual band radio chipsets or forcing the use of the 802.11a standard.

Throughput: 4 points. TDLS optimizes performance by establishing a direct link between devices so that they can communicate directly in a more efficient way compared to the typical infrastructure Wi-Fi network (BSS). In a BSS packets that are sent between two devices pass through the AP. The first device will send the packet to the AP and the AP then forwards that packet to the second device. In that typical scheme, data packets are transmitted twice over the medium to deliver just one data packet from one device to another. However, if two devices are within communication range of one another, then a

¹⁰As of June 2010 there were no TDLS devices available. The 23rd August 2012 the Wi-Fi Alliance started its TDLS device certification program and there were only 4 certified TDLS devices, mainly PCI boards and Dual Band chipsets.

direct link can reduce by half the number of packet transmissions. Such links increase the efficiency of the network, especially if the two devices are relatively closer to each other than to the AP. Over 802.11g at 54 Mbps data rate, the maximum net throughput figure of around 28 Mbps could be achieved by the direct link between TDLS devices.

In addition, TDLS also provides support for devices to negotiate an alternative channel, reducing congestion at the original channel. Specifically, if two TDLS-linked devices are dual-band they may choose to dynamically switch to a 40 MHz 802.11n channel in the 5 GHz band. The net result is a **significant improvement in performance, latency and network capacity**.

Implementation: 1 point. Due to its simplicity and limited functionality, it would be very difficult to implement the solution, the complete system, using TDLS devices. On the top of that, it seems a pretty closed/limited standard as it would be difficult to develop additional features over it.

Installation: 2 points. The installation and deployment process of the solution over a large healthcare facility, based on the TDLS technology would require a complex planning guaranteeing AP coverage for both the locations of MP70s and X2s that would be supposed to communicate directly via the TDLS Direct Link. Furthermore it will make necessary to have a total AP coverage all along the facilities, as this technique needs the AP presence to setup every Direct Link.

TDLS 802.11z suitability	Characteristic's points
Functionality	2
Hardware requirements and availability	2
Simplicity	4
Flexibility	3
Throughput	5
Implementation	1
Installation	2
Total score	19

Table 4.6: TDLS 802.11z suitability points

Figure 4.15 shows all the scores given to the 802.11z TDLS technique in a spider-graph. In that kind of graph, the greater the blue surface covered by the features scores, the more suitable a technique is.

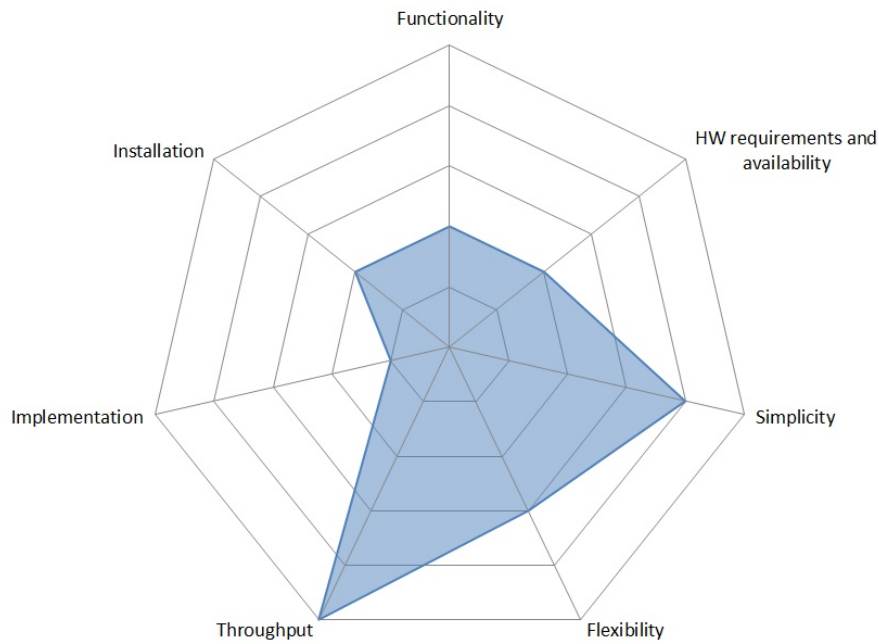


Figure 4.15: TDLS 802.11z strengths and weaknesses

Summing up a total of **just 19 points**, despite TDLS's remarkable simplicity and achieving a theoretical high throughput for a BSS, the 802.11z standard got one of the lowest scores amongst all the reviewed techniques, being automatically discarded because of its **overly strict hardware requirements** meaning as well a low *availability of platforms* together with the practical difficulties to implement a solution over this approach.

4.2.3 Wireless Distribution System (WDS)

A Wireless Distribution System is a configuration that enables the wireless interconnection of access points in an IEEE 802.11 network. It enables the expansion of a wireless network making use of multiple APs without the need for a wired backbone network (the Distribution System) to link them, as is traditionally required. An advantage of WDS over other possible configurations is that it preserves MAC addresses of frames across links between access points, and above all it allows the wireless extension of a network to locations where cabling is not possible or inefficient to deploy.

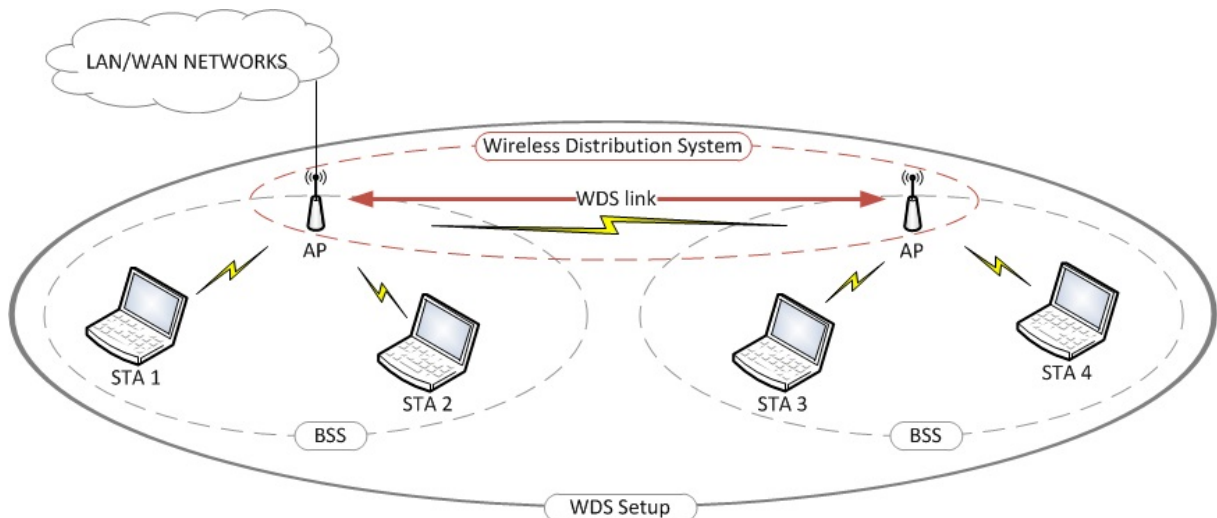


Figure 4.16: *Wireless Distribution System (WDS) setup*

An WDS access point can be either a Master, Relay or Remote WDS AP. A Master WDS AP is typically connected to the wired Ethernet or other LAN/WAN networks. A Relay WDS AP bridges data between the Master WDS AP, other Relay WDS AP, wireless clients and Remote WDS APs. A Remote WDS AP accepts connections from wireless clients and passes them to Relay or Master WDS APs. Connections between “clients” are made using MAC addresses rather than by specifying IP addresses.

All devices in a Wireless Distribution System must be configured to **use the same frequency channel**, same **authentication mode and** identical **encryption level** if used (with same encryption method and keys). WDS also requires every WDS AP to be configured to forward packets. But they can be configured to broadcast different service set identifiers (SSIDs). Another limitation is that the LAN network configuration of all of the WDS APs must be configured to operate in the same LAN network address range. And if DHCP is used, that task should usually be left to the Master WDS AP acting as a DHCP server.

WDS may also be referred to as *repeater mode* because it appears to merely bridge incoming packets, forwarding them to their final destination, nevertheless WDS APs accept wireless clients at the same time, unlike traditional bridging devices. It should be noted, however, that throughput in this method is at least halved (in the best case scenario, after the first hop) for all clients connected wirelessly.

Operation details

In LAN networks the recipient MAC address (Destination) and the sender MAC address (Source) are always included in a data frame transmitted through the network. When sender or recipient stations are located in different segments of the network, a bridging device as a router or AP is needed in between, to “bridge” frames from one segment to the other. In that case an additional third address is used in every frame: the MAC address of the physical interface in the bridging device for each segment, to where the stations direct their frames as a first step.

In wireless LANs transmissions, according to the IEEE 802.11 standard, frames have addressing fields in the header for up to four MAC addresses. These four fields are used when needed depending on the values of the frame control fields “To DS” and “From DS”.

To/From DS Frame Control fields		
To DS	From DS	Meaning
0	0	A data frame direct from one STA to another STA within the same IBSS (ad hoc mode) as well as all MGMT and control frames
0	1	Data frame exiting the DS
1	0	Data frame destined for the DS
1	1	Wireless distribution system (WDS) frame being distributed from one AP to another AP

Table 4.7: *To/From DS Frame Control field value combinations in data type frames*

In a general case of frames transmitted between clients of a wireless LANs (even for *ad hoc* IBSS stations), just three physical addresses are needed: a wireless client associated to an AP always directs its traffic to the AP indicating the AP’s MAC address (1) as its direct destination, and with its own MAC address (2) as “signature” of the sender station. The MAC address of the final destination (3) must be indicated too, in order for the AP to know where it has to relay the frame to.

Meanwhile, in the case of a WDS transmission, involving a sender device, a destination device and at least in each WDS hop two WDS access points, the four-address frame format is required to have fully mapped the original source and final destination of frames and the MACs of the two WDS APs the frames go through.

The IEEE 802.11-1999 standard did not define the WDS capability as a standard function ¹¹ nor how to implement it specifically, just defined the mechanisms needed for WDS operation with the 4-address frame format to allow its operation. As so it remained up to every AP’s manufacturer implementation how to technically solve the equation. That conducted to possible incompatibilities of WDS operation between devices by different vendors or even between APs from different series or product families of the same vendor.

¹¹Clearly indicated at the document “WDS Clarifications” http://www.ieee802.org/1/files/public/802_architecture_group/802-11/4-address-format.doc
Addresses and Frame Control fields tables from the document are reproduced for clarity on the addresses explanations in tables 4.7 and 4.8.

To DS	From DS	Address 1 Receiver Address (RA)	Address 2 Transmitter Address (TA)	Address 3	Address 4
0	0	Destination Address (DA)	Source Address (SA)	BSSID	N/A
0	1	Destination Address (DA)	BSSID	SA	N/A
1	0	BSSID	Source Address (SA)	DA	N/A
1	1	RA (Destination WDS AP)	TA (Source WDS AP)	DA (Destination STA/AP)	SA (Source STA/AP)

Table 4.8: Data frames address fields

In WDS each access point assumes multiple roles with a single physical wireless device. It acts as a coordinator like a normal AP in a standard BSS and as such connects wireless stations to the infrastructure, while it maintains the WDS wireless connections to other WDS APs. To make it possible **the frequency channel of every one of this connections must coincide.**

Roaming stations between access points coverage areas (BSS or cells) that are interconnected by a WDS link work exactly the same as for cells that are interconnected via a wired DS. The effect of a station relocation from one cell to another is that the bridge learn tables will be updated to reflect the new location of the station. This is done by the hand-over request messages that are part of the IAPP (Inter Access Point Protocol) according to the standard.

In figure 4.17 a possible configuration of a WDS extension of a wireless network is achieved fixing the WDS APs and their connecting clients to the same frequency channel, set to channel 6 to avoid channel overlapping with another neighbour cell formed by a traditional (non-WDS) AP working at channel 1.

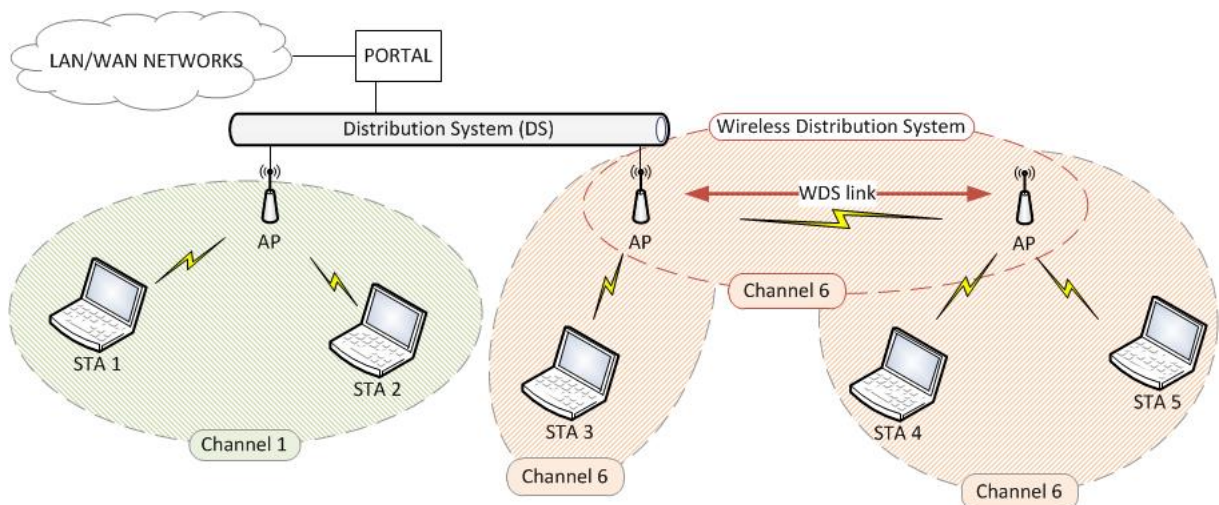


Figure 4.17: Wireless Distribution System (WDS) detail of channel configuration

Possible **topologies** of an WDS network extension include several different configurations, considering the flexibility that WDS offers.

Chain setup The most natural extension of a two-AP setup (shown in figure 4.16) is the chain setup, depicted in figure 4.18. In the left of the figure a wireless client labeled as STA1 connects as a normal STA to a WDS Master AP that at the same time connects the Wireless Distribution System to other LAN/WAN networks. The AP in the center of the image acts as a Relay WDS AP and the access point in the right side acts as a Remote WDS AP. In this setup's example throughput would be reduced up to a third of its nominal value given that the packets must travel up to three times over the air: two relay hops, in addition to the original wireless transmission. In the chain setup all the WDS stations are set to point-to-point connection specifying the MAC address of their couple station.

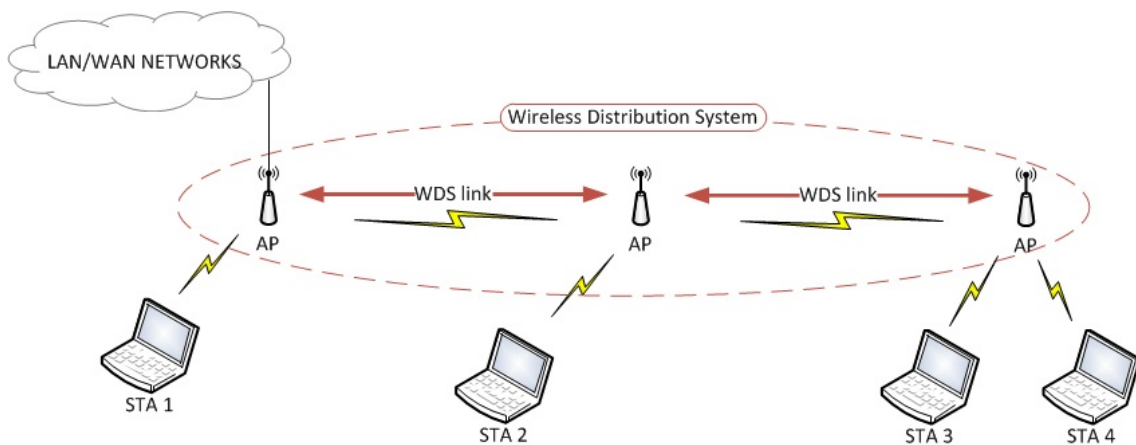


Figure 4.18: *Wireless Distribution System (WDS) chain configuration*

Star setup While the chain setup is useful for covering a long line-shaped area (as a long corridor or street in an outdoor deployment), the star setup allows greater degrees of freedom allowing to cover a wider area without the need of extra hops but adding additional multiple remote WDS APs, as depicted in figure 4.19. In that setup the Master WDS AP is set to point-to-multipoint connection with all the remote APs MAC address in different ports (see footnote, as depending on the vendor the maximum number of different branches on the star setup cango up to 6 Remote WDS APs), while WDS Remote APs are all set to point-to-point connection specifying the same MAC address of the Master WDS AP.

Combination topologies Combinations of chain setup and star setup could be made (as long as maximum number of WDS hops and maximum number of different simultaneous WDS connections are not surpassed) in order to cover a diverse-shaped larger area where it is not practical to deploy a wired DS to connect additional AP. However it must be kept in mind that each additional WDS hop represents the additional CSMA/CA mechanism delays, and the consequent throughput shortening. Spanning Tree Protocol (STP) to prevent loops on the switching routes must be used if there is any chance a loop-like path could be formed within a complex topology.

Regarding the **throughput** reduction inherent to WDS connections, as it could be deduced from the reasons given, in general case the throughput figures would go down to $B_N = \frac{B}{N+1}$

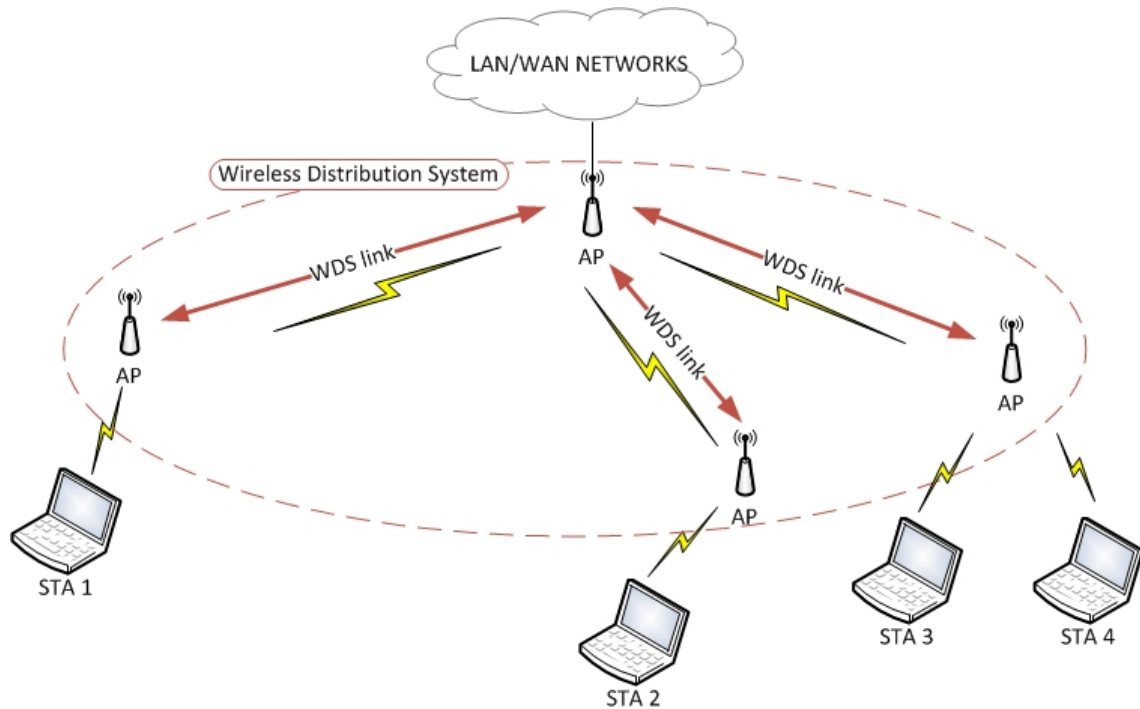


Figure 4.19: *Wireless Distribution System (WDS) star configuration*

where B is the nominal non-WDS throughput, N the number of WDS retransmissions over the air or *hops* (implying $N + 1$ transmissions over the air of the same frame) and B_N the resulting throughput.

According to Access Point manufacturers documentation the maximum number of hops lies between 1 and 2 WDS hops, depending on the specific hardware product.¹²

So for the aforementioned typical values of maximum WDS hops, the throughput reduction $B_{WDS_N} = \frac{B}{N+1}$ could be simplified to the following two cases, for a transmission of a packet from a wireless station to the infrastructure wired network and going across the WDS wireless link:

1 WDS hop throughput $N = 1$ hops, $N + 1 = 2$ radio transmissions $\Rightarrow B_{WDS_N} = \frac{B}{N+1} = \frac{B}{2}$

¹²*Proxima Wireless* with their Orinoco AP-800 series WLAN routers support **up to 6 remote WDS APs** connections in a star setup and **at least 2 hops** in a chain setup, promising an unprecedented throughput of up to 130 Mbps in 1 hop, using a proprietary *WDS-11n* mode (with a nominal non-WDS throughput of 300 Mbps) making use of frame aggregation and 802.11n MIMO with 40 MHz width channels . URL: <http://www.proxim.com/downloads/Technical-Guides/ORiNOCO-AP11n-Software-Management-Guide-SWV4.1.pdf> *Zyxel* APs have a **maximum WDS hop count of just one or two**, depending on the AP model. URL: <http://kb.zyxel.com/KB/searchArticle!gwsViewDetail.action?articleOid=014302&lang=EN> An interesting product on this manufacturer catalogue though are WLAN controllers, rack mounted hardware which allows the remote set-up and configuration of up to 512 APs allowing central management as auto provision for WDS deployments without the need of manually specifying MAC addresses and channels to WDS stations. *Netgear* APs allow a **maximum of two hops**, but with the strict limitation of **not allowing wireless clients** to associate with the WDS stations. In a **single WDS hop** setup *Netgear* APs would allow wireless clients to connect in any case. URL: http://kb.netgear.com/app/answers/detail/a_id/9588

Throughput would be halved compared to using a traditional wired DS. So considering IEEE 802.11g operating at a maximum raw data rate of 54 Mbps, which in practice delivers a maximum net throughput of 27.9 Mbps due to protocols overhead[35], with 1 WDS hop a maximum net throughput of $B_{WDS_1} = 13.95Mbps$ could be obtained.

2 WDS hops throughput $N = 2$ hops, $N + 1 = 3$ radio transmissions $\Rightarrow B_{WDS_1} = \frac{B}{3}$

Throughput would be halved compared to using a traditional wired DS. Using IEEE 802.11g at 54 Mbps with 2 WDS hop a maximum net throughput of $B_{WDS_2} = 9.3Mbps$ could be achieved.

Power management in WDS

Power management in WDS networks does not present any difference with the original standard power management functions in 802.11 networks, as described previously in section 4.2.

Suitability

WDS offers additional flexibility compared to extending a wireless network through wired Distribution Systems keeping the extension costs contained, and as such can be applied in many useful situations (small offices or household networks). However there has to be kept in mind that this suitability assessment regards to whether the WDS approach suits the application under study.

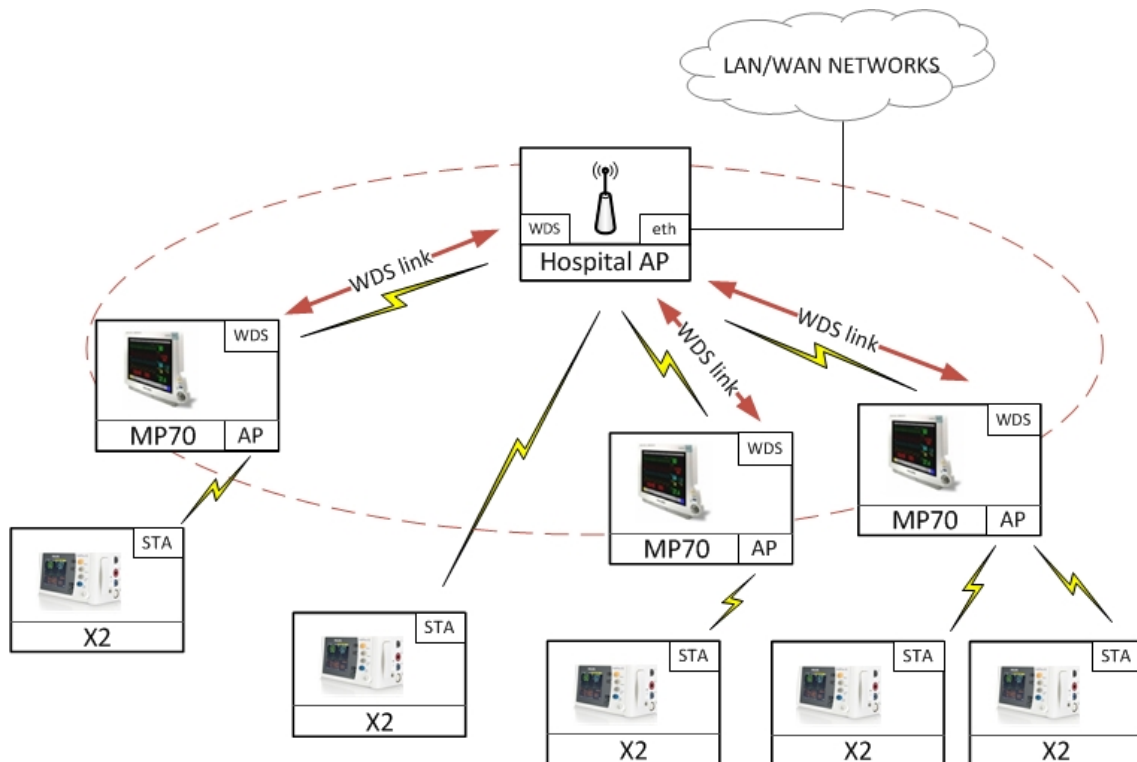


Figure 4.20: *Wireless Distribution System (WDS) applied to the Philips Patient Monitoring system*

Functionality: 1 WDS provides with the same functionality as the 802.11 services the standard defines (legacy AP-STA authentication, association, etcetera) without incorporating any new features other than using the fourth address format in the header frames as mentioned in the operation details section.

Hardware requirements and availability: 3 WDS as a proprietary solution, in that sense it does not require a specific hardware, but depending on the manufacturer implementation of WDS, interoperability issues could arise between devices from different vendors.

Defined by IEEE 802.11 standard, but not certified by Wi-Fi Alliance, some of the platforms on the market support WDS. But some others might not have a firmware implementing it, and still comply with the standard.

Simplicity: 4 One could say WDS is a simple solution, given that it mainly is a Layer 2 bridging on top of a Layer 1 PHY transmission with some constraints. For better and for worse.

Flexibility: 1 Channel must be the same on all the WDS APs connected and their clients. In our case, that would imply that all the MP70's in the coverage range of an Hospital AP should be configured to the same working frequency as the Hospital AP, and the X2s connecting to the MP70s too (see figure 4.20). In that sense hardcoded MAC address represents that WDS clearly is a rigid system, and additional developments would have to be devised in order to adapt it to the more flexible needs of a real system.

Throughput: 3 Half throughput compared to direct link without WDS bridging, in the best case, i.e transmission through just one WDS link (caused because of air retransmission of the packets as discussed in the operation details section). As the coverage area of several access points is larger than the one covered by a single AP, the CSMA/CA functioning could be negatively impacted. Even the classic *hidden node* problem could be found if STAs are found too far away from each other under the coverage of different WDS APs so they cannot detect each others transmissions over the air, leading to too many collisions and retransmissions thus meaning a further reduction of the throughput. Besides, in a long chain topology setup, end-to-end latency issue might be substantial regardless of the inherent throughput reduction with each WDS additional hop.

Implementation: 2 The strict requirement of specifying the MAC addresses of the destination routers hardcoded in every WDS AP's configuration, poses an additional overhead that would make much more difficult the implementation of the solution.

Installation: 1 As with the implementation issues, the hardcoding of MAC addresses represents an important overhead that would make the installation process a difficult or time-consuming task, as every node would require specific configuration.

Figure 4.21 shows all the scores given to the WDS technique in a spider-graph. In that kind of graph, the greater the blue surface covered by the features scores, the more suitable a technique is.

WDS suitability	Characteristic's points
Functionality	1
Hardware requirements and availability	3
Simplicity	4
Flexibility	1
Throughput	3
Implementation	2
Installation	1
Total score	15

Table 4.9: WDS suitability points

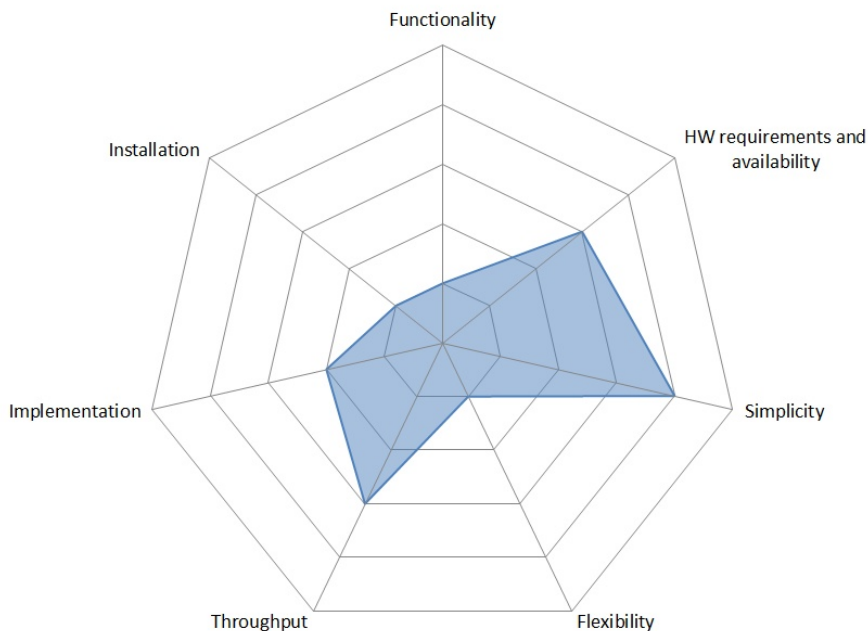


Figure 4.21: WDS strengths and weaknesses

Summing up a total of **only 15 points**, despite its notable simplicity, the WDS technique got **the lowest score** amongst all the techniques assessed, being automatically discarded mainly because of its **low flexibility due to the necessary hardcoding** of stations MAC addresses for its configuration together with an insufficient functionality and availability of pairing functions *per se*.

4.2.4 Wi-Fi Direct™

Wi-Fi Direct™ (hereafter referred to simply as Wi-Fi Direct), formerly known as the Wi-Fi Alliance Peer-to-Peer (P2P) Specification, is a **current interpretation of the original IEEE 802.11 ad hoc mode** with additional functionality and more adapted to nowadays use cases. It provides with improved security and pairing functionality.

The Wi-Fi Direct certification was adopted in October 2010 by the WFA¹³.

By definition, a Wi-Fi Direct device is capable of a peer-to-peer connection, and can support either an infrastructure or a direct connection with another device. Wi-Fi Direct devices have the ability to join infrastructure networks as legacy stations (STAs), and must support Wi-Fi Protected Setup (WPS) enrollee functionality.

Wi-Fi Direct-certified devices (hereafter Wi-Fi Direct devices) can connect to each other on a one-to-one basis, or as a group. Many Wi-Fi Direct devices can also connect with multiple devices at the same time. This group connection is known as one-to-many because one device acts as the gatekeeper to invite other devices and determine whether devices requesting to join the group are allowed. Only devices that receive permission from the gatekeeper (or group owner) device are allowed to connect to other devices in the group.

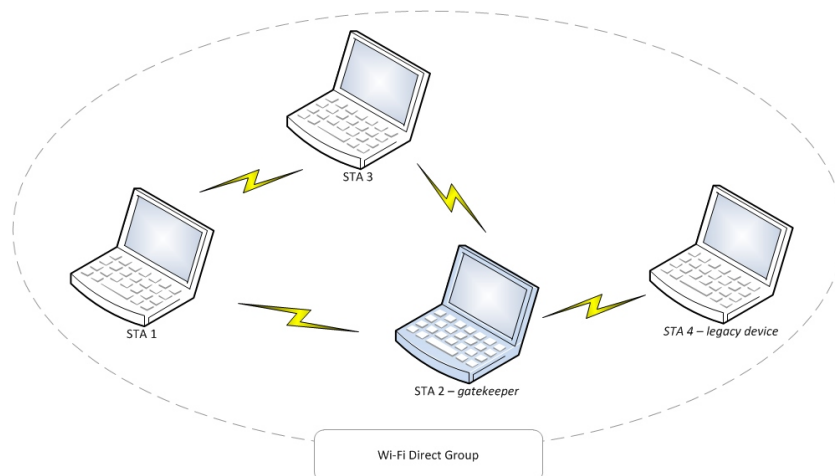


Figure 4.22: *Wi-Fi Direct example setup*

For improved compatibility, a Wi-Fi Direct Group may be comprised of both Wi-Fi Direct devices and legacy devices. Legacy devices can only function as clients within a Group, formed on advance by a compliant Wi-Fi Direct device.

¹³As of June 2010 it was not still available and was expected to be adopted by the end of 2010, expecting the first Wi-Fi Direct™ certified products to be on the market by 2011. In 2014, 45% of all Wi-Fi devices were Wi-Fi Direct certified. Nowadays, for example every Android smartphone since v4.0 includes Wi-Fi Direct connectivity. URL: <http://www.wi-fi.org/discover-wi-fi/wi-fi-direct>

Operation details

Wi-Fi Direct devices connect by forming Groups (in a one-to-one or one-to-many topology) that function similarly to an infrastructure BSS. A single Wi-Fi Direct device is in charge of the Group, including controlling which devices are allowed to join and when the Group is started and terminated. This device, the gatekeeper, appears as an AP to legacy clients, and provides some of the services commonly provided by the AP in a BSS.

Nevertheless, it is worth noting that because Wi-Fi Direct devices do not duplicate the full functionality of infrastructure APs, traditional APs will continue to be the best choice for meeting the needs of stationary, fixed networks in homes, hotspots and enterprises.

In terms of requirements regarding the devices capabilities, all Wi-Fi Direct devices must be capable of being in charge of a Group, and must be able to negotiate which device adopts this role when forming a Group with another Wi-Fi Direct devices. Wi-Fi Direct devices must also support mandatory mechanisms as Device Discovery and Power Management. Wi-Fi Direct devices may support optional features including Managed Device mechanisms and Concurrent infrastructure connections, as shown in table 4.10.

Device Discovery Device Discovery is used to identify other Wi-Fi Direct devices and establish a connection. It is **accomplished using a scan similar to that used to discover infrastructure APs**. Users can select a discovered device for connection. If the target is not already part of a Group, a new Group is formed. If the target is already part of a Group, the searching Wi-Fi Direct device may attempt to join the existing Group. Wi-Fi Protected Setup is used to obtain credentials and authenticate the searching Wi-Fi Direct device.

Service Discovery Service Discovery is an optional feature that enables the advertisement of services supported by higher layer applications (i.e., Bonjour, UPnP, Web Service Discovery) to other Wi-Fi Direct devices. Service Discovery can be performed at any time (e.g. even before a connection is formed) with any other discovered Wi-Fi Direct device.

Group Formation A Group may be created by a single Wi-Fi Direct device. This is required when connecting a legacy device. When a connection between two Wi-Fi Direct devices is established, a Group may be formed automatically; in this case the devices will negotiate to determine which one is in charge of the Group. The device in charge, the gatekeeper, always decides if it is a temporary group (single instance) or persistent group (multiple, recurring use).

After a Group is formed, a Wi-Fi Direct device may invite another Wi-Fi Direct device to join the Group. The optional **Invitation** mechanism can also be used to request that a previously used persistent Group be reformed. The decision of whether or not to accept an invitation is left to the invited Wi-Fi Direct device.

The **Client Discovery** capability makes it easier for users to locate and connect to a specific device or device type, providing a specific service or functionality.

	Mandatory	Optional
Device Discovery: Mechanism to find Wi-Fi Direct devices and exchange device information.	x	
Service Discovery: Mechanism to facilitate discovery of higher-layer services. Can be exercised prior to establishing a Wi-Fi Direct device connection.		x
Group Formation: Mechanism to determine which Wi-Fi Direct device is in charge of the Group. – Invitation: Mechanism that allows a Wi-Fi Direct device to invite another Wi-Fi Direct device to join an existing Group. – Client Discovery: Mechanism enabling a Wi-Fi Direct device to discover which Wi-Fi Direct devices are in an existing Group.	x	x
Power Management – P2P-PS and P2P-WMM-Power Save: Adaptations of legacy Power Save mechanisms that enable additional savings for Wi-Fi Direct devices. – Notice of Absence: Technique enabling a Wi-Fi Direct device that is in charge of a Group to reduce power consumption by communicating a planned absence. – Opportunistic Power Save: Technique enabling Wi-Fi Direct device that is in charge of a group to reduce power consumption by entering a doze state while connected Wi-Fi Direct devices are dozing.	x x x	

Table 4.10: Key mechanisms defined in the Wi-Fi Direct Specification

Power Management Since the efficient use of power is critical for portable devices, Wi-Fi Direct Specification includes power management mechanisms that can reduce power consumption for devices regardless of role within a Group, while maintaining valuable discovery capabilities. While all Wi-Fi Direct devices implement these mechanisms, realization of power savings depends on the settings and interaction between devices in a given environment. Some of the Power Management capabilities are based on standard Wi-Fi Power Save, with adapted mechanisms referred to as P2P-PS. The Specification introduces two new power savings mechanisms to enable a device in charge of a Group to save power:

The **Notice of Absence** mechanism makes it possible to signal a planned absence, either single or periodic.

Opportunistic Power Save allows to the Wi-Fi Direct device in charge of the Group to save power by entering a doze state when all connected Wi-Fi Direct devices are also in a doze state. To maintain Device Discoverability while using Power Management, the Wi-Fi Direct device in charge of the Group is available on a periodic basis. Searching devices are aware that Power Save mechanisms may be in use. Power management mechanisms are available only for use in Groups in which only Wi-Fi Direct devices are associated. If legacy devices are present, these power management functions cannot be employed. These mechanisms can be used together to maximize doze time, a particularly important capability since in many cases Wi-Fi Direct devices are battery-operated.

When initially forming a Group, a Wi-Fi Direct-certified device will signal to other devices in the area that it can make a connection. The user can view available devices and ask them to connect. In some cases, the user might receive an invitation to connect to another Wi-Fi Direct certified device and then decide whether to accept the invitation or not. Depending on the device the action required to do so may be to push a connection button on the device, accept a pop-up window request, or for example “tap-to-connect” using NFC.

Wi-Fi Direct devices establish a connection independently from the network and from current network conditions and use social channels (channels 1, 6 and 11 in the 2.4 GHz band) to locate other devices to which they can connect, and then select an operating channel.

Once a connection is confirmed using Wi-Fi Protected Setup, the devices make a secure connection to help protect their communication. This secure connection is completed by industry-standard WPA2 security. Once two or more Wi-Fi Direct devices connect directly, they have formed a Wi-Fi Direct Group.

In 2014, Wi-Fi Alliance introduced several enhancements to Wi-Fi Direct to add support for pre-defined services designed to improve user experience and accelerate developer innovation, including:

- **Wi-Fi Direct Send Service**, to facilitate file sharing among devices. It enables a file browser application to find devices that support the Send service before creating a connection.
- **Wi-Fi Direct Print Service**, to print documents with a single command. Based on

Internet Printing Protocol (IPP) 2.0, enables model-independent printing with a common driver and allows users to discover and print directly to Wi-Fi Direct printers without the need for drivers or needing to join a network. In an office environment, the Print service makes it easier for corporate IT to maintain security, since a visitor can connect directly to a printer, instead of going through the office network.

- **Wi-Fi Direct for DLNA, Play Service**, enables users to have a control interface to play encoded media to/from other devices. An advantage of implementing the Play service is that it enables connectivity to most existing devices by supporting DLNA standard, for a better interoperability enabling devices to discover each other before connecting for streaming.
- **Miracast integration, Display Service**, to implement the updated device and service discovery mechanisms of Wi-Fi Direct to enable screen mirroring and display in a single step, offering an instant, low-latency control interface to other devices.

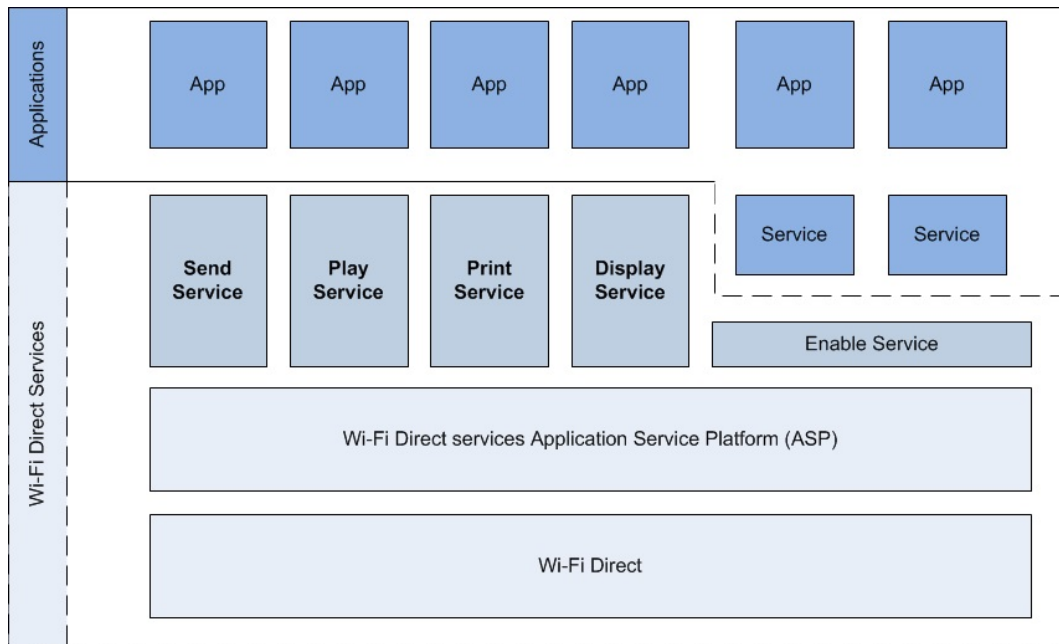


Figure 4.23: *Wi-Fi Direct services architecture*

The enhancements added to the specification define an application service platform (ASP) and 4 industry-standard services that allow users to share files, stream media, and print documents, no matter what vendor made the device, phone, display, printer, or any other device. In addition, an API enables developers to build applications that take advantage of P2P connections. That latter point must be remarked, as a limiting fact about Wi-Fi Direct is that it relies in upper layer applications for the end-user to benefit from the direct connections between devices.

The ASP provides:

- Pre connection service advertisement and discovery.

- A standardized approach for users to initiate device-to-device connections.
- Automatic connection re-use to efficiently support multiple, simultaneous services (user tasks).
- Management of the underlying connectivity methodology, alleviating the service implementer from needing to understand or manage those functions for each service.

The Wi-Fi Direct API reduces the complexity of building an application for Wi-Fi Direct devices by abstracting the details of the underlying technology. In addition, developers can extend functionality without waiting for Wi-Fi Direct services updates. Internal development groups and third-party developers can create new services on top of the Application Service Platform, while still maintaining interoperability with other devices. Each application or service created using the Enable interface interacts with the ASP to advertise itself, manage ASP sessions, and manage listening network ports associated with ASP sessions. There can be several Enable applications active at a time and an application can have simultaneous Wi-Fi Direct advertisements and sessions.

Advanced functions Optional advanced functions are up to each vendor to be implemented in their Wi-Fi Direct devices, and relate to the ability to withstand simultaneous connections and re-instantiate them.

Persistent Groups allows a previously established Group to be re-invoked at a future time without the need of re-provisioning again from scratch.

Concurrent Connection allows to maintain multiple connections simultaneously. Connections can be to Groups and/or legacy AP.

Multiple Groups: if implemented, a Wi-Fi Direct Device is able to maintain membership in multiple Groups simultaneously.

Cross-connection: Allows the Wi-Fi Direct device in charge of a Group to provide infrastructure access to other devices in the Group.

Managed environments Operation in managed Wi-Fi environments (e.g. enterprise, hotspots, etc.) was an important consideration in the creation of the Wi-Fi Direct Specification. To promote efficient use of wireless bandwidth, Wi-Fi Direct devices do not use 802.11b rates (1, 2, 5.5, or 11 Mbps) for data or management frames (restricting Probe Request frames sent to both Wi-Fi Direct devices and Legacy Devices), neither respond to requests indicating support only for 802.11b rates. This decreases the air time consumed by signaling between Wi-Fi Direct devices.

A WLAN AP may implement capabilities that allow it to manage Wi-Fi Direct devices, enabling robust protection and isolation of the enterprise infrastructure network. A WLAN AP with this capability may deauthenticate any Wi-Fi Direct device from the infrastructure network for out-of-policy behavior and communicate the reason for that action. For example, in an environment

where controlled access to infrastructure network resources requires each device to authenticate, a Wi-Fi Direct enabled WLAN AP may communicate to all client devices that Cross-connection is not allowed. All Wi-Fi Direct devices are required to comply with this policy.

Suitability

The direct substitute and evolution of *ad hoc mode* is nowadays much more suitable for any elaborate implementation than its predecessor. In the same way, although TDLS forms a direct link between two client devices, TDLS is not the same as, nor does it replace Wi-Fi Direct: TDLS operates in the background of a Wi-Fi network to optimize performance, while Wi-Fi Direct-certified devices can quickly connect to one another without the need of any infrastructure centralized device or network connection.

Considering the enterprise environment where network control and devices identification are interesting to have, the *peer-to-peer* Wi-Fi Direct specification does include mechanisms for management, and devices identify themselves to a “Wi-Fi Direct aware AP” and by this means can allow to be managed.

For all the aspects considered, as we detail in the next points following our suitability assessment methodology, the Wi-Fi Direct approach would be the first choice for implementing the solution, if it was not for its unavailability¹⁴.

Functionality: 5 Sporting a whole set of inherent useful functions, Wi-Fi Direct is one of the most functional alternatives reviewed¹⁵. Combining advanced functions, like Persisting Groups, and Cross-connection, Wi-Fi Direct would be a good alternative over which

Hardware requirements and availability: 1 No special hardware would be needed for having a Wi-Fi Direct communication between devices *per se*, **provided that at least one of the devices was a Wi-Fi Certified device**. In our case, the Wi-Fi Direct device would have to be at least the MP70 bedside monitor.

The penetration of Wi-Fi Direct has grown rapidly from the launch of the certification program **in 2010, when there were no available devices yet**. According to ABI Research¹⁶, more than 2.4 billion Wi-Fi Direct devices shipped already in 2014, making up forty-five percent of all Wi-Fi devices. This percentage was expected to increase to eighty-three percent by 2019 as the technology is adopted across a wide variety of markets, including consumer, mobile, automotive, and emerging markets.

Simplicity: 3 Wi-Fi Direct can be considered relatively simple as the *ad hoc* mode but more complex than its predecessor, taking into account the additional features and mechanisms brought by this evolution of the classical *ad hoc* connection.

Flexibility: 4 Wi-Fi Direct breaks several constraints compared with other alternative ap-

¹⁴As of 2010 when the study was carried out.

¹⁵Although some of the most interesting functions were introduced as recently as in 2014.

¹⁶Reports at <http://www.wi-fi.org/discover-wi-fi/wi-fi-direct>

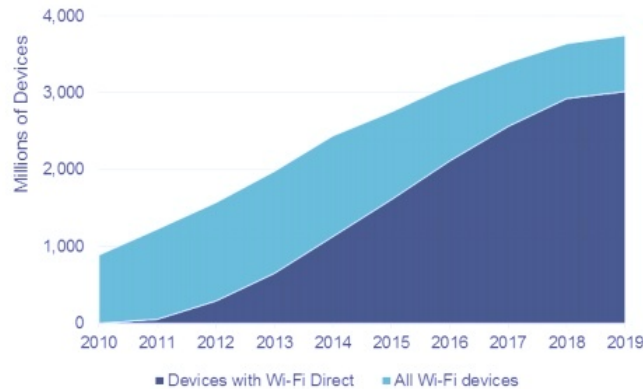


Figure 4.24: *Global Wi-Fi Direct devices distributed (2014, ABI Research)*

proaches, in terms of backwards compatibility with legacy STAs, and incorporated functions that address the identified issues with pairing and device discovery, allowing a more flexible implementation.

Besides, the additional functions introduced in 2014 in the specification, specially the advanced ones related with group management, offer flexibility in the form of belonging to multiple groups at the same time, and the ability of reconnection to previously established connections, allowing the implementation to focus on another issues.

Also the pre-defined services allow easier integration with the application layer. With a connection framework that is distinct from the applications themselves, Wi-Fi Direct offers developers a flexible way to implement designs. The P2P connection can be managed by the application level, a management function, or even the operating system. In addition, this flexible approach avoids forcing a connection to be dedicated to a single task (which would prevent it from being used by other applications).

Throughput: 5 As in TDLS, Wi-Fi Direct optimises performance by establishing a direct link between devices so that they can communicate directly in a more efficient way compared to the typical infrastructure Wi-Fi network, in which packets must be sent through the AP to go from one device to another.

The advertised “speed” of Wi-Fi Direct Certified devices is up to 250 Mbps¹⁷, but of course the net throughput attained between a particular couple of Wi-Fi Direct devices depends on the specification used 802.11a, g, or n, as well as the particular characteristics of the devices and the state of the physical environment (congestion, radio interference, etcetera).

Implementation: 4 If the Wi-Fi Direct approach was selected, the implementation of a complete solution addressing the target problematic would be relatively easy to face, considering the good alignment between this technique’s functionality and the required one, the flexibility and the expected throughput make it a

¹⁷URL: <http://www.wi-fi.org/knowledge-center/faq/how-fast-is-wi-fi-direct>

Installation: 4 With such a flexible approach, installation and deployment in the hospital facilities would not present remarkable obstacles or difficulties. It would be relatively easy to deploy a solution based on Wi-Fi Direct.

Wi-Fi Direct™ suitability	Characteristic's points
Functionality	5
Hardware requirements and availability	1
Simplicity	3
Flexibility	4
Throughput	5
Implementation	4
Installation	4
Total score	26

Table 4.11: *Wi-Fi Direct™ suitability points*

Figure 4.25 shows all the scores given to the Wi-Fi Direct™ technique in a spider-graph. In that kind of graph, the greater the blue surface covered by the features scores, the more suitable a technique is.

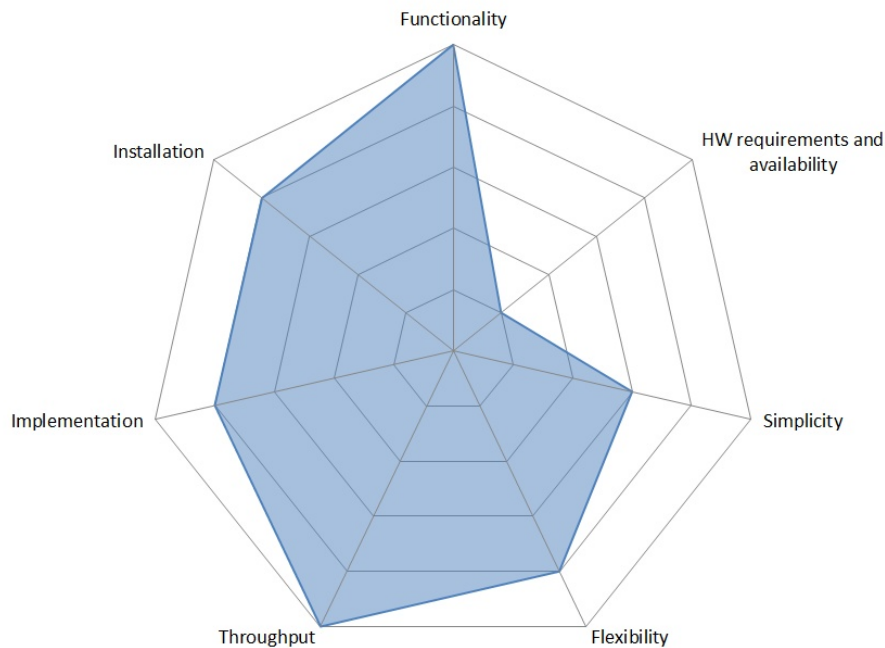


Figure 4.25: *Wi-Fi Direct strengths and weaknesses*

Summing up a total of **26 points**, Wi-Fi Direct feature **outstanding throughput and functionality**. However, despite its remarkable score, the **unavailability of hardware supporting**

Wi-Fi Direct operation by the time this assessment was carried out, discarded automatically the selection of this technique for implementing the solution to our problematic.

4.2.5 Mesh networking (802.11s)

In general term, a mesh network is the one in which each node is directly connected with others to form a mesh structure. When all nodes are connected together, it is said that the network is fully meshed. Otherwise it is said that the network is partially meshed. Mesh networks are formed of two main types of nodes: regular mesh nodes (or MSTAs, Mesh STAs, clients with mesh connectivity) and mesh routers with additional functions (MAPs, Mesh Access Points, and MPPs, Mesh Portals which connect the mesh network with other networks). The backbone consists of mesh router nodes which are responsible of forwarding packets inside the network and towards its destination, comparable to the Distribution System in a IEEE 802.11 ESS. While the access network, normally disposed at the borders of the backbone, is in charge of providing network access to both conventional legacy clients and mesh clients.

Mesh routing protocols are in charge of automatically determine the best route for every moment and reconfigure the network dynamically in case of an event affecting its topology, as when a link becomes inactive.

Some of the **main features** of mesh networks are the following:

Dinamic topology: The mesh nodes can be mobile and autonomous. For these reasons, the network topology may be different every time.

Multihop: One of the most important characteristics of a mesh network is the multihop capability. Thanks to the routing protocols that are used, a node can communicate with another that is outside its range of coverage through other nodes which act as intermediate nodes.

Multipoint-to-multipoint: Each node of the wireless network can communicate with any other node in a multipoint-to-multipoint configuration. Wireless networks using this configuration must have links with high capacity. Even with this configuration the problem of concurrent access to the shared medium still occurs.

Autoconfiguration, self-healing, and self-formation: These networks have a flexible infrastructure, easy deployment and configuration, and the ability to deploy the network as it is needed.

Dependency on power consumption depending on the nodes: Thanks to the low mobility of mesh routers, they have no problems with power consumption as they can be powered continuously. Instead, clients with high mobility need to consume minimal power to achieve the greatest possible autonomy time.

Compatibility and interoperability with existing wireless networks: Mesh networks are usually based on the IEEE 802.11 technology or proprietary technologies and can work with networks using other technologies such as WiMAX or ZigBee.

Regarding the possible **network topologies**, depending on nodes functionality (if they are mesh routers or mesh clients) and their disposition we can distinguish three types of mesh

networks[28]:

Mesh backbone network: the most used one, in which mesh routers form an infrastructure and clients connect to the mesh routers in the borders of the backbone which act as gateways. See figure 4.26.

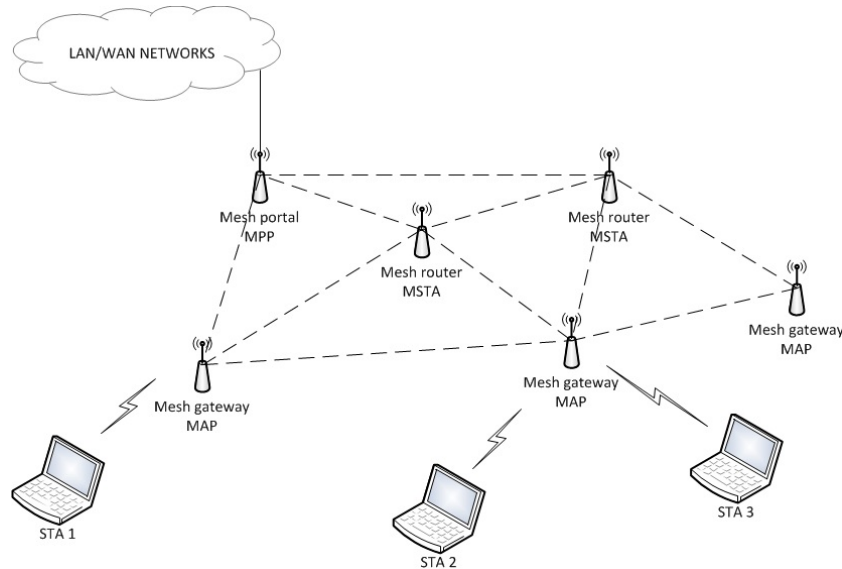


Figure 4.26: Mesh backbone example setup

Mesh clients network: This type of configuration provides peer-to-peer connections between mesh client devices. In this architecture, the network is constituted by client nodes provided with both functionalities for routing and auto-configuration. In the figure 4.27 we can see an example setup of these networks. The mesh client network uses only one common wireless access technology. When a message is transmitted to a remote node, it can travel through different mesh nodes until reaching its destination.

Hybrid mesh network: This architecture combines the previous two architectures. We can observe a typical scheme of a hybrid mesh network in fig. Mesh clients can access the network via mesh routers and they can also do so from other mesh clients. Coverage within the mesh network is available through the routing capabilities of every node. Illustrated in figure 4.28.

In terms of the **number of available radios** in every mesh device, we can distinguish between:

Single-radio wireless mesh devices: With this configuration all nodes work as access points. Each mesh node supports its local clients while sending traffic to other mesh nodes, all over the same radio interface, ie, a single radio is used for client access and for communication between nodes (backhaul traffic).

The main problem is that the flow is shared between access and backhaul traffic. With this configuration, the capacity is reduced since interference between transmissions of different access points to the same channel used throughout the network occur. As a

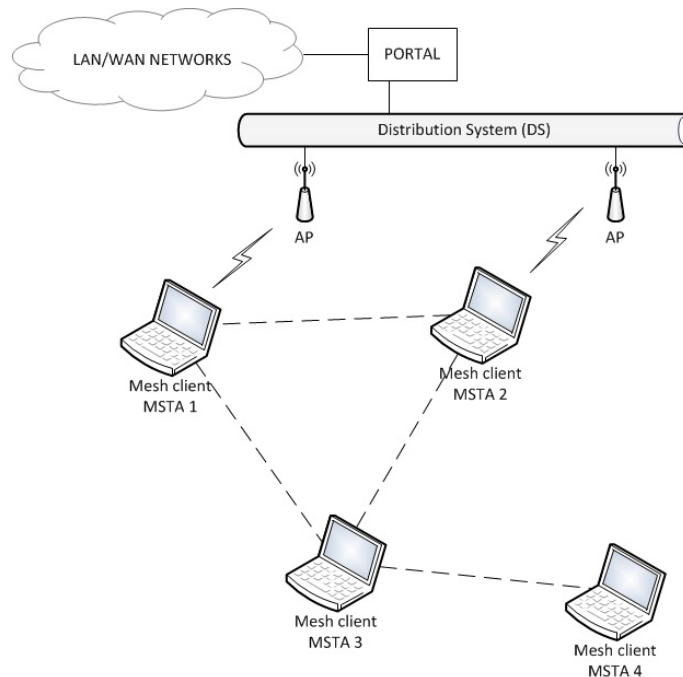


Figure 4.27: Mesh clients network example setup

result unpredictable delays could be introduced in the system as it grows the number of hops that a packet has to jump to go from one end of the network to the other.

Dual-radio wireless mesh devices: In this configuration, each mesh node has two wireless radio interfaces. One of them is used to give access to clients and the other for backhaul traffic exclusively. Each radio works on a different frequency channel. In a possible configuration, the interface used for client access works at 2.4 GHz (different channels for adjacent APs) and the other interface for backhaul at 5 GHz (the same channel on all APs). The main problem with this setup is that it cannot perform simultaneous operations of sending backhaul traffic. This results in a reduction in the backhaul system capacity.

A generalization of that last one configuration would be the *multi-radio wireless mesh* in order to totally separate client access traffic from backhaul, with the cost of an important increase in complexity, power consumption and management overhead.

As mentioned before, **routing protocols** are a basic piece of mesh networks. Routing protocols are responsible for determining how and how often mesh nodes have to send each other information to find different paths to possible destinations in their network.

The main objectives of any routing protocol are the following:

Minimum control overhead: Control messages consume bandwidth, processing resources and power. For these reasons, it is very important that a routing protocol does not transmit excessive control messages to monitor the network.

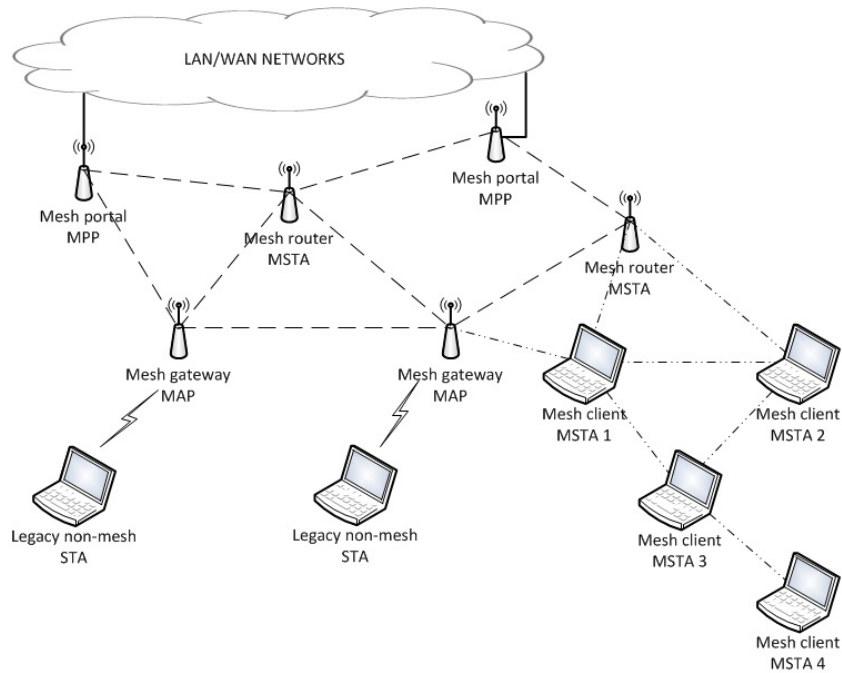


Figure 4.28: Mesh hybrid network example setup

Minimal processing overhead: If processing algorithms are computationally complex, this implies a high power consumption. This would be something to avoid in terms of power saving, in any network.

Ability to multi hop routing: A protocol should be able to find multihop routes between two nodes when the destination and source node are more than just a hop away.

Maintaining dynamic topology: As nodes can have a certain degree of mobility, it is very likely that the network topology is constantly changing. Route changes for this reason should be quickly recalculated associated with minimal overhead.

Loop prevention: A loop occurs when a message passes through a node that has already been used to send that message before. It is fundamental to address this problem quickly when it occurs because it consumes bandwidth unnecessarily and can cause severe congestion problems or even collapse.

The use of IP level routing in a mesh network is a real benefit to give a level of consistency to multihop networks. Typically, routers are the main nodes and may be assigned multiple IPs in their different interfaces. A layer two protocol can set point-to-point communications between adjacent nodes while a layer three protocol can route data to a distant node through intermediate nodes performing end to end communication.

Following, some of the most used routing protocols and their categorization are presented:

Proactive routing protocols: Derived from the vector protocols based on distance, take into account the state of the link (distance vector and link state protocols). The main feature

of these protocols is that each node maintains a route to each other node in the network at all times. Through small transmissions of information, node status routes are exchanged from time to time to keep updated routing table in every node.

The main advantage is that each node has all routes to all nodes available when needed. However, one disadvantage of these protocols is the high number of control messages flowing through the network in order to have the correct network topology at all times. This problem is exacerbated the larger the network is, or the more the nodes move within it. The use of proactive protocols in networks where a significant number of data sessions of short duration within the network is quite interesting. In this situation, the overhead is justified because all those routes are expected to be used.

There are several proactive protocols among which we highlight the Destination-Sequenced Distance Vector Routing (DSDV), the Topology Dissemination Based on Book-Path Forwarding (TBRPF), and the Optimized Link State Routing Protocol (OLSR).

Reactive routing protocols: Reactive routing techniques are also called *on demand* routing techniques. With these protocols, overhead messages to maintain routes are lower. Routes are discovered only when necessary for transmission.

The advantage of proactive protocols is that when a route is needed it is already available. This is an important advantage in wired networks as well as for networks with low mobility. As the protocol keeps maintained all active routes it can produce a high number of control messages with the consequent high cost for the network. For this reason, reactive protocols do not keep at all times a route between all pairs of nodes.

The main advantage of these protocols, as mentioned earlier, is the smaller number of control messages generated. The most important drawback, is the time it takes for a node to discover a route, called acquisition latency.

Some of these protocols are Ad Hoc On-Demand Distance Vector Routing (AODV) and Dynamic MANET On-demand (DYMO), but others are also important as the Dynamic Source Routing (DSR), the temporally Ordered Routing Algorithm (TORA).

Hybrid routing protocols: There are protocols that combine the characteristics of proactive and reactive protocols. These protocols divide the network into zones and serve as a proactive protocol within those areas, and then as reactive ones to perform routing between different areas. These protocols are interesting to be used when the network is large. Some hybrid protocols are the Zone Routing Protocol (ZRP) and the Distance Routing Effect Algorithm.

Geographic routing protocols: These protocols are based on proactive and reactive techniques but specifically incorporate geographic information to help with the routing maintenance. This information may be GPS data collected by every node such as geographical coordinates, or may be obtained through a fixed coordinate system with reference points and relative position between nodes. The use of location information may reduce overhead control messages generated in the network. An example of geographic protocol is the

Location-Aided Routing (LAR) protocol.

Operation details

The IEEE 802.11s amendment defines mesh extensions to IEEE Std 802.11-2007, enabling new applications of Wi-Fi technology to mesh networks, including automatic topology learning and dynamic configuration of routes to different destinations. Specifically the amendment takes advantage of the MAC and physical layers of IEEE 802.11 over mesh networks to create a distribution system that supports wireless unicast, multicast, and broadcast communications through the mesh.

With this specification, each mesh node can relay messages on behalf of any other node on the network. The mesh configurations allow a complete network auto-configuration and increased available bandwidth the more the nodes in the network are. 802.11s was designed to support scenarios over mesh networks in environments such as college campuses, businesses or offices. Additionally, it also defines military and emergency communications scenarios; i.e. different applications where to benefit from its flexibility and adaptability.

A possible implementation of a mesh system architecture, shown in figure 4.29 could be the following[39]:

- This architecture is based on a **standard 802.11 network interface card** (NIC) for basic transmission functionality, as beaconing and frame acknowledging, which are time critical.
- On top of it, the **802.11 driver** for the NIC accommodates the mesh modules, additionally to the standard wireless driver modules, for extended mesh functionality: the *mesh manager* and *mesh data forwarder*.
 - The **mesh manager** is responsible for establishing and maintaining links with neighbouring mesh stations. It records the associated MSTAs in the mesh neighbour table and removes an entry from the table if it does not receive a beacon from that MSTA for a certain period.
 - When receiving data, the receiving handler (RX handler) sends mesh data frames to the **mesh data forwarder**. The mesh data forwarder validates the connection status of the transmitter in the mesh neighbour table. Then, if the frame still needs to be relayed in the mesh, it sends the frame to the transmission handler (TX handler). If the own node is the final destination of the packet or the node is a mesh AP or a mesh portal that bridges frames to their destination on a external network, the data frame is sent to the upper layer of the protocol stack.
- On top of everything, mesh APs and mesh portals count on a link-layer bridge module, called **Ethernet Bridge**, which processes the remaining task of bridging traffic between different interfaces (to legacy STAs, wired 802 LANs, or any other network connected).

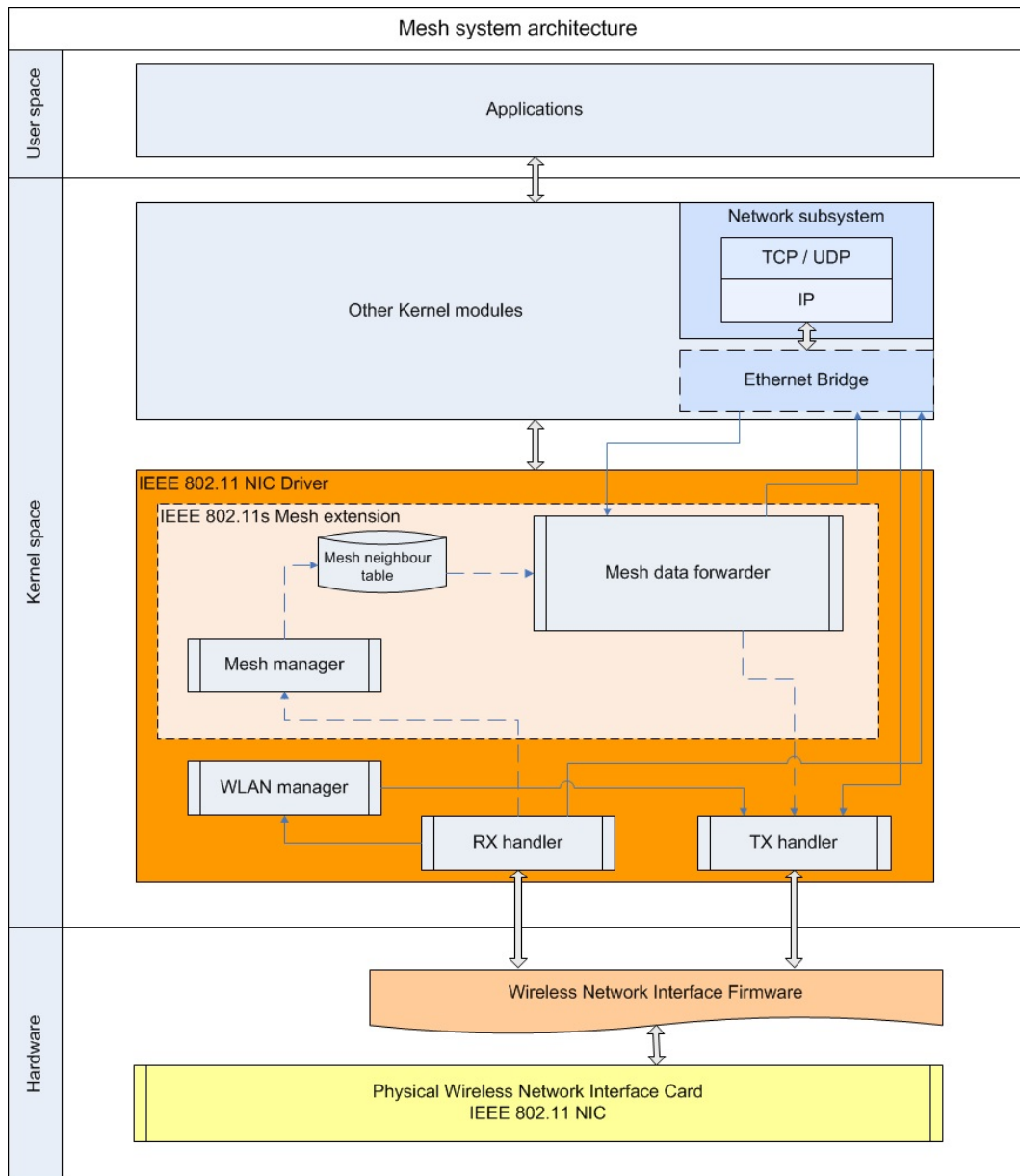


Figure 4.29: Mesh system architecture

While four-address frames are originally supported by the IEEE 802.11 standard for WDS transmissions, as shown in 4.8, in order to support non-mesh stations in 802.11s six-address frames are needed. The two additional addresses are the Mesh Source Address and the Mesh Destination Address:

SA: Source Address MAC of the node which generated the original frame

DA: Destination Address MAC of the final destination of the frame

TA: Transmitter Address MAC of the node which transmitted the frame. Can be the same

as the SA, or any Mesh STA forwarding the frame on behalf of the original source

RA: Receiver Address MAC of the node which receives the frame. MAC of the immediate next hop

Mesh SA: Mesh Source Address MAC of the node which inserted the frame in the mesh network on behalf of the original source

Mesh DA: Mesh Destination Address MAC of the last node in the mesh network which will handle the frame

Suitability

The adoption of wireless mesh networks is interesting for a great number of applications which can benefit from its high flexibility and high grade of functionality.

Nevertheless mesh networks imply additional issues introduced by its particular topology. Furthermore, some applications do not benefit as much as others from the characteristics of mesh connections.

For example, when thinking already in the application of WMN to our case, there is not a justified need for multihopping functionality between nodes, neither dynamic routing, in our given scenario. This would not directly discard the mesh technique as it is more an excess of functionality than a defect regarding the given necessities. But it would introduce additional complexity to the network, as it is shown in figure 4.30, where a possible mesh setup is applied to the Philips Patient Monitoring system.

In that figure, the hospital APs are standard legacy APs (as we cannot assume that the hospital would change all their existing AP devices deployed all along the facilities). MP70 bedside monitors are mesh stations, MSTAs, able to interconnect between them in a mesh fashion, and at the same time act as APs to the X2 portable monitors which in this case would be legacy STAs. In that setup, an X2 willing to connect to the network to forward patient data would be able to connect to any MP70 in its vicinity, as being a mesh station it would forward the data to the adequate MP70. Nevertheless, the patient assignment process would not be assimilated with the wireless connection, as the patient data information flow would not correspond with the physical wireless link (which could go hopping through different several nodes).

Following, the suitability of IEEE 802.11s mesh specification is assessed in the several relevant aspects.

Functionality: 4 High grade of functionality for overcoming the issues raised by the use of mesh topologies. No need for multihop functionality, neither dynamic routing, in the given scenario, however, do not justify the use of mesh networking in our case.

Hardware requirements and availability: 2 It was expected that Wi-Fi product implementations would commonly include mesh functionality in both AP and station devices.

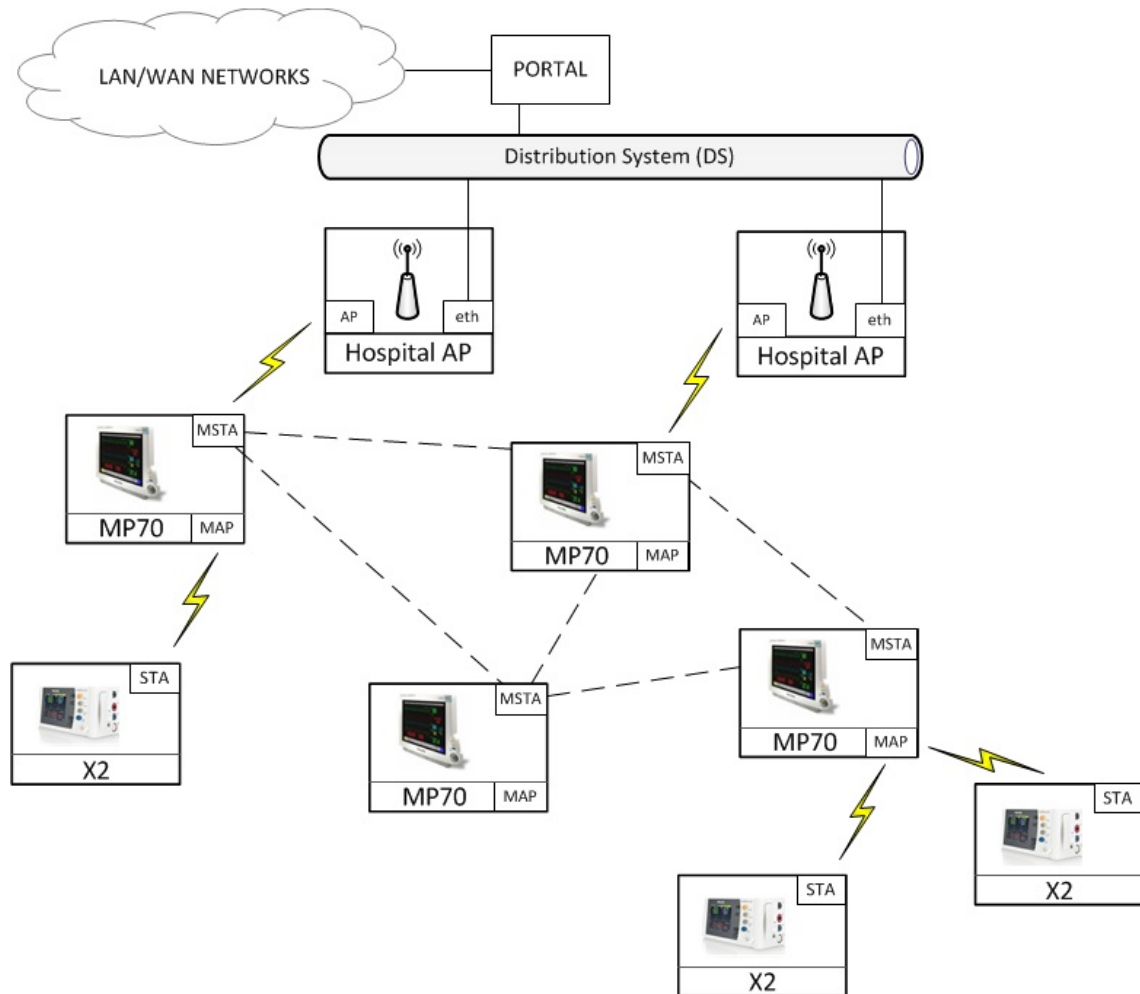


Figure 4.30: IEEE 802.11s mesh approach applied to the Philips Patient Monitoring system

Nowadays normally only professional-grade products, like outdoor wireless mesh routers and industrial wireless equipment¹⁸, are designed specifically for mesh networking.

Simplicity: 2 Mesh nodes are more complex than standard 802.11 Wi-Fi devices in general, and the mesh topology introduces additional complexity, because of the additional freedom degrees it provides.

Flexibility: 5 The most flexible technique as it would adapt to any nodes disposition and topology. Autoconfiguration, self-healing, and self-formation functionalities are a clear expression of the mesh networks' flexibility.

Throughput: 3 Although optimal route dynamic on a multihop configuration would reduce the number of hops needed to deliver the patient information to the final destination in the hospital network, the use of mesh technique would reduce considerably the final

¹⁸Aruba Networks, Cisco, and OpenMesh professional products include mesh functionality, generally for extending coverage on outdoor facilities, to points where it is not possible to deploy wired standard APs

throughput compared to one-hop wireless communication. As seen in depth analysis for the WDS technique in the corresponding section 4.2.3, the throughput would be in the best case halved. That is considering $N = 1$ hops, $N + 1 = 2$ radio transmissions $\Rightarrow B_{mesh_N} = \frac{B}{N+1} = \frac{B}{2}$

So considering IEEE 802.11g operating at a maximum raw data rate of 54 Mbps, which in practice delivers a maximum net throughput of 27.9 Mbps due to protocols overhead[35], with 1 mesh hop a maximum mesh throughput of $B_{mesh_1} = 13.95Mbps$ could be obtained.

In a general case the throughput figures would go down to $B_N = \frac{B}{N+1}$

A naive estimation to the throughput figure in function of hop number, as a first approximation considering the multihop transmission for just the traffic of a node under study and disregarding backhaul traffic, for number of hop values from 0 to 10 hops is calculated in table 4.2.5 and represented graphically in figure 4.31:

N	0	1	2	3	4	5	6	7	8	9	10
B(N) [Mbps]	27,9	13,95	9,30	6,98	5,58	4,65	3,99	3,49	3,10	2,79	2,54

Table 4.12: *Approximated mesh throughput in function of number of hops*

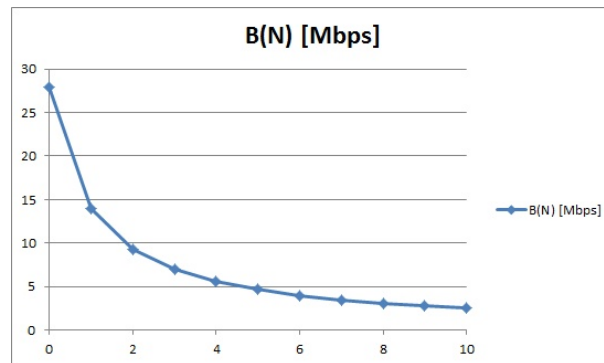


Figure 4.31: *Approximated mesh throughput in function of number of hops*

Furthermore, with the use of a single radio, as the hardware requirements of our problematic specified, the congestion would be high as all the mesh nodes and legacy STAs under the coverage of the same hospital AP would have to work in the same frequency channel, thus reducing importantly the achievable net throughput.

Implementation: 3 The additional complexity introduced by mesh networking would make more difficult to implement the solution to our problematic using 802.11s.

Installation: 5 In the other hand, the installation and deployment processes would be easier, benefiting from the additional flexibility, specially in terms of nodes coverage and auto-configuration.

Figure 4.32 shows all the scores given to the 802.11s Mesh technique in a spider-graph. In that

Mesh 802.11s suitability	Characteristic's points
Functionality	4
Hardware requirements and availability	2
Simplicity	2
Flexibility	5
Throughput	3
Implementation	3
Installation	5
Total score	25

Table 4.13: Mesh 802.11s suitability points

kind of graph, the greater the blue surface covered by the features scores, the more suitable a technique is.

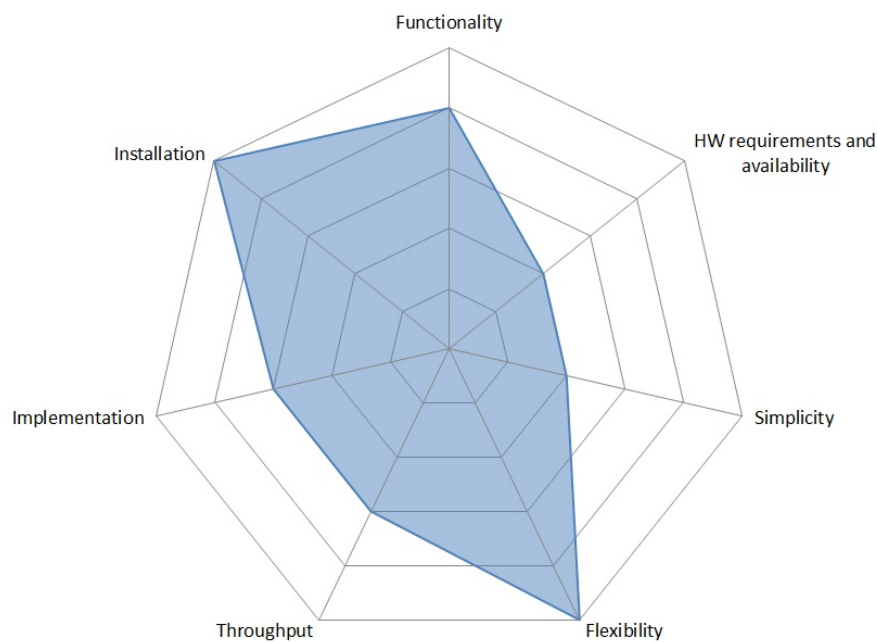


Figure 4.32: 802.11s Mesh strengths and weaknesses

In conclusion, although obtaining a remarkable score of **25 points** in the suitability assessment, in part thanks to its **high grade of functionality and flexibility**, 802.11s mesh technology is **discarded** from our implementation due to its **higher level of complexity** respect other techniques and lack of availability of products clearly supporting it.

4.2.6 SoftAP

The SoftAP approach relies in the virtualization of a physical wireless adapter, to convert it into more than one virtual wireless adapter.

Its name, which stands for *software access point*, is a slight abuse of the term given the current popularization of inexpensive USB Wi-Fi adapters, designed initially to allow Wi-Fi connectivity to devices as clients, but whose drivers support software emulation of the basic AP functionalities. These modified drivers, such as the HostAP Linux driver developed by Jouni Malinen[33], merely allow WLAN cards to perform the functions of an IEEE 802.11 access point, that is to operate as a true BSS Master. The use of a typical configuration allows to establish an AP in a computer making use of its wireless adapter (working in AP mode), and depend on a wired Ethernet adapter or an additional physical wireless adapter (working in client mode) installed in the computer to connect it to a given network, such as the Internet or a corporative network.

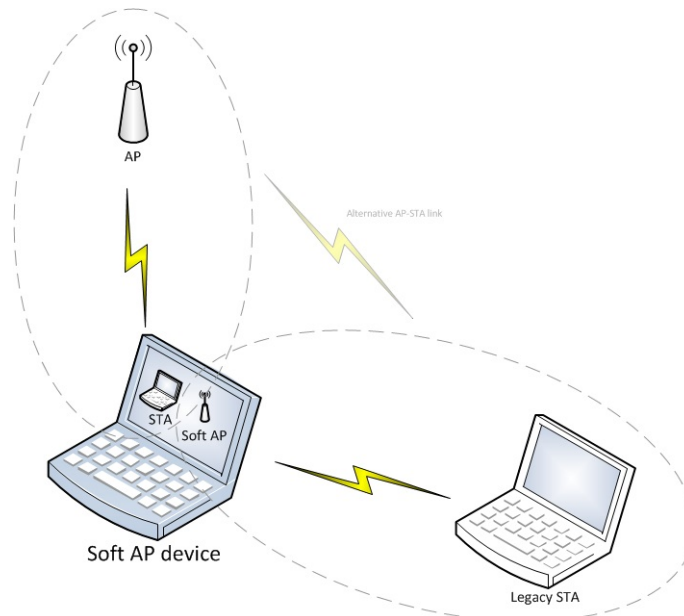


Figure 4.33: *SoftAP example setup, connected simultaneously to an AP in STA mode and with a legacy STA connected to the virtual access point created by the SoftAP*

In contraposition, with the SoftAP approach a single physical wireless device is used to connect as a client to another AP (normally a *hardware AP*), while at the same time acting as a “virtual” AP (a *software AP* in contraposition) itself allows other wireless-STAs operating in client mode to connect to it and route their traffic to the network provided by the previously mentioned AP.

Operation details

This solution is technically possible by the use of no less than two virtual wireless adapters, one in client mode (acting as a STA) and the other(s) in AP mode, up and running simultaneously. Thanks to the virtualization of wireless adapters is also possible to broadcast more than just

one SSID[19], so that allowing flexibility and a wide range of configuration options.

The working principle in this mode of operation is based on the sharing of the processing tasks related with attending the requests of the several virtual wireless network interfaces enclosed in a single physical wireless hardware.

A possible architecture for a SoftAP device would be the following, shown in figure 4.34: The card's firmware takes care of the time critical tasks like beaconing and frame acknowledging, while leaves other management tasks to the driver. This driver implements the basic functionality needed to initialize and configure the wireless card, to send and receive frames, and to gather statistics. In addition, it includes an implementation of the 802.11 Standard AP functions: authentication (and deauthentication), association (reassociation and disassociation), data transmission between two wireless stations, power saving (PS) mode signaling and frame buffering for PS stations. Overall, in the case of a Linux system, the driver is loaded as a module in the kernel, which implements all other aspects of the network stack.

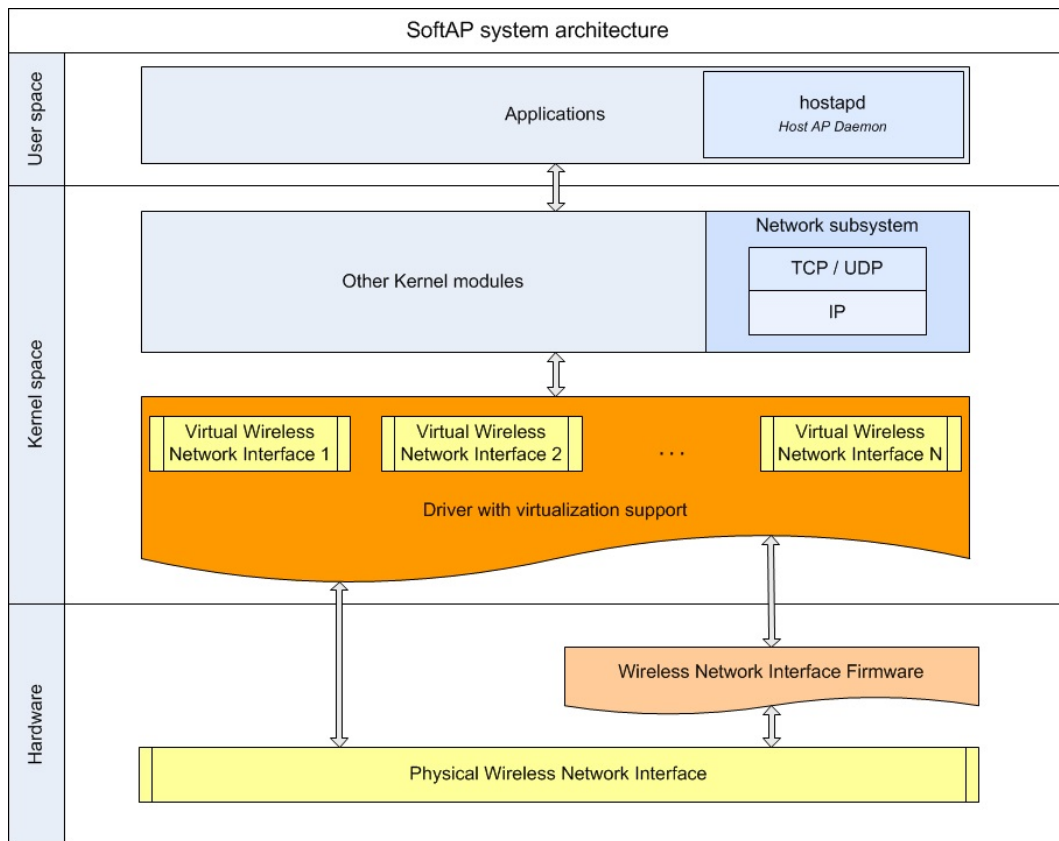


Figure 4.34: *SoftAP system architecture and relation between the Hardware, Kernel and User levels*

Shown in figure 4.30 there is a possible SoftAP setup applied to the Philips Patient Monitoring system. The hospital APs would be standard legacy APs (as we cannot assume that the hospital would change all their existing AP devices deployed all along the facilities). MP70 bedside monitors would be SoftAP devices, as STA clients connected to the facility infrastructure network

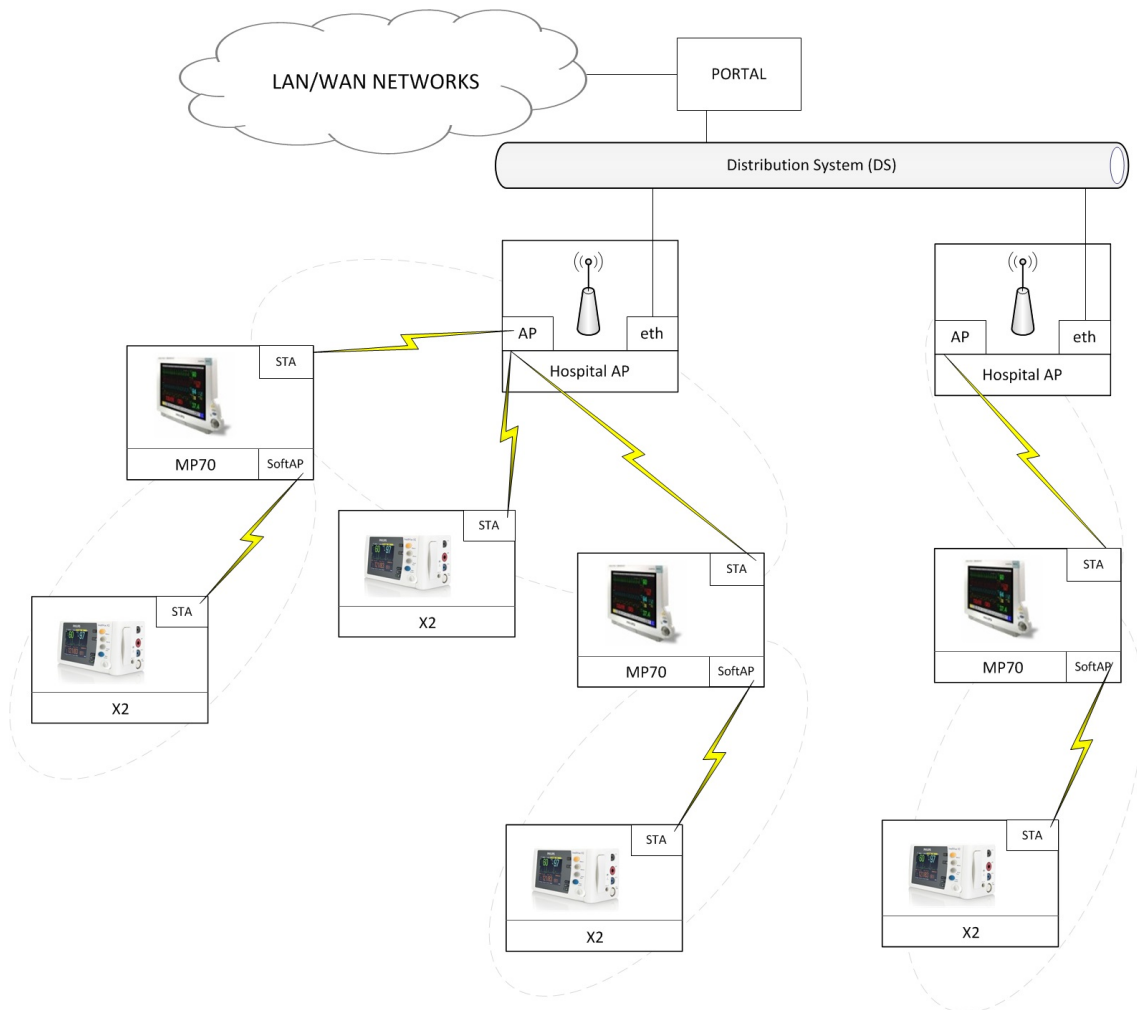


Figure 4.35: *SoftAP approach applied to the Philips Patient Monitoring system*

through hospital APs, and at the same time act as APs to the X2 portable monitors which in this case would be legacy STAs.

In that setup, an X2 willing to connect to the backbone system to send patient data would be able to connect to any MP70 or AP (while in a corridor or waiting room) in its vicinity which would forward the data upstream to the infrastructure network. Nevertheless, in order to complete the patient assignment process it would have to connect directly to the corresponding MP70, as the patient assignment would be assimilated with the wireless connection, and thus the patient data information flow would indeed correspond with the physical wireless link.

Suitability

The SoftAP approach, as detailed in this technique's description, is based on the coexistence of a STA and an AP (or several) functioning in the same Wi-Fi device. Taking this into consideration,

in first place for embracing the SoftAP technique the device has to be able to operate as an AP, an operation mode not supported by all the combinations of chipsets, drivers and hardware. This fundamental aspect on the suitability of the SoftAP technique is discussed together with the rest of points of the suitability assessment:

Functionality: 3 The standard functions provided by the 802.11 services are available with the SoftAP approach, as in any device operating in client mode. Furthermore, as the device is acting also as an AP, it includes the Distribution services inherent to the AP mode, to allow clients to associate and disassociate to it, and the ones relating normally to the Distribution System (routing, NAT,...).

SoftAP's native pairing procedure corresponds just to the AP-STA association when the SoftAP is acting as an AP. Nevertheless, as it is reviewed in the "Implementation" assessment, developing a set of pairing methods customized for the needs of the monitoring system would be relatively easy and at the same time more convenient than relying just in the native pairing method of some generic ad hoc technique.

Hardware requirements and availability: 4 Depending on the drivers of the wireless adapter and the chipset in which it is built on, there exists support for AP mode or not[38]. In our case, Atheros is the manufacturer of both the AR55213A used in the MP70 bedside monitor and the AR6K chipset series used in the X2 portable monitor, as well as the more recent AR9K and AR10K. While the *ath5k*¹⁹ linux wireless driver for the first AR5K family of chipsets and the more recent ones supported AP mode and even mesh mode, the *ath6k*²⁰ driver did not support these modes, preventing the SoftAP technique to be implemented on it or forcing to use other alternative drivers as the, currently superseded although still powerful, *madwifi*²¹ in combination with the *HostAP*[33] daemon.

Available commercial implementations of SoftAP-like products:

- Microsoft provides a similar function as a built in option in its latest O.S., Windows 7, referred to as Virtual Wi-Fi.
- A minority of the latest released Intel wireless adapters includes an implementation similar to this solution under the name of My WiFi, with some other functionalities (algorithms for easy device discovery and pairing).
- Apple's AirPort card only supports AP mode, like other USB Wi-Fi adapters, but not multiple virtual wireless network interfaces.
- Since Android version 2.2 practically all devices allow *tethering*, that means also support AP mode, for sharing a mobile broadband internet connection to other Wi-Fi devices through the creation of an SSID. Nevertheless it does not support multiple

¹⁹Ath5k is a completely free and open-source (FOSS) wireless driver for Atheros based wireless chipset versions AR5xxx in the Linux Kernel, evolved out of MadWiFi, URL: <https://wireless.wiki.kernel.org/en/users/Drivers/ath5k>

²⁰'ath6kl' is the FullMAC wireless driver for Atheros AR600x family of chips, URL: <https://wireless.wiki.kernel.org/en/users/drivers/ath6kl>

²¹URL: <http://madwifi-project.org/>

virtual wireless network interfaces either.

Simplicity: 4 The SoftAP approach represents the most natural technique to guarantee a simultaneous connection with an external AP and providing connectivity to a client (or clients in the general case) at the same time, translating this with conceptual simplicity into an AP plus a STA in the same device.

Flexibility: 4 As well as simple, the SoftAP approach would flexibly adapt to different implementations. Every device enabled with SoftAP operation would be able to act as an AP or as a STA, allowing a wide variety of different approaches on how to implement a possible solution for our problematic.

Throughput: 4 Depending on the specific embrace of the SoftAP approach and the hardware wireless adapter used, net throughput could be slightly reduced compared with an equivalent setup in which a device with two separate radios transmitting in different channels would be used. Obviously the sharing of the hardware resources by two or more virtual adapters and their running connections will affect the overall performance. Nevertheless, keeping both the AP-side and the STA-side of the SoftAP in the same channel would prevent time consuming channel switching periods, and keeping the net SoftAP throughput figures in the same magnitude order as with alternative solutions using a single radio, taking into account that for every approach the packets must be transmitted twice over the air (2 hops) to reach the AP from the remote station.

Implementation: 4 Developing the adequate device discovery and pairing methods, exploiting the openness of the SoftAP approach could be relatively easy to implement a set of functionalities and procedures for the patient monitoring devices prototyping and later production.

Installation: 4 Each MP70 bedside monitor should be installed and configured under the coverage area of an hospital AP. Apart from that constraint, the installation process should be simple, as the relation between each X2 portable monitor and the MP70 it would connect to, would be taken care by the pairing mechanism by the user, without the need of a previous configuration, as all nodes would be pre-charged with a standard configuration.

SoftAP suitability	Characteristic's points
Functionality	3
Hardware requirements and availability	4
Simplicity	4
Flexibility	4
Throughput	4
Implementation	4
Installation	4
Total score	27

Table 4.14: *SoftAP suitability points*

Figure 4.36 shows all the scores given to the SoftAP technique in a spider-graph. In that kind of graph, the greater the blue surface covered by the features scores, the more suitable a technique is.

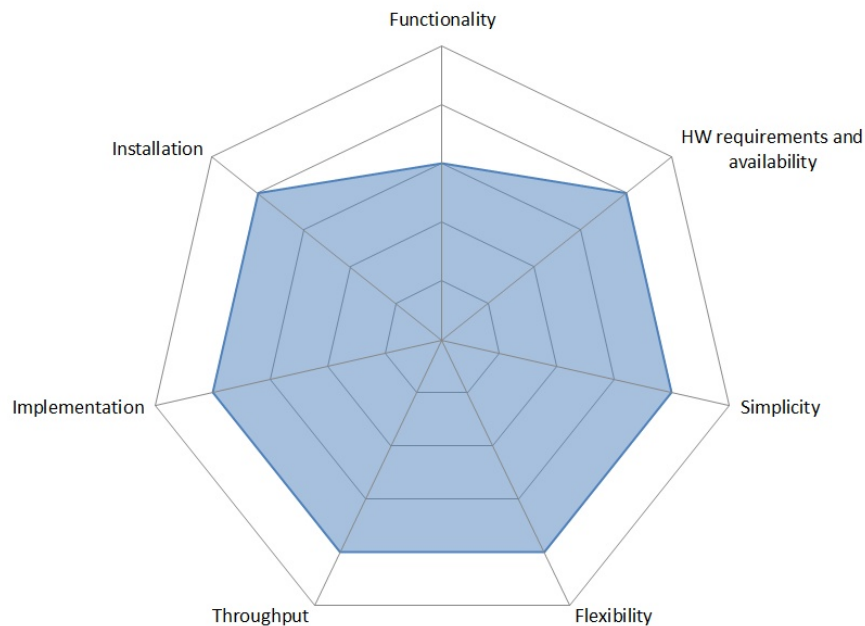


Figure 4.36: *SoftAP strengths and weaknesses*

With **27 points** in the suitability assessment, SoftAP technique **achieved the highest score** among all the reviewed techniques, thanks to its **balanced scores in each aspect** assessed. Given the availability of chipsets and drivers sets supporting SoftAP and multi-SSID operation, its relative simplicity and openness to facilitate implementations on top of it and its estimated throughput figures this technique **compensates the lack of inherent functionality** compared to other more pairing-oriented *ad hoc* techniques.

4.2.7 Bluetooth 3.0

Launched by Ericsson around 1994, Bluetooth is a short wavelength radio communication technology well established today as an alternative to Wi-Fi connectivity for short-range data transfer between electronic devices.

The Bluetooth specifications development is taken care by the Bluetooth Special Interest Group (SIG), formed in 1998 by five companies, but has become a *de-facto* industry standard with 30,000 member companies in 2016.

The first specification, Bluetooth 1.0 was released in 1999, conceived as a wireless alternative to serial data cables by the use of radio transmission. Since then, several specifications and improvements have been released:

- 2002: IEEE 802.15.1 specification conformity with Bluetooth
- 2003: Bluetooth Core Specification Version 1.2 adopted
- 2004: Core Specification Version 2.0 Enhanced Data Rate (EDR) adopted
- 2009: Bluetooth Core Specification Version 3.0 + HS adopted
- 2010: Adoption of Bluetooth Core Specification Version 4.0 with Low Energy (LE) technology²².

Taking advantage of an *alternate MAC/PHY*, an innovative method of radio substitution, the speed of 802.11 networks is achieved with **Bluetooth 3.0 + HS (High Speed)**, while allowing well known Bluetooth protocols, profiles, security, and pairing to be used in consumer devices while achieving faster throughput with the momentary use of a secondary radio already present in the device.

Higher transmission rates are achieved by using IEEE 802.11-2007 as an Alternate MAC/PHY with the use of PAL (Protocol Adaptation Layer) and 802.11 Enhanced Rate PHY (ERP).

Besides, by using that couple of different radios in Bluetooth 3.0 + HS the following principal benefits are achieved:

- **Reduced power consumption**, by using the high speed radio only when in transmission, increasing battery duration for devices relying in low power connection models when idle.
- **Enhanced power control** limiting connection drop-outs and maximizing range, adding closed loop power control.
- Improved user experience thanks to **lowered latency rates**, by the use of Unicast Connectionless Data for quickly sending small bursts of data (without establishing an explicit

²²Posterior more recent developments introduced were in 2013 Bluetooth 4.1 introducing the Internet-of-Things IoT. And in 2014 Bluetooth 4.2 adding features for IP connectivity, privacy and increased speed.

L2CAP channel).

- Enhanced security, thanks to the use of **Read Encryption Key Size**, which enables the host to determine the negotiated encryption key size to determine security requirements.

Operation details

While each Bluetooth implementation has specific requirements detailed in the corresponding, the Bluetooth core system architecture has many consistent elements. The system includes an RF transceiver, baseband and protocol stacks that enable devices to connect and exchange data.

Bluetooth devices exchange protocol signaling according to the core specification. Core system protocols are the radio (RF) protocol, link control (LC) protocol, link manager (LM) protocol and logical link control and adaptation protocol (L2CAP), all of which are fully defined in the Bluetooth specification.

The three lower system layers (radio, link control and link manager protocols) are often grouped into a subsystem known as the **Bluetooth controller**. This is a common implementation that uses an optional standard interface, the **Host to Controller Interface (HCI)** which enables two-way communication with the rest of the system, called the **Bluetooth host**.

Physical (PHY) Layer: Controls transmission and reception of the 2.4Ghz radio with Bluetooth communication channels.

For Bluetooth, which uses frequency hopping spread spectrum (FHSS) at 1600 hops/second, the ISM band is split into 79 channels of 1 MHz (with a lower guard band of 2MHz and an upper guard band of 3.5 MHz)[40].

For Bluetooth Low Energy the ISM band is split into 40 channels of 2 MHz (also with a lower guard band of 2MHz and an upper guard band of 3.5 MHz):

- 3 advertising channels: 37 at 2402 MHz, 38 at 2416 MHz and 39 at 2480 MHz.
- 37 data channels: 0 to 10 from 2404 to 2424 MHz, and 11 to 36 from 2428 to 2478 MHz.

The Bluetooth physical channel is sub-divided into time slots and transmission occurs using time division duplexing (TDD). The time slot length is a function of the frequency hop rate resulting in a nominal length of 625 microseconds.

Link Layer: Defines packet structure/channels, discovery/connection procedure and sends/receives data. It can be defined by a state machine²³ with five states: Standby, Advertising, Scanning, Initiating and Connection (with the Master Role and the Slave Role as possible roles in Connection state).

²³Excerpts and state machine scheme from <https://www.bluetooth.com/specifications/bluetooth-core-specification/technical-considerations>

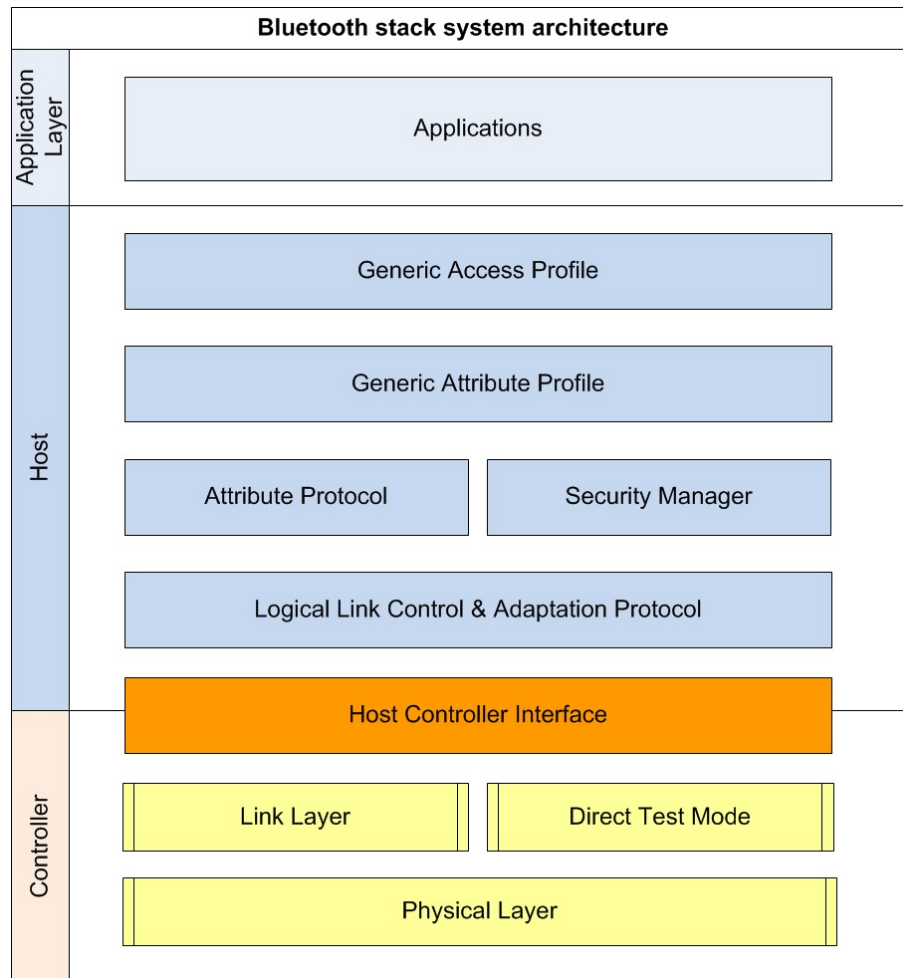


Figure 4.37: Bluetooth core stack architecture

Direct Test Mode: For testing purposes, allows to instruct the PHY layer to transmit or receive a sequence of packets, through submitting commands via the HCI or a 2-wire UART interface.

Host to Controller Interface (HCI): Optional standard interface between the Bluetooth controller subsystem (the three bottom layers) and the Bluetooth host.

Logical Link Control and Adaptation Protocol (L2CAP) Layer: A packet-based protocol that transmits packets to the HCI or directly to the Link Manager in a hostless system. Supports higher-level protocol multiplexing, packet segmentation and reassembly, and passes quality of service information on to higher layers.

Attribute Protocol (ATT): Defines the client/server protocol for data exchange once a connection is established. Attributes are grouped together into meaningful services using the Generic Attribute Profile (GATT).

Security Manager: Defines the protocol and behavior that manages pairing integrity, au-

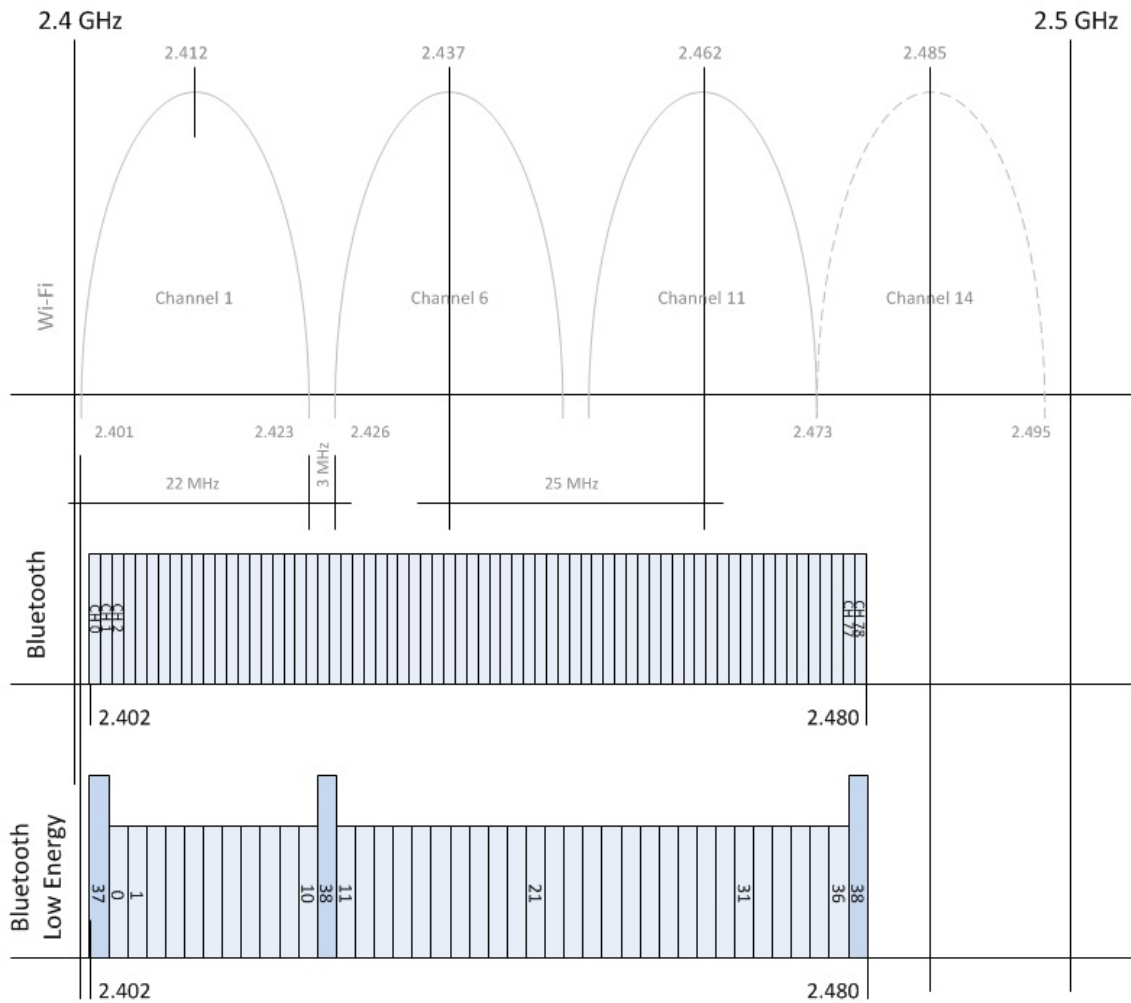


Figure 4.38: Bluetooth 1 MHz and Bluetooth LE 2 MHz channels compared with 802.11b DSSS 22MHz channel width (non overlapping channels)

label:btchannels

authentication and encryption between Bluetooth devices, and provides a toolbox of security functions that other components use to support almost any level of security needed by diverse applications.

Generic Attribute Profile (GATT): Using the Attribute Protocol, GATT groups services that encapsulate the behavior of part of a device and describes a use case, roles and general behaviors based on the GATT functionality. Its service framework defines procedures and formats of services and their characteristics, including discovering, reading, writing, notifying and indicating characteristics, as well as configuring the broadcast of characteristics.

Generic Access Profile (GAP): Works in conjunction with GATT in Bluetooth LE implementations to define the procedures and roles related to the discovery of Bluetooth devices and sharing information, and link management aspects of connecting to Bluetooth devices.

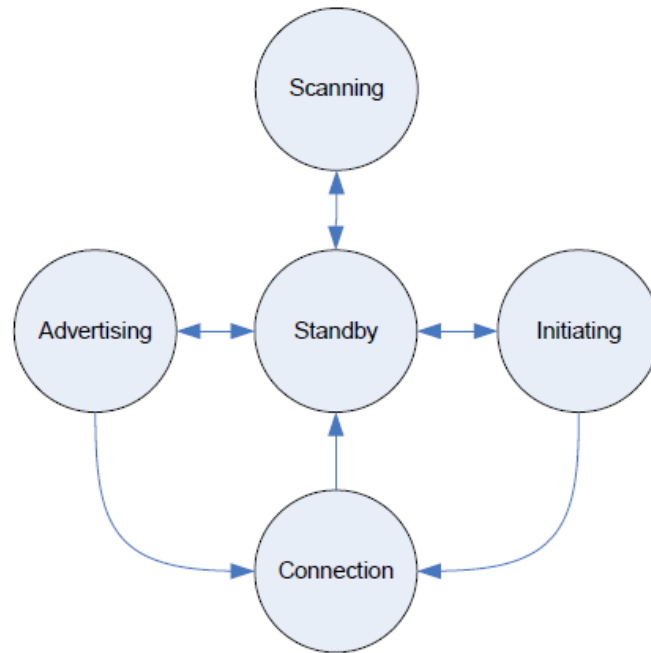


Figure 4.39: *Bluetooth state machine diagram*

From a logical point of view, Bluetooth belongs to the contention-free token-based multi-access networks. In a Bluetooth network, one node has the role of master, and all other Bluetooth nodes are denominated slaves. The master decides which slave node has access to the channel to transmit in every moment.

The nodes sharing the same channel (i.e., synchronized to the same master) form a *piconet*, which is the most basic formation of a Bluetooth network. A piconet contains a master node and up to seven active slaves (i.e. taking part in a data transmission). Nodes with Parking state are stations synchronized with the master which are not participating in any data transmission.

Suitability

In short, Bluetooth 3.0 + HS provide with the simplicity and ease of connection of Bluetooth combined with the speed and energy efficiency of 802.11.

One important concern for IT management at facilities like a hospital when assessing whether to use a technology like Bluetooth when already having a deployed Wi-Fi 802.11b/g network, which both share the same frequency range in the 2.4 GHz ISM band would be the *coexistence problems* that could occur. Fortunately since Bluetooth version 1.2 Adaptive Frequency Hopping (AFH) was introduced:

- The WLAN systems use direct sequence spread spectrum (DSSS) or OFDM technology with channel bandwidths up to 22 MHz.

- Bluetooth systems use FHSS technology over 79 channels spaced 1 MHz apart.

When both systems coexist, there is a 28% chance of collision between the two devices (22/79). Using AFH specified in v1.2, the Bluetooth system is capable of measuring interference, such as a WLAN signal, and avoiding those frequency channels with known interference. The system can adjust its number of usable channels down to 20 if necessary in order to avoid such possible interference.

Functionality: 5 Bluetooth has been stacked with many features, providing full functionality since its definition and its first versions, as will be detailed in section 5.2 for reviewing pairing and device discovery mechanisms.

Moreover the concept of *profiles* in Bluetooth enabled manufacturers to develop their products according a precise fitting to several different and very specific use cases, thus improving usability and user experience. Profiles are definitions of possible applications and specify general behaviors that Bluetooth enabled devices use to communicate with other Bluetooth devices. Profiles build on the Bluetooth standard to more clearly define what kind of data a Bluetooth module is transmitting.

Example profiles: Blood Pressure Profile, Continuous Glucose Monitoring Profile, Weight Scale Profile, Heart Rate Profile, Health Thermometer Profile, Pulse Oximeter Profile.

Hardware requirements and availability: 1 Bluetooth 3.0 availability is low. Very few or just custom platforms support the given technique, since its recent approval²⁴.

Besides, Bluetooth 3.0 + HS requires the alternate 802.11 PHY to operate at both 2.4 and 5 GHz, thus establishing another constraint in terms of hardware requirements.

Simplicity: 4 If it was not for the constraints posed by the hardware requirements and availability, the grade of complexity of the solution if it was implemented with Bluetooth would be more than acceptable. But the alternate MAC/PHY introduced in version 3.0 + HS represents an additional grade of complexity to this technique.

Flexibility: 3 As the use of an alternate MAC/PHY is an interesting feature for applications

²⁴As of June 2010. At the time of writing there are multiple options that combine Bluetooth 3.0 + HS plus 802.11 technologies on a single chip available in the market from several hardware companies in their portfolios. To name a few:

— MediaTek RT3290, 802.11ac plus Bluetooth 3.0 Half MiniCard Combo SoC <http://www.mediatek.com/en/products/connectivity/wifi/pc/combo/rt3290/>

— Advantech EWM-W141H 802.11b/g/n WiFi with Bluetooth 3.0+HS combo half size miniPCle card module [http://support.advantech.com/Support/DownloadDatasheet_New.aspx?Literature_ID=4a4d273b-9c58-4998-8883-5cd02540eee5&utm_source=support.advantech.com.tw&utm_medium=Download&utm_campaign=EWM-W137H_EWM-W141H_DS\(06.11.12\)](http://support.advantech.com/Support/DownloadDatasheet_New.aspx?Literature_ID=4a4d273b-9c58-4998-8883-5cd02540eee5&utm_source=support.advantech.com.tw&utm_medium=Download&utm_campaign=EWM-W137H_EWM-W141H_DS(06.11.12))

— Broadcom BCM943224HMB Dual-band 802.11n and Bluetooth 3.0 Half MiniCard SoC <http://www.broadcom.com/products/wireless-connectivity/bluetooth/bcm943224hmb>

Apart from the numerous heterogenous devices which include Bluetooth connectivity, which surpassed the 2 billion annual shipments figure in 2012, 3 years after the 3.0 + HS specification was adopted. And 3 billion in 2014, according to that same year Bluetooth SIG Annual Report (URL: <https://www.bluetooth.org/en-us/Members/Annual-Report/2014-Annual-Report/default.aspx>), and expected to reach almost 5 billion by 2018, according to ABI Research data.

highly power consumption dependant or with a bursty data transmission pattern, in our case the monitoring of human physiological data produces a deterministic and periodic communication scheme[25]. For that reason the alleged flexibility of Bluetooth 3.0 + HS in the sense of the alternate MAC/PHY is not so valuable. In terms of scalability, Bluetooth scatternets are not commonly deployed in large facilities, given their difficulty to be managed and the possible coexistence issues with other 2.4 GHz networks like 802.11 which are deployed in hospitals and used by this same solution, at least from the MP70 STA-side to the hospital legacy APs.

Throughput: 4 With the smart use of the *alternate MAC/PHY* radio substitution, 802.11 speeds are achieved with this advanced Bluetooth specification, traducing in a **theoretical net throughput of up to 24 Mbps** when the alternate PHY is based on 802.11 at 54 Mbps data rate.

Implementation: 1 Implementing the solution to our problematic over Bluetooth would drive to more obstacles than benefits it would bring, even after integrating the necessary additional hardware supporting Bluetooth 3.0 + HS into both the X2 portable monitors and the MP70 bedside monitors, their functioning would have to be integrated with the STA side in the MP70 to forward data to the hospital network.

Installation: 1 The installation and deployment process of the solution over a large healthcare facility, based on the Bluetooth 3.0 + HS specification would not be easy neither brief, since it would require to set up specific configuration on each device. Previous integration with the current hardware would also be difficult and time-consuming.

Bluetooth 3.0 suitability	Characteristic's points
Functionality	5
Hardware requirements and availability	1
Simplicity	4
Flexibility	3
Throughput	4
Implementation	1
Installation	1
Total score	19

Table 4.15: *Bluetooth 3.0 suitability points*

Figure 4.40 shows all the scores given to the Bluetooth 3.0 technique in a spider-graph. In that kind of graph, the greater the blue surface covered by the features scores, the more suitable a technique is.

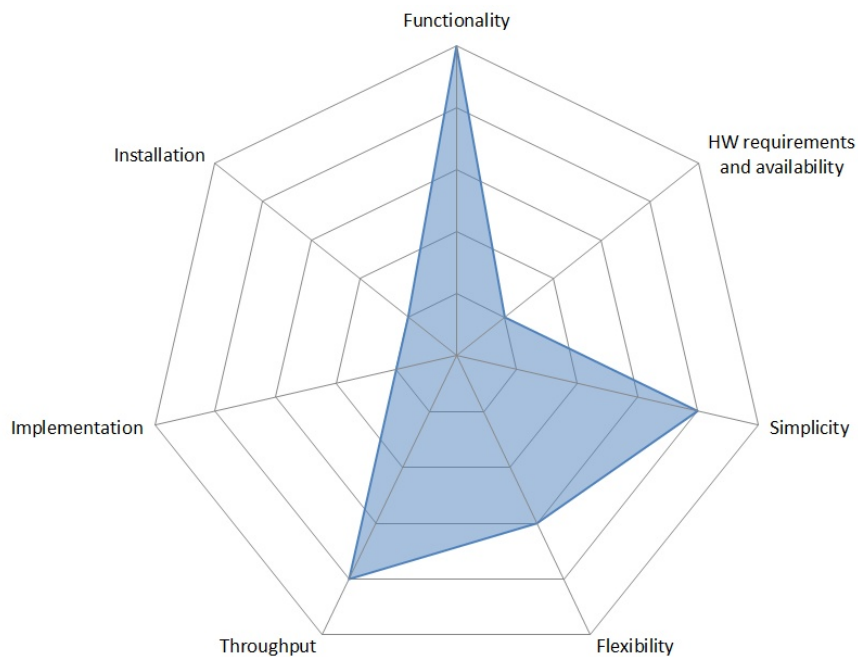


Figure 4.40: *Bluetooth 3.0 strengths and weaknesses*

In conclusion, obtaining a relatively low score of **19 points** in the suitability assessment, although presenting a **high grade of functionality and expected high throughput**, Bluetooth 3.0 + HS technology is **discarded from our implementation due to its lack of availability** by the time this assessment was carried out and due to the difficulties it would present when implementing and deploying a complex solution based on this technique.

4.3 Suitability assessment and technology selection decision summary

Following our own custom designed *technology evaluation methodology* as detailed in first place in section 4.1, we assigned scores to each *ad hoc* technique following a common criteria for each characteristic and comparing all them objectively in a balanced scorecard.

Table 4.16 details the ad hoc techniques comparison balanced scorecard, in full-page landscape configuration for a better visualization. The individual scores come from the specific suitability assessment results in every ad hoc technique review section, from 4.2.1 to 4.2.7.

Characteristic	IBSS	TDLS 802.11z	Mesh 802.11s	Wi-Fi Direct™	WDS	SoftAP	Bluetooth 3.0 + HS
Functionality	1	2	4	5	1	3	5
Hardware requirements and availability	5	2	2	1	3	4	1
Simplicity	5	4	3	3	4	4	4
Flexibility	3	3	5	4	1	4	3
Throughput	5	5	3	5	3	4	4
Implementation	1	1	3	4	2	4	1
Installation	3	2	5	4	1	4	1
Total score	23	19	25	26	15	27	19

Table 4.16: *Ad hoc techniques suitability balanced scorecard*

We chose the **SoftAP** approach because of its higher score, as indicated in green in the table 4.16, for all the aforementioned advantages described in subsection 4.2.6:

With **27 points** in the suitability assessment, SoftAP technique **achieved the highest score** among all the reviewed techniques, thanks to its **balanced scores in each aspect** assessed. Given the availability of chipsets and drivers sets supporting SoftAP and multi-SSID operation, its relative simplicity and openness to facilitate implementations on top of it and its estimated throughput figures this technique **compensates the lack of inherent functionality** compared to other more pairing-oriented *ad hoc* techniques.

As justified in section 4.1.1, we chose **802.11g as the most appropriate IEEE 802.11 specification** over which to implement our **SoftAP approach** based wireless patient monitoring solution, collecting the final decision on the technology selection to sum-up in table 4.17.

Technology selection decision	
ad hoc approach selected	SoftAP
IEEE 802.11 specification selected	802.11g

Table 4.17: *Technology selection decision*

Chapter 5

Solution design

The specific problematic of the dual-link scenario (as introduced in section 3.1.2) is discussed in this chapter and a solution to address it is proposed, offering an overview of its principles of operation, once the existing available ad hoc techniques and Wi-Fi technologies were analysed in chapter 4 and the decision was to implement it over 802.11g based on the Soft AP approach.

5.1 Dual-link scenario problematic

In the current scenario, the Philips X2 portable patient monitor is directly connected to the MP70 bedside monitor by a MSL cable¹ during normal operation, as it is described in section 3.1.1. On the other hand, in the target dual-link scenario the wired direct connection is replaced by a Wi-Fi ad hoc wireless link.

Replacing the cable that bonds one device to the other, physically as well as logically, by a wireless connection represents a wide problematic, which traduces to several issues to be addressed by our solution:

- Wireless links do not tie together two devices in a 1:1 manner, as cable connections do.
- A given physical wireless connection between two devices, that can change dynamically, does not imply the same logical link for the patient physiological information flow.
- A monitoring device may be wirelessly connected to a second device (like a hospital's infrastructure AP) which will forward the patient information to a third device (a bedside monitor or a monitoring central, like the Philips IntelliVue Information Center).
- There exists a derived major loss of certainty that data received via the current wireless link corresponds to the accurate patient.

¹The Measurement Link cable is an specific cable with a proprietary ODU connector, that includes a power connection of a 48V voltage, a RS-422 compliant serial connection and a IEEE 802.3 10-Base-T LAN connection[20].

For the aforementioned reasons, two fundamental functionalities to be considered arise: **Pairing** and **Device Discovery**.

5.1.1 Derived use cases

We devised several use cases, derived from the original scenario, which exemplify the mentioned issues that could arise when using the wireless patient monitoring in the dual-link use case:

Use case 1 – *Wire replaced by wireless connection between X2-MP70*

In this use case the wireless link is equivalent to the patient info connection. MP70 is unassigned. The X2 has a **PatientID** already assigned, arrives to the coverage area of the MP70 AP and connects to it. The connection process is initiated by the user and

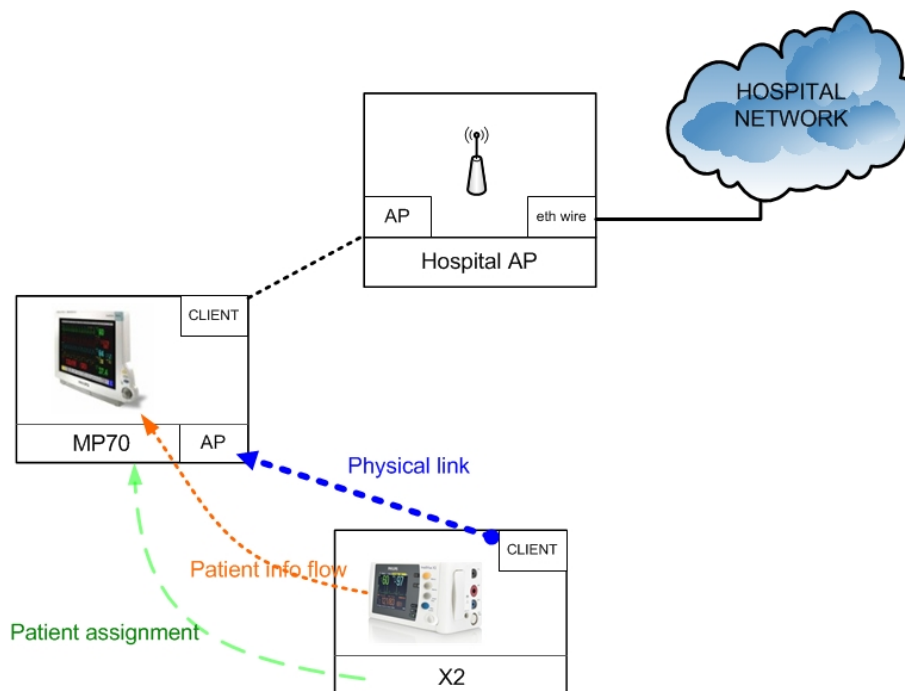


Figure 5.1: Use case 1. Wire replaced by wireless connection between X2-MP70

Use case 2 – *X2 connects to the hospital infrastructure APs when there is no MP70 available*
 In this use case the X2 keeps connected to hospital APs until it roams to the first available MP70. MP70 is unassigned. The X2 has a **PatientID** already assigned, is under hospital AP coverage and arrives to the coverage area of the MP70 AP.

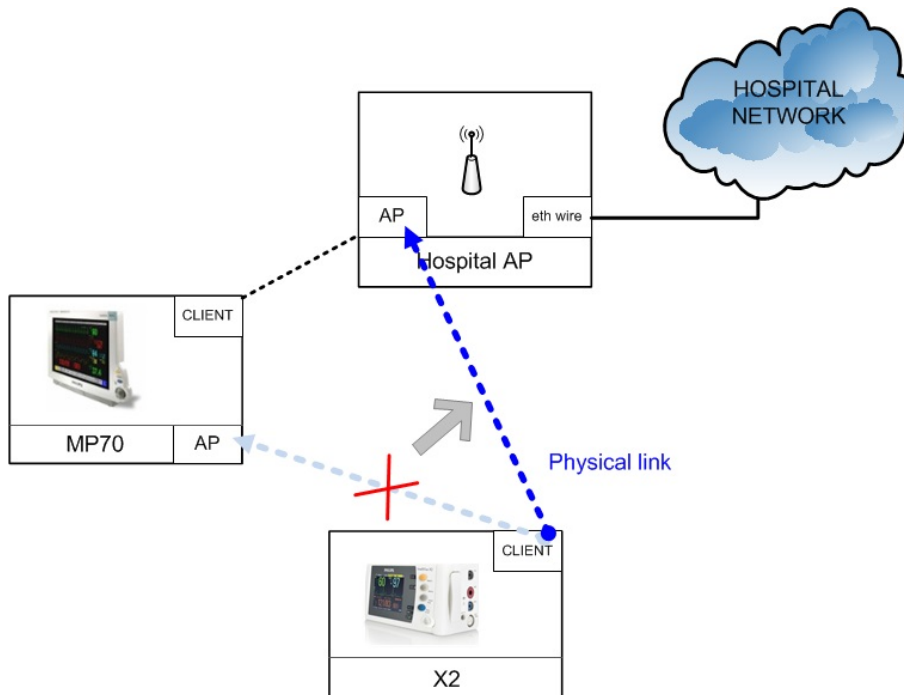


Figure 5.2: Use case 2. X2 connects to the hospital infrastructure APs when there is no MP70 available

Use case 3 – X2 replacement with already assigned MP70 and PatientID

MP70 is already assigned, and has a `PatientID` (previously assigned by the X2 or by the application layer, not in the scope of this study, through the backend/information center). The “fresh” X2 is unassigned and arrives to the coverage area of the MP70, to which it connects. The X2 is assigned to the patient and starts sending the patient information.

Use case 4 – Patient info connection independent from physical wireless link

In this use case the wireless link is different from the logical patient info flow. The X2 has a `PatientID` already assigned and arrives to the coverage area of several MP70s. MP70s may have not been initially assigned. The X2 cannot determine by itself to which MP70 connect to. A pairing mechanism is needed, as well as a patient assignment mechanism. After connecting to the first available MP70, the patient is assigned to the right MP70, and the X2 redirects patient information flow to it, through the hospital AP.

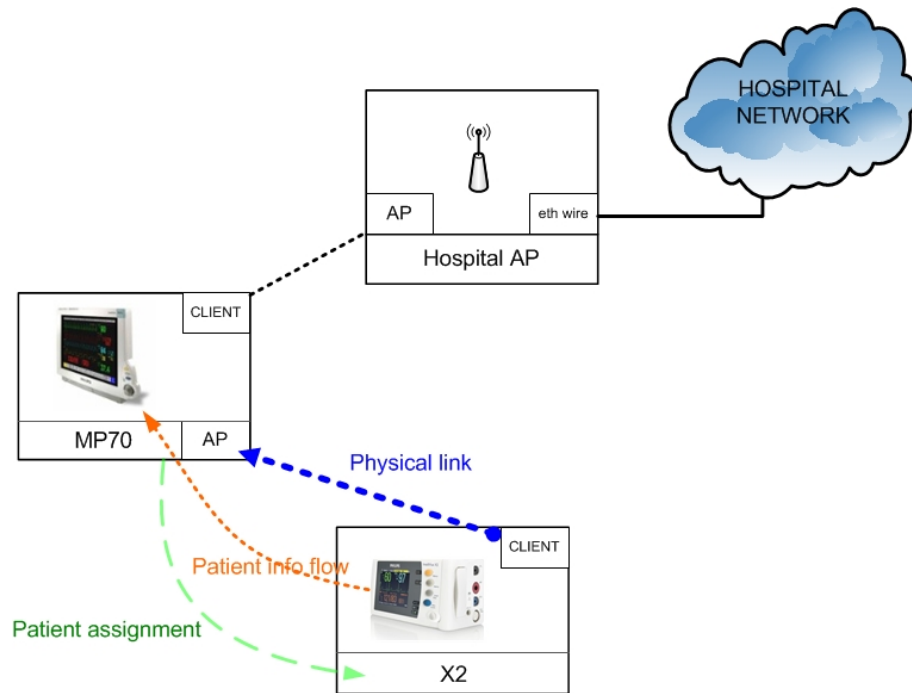


Figure 5.3: Use case 3. X2 replacement with already assigned MP70 and PatientID

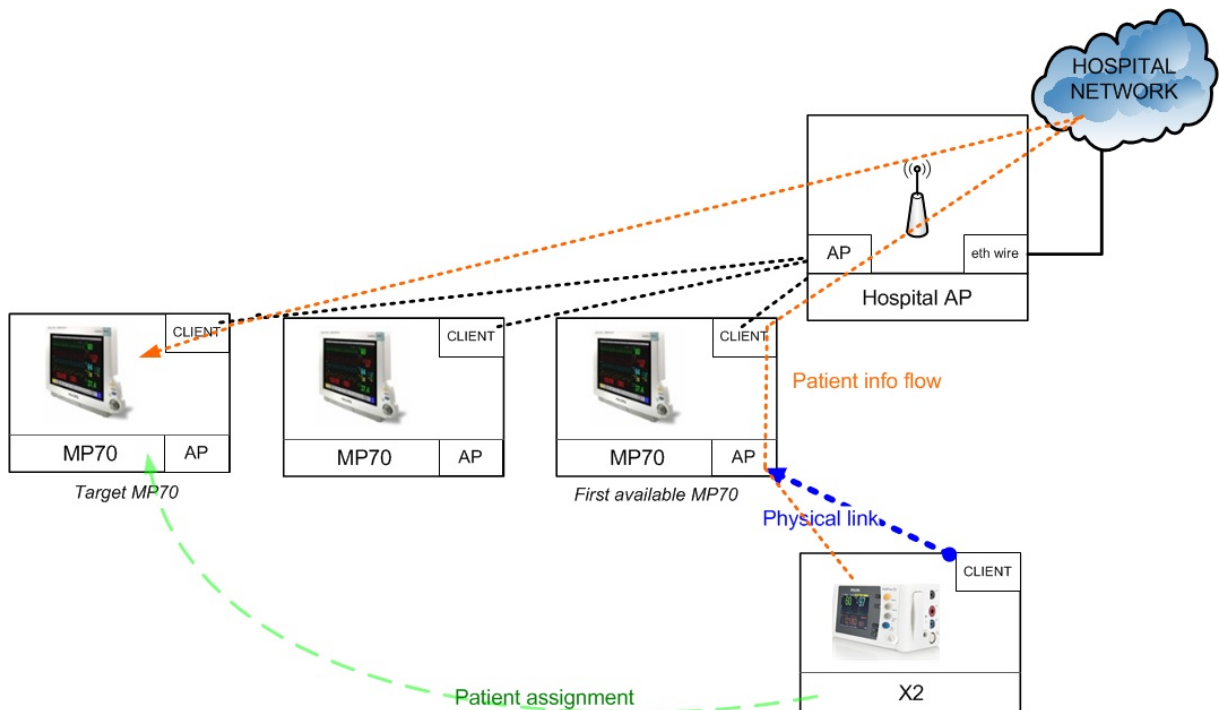


Figure 5.4: Use case 4. Patient info connection independent from physical wireless link

5.2 Pairing and device discovery

While automatic setup procedures are well-known for wired network setup, e.g. IP autoconfiguration, DHCP assignment, etcetera, in wireless networks there is even no physical connecting step as plugging a cable in a port, but exactly this makes **automatic setup only possible under specific circumstances**.

The reason lies in the nature of wireless transmission that spreads beyond typical area boundaries like walls. Therefore, the network may also be in reach of devices (other user's devices, neighbour networks, attackers) that the user does not want to connect to or even do not belong to the network. Concretely, there are two main issues for automatic setup of wireless networks:

1. The membership problem:

- During network setup neither a new device nor the network can automatically decide whether they belong together if there are multiple options (e.g. the patient's bedside monitor and the next-room patient's bedside monitor).
- Patient assignment faces an analogous problem: if there are multiple options (different possible couplets of patient ID and device), an initial *totally* automatic patient assignment is not possible.

2. The initial security harm: For wireless networking there is no secure auto-configuration of initial secrets, since in the initial situation, when no security is configured, the communication can be eavesdropped by a nearby attacker. Advanced techniques like public key encryption could even be compromised by elaborate attacks like man-in-the-middle.

In conclusion, all wireless connection setup solutions have to address these issues. There may be special boundary conditions, but in the general case, additional user interactions are inevitable in the setup process. The challenge is to find the right balance between simple and intuitive user configuration steps while assuring reliable system functions to form error-free and secure connections.

5.2.1 Pairing mechanisms discussion

The pairing mechanism is meant to address one of the membership issues we identified: The problem to configure into the right relationship between devices if there are multiple equivalent alternatives, since a portable monitor may be paired with just one bedside monitor at once.

As described in section 4.2.7, initially conceived as a substitute for RS-232 serial cable connections, Bluetooth is the perfect example of a Personal Area Network (or PAN) where the cable replacement with a wireless connection brought the pairing issue, which was cleverly addressed by this solid industry standard's pairing mechanisms, taking into account that most Bluetooth devices are small in size, battery operated and are provided with reduced input methods.

Bluetooth pairing is an initialization procedure by which two devices that are communicating

for the first time create a common link key that will be used for subsequent authentication[24].

Pairing mechanisms have changed significantly since the introduction of *Secure Simple Pairing* in Bluetooth 2.1. This technology is the most complete showcase of different pairing mechanisms since the most simple to the most advanced one, reviewed in the following lines.

Legacy pairing: the only method available before Bluetooth 2.1. Each connecting device must enter a PIN code and pairing is only successful if the PIN code introduced in both devices coincides. Any 16-byte UTF-8 string may be used as a PIN code, however not all devices may be capable of entering all possible PIN codes because of the aforementioned possible reduced input methods in some devices. Therefore, depending on the input capabilities of each device, Legacy pairing mechanisms can be classified in:

Limited input devices: These devices usually have a fixed PIN, in most of the cases “0000” or “1234”, that is hardcoded into the device. The obvious example of this class of device is a Bluetooth Hands-free headset, which generally would have very limited inputs.

Numeric input devices: for devices with a limited keyboard or numeric keyboard like classic mobile phones. It is based in allowing the user to enter a numeric value up to 16 digits in length.

Alpha-numeric input devices: They allow a user to enter full UTF-8 text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may enter. PCs and smartphones are examples of these device type.

Secure Simple Pairing (SSP): A Bluetooth 2.1 device may only use legacy pairing to inter-operate with a 2.0 or earlier device. Secure Simple Pairing is required by Bluetooth 2.1. and uses a form of public key cryptography, having the following modes of operation:

“Just works”: As implied by the name, this method *just works*. **No user interaction is required;** however, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typically used for legacy pairing by this set of limited devices. This method provides no man in the middle (MITM) protection.

Numeric comparison: If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to ensure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, **assuming the user confirms on both devices and actually performs the comparison properly.**

Passkey Entry: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then

enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both cases provide MITM protection.

Out of band (OoB): This method uses an external means of communication (such as NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OoB mechanism. This provides only the level of MITM protection inherent to the OoB mechanism.

5.2.2 Device Discovery mechanisms discussion

The purpose of the Device Discovery functionality is:

- to ease the self discovery of the different devices (X2 and MP70) assigned to the same patient,
- in order to have a wireless connection between them,
- desirably with the lesser human interaction possible,
- timely and in a reliable way.

To sum up, it should reduce the time needed for the reconnection between a couplet of X2 and MP70 assigned to the same patient, but unlinked due to any cause (out of range, patient moved temporarily to a different location inside the facilities, i. e. surgery room, etcetera). And carry this reconnection out, automatically if possible, assuring that both devices correspond or “belong” to the same patient.

Our device discovery proposal considers both active and passive scanning.

Passive scan device discovery

This approach is based on passively listening for the periodic beacon frames sent by the MP70s in each channel. These beacons are separated by the Beacon Interval time. A common value for this parameter is 100 ms. Taking into account the 13 channels in the 2.4 GHz frequency band, plus the 19 channels in the 5 GHz band (available in Europe) there would be a total of $n_{ch} = 32$ channels if we use *combo a/b/g* wireless cards. Considering also that, according to figures given by related literature[36][37]:

- wireless cards can take between $200\mu s$ and 20 ms for the channel switching, T_{switch}
- the scanning process initiated by the “sensor” portable monitor (X2) will have to wait at least the Beacon Interval time in each channel in order to catch at least one beacon frame, and this parameter is usually set to $T_{BeaconInt} = 100 ms$;

Therefore, a pessimistic approximation for calculating T_{scan} , the time spent in the full passive scan would sum

$$T_{scan} = n_{ch} \cdot (T_{switch} + T_{BeaconInt}) = 32 \cdot (20 \frac{ms}{ch} + 100 \frac{ms}{ch}) = 3.84 s$$

And an optimistic approximation for the passive scan would sum

$$T'_{scan} = n_{ch} \cdot (T'_{switch} + T_{BeaconInt}) = 32 \cdot (0.2 \frac{ms}{ch} + 100 \frac{ms}{ch}) = 3.21 s$$

If only the 13 channels in the 2.4 GHz frequency band are considered because of using b/g wireless cards, the figure for the most optimistic case is reduced to

$$T''_{scan} = n'_{ch} \cdot (T'_{switch} + T_{BeaconInt}) = 13 \cdot (0.2 \frac{ms}{ch} + 100 \frac{ms}{ch}) = 1.03 s$$

And in the case of scanning in the subset of the 3 non-overlapping channels in 2.4 GHz it would go down to

$$T'''_{scan} = n'_{ch} \cdot (T'_{switch} + T_{BeaconInt}) = 3 \cdot (0.2 \frac{ms}{ch} + 100 \frac{ms}{ch}) = 0.3 s$$

From the calculations above it can be deduced that the dominant term is the waiting for the beacon interval.

Optimisation — If in order to improve these results, the Beacon Interval parameter is decreased, the rate of beacons will increase. This will make the first association and roaming processes more responsive; however, the network will incur in an additional overhead and throughput will go down. In addition, stations (X2) using power save mode will need to consume more power because they will need to awaken more often, which would reduce power saving mode benefits. There would be some other strategies to speed up the passive scan phase. For example, as creative and infeasible as synchronizing the MP70s in order to staggering the beacons, so the scanning station (X2) will find the beacons one followed by the other and so on, just after switching to the next channel.

Passive scan device discovery algorithm — Flow diagram in figure 5.5 shows a passive scan version of the device discovery algorithm with Linux shell pseudo-code annotations.

Active scan device discovery

In active scanning, the scanning station (X2) is the one who initiates the process by broadcasting a probe request frame on the channel it is scanning on and all MP70s within range respond with a probe response. Active scanning enables stations (X2s) to receive immediate response from MP70s, without waiting for the beacons transmission. The issue, however, is that active scanning imposes additional overhead on the network because of the transmission of probe and corresponding response frames.

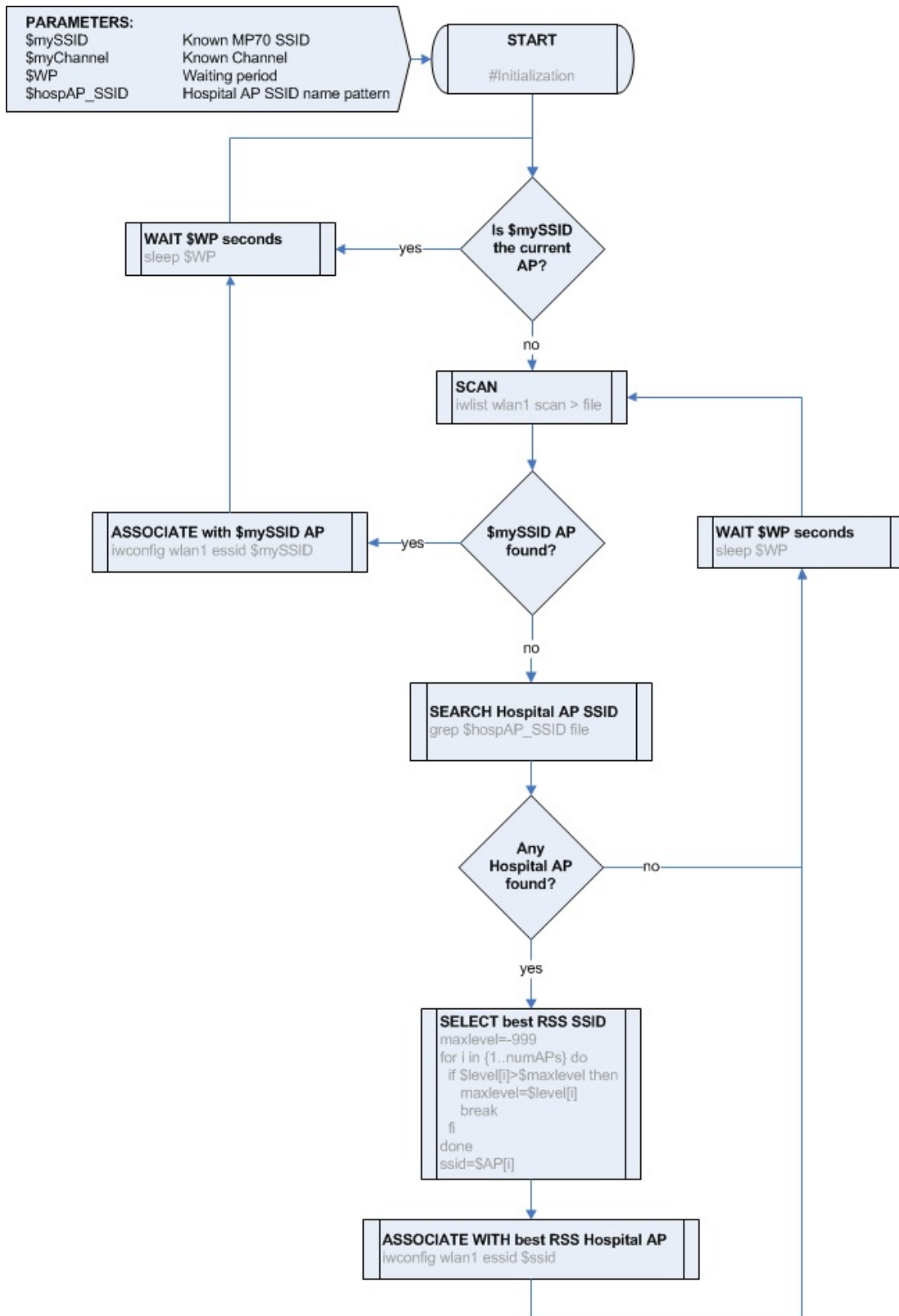


Figure 5.5: Device Discovery algorithm (passive)

Optimisation — Active scan is faster than passive scan by itself, but there are also a number of strategies to optimise it:

- Interleave scan periods with data transfer periods, taking advantage of the Power Save Mode to protect data loss.
- Send probe requests just in a subset of non overlapping channels (i.e. 1, 6 and 11), which could be chosen by the IT management at the hospital.
- Include data from known neighbouring MP70s in the beacons (in Additional Elements or in multiple SSIDs belonging to the same MP70).
- Or even associate to the first MP70 found, get precise information from the application layer (out of the scope of this study) at the backend, and switch directly to the proper channel.

Passive scan device discovery algorithm — Flow diagram in figure 5.6 shows an active scan version of the device discovery algorithm with Linux shell pseudo-code annotations.

5.2.3 Alternative solutions considered

There are two general methods for the initial setup to establish a wireless network and its settings or setup credentials: In-Band and Out-of-Band approaches.

In-band approaches do not need any additional hardware or device, while using the main wireless communication medium/protocol.

- Advantage: for many devices this means “just software”.
- Disadvantage: trade-off between simplicity (ease-of-use) and security/reliability is inevitable.

Proximity based pairing — A less trustworthy (in principle) approach would be to carry out a proximity based pairing. It should address the pairing issue determining which device to connect to just by the distance to the other device, pairing to the closest one while the nurse would put the portable device in proximity to the corresponding bedside monitor.

There is at least one interesting example[31] of a proximity based mechanism, called *Amigo*, to authenticate co-located devices using knowledge of their shared radio environment as proof of physical proximity. The evaluation results show that the *Amigo* technique is robust against a range of passive and active attacks. The key advantages of the technique are that it does not require any additional hardware to be present on the devices beyond the radios that are already used for communication, it does not require user involvement to verify the validity of the authentication process, and it is not vulnerable to eavesdropping.

Out-of-band approaches could also be an option for addressing the initial pairing and patient assignment. As it is proposed in [30], third devices can be used to establish the link between

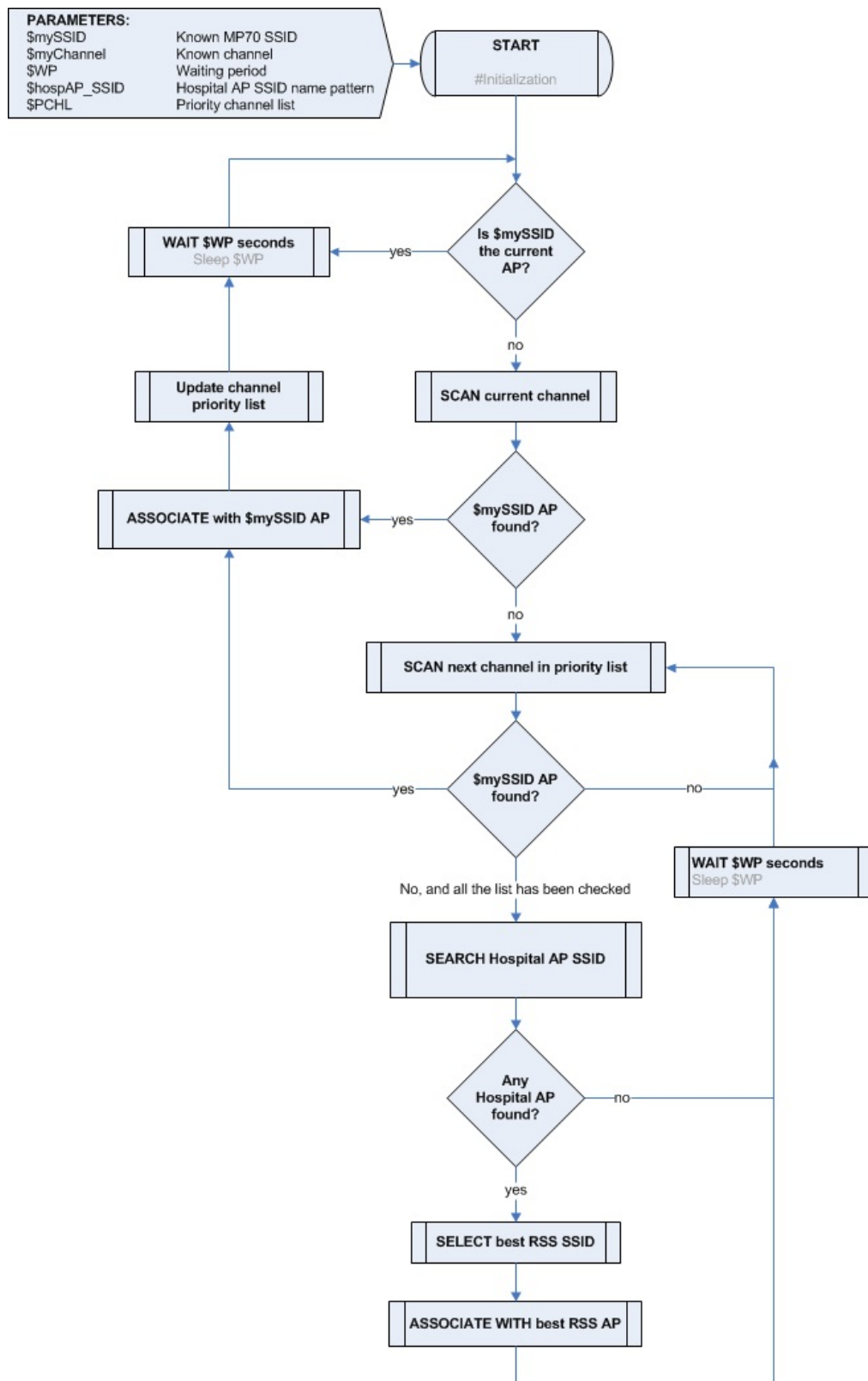


Figure 5.6: Device Discovery algorithm (active)

two devices. In that article, a set-up pen is proposed as the third device to intervene in the mechanism. This set-up pen is a small device used to send a unique identifier for starting the set-up procedure between two Medical Sensor devices. Assuming that upon entering the hospital each patient will be equipped with his patient identifier, which is attached to the patient's body, in any sort of bracelet, sticker or tag. The patient identifier contains the patient's name and other demographic data. To pair a medical sensor or monitoring display to the patient, the clinician uses his personal set-up pen and points to the patient identifier and then to the sensor to be paired (or vice versa) through sending a coded IR signal, after activating a button on the set-up pen. Every clinician would have his own personalized portable set-up device, which would send an unique ID via an infra-red signal. The ID sent by the set-up device would uniquely identify the clinician. The patient identifier node would store the clinician's identification that started the association.

NFC — An up-trend technology in out-of-band pairing, that could be considered is Near Field Communication or NFC. Unlike radio-transmission based wireless communication like 802.11, NFC transmits data via inductive loading. This limits the working range of NFC links to a few centimeters (between 10 to 25 cm of range usually). In that sense, NFC required close proximity provides with a more secure Out-of-Band channel than the more generic RFID technology allows. While it represents a good fit for many use cases, as cheap passive RFID tags are used nowadays in a broad variety of sectors, RFID has some issues: the range of the communication could be drastically increased by eavesdropping with a very directive antenna, up to 100 meters. Nevertheless, there are situations in which the “almost touching” nature of NFC may, for hygiene reasons, be inappropriate and for which the notion of proximity could be better suited by a larger distance. Lastly, NFC does add additional cost, size and weight to a mobile device in addition to the standard or “far-field” communication already present.

In conclusion, taking into account the scenario requirements related to hardware, as in subsection **3.2.3**, we discarded **Out-of-Band alternatives for addressing the pairing** issues, focusing on using an in-band approach. Devising our own strategies to **exploit the 802.11 MAC layer and 802.11 services to implement pairing and device discovery mechanisms**, we avoided making assumptions on the clinical and administrative procedures at the hospital, as the possible use of patient identification tags or bracelets.

5.3 Solution design description

Our solution is based on the exploitation of the 32-byte SSID periodic broadcasting in Beacon frames. This feature is exploited both in the X2 portable monitor and in the MP70 bedside monitor.

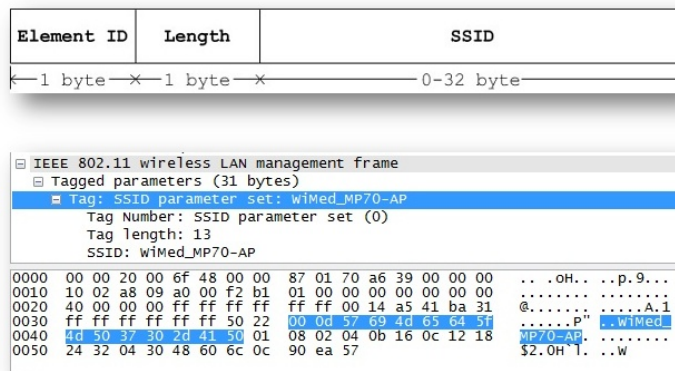


Figure 5.7: SSID field schema and SSID example in a packet capture

In the X2, the SSID opportunistic use is achieved alternating the usual station mode (STA mode) for a typically client device in a infrastructure Wi-Fi network to connect to the MP70, with operation in access point mode (AP mode) to be able to broadcast relevant information through the SSID of the X2's AP. During AP mode operation in the X2, the association or connection of other stations to it is not allowed, the only finality of this operation is to broadcast information openly in AP beacon frames.

The multi-SSID feature that SoftAP allows, used in the MP70 bedside monitor, allows us to broadcast different information, IP addresses, statuses, patient IDs, etc. even if an AP with a useful SSID broadcasting does not allow any other device to connect to it.

To give an abstract description of the behaviour of the system the state diagram of both, MP70 bedside monitor and X2 portable monitor units, are shown in figures 5.11 and 5.12, described in section 5.3.1.

Regarding the relations, between devices and patients, and their cardinality the following considerations must be taken into account:

- Every patient can only be associated to one X2 portable monitor; as the measurement cables tie physically the patient together with its measuring X2 portable monitor. If the X2 batteries run out of charge, the device will be replaced with another fresh one but at any moment the patient will be associated only with one X2. For that reasons the **relation between patients and X2s is one to one (1:1)**.



Figure 5.8: X2 portable monitor and measuring cables

- An X2 can connect to many MP70s in its vicinity depending on its location: in a hospital room, in a surgery operation theatre, in an emergency room, in an intensive care unit... For that reasons the **relation between X2s and MP70s is one to many (1:N)**.



Figure 5.9: Different uses for MP70 monitor: bedside, anaesthesia and operation room configurations

- The **relation between patient and MP70** is, therefore also, **one to many (1:N)**.

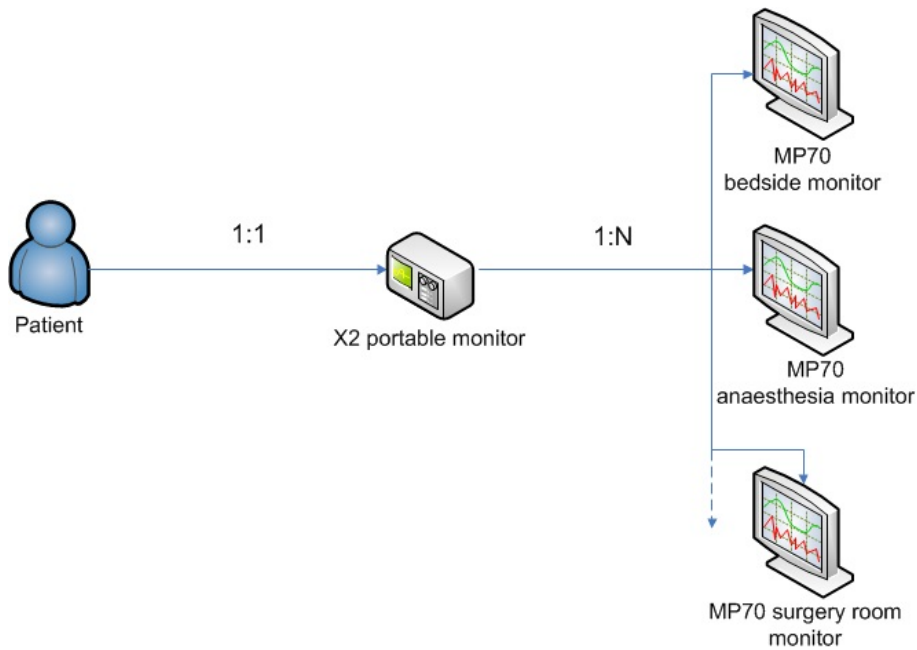


Figure 5.10: Cardinality relations between patients, portable monitors and bedside monitors

5.3.1 State diagrams

MP70 bedside monitor state diagram – The state diagram of the patient monitoring unit, the MP70 bedside monitor, is composed of three states as shown in figure 5.11: *FREE*, *LINKED* and *UNLINKED*.

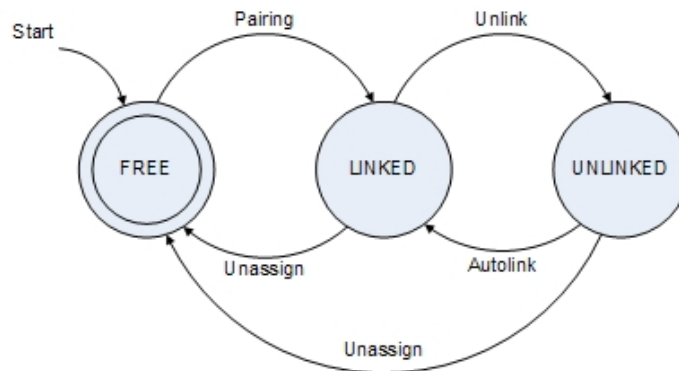


Figure 5.11: MP70 bedside monitor state diagram

- The starting state is *FREE*. Initially the unit is not assigned to any patient, and there is no data link to any X2 portable monitor, the link is not established.
- After the pairing procedure with an X2 portable monitor, marked by the transition *Pairing*, the next state is *LINKED*. In this state the unit is assigned to the patient indicated by the *PatientID*, that is generated and transmitted by the X2 portable monitor to the MP70

bedside unit as it is illustrated in figures 5.14 and 5.15. Besides the data link is established, therefore the patient’s physiological data can be displayed and forwarded to the Hospital access point.

- Should the patient be transferred to a different location equipped with MP70 bedside monitoring units, the transition *Unlink* would be effectuated, passing to *UNLINKED* state. In this third state the unit is still assigned to the same *PatientID* while the data link is not in use.
- Symmetrically, the unit will search periodically for the presence of the former X2 portable monitor in its coverage range, following the *Autolink* transition if found, going back to *LINKED* state.
- Alternatively, the MP70 unit would be *FREE* again if it was manually *Unassign*’ed.

To sum up, table 5.1 shows the link and patient assignment status for the three possible states of the patient monitoring unit.

		States		
		FREE	LINKED	UNLINKED
Link		Unestablished	Linked	Unlinked
Patient assignment		Unassigned	Assigned	Assigned

Table 5.1: Link and patient assignment status for the MP70 bedside monitor’s states.

X2 portable monitor state diagram – The state diagram of the measuring unit, the X2 portable monitor, is composed of three states, as shown in figure 5.12: *FREE*, *ASSIGNED* and *LINKED*.

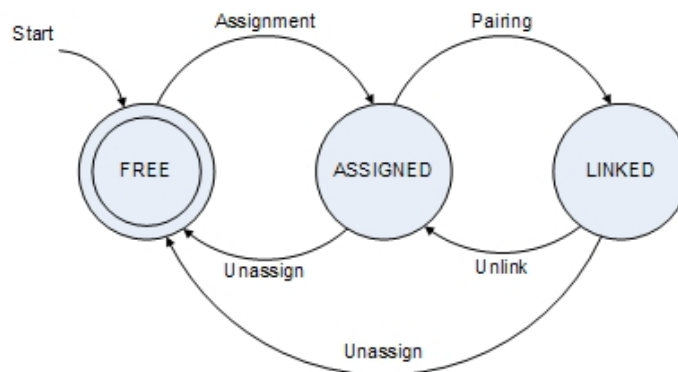


Figure 5.12: X2 portable monitor state diagram

- The starting state is *FREE*. Initially the unit is not assigned to any patient, and there is no data link to any MP70 bedside monitor, the link is not established.
- When a patient is admitted, in the admission desk the patient demographics are retrieved from the HIS (Hospital Information System) and downloaded into the fresh X2. The X2

portable monitor will then generate a random `PatientID` number, in order to broadcast it for the pairing purposes, without revealing patient data over the air in clear text (as the SSID is always broadcasted in clear). It will become an *ASSIGNED* unit then, after the *Assignment* process finishes, ready to be paired with an MP70 bedside monitor.

- Then, after the subsequent pairing procedure with an MP70 bedside monitor, marked by the transition *Pairing*, the next state will be *LINKED*. In this state the unit is still assigned to the patient. Besides the data link is established, therefore the patient's physiological data is sent to the MP70 to be displayed and forwarded to the Hospital access point.
- Should the patient be transferred to any different location, the transition *Unlink* would be effectuated, passing to *ASSIGNED* state again. In this state the unit is still assigned to the same `PatientID` while the data link is not available. The unit will be scanning, looking for its previously paired MP70 or any other available MP70 to connect to, through the *Pairing* to go back to *LINKED* state again. If there are no available MP70, it will also try to connect to the hospital APs in range. This connection to the hospital legacy APs doesn't modify the current state, *ASSIGNED*.
- In case the X2 portable monitor runs out of battery², it would stop transmitting and storing patient data before automatically being *Unassign*'ed, so that a fresh X2 assigned to the patient could substitute it.
- Alternatively, the X2 unit would be *FREE* again if it was manually *Unassign*'ed from any of the other states.

To sum up, table 5.2 shows the link and patient assignment status for the three possible states of the X2 portable monitoring unit.

		States		
		FREE	ASSIGNED	LINKED
Patient assignment	Link	Unestablished	Unestablished	Linked
		Unassigned	Assigned	Assigned

Table 5.2: *Link and patient assignment status for the X2 portable monitor's states.*

5.3.2 Pairing process diagram

Taking into account the cardinality relations exposed in figure 5.10, we decided to design the pairing process as a *sensor-initiated* process, versus an *infrastructure-initiated* approach. This means that the X2 portable monitor, which has a 1:1 relation with the patient (as the connected measuring cables clearly indicate), initiating the pairing process with an MP70 bedside monitor would have much more sense than the other way around, one of several MP70 bedside monitors which the patient could be assigned would initiate the pairing process.

²That occurrence should not take place before 72 hours of continuous operation, considering the average inpatient hospital stay, according to [26].

The pairing process, including a **device discovery** phase, is described visually in flow diagrams which illustrate the user interaction on the aforementioned process, figures 5.14 and 5.15. The legend for the flow diagrams, figure 5.13, introduces the symbols describing the process in the flow diagrams.

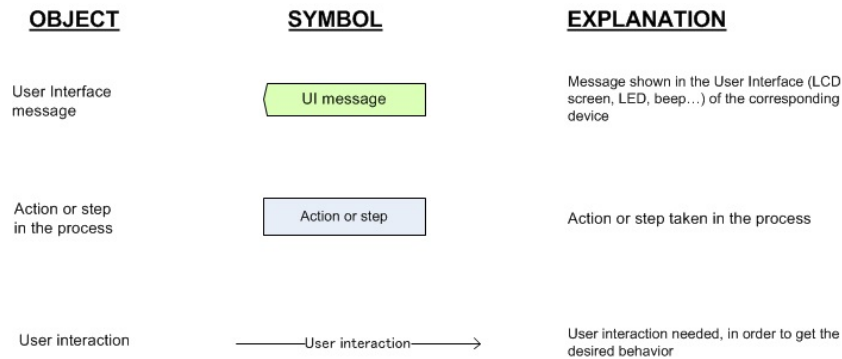


Figure 5.13: *Pairing process and user interaction flow diagrams legend*

Description of the pairing process diagram

- Initially (upper part of figure 5.14) the X2 is not assigned to any patient, and there is no data link to any MP70 bedside monitor, the link is not established.
- The MP70 is neither assigned to any patient, and there is no data link to any X2 portable monitor. The MP70 is constantly scanning as a client (STA) and looking for an SSID indicating there is an unpaired X2 assigned to a patient.
- A patient is admitted, at the admission desk the patient demographics are retrieved from the HIS and downloaded into the X2. The X2 generates a random **PatientID** number, for pairing purposes without revealing patient data in the SSID information exchange. The X2 is thus assigned to a patient, ready to be paired with an MP70 bedside monitor.
- The Device Discovery phase starts when the user triggers at the X2 the scanning for an unassigned MP70. If any free MP70s are found, the X2 changes to AP mode and broadcasts its beacon in the channel where it has found the free MP70.
- Meanwhile the MP70, which was scanning for an unpaired X2 assigned to a patient, detects a candidate X2 to be paired to. So it changes its secondary SSID to broadcast the candidate **patientID** of the X2, and includes its MAC (broadcasted previously in the X2 beacon frame) in the allowed connection list. At the same time, the MP70 shows with an extended GUI in its bedside big screen, the **PatientID** and its IP address. In that way the user is able to confirm that the **PatientIDs** coincide in both devices. If more than one MP70, in the same room or hospital floor, would be free and expecting to connect to an unpaired X2 assigned to a patient, there could be a possible confusion between MP70s. To avoid that situation, a list of candidate MP70s is displayed in the reduced GUI of the X2. So the user is able to choose from the list, which IP corresponds to the desired MP70 which is at the same time displaying its IP through the screen.

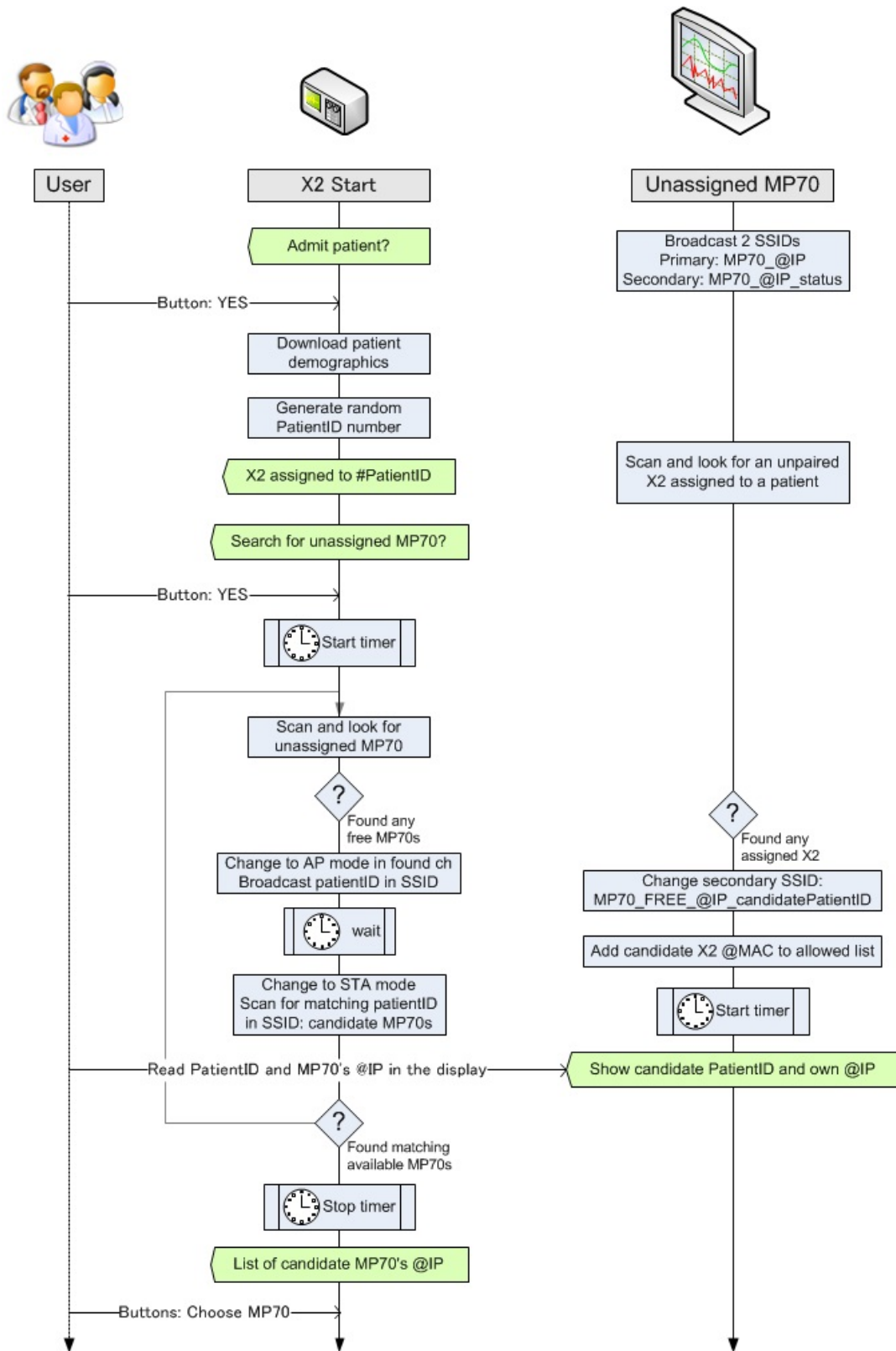


Figure 5.14: Pairing process and user interaction, part 1

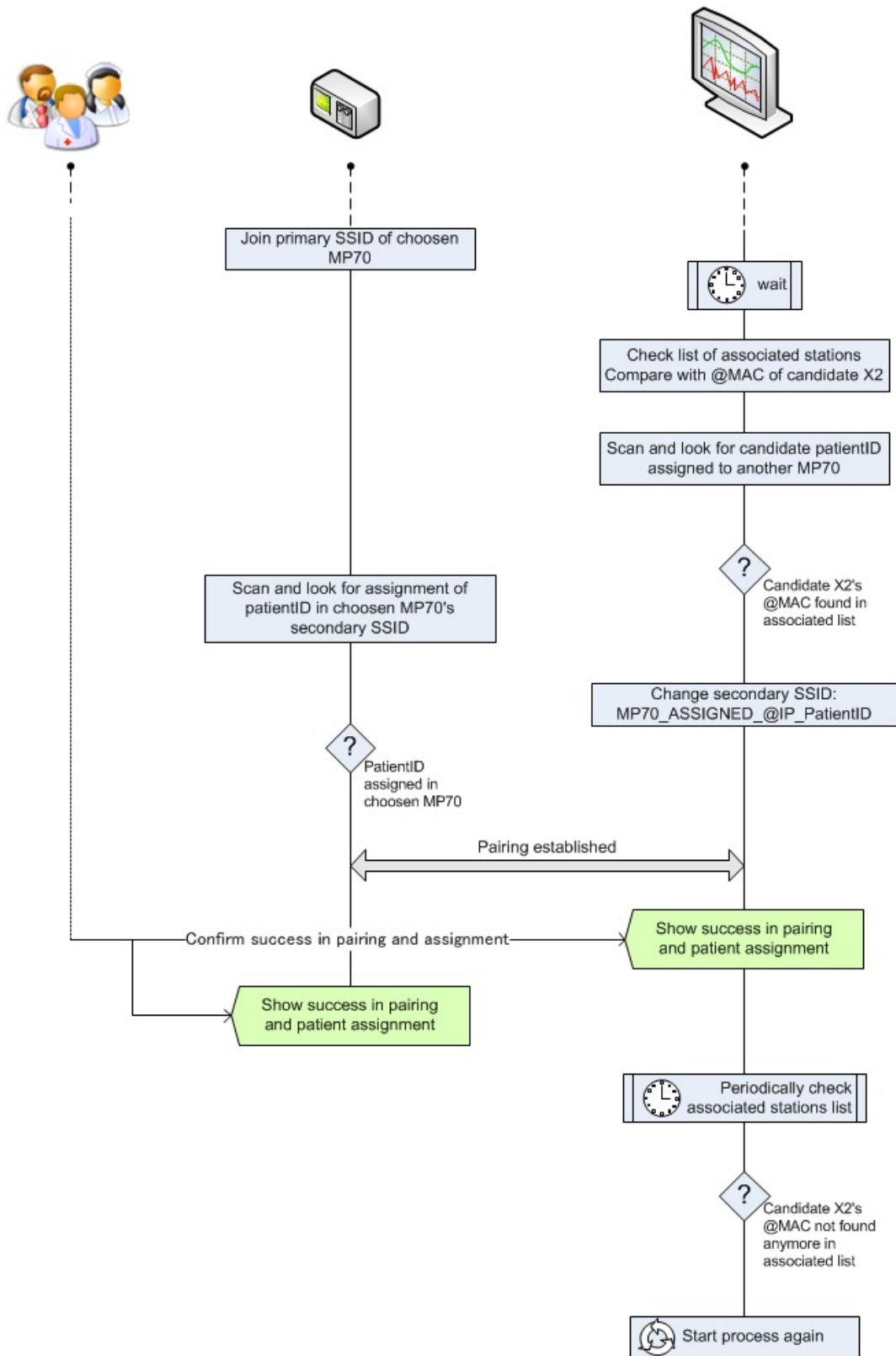


Figure 5.15: Pairing process and user interaction, part 2

The process follows in the upper part of figure 5.15 after the user chose the desired MP70 in the X2 GUI.

- The X2 associates as a client (STA) to the primary SSID of the chosen MP70.
- The MP70 confirms that the associated STA corresponds with the expected candidate X2 and the expected PatientID and broadcasts its status change in the secondary SSID.
- The X2 confirms that the MP70 is broadcasting the expected PatientID
- When both devices confirmed the assignment one in each other, the pairing is established and the pairing process ends, showing the success in both devices GUIs.
- The MP70 remains periodically checking if the paired X2 is still associated. If not, it changes its status accordingly (as it is not linked anymore) and starts the scan process again.

Chapter 6

Implemented platform

The current chapter covers the design and development of an open source implementation in an embedded Linux platform, based on the selected SoftAP Wi-Fi technology, the IEEE 802.11g specification and the designed solution according to the decisions taken in previous chapters 4 and 5.

After analysing the existing available wireless technologies and Wi-Fi specifications, and devising the principles of operation of our *dual-link solution* for the wireless patient monitoring, we had to decide on the specific hardware technology to implement a Soft AP dual-link prototype platform.

The main goal of this part of the project was to procure a physical prototyping embedded platform on which implement the dual-link solution we devised, to have it running under desired test conditions in order to validate, carrying out the experiments described in chapter 7, whether this prototype satisfied the requirements indicated in section 3.2.

Key points considered for the implemented platform:

- Proof of concept: to show feasibility with basic functionality.
- Open source benefits: flexibility, reliability, stability and auditability, among others.
- Hardware platform:
 - Implementation on a platform of embedded devices.
 - Each prototype device could act as a different logical device (MP70, X2).
 - Portability, possibility of battery-powered devices.
 - Easier transfer, easier setup: plug and play.
 - Easy interaction with User Interface: buttons, displays and LEDs (instead of a complex or unrealistic GUI through PC simulations).

- Embedded Linux routers for an improved demonstrableness and connectivity.

6.0.3 Linux-based router embedded platform

For the aforementioned reasons, we chose a Linux-based router embedded platform in which to demonstrate the function of our implementation. For that purpose we utilized a Linux based *Linksys WRT54GL* router by Cisco. Its adaptability, reliability, stability and ease of tuning given the native Linux operating system was a primary reason to opt for that hardware, together with the 802.11g support, as it was chosen above the rest of the considered technologies reviewed in section 4.3.



Figure 6.1: *Linksys Linux based WRT54GL router by Cisco*

This router admits several customized Linux firmware available from third parties, since it counts on a wide amateur scene of open source users and developers. These firmwares offer, for developers, an appropriate framework to build an application without having to build a complete firmware around it; and for users, the ability for full customization.

Precisely, the Linksys WRT54GL counts on internal available General Purpose Input/Output (GPIO), JTAG (JP1) and UART (JP2) serial ports. Several modifications can be made by using these ports. Figure 6.2 shows the router embedded board and its chip distribution.

The WRT54GL is based on the Broadcom BCM5352EL system, a low-cost, high performance system-on-chip (SoC) for residential and small office markets equipped with a 200-MHz MIPS32 CPU core with 16 KB instruction cache, 8 KB data cache, and 256 B prefetch cache and a Memory Management Unit (MMU) for high-level Real-Time Operating System support.

The BCM5352EL SoC integrates the high-performance MIPS32 processor, IEEE 802.11 b/g MAC/PHY, SDRAM controller, and a configurable five-port Fast Ethernet (FE) switch. This system provides with wireless LAN connectivity supporting data rates of up to 125 Mbps that is backward-compatible with standard 802.11 b/g.

For further detail see Appendix B.1.

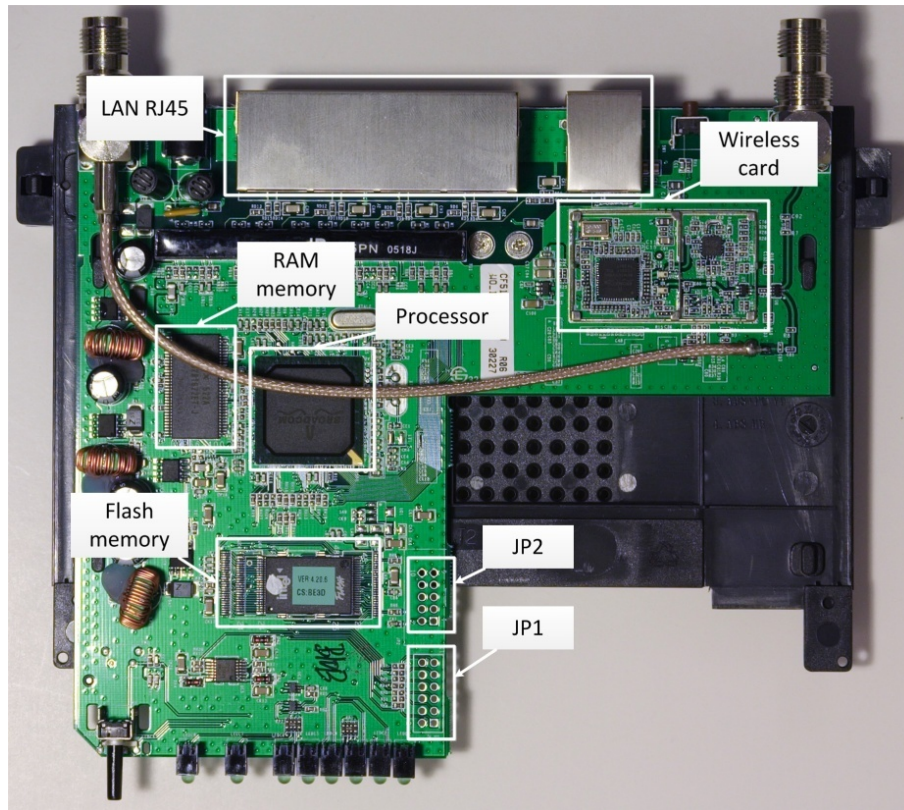


Figure 6.2: *Linksys WRT54GL board distribution*

6.0.4 Firmware for the embedded-Linux router

The router we chose has several customized Linux firmwares available from third parties, since it counts on a wide amateur scene of open source users and developers. These firmwares offer, for developers, an appropriate framework to build an application without having to build a complete firmware around it; and for users, the ability for improved customization compared with the stock firmware.

In table 6.1 we collected the four most known firmwares that run on the WRT54GL router, comparing their features and compatibility.

Among all the available options we chose two different firmwares for supporting the required functionalities in both devices that would represent the X2 portable monitor (which requires the implementation of a simple GUI, to allow user interaction) and the MP70 bedside monitor (which requires SoftAP operation and multiple SSIDs support), respectively:

Tomato Linux firmware

Tomato uses the Linux kernel and most of the utilities provided in the original Linksys' WRT54GL source code as a starting point. Besides major GUI changes respect the original Linksys web interface with real-time bandwidth and connection monitoring, the major part of the code inside has undergone extensive improvements for outstanding stability, fix known bugs and problems

Features	HyperWRT	Tomato	DDWRT	OpenWrt
WRT54GL v1.x Support	Yes	Yes	Yes	Yes
Adjustable Transmit Power	Yes	Yes	Yes	Yes
Wireless Channels	14	14	14	14
Telnet	Yes	Yes	Yes	Yes
Secure shell SSH	Yes	Yes	Yes	Yes
Startup/Firewall Scripts	Yes	Yes	Yes	Yes
Wireless MAC address clone	No	Yes	Yes	Yes
JFFS2 R/W Partition	No	Yes	Yes	Yes
WDS Support	Yes	Yes	Yes	Yes
Max Wireless Associated Clients	No	Yes	Yes	Yes
Ad-hoc Mode	Yes	Yes	Yes	Yes
Multiple SSID	No	No	Yes	Yes
AP+WDS	Yes	Yes	Yes	Yes
Soft-AP (simultaneous STA+AP)	No	No	No	Yes
VLAN Support	No	Yes	Yes	Yes
IPKG package installation	No	No	Yes	Yes
Mesh networking	No	No	No	Yes
iwconfig tool	No	No	Yes	Yes
Programmable SES button (to launch custom scripts)	Yes	Yes	Yes	Yes
Regular updates and bug fixes	Latest 2006	Yes	Yes	Yes
Type of shell	Busy Box ash			
Shell support arrays	No	No	No	No

Table 6.1: Embedded Linux distributions, features and compatibility

Key Features			
HyperWRT	Tomato	DDWRT	OpenWrt
Fidelity to the official Linksys firmware	Easy to program internal serial port for UI (LCD, buttons, etc.)	Micro firmware version fits in 2MB	Highly tunable wireless management through Linux shell
	Lightweight and improved stability		SoftAP support (simultaneous AP+STA) and multiple SSIDs

Table 6.2: Embedded Linux distributions, key features

in Broadcom-based firmware, and optimize and reduce the size of the OS to the lightest possible.

Specifically we chose Tomato firmware because of its **incomparable stability** (reduced tendency to reboots), and because it provides with **support for writable JFFS2 filesystems**, enabling the programming of additional extension boards through the serial interfaces.

OpenWrt

OpenWrt is described as a Linux distribution for embedded devices. Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management.

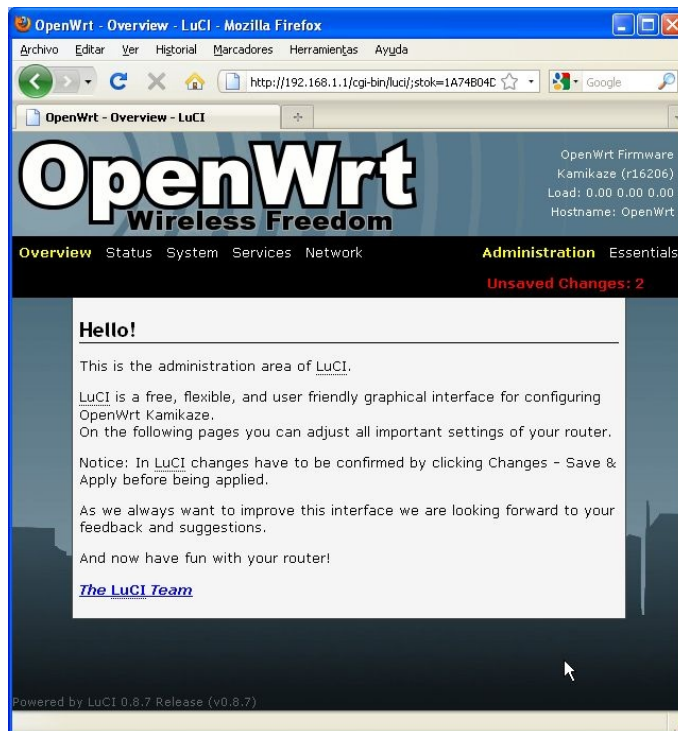


Figure 6.3: OpenWRT configuration web interface

with no moving parts. URL: <http://www.via.com.tw/>

Soekris

A number of Soekris models work well as access points, with and without PCMCIA. All Soekris boards boot from Compact Flash, and come standard with multiple Ethernet interfaces, a mini-PCI slot, hardware watchdog, serial console, and an AMD 133 MHz processor. They are all fanless boards and use a DC power supply. URL: <http://www.soekris.com/>

OpenBrick

Another popular embedded solution is the OpenBrick. The typical OpenBrick has a 300 MHz (fanless) Geode processor, boots from Compact Flash and has on-board NIC and PCMCIA slots. It runs on DC power and, unlike the Soekris, also has USB ports (although it does not have a mini-PCI slot). URL: <http://www.openbrick.org/>

6.1 Open source platform implemented

As a first contact with OpenWrt firmware configuration in WRT54GL routers, we developed a preliminary implementation with the most basic *ad hoc* dual-link approach supported by OpenWrt over the WRT54GL: WDS.

This basic UI X2 implementation with WDS link in the MP70 is presented in Appendix C to complement the final implementation described in this chapter.

6.1.1 Soft-AP with OpenWrt and Tomato in WRT54GL routers equipped with UI

Materials

- 2 x Linksys WRT54GL router by Cisco with OpenWRT Linux OS version *Kamikaze 8.09.1*.
- Linksys WRT54GL router by Cisco with Tomato Linux OS v1.25
- ICSP 10 pins (5x2) port connector
- AVR-MT-128 display and interface board (fig. 6.5):
 - 16x2 LCD display
 - 5 buttons
 - LED, relay, buzzer
 - AVR-MT128 is a simple but powerful board which uses the MCU ATMega128 from Atmel. With its LCD, buttons, relay and variety of interfaces such as RS232 (in two variants - 4 pins and DB9), JTAG, ICSP, Dallas, etc. this board is suitable for a wide variety of embedded systems applications.
- AVR-PG1B (serial port) 10 pin ICSP AVR microcontroller programmer (fig. 6.8).
- Custom 12V battery pack.

For further detail on the hardware specification see Appendix B.

Methods

For representing the **X2 portable monitor with extended User Interface** we used a Linux-based WRT54GL router loaded with Tomato firmware v1.25. We modified it extensive and carefully, so that all the modification components could remain mounted inside of the original

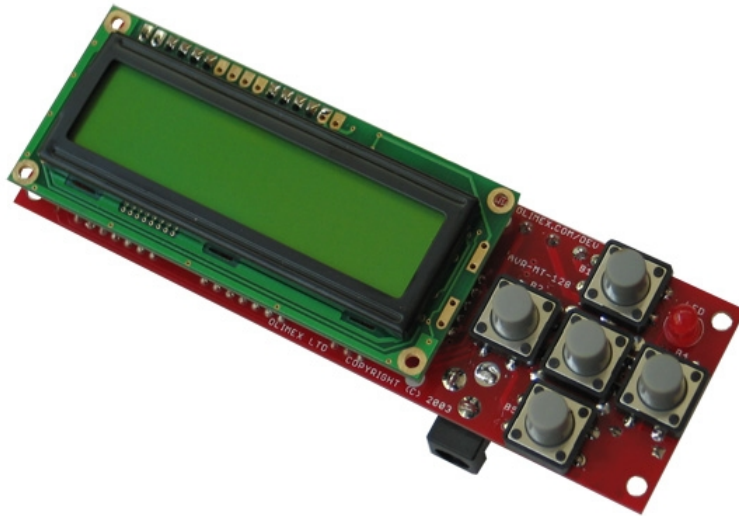


Figure 6.5: *AVR-MT-128 display and interface integrated board*

case, for a cleaner and nicer implementation.

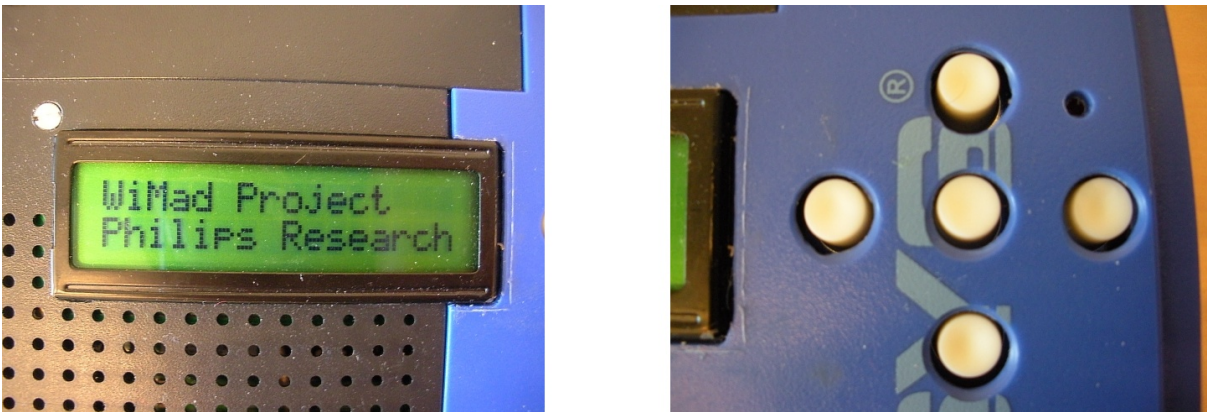


Figure 6.6: *Detail of LCD display and UI buttons installed directly in the router cover*

We drilled holes for mounting the AVR-MT128 board directly on the case, with the LCD screen and the buttons popping out from the upper cover (see figure 6.6). We wired the DC power input from the router to the board input for solidary power of both the router and the board (see figure 6.7).

In order to be able to program the board while it was already mounted inside the router, we drilled a lateral overture and installed a 10 pin ICSP 5x2 connector, wired directly to the ICSP connection in the board.

To connect the router to the AVR board, we wired directly the Tx and Rx of serial port 1 (ttyS1) in the router board with the corresponding connectors in the RS232 header, and the common grounds together.



Figure 6.7: *Detail of power input wired solidary to the router DC input (red and black braided wires)*

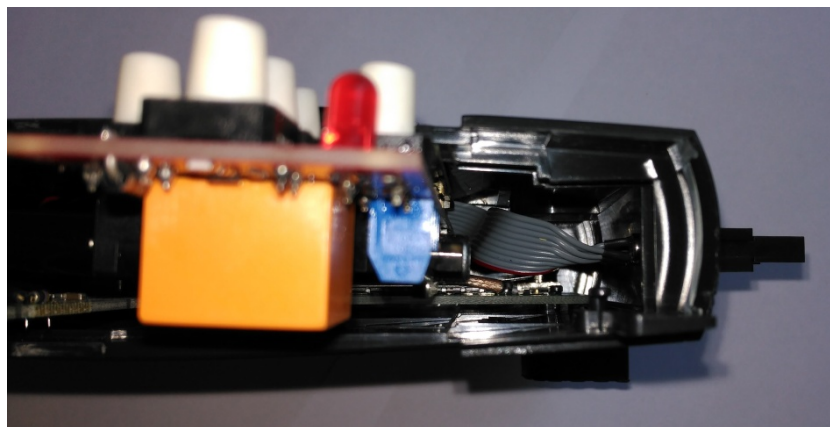


Figure 6.8: *Detail of external ICSP port wired to the AVRMT128 ICSP port (grey bus)*

Pin 1	VCC	Pin 2	VCC
Pin 3	Tx (ttyS1)	Pin 4	Tx (ttyS0)
Pin 5	Rx (ttyS1)	Pin 6	Rx (ttyS0)
Pin 7	N/C	Pin 8	N/C
Pin 9	GND	Pin 10	GND

Table 6.3: *JP2 pinout serial header in WRT54GL*

We programmed the AVR Microcontroller with the help of an AVR-PG1B (serial port) 10 pin ICSP AVR microcontroller programmer, shown in figure 6.10, together with the router to display in the board LCD screen the commands written to the serial port of the router board, and to read the buttons pressed in the board and write the signals to the receptor of the router's serial port.

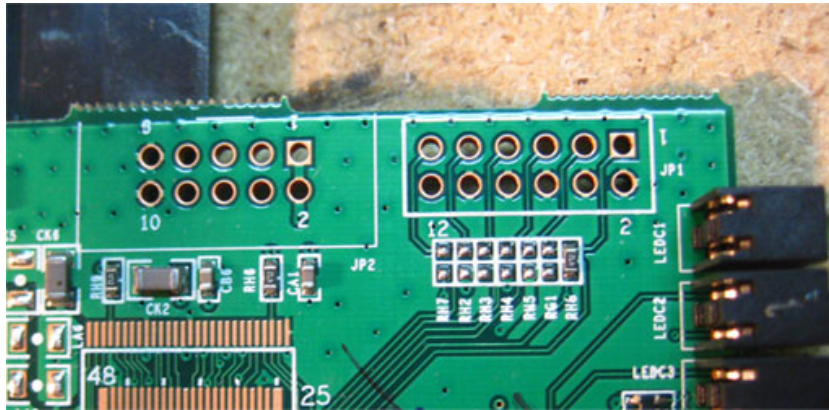


Figure 6.9: JP2 RS232 pinout for serial connection WRT54GL-AVRMT128

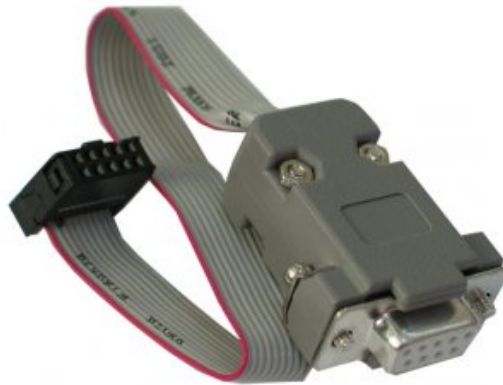


Figure 6.10: AVR-PG1B (serial port) 10 pin ICSP AVR microcontroller programmer

For making the user interaction more complete and demonstrable, we developed an advanced GUI with an interactive menu, fully usable through the navigation keys in the board. Operating the menu, the pairing process was triggered, and the user interaction steps were taken. The development was uploaded to the router as a shell script, implementing the X2 operation as the solution devised in chapter 5, as was described in figures 5.14 and 5.15 which translated to the specific implementation is described in 6.15, 6.16. See appendix D for more detail on the scripts.

Link to demo video demonstrating the GUI interactive menu usage, URL: <https://goo.gl/La5c3r>².

²The URL can be obtained from scanning the QR code image with an Android app like Google *Googles* available at URL: <https://play.google.com/store/apps/details?id=com.google.android.apps.unveil> or any other barcode scanner.



Figure 6.11: QR image link to demonstration video <https://goo.gl/La5c3r>

The internal aspect of the WRT54GL router with AVR MT128 modification is shown in figure 6.12 together with the external aspect and overall result of the advanced UI X2 implementation.

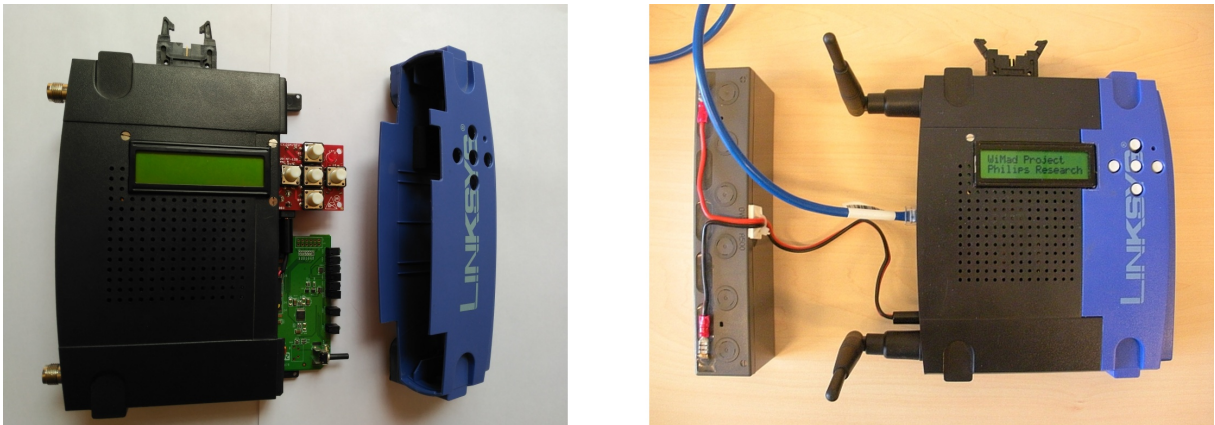


Figure 6.12: Overall result and internal aspect of the WRT54GL router with AVR MT128 modification

To represent the MP70, acting as the dual-link connection device, we used one of the routers loaded with the image of OpenWRT *Kamikaze 8.09.1* version. We developed an script (see the script in appendix D) implementing the MP70 operation as the solution devised in chapter 5, as was described in figures 5.14 and 5.15 which translated to the specific implementation is described in 6.17, 6.18.

The second OpenWrt router was used as an standard AP connected to the wired LAN, representing the hospital AP, as shown in figure 6.19. In that case, the external aspect of both routers representing the MP70 and the Hospital AP did not change externally (figure 6.13), only the network and wireless parameters in the OpenWrt configuration changed from the first implementation, as detailed in Appendix D, section D.2.

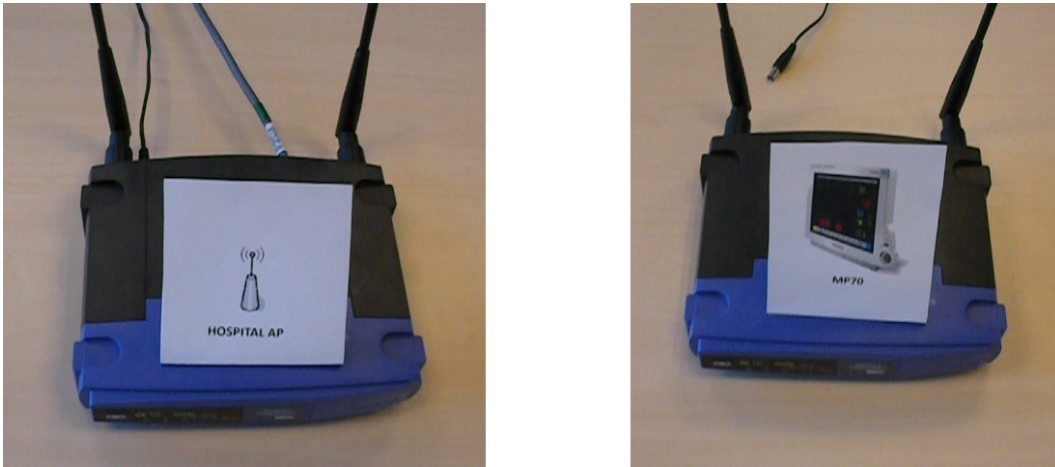


Figure 6.13: Hospital AP and MP70 connected through WDS link

Implemented algorithms

With the use of the `wl` command for accessing and controlling the routers' wireless hardware, we configured the radios to operate in different modes and activate specific functionalities, that cannot be configured with the firmware's web interface. Commands used, shown in order of appearance in the flow diagrams 6.15 to 6.18:

- `wl rand` Returns a pseudo-random number generated with values depending on the wireless controller state.
- `wl -a ADAPTER_NAME COMMAND` Applies the `COMMAND` to the wireless adapter named `ADAPTER_NAME`.
- `wl ap` Set AP mode: 0 (STA) or 1 (AP).
- `wl scan` Initiate a scan.

Default an active scan across all channels for any SSID. Optional argument: SSID, the SSID to actively scan (probe). Options:

```

-s S, --ssid=S           SSID to scan
-t ST, --scan_type=ST   [active|passive] scan type
--bss_type=BT           [bss/infra|ibss/adhoc] bss type to scan
-b MAC, --bssid=MAC     particular BSSID MAC address to scan
-n N, --nprobes=N       number of probes per scanned channel
-a N, --active=N        dwell time per channel for active scanning
-p N, --passive=N       dwell time per channel for passive scanning
-h N, --home=N          dwell time for the home channel between scans
-c L, --channels=L      comma or space separated list of channels to scan

```

NOTE: `wl scan` does not work in AP Mode. To scan, previously the AP mode has to be disabled:

```
wl ap 0
wl scan
wl scanresults
wl ap 1
```

- `wl scanresults` Return results from last scan.
- `wl channel` Set the operating channel. Valid channels for 802.11b/g (2.4 GHz band) are 1 through 14.
- `wl ssid` Set or get the current SSID. Setting will initiate an association attempt if in infrastructure mode, or join/creation of an IBSS if in IBSS mode, or creation of a BSS if in AP mode.
- `wl macmode` Set the mode of the MAC list. 0 - Disable MAC address matching. 1 - Deny association to stations on the MAC list. 2 - Allow association to stations on the MAC list.
- `wl assoclist` AP mode only: Get the list of associated MAC addresses.

Other interesting commands, specifically to toggle and tune the scan process:

- `wl scan_channel_time` Get/Set scan channel dwell time.
- `wl scan_home_time` Get/Set scan home channel dwell time.
- `wl scan_nprobes` Get/Set scan parameter for number of probes to use per channel scanned.
- `wl scan_passive_time` Get/Set passive scan channel dwell time.
- `wl scan_unassoc_time` Get/Set unassociated scan channel dwell time.
- `wl passive` Puts scan engine into passive mode.

Flow diagrams with the shell script implementation detailing the commands used on the pairing process for the X2 portable monitor [6.15](#), [6.16](#) and for the MP70 bedside monitor [6.17](#), [6.18](#). Legend for the flow diagrams: [6.14](#).

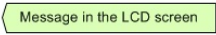
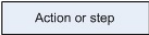
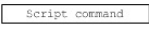

<u>OBJECT</u>	<u>SYMBOL</u>	<u>EXPLANATION</u>
LCD screen message		Message shown in the LCD screen of the corresponding device
Action or step in the process		Action or step taken in the process
Script command		Command to be included in the shell script, in order to get the desired behavior
User interaction		User interaction needed, in order to get the desired behavior

Figure 6.14: *Pairing, assignment and device discovery flow diagrams legend*

Network topology

Figure 6.19 shows the basic setup's network topology. In the figure the basic set formed by a Hospital AP, an MP70 bedside monitor and an X2 portable monitor, is shown together with its network topology details:

- **Hospital AP** has a static hospital LAN network IP address assigned, since it is a fixed device, installed in the ceiling in a specific point, according to the deployment plan which has into account coverage areas and wired accessibility to power and wired network.
- The **MP70** is also a fixed device, installed in the bedside of every hospital room, surgical operation theatre and Intensive Care Unit room, with accessibility to a power plug and under the coverage area of a Hospital AP. Thus, in its STA side it is assigned a static IP address, in the Hospital AP subnet.
- The **X2** is a portable device, which goes together with the patient, where he/she goes. Its relative position and the association with a given MP70 is not fixed given its relative degree of mobility. Thus, it counts on a dynamically assigned IP address by the DHCP server running in the AP side of the MP70 which forms a different subnet.

Figure 6.20 shows a more complex network topology. In the figure the basic set is accompanied by a second MP70 connected to the same Hospital AP, and with an X2 connected to it forming a different subnet, which could be in a different channel from the first MP70 considered. The figure also shows a third X2, assigned to a different patient but unlinked, connected to the MP70 just to forward data to the Hospital network. In a general case it could connect also to the Hospital AP, but it connects to the best RSS available AP, in that case the MP70.

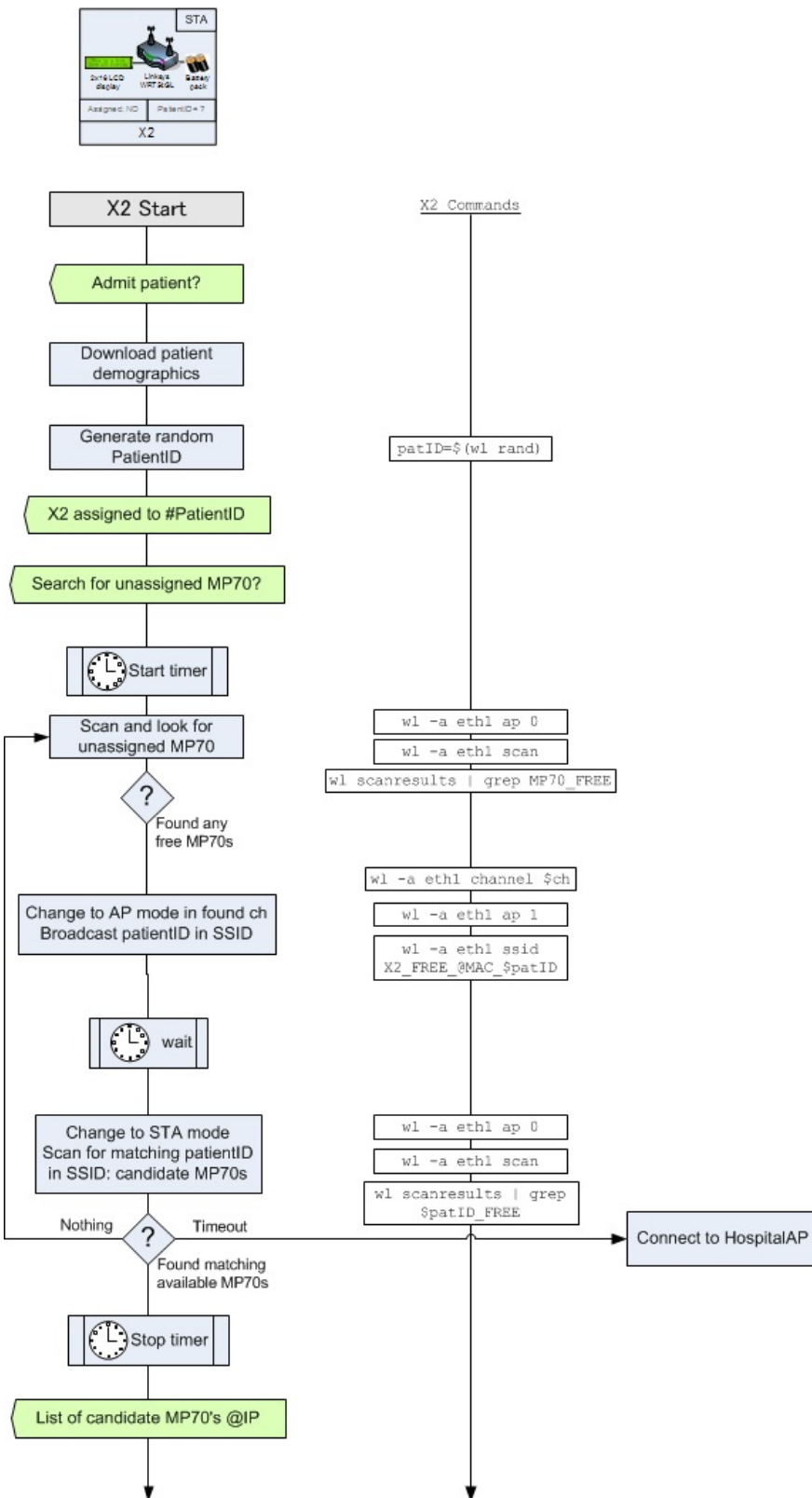


Figure 6.15: Pairing process implementation flow diagram, X2, part 1

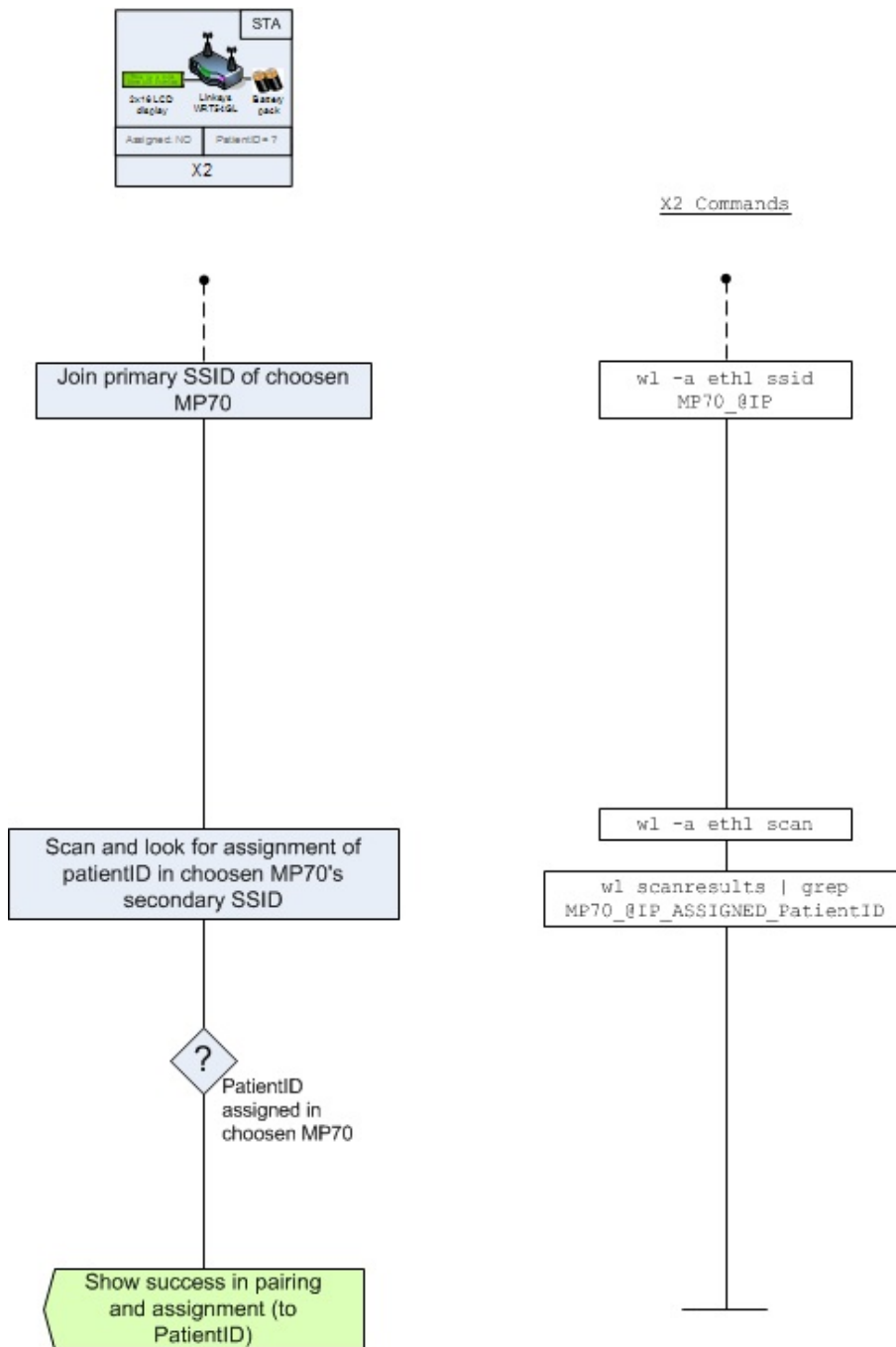


Figure 6.16: Pairing process implementation flow diagram, X2, part 2

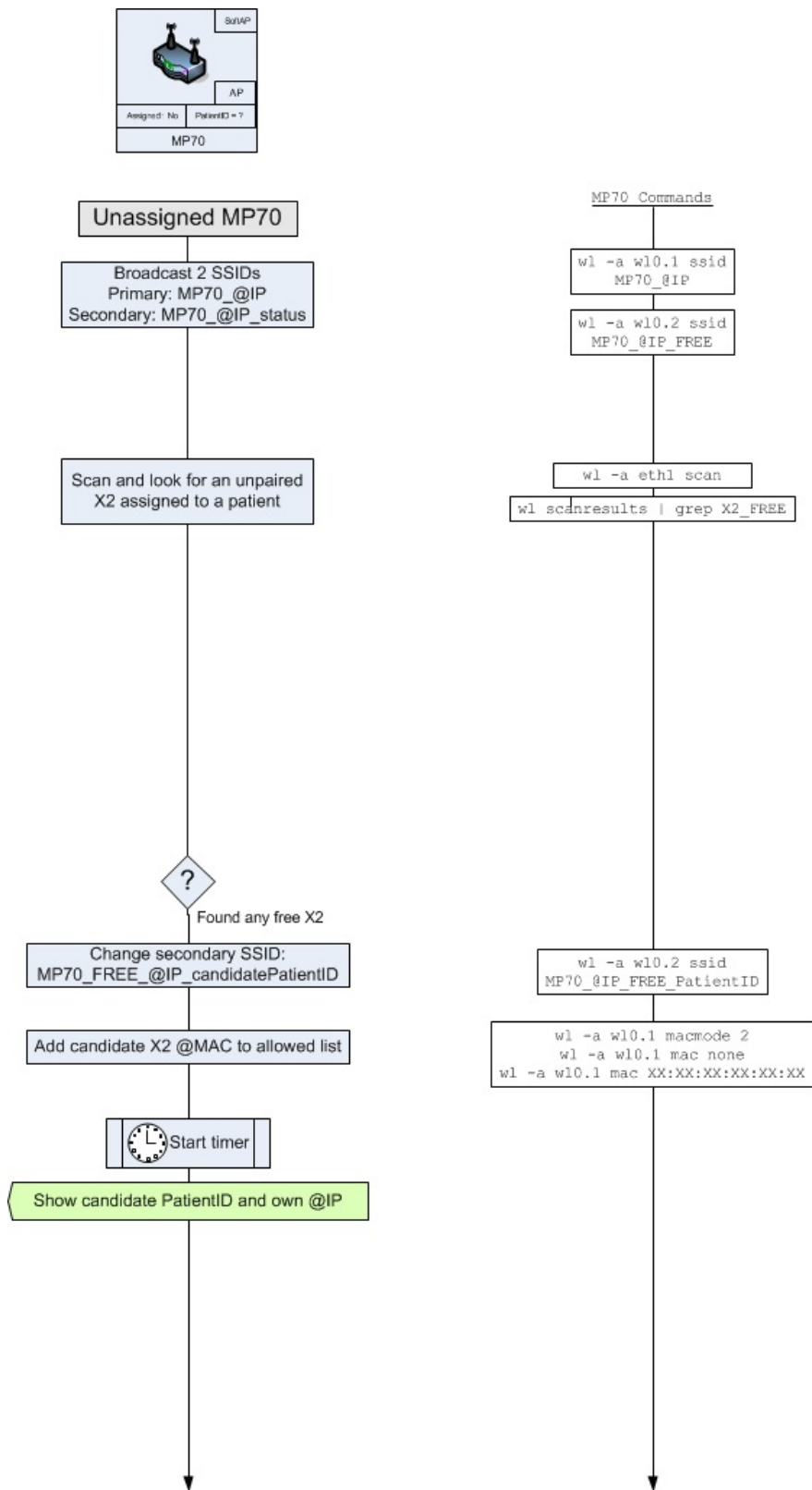


Figure 6.17: Pairing process implementation flow diagram, MP70, part 1

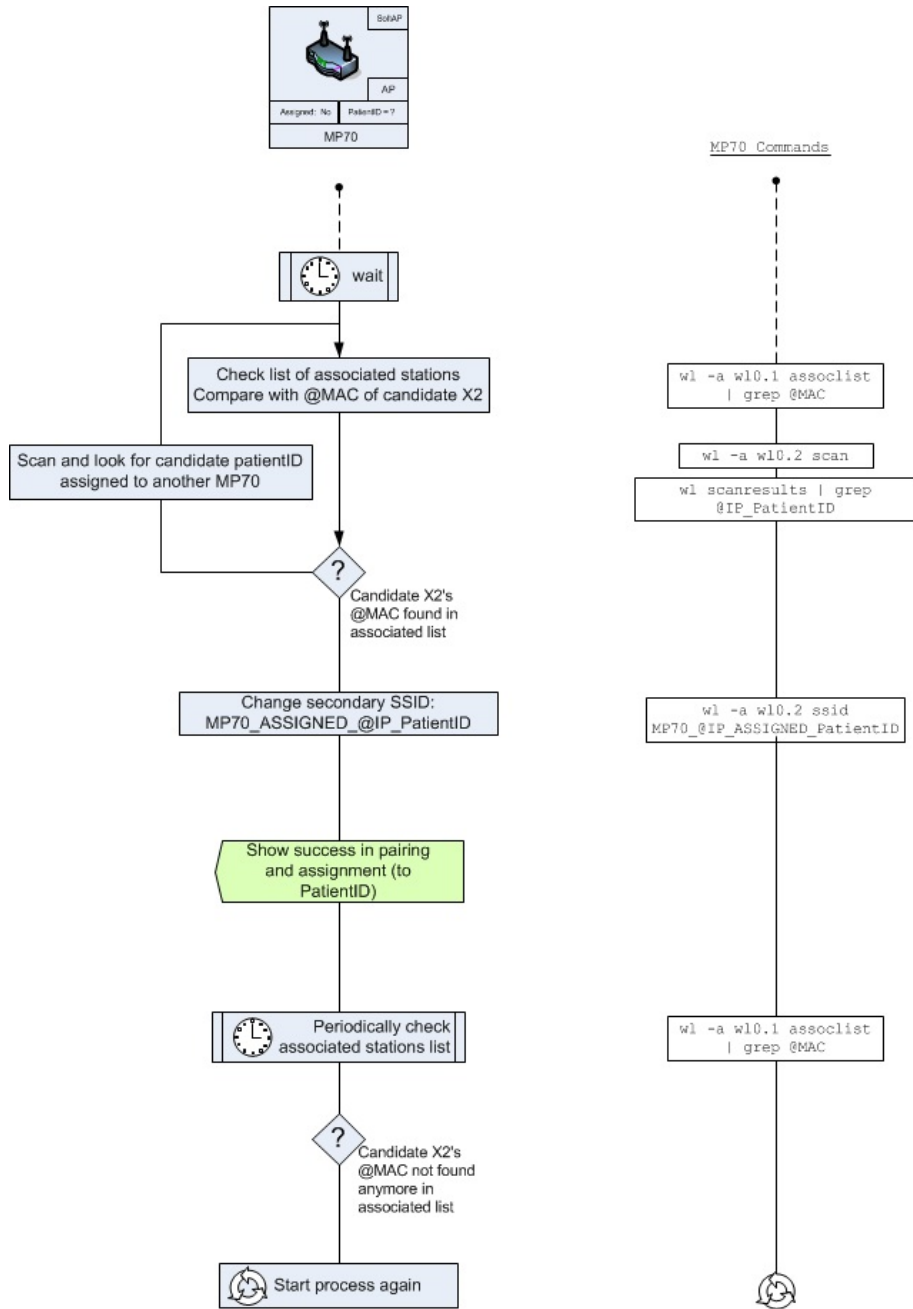


Figure 6.18: Pairing process implementation flow diagram, MP70, part 2

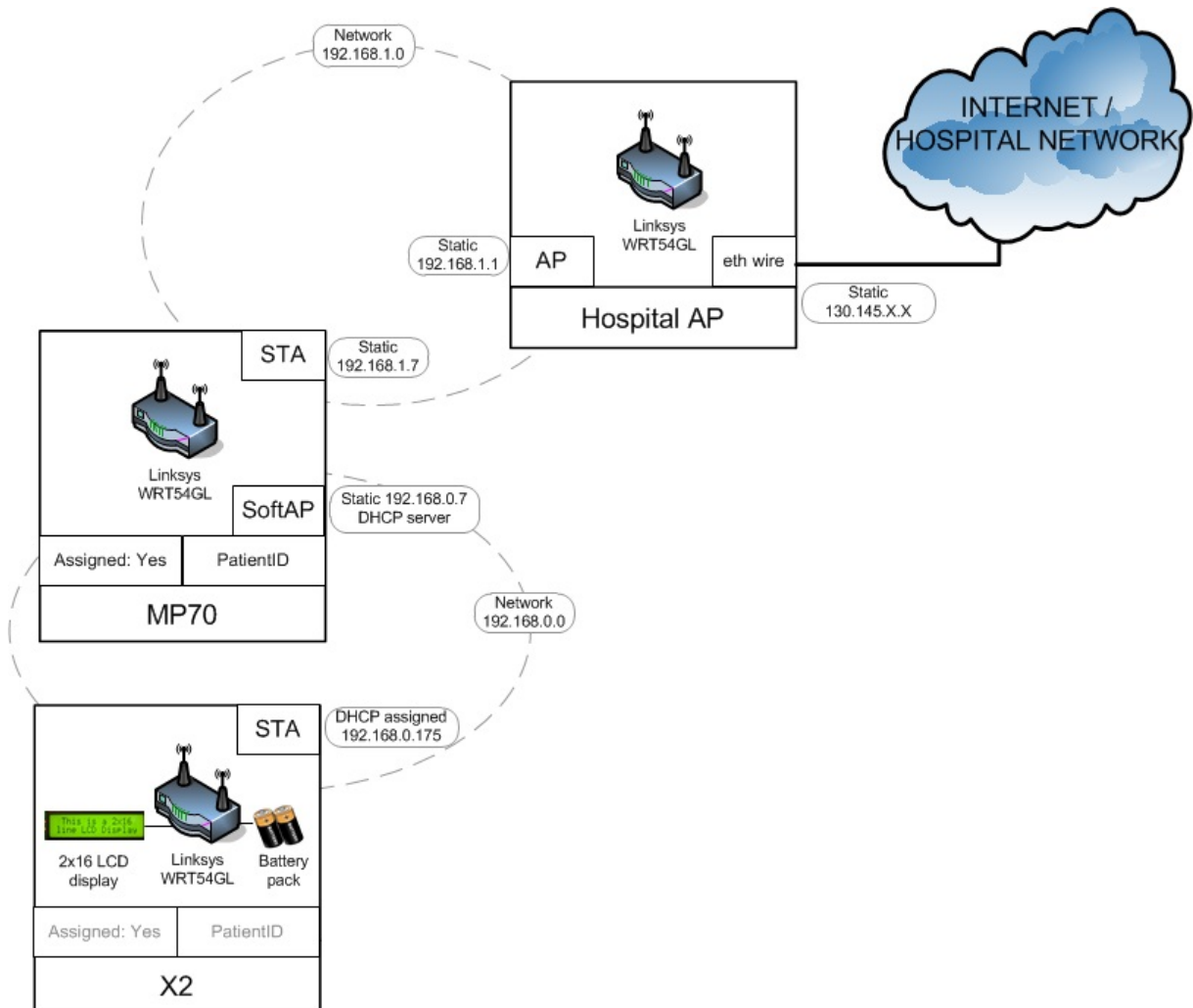


Figure 6.19: Network topology, basic setup

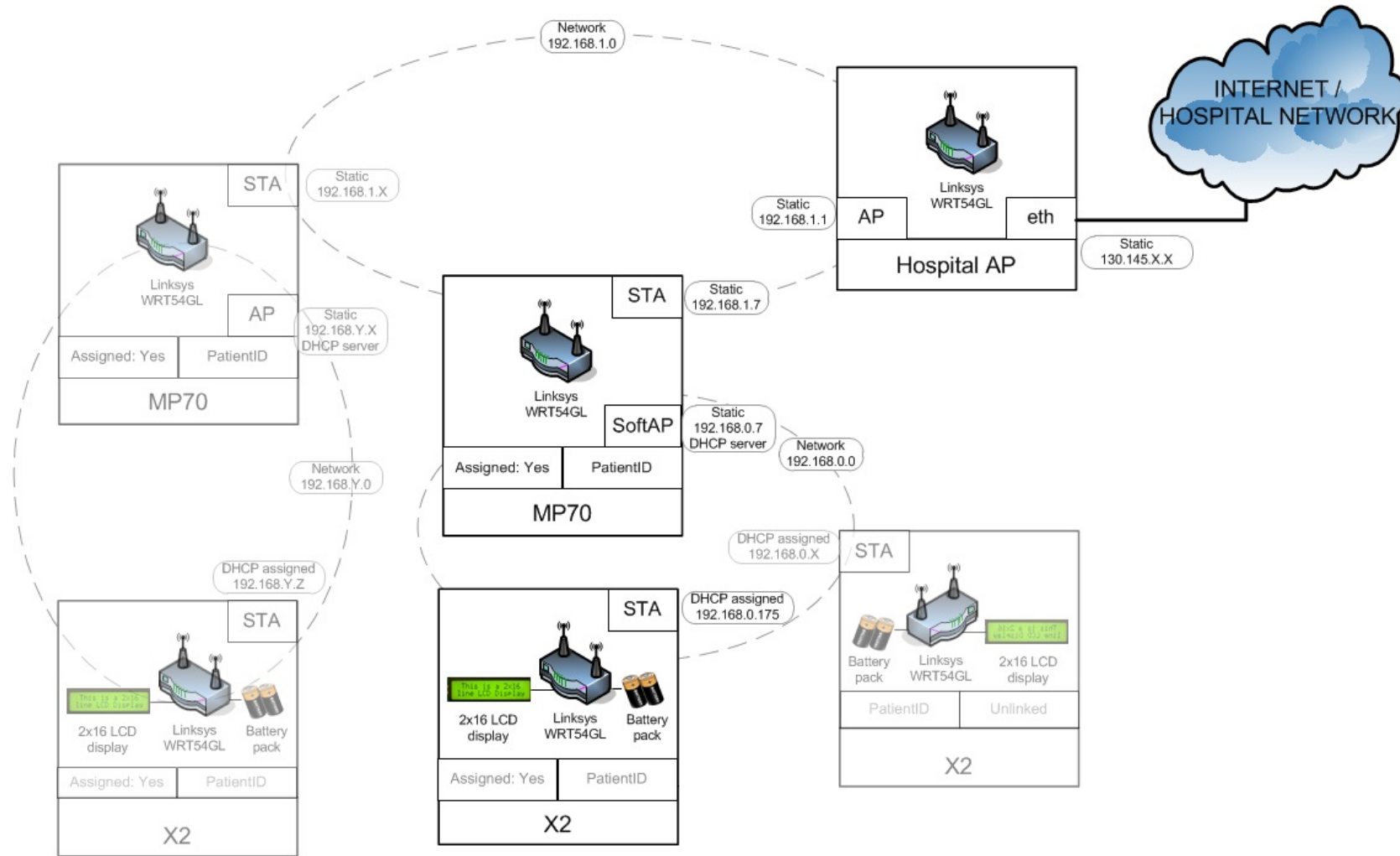


Figure 6.20: Network topology, extended and generalized setup

Chapter 7

Experimental evaluation

This chapter comprises the description, motivation, results and interpretation of the results of the evaluation experiments carried out on the open source implementation.

In general, the finality of carrying out the experiments was to test with reproducible conditions the so called “Use case 1” (see figure 5.1) in which the wire connection is replaced by a wireless connection between the bedside patient monitor and the portable monitor.

Specifically, the main motivations to carry out the experiments were:

- to demonstrate the viability of the scenario,
- to evaluate the time consumption of the scanning procedure (for the Device Discovery functionality),
- to evaluate the reliability of the scanning procedure (prior to the pairing mechanism),
- and to evaluate if the bandwidth, delay and jitter measured values met the requirements.

We translated the Scenario 1 into an experimental setup making use of the Linux-based router embedded platform elements developed in chapter 6 to act as the scenario elements, see figure 7.1, to be used all along the experiments described in the current chapter.

The experimental setup comprised:

X2: WRT54GL router with Tomato firmware equipped with the advanced GUI. Battery operated. Connected to Linux laptop PC via ethernet management port, to perform measures.

MP70: WRT54GL router with OpenWrt configured as AP+STA (Soft-AP). With the custom scripts we developed pre-loaded.

Hospital AP: WRT54GL router with OpenWrt firmware configured as an standard 802.11g AP.

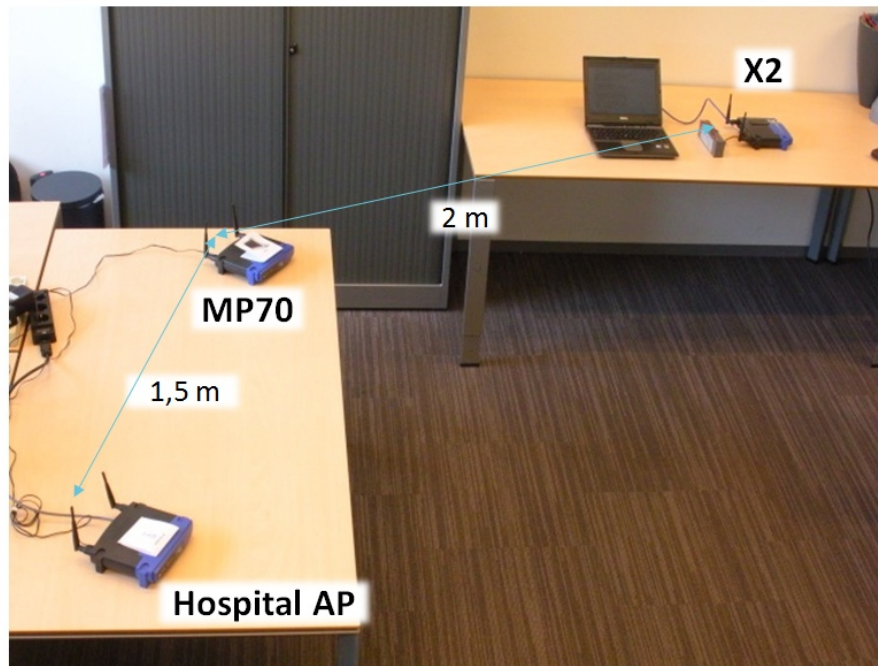


Figure 7.1: *Experimental setup*

7.1 Experiment 1: Channel usage characterization

As an initial calibration experiment, we devised a survey of the radio frequencies used by WiFi signal. In particular in this experiment we conducted a WiFi packet capture and its posterior analysis in different frequency channels and different moments of the day:

- Characterization of the environment without additional traffic load
- Characterization of the environment with additional traffic load

7.1.1 Motivation to carry out the experiment

In order to have certain knowledge on the particular conditions of the Wi-Fi channel usage during the development of the following experiments we carried out this first experiment.

Passive wireless network monitoring like we utilised is commonly used to discover how many Wi-Fi devices are using the spectrum in a given area and how busy the available frequency channels are in a specific geographical area. This helps with the planning of Wi-Fi networks and to reduce interference with other devices by choosing the least used channels for a new Wi-Fi network deployment.

7.1.2 Description of the experiment

Three measurements of 10 rounds of 2 minutes length were performed in different conditions and moments of the day, in order to characterize the WiFi environment usage in the experimental setup surroundings. The results were then averaged for every measurement and interpreted.

We used **Wireshark** (see figure 7.2) packet-sniffing software in a laptop equipped with an 802.11 wireless NIC in monitor mode to make the measure less intrusive avoiding to affect the results with the capturing process.

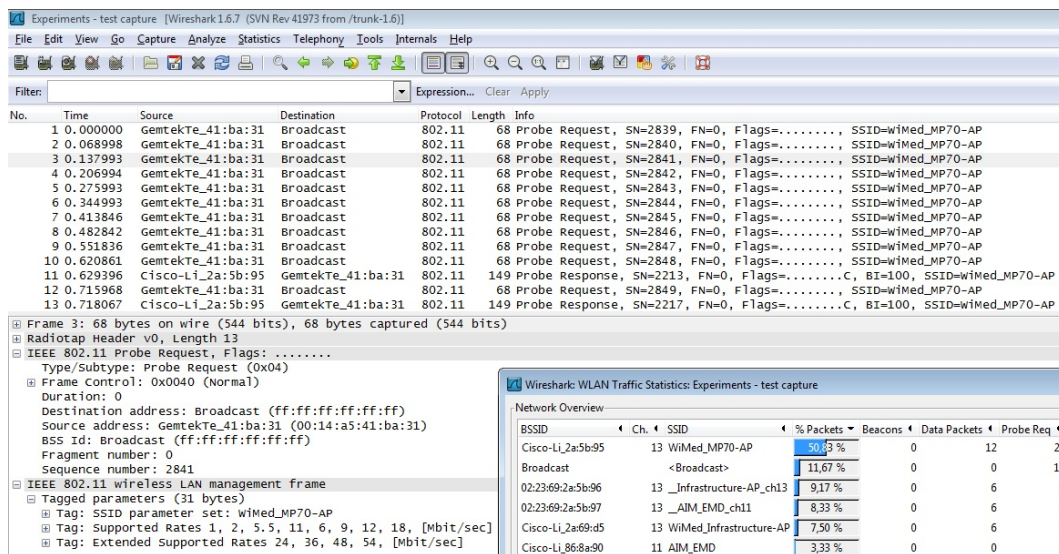


Figure 7.2: Wireshark - Network Protocol Analyzer

Monitor mode allows the capture of all traffic received from the wireless network. Unlike promiscuous mode, which is also used for packet sniffing, monitor mode allows packets to be captured without the need to associate with an AP on advance. So it enables the possibility to monitor packets from all APs around.

Monitor mode is restricted to listen to a single wireless channel at a given moment, though this depends on the wireless adapter's driver, its firmware, and features of its chipset.

Wireshark analysis tools allowed us to determine the proportion of IEEE 802.11 management frames versus data frames, and average figures as packet rate per second, average packet size, throughput and the number of APs present in each frequency channel (see figure 7.3).

We used **Netperf**¹ to generate an additional traffic load and to measure the throughput that the generated data stream was able to achieve.

¹Netperf is a non-commercial network performance measurement software. It is available for Linux and Windows operating systems. Designed following a client-server model, Netperf allows the measurement of unidirectional stream throughput on top of the TCP and UDP protocols, i.e. the net data rate considering all the protocols and overheads. Furthermore it allows for variation in several parameters, as the sent signal socket size, the received signal socket size, the size of the sent signal blocks, and so on, in order to fully characterize a wired or wireless connection.

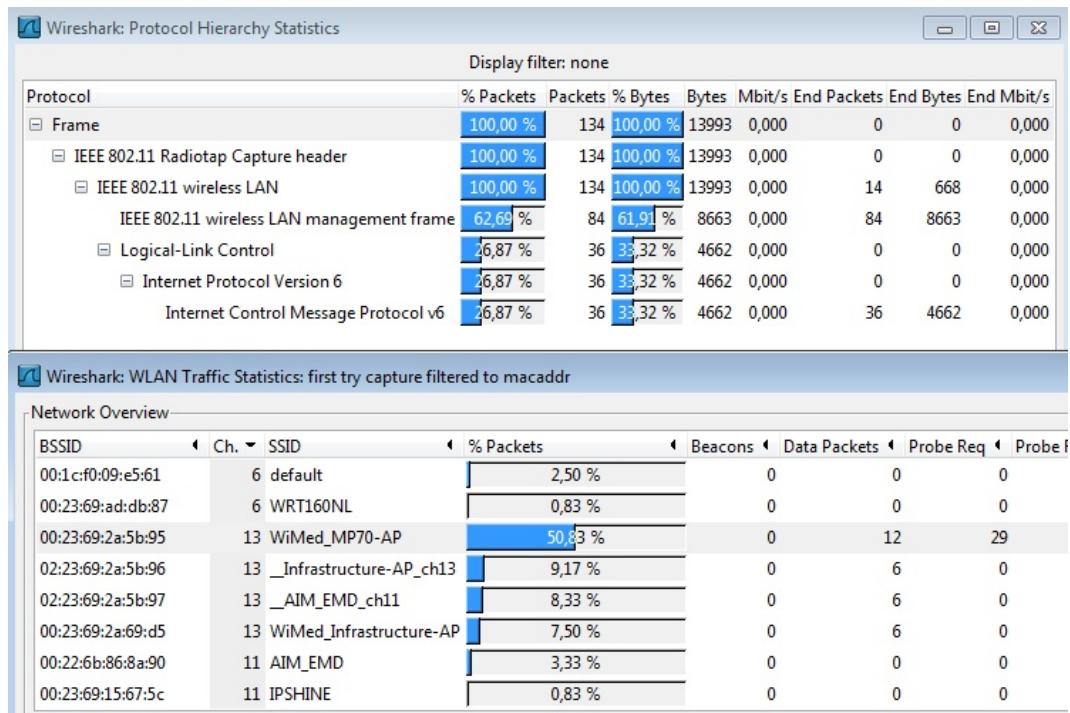


Figure 7.3: Wireshark - Network Protocol Analyzer - Statistics analysis

Netperf was invoked from the origin of the TCP stream at the MP70 with the following command:

```
netperf -H DESTINATION_IP -l LENGTH -t STREAM_TYPE
```

Specifically, for a 2 minutes long TCP stream directed to the Hospital AP with IP address 192.168.1.1:

```
netperf -H 192.168.1.1 -l 120 -t TCP_STREAM
```

In this experiment we were interested only in generating a high load on the channel, rather than in the achievable throughput but it was still necessary to make use of the netserver program on the destination Hospital AP, listening for connections on the default port 12865.

```
root@OpenWrt:~$ netserver
Starting netserver at port 12865
```

The results obtained were displayed when the netperf test ended on the console of the device originating the TCP stream, the MP70 bedside monitor.


```

TCP STREAM TEST from 192.168.1.7 port 0 AF_INET to 192.168.1.1
(192.168.1.1 ) port 0 AF_INET
Recv  Send  Send
Socket Socket Message Elapsed
Size  Size  Size  Time  Throughput
bytes bytes bytes secs.  10^6bits/sec
87380 16384 16384 120.00 21.14

```

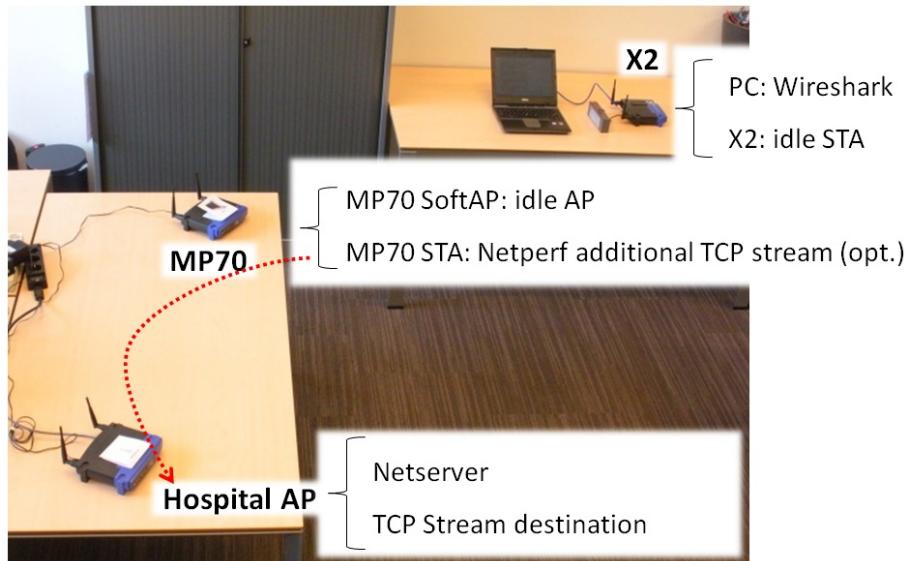


Figure 7.4: Experiment 1 setup: Channel characterization

7.1.3 Results of the experiment

Characterization of the environment without additional traffic load

- Measurement 1. Scenario: isolated hospital room, night time (low activity period).
- Date and time: 22-6-2010 20:00 (empty office)
- Conditions: 10 rounds of 2 minutes observing each channel. No additional traffic load
- Interpretation: Mainly management frames, almost no data frames. Small packet size (less than 200 bytes). Low data throughput. The less utilized channel was channel 6 at 2.437 GHz with 0% of data frames (the remaining percentage up to 100% corresponds to LLC - Logical Link Control frames). See table 7.1.
- Measurement2. Scenario: normal hospital room, daytime (normal RF activity period).
- Date and time: 23-6-2010 10:00 (busy office)
- Conditions: 10 rounds of 2 minutes observing channel 6. No additional traffic load

	ch 1	ch 6	ch 11
Number of APs in channel	6	5	5
Average packets/s	58	52	42
Average packet size [bytes]	196	182	195
Average throughput [MB/s]	0,091	0,076	0,066
% 802.11 mgmt frames	78%	98%	93%
% 802.11 data frames	8%	0%	4%

Table 7.1: *Experiment 1. Measurement 1. Characterization of the environment without additional traffic load*

- Interpretation: Mostly management frames, few data frames (less than 10%). Small packet size (less than 200 bytes). Low data throughput. Measures focusing on channel 6 at 2.437 GHz (the less utilized channel). See table 7.2.

	ch 6
Number of APs in channel	5
Average packets/s	70
Average packet size [bytes]	175
Average throughput [MB/s]	0,098
% 802.11 mgmt frames	84%
% 802.11 data frames	9%

Table 7.2: *Experiment 1, Measurement 2. Characterization of the environment without additional traffic load*

Characterization of the environment with additional traffic load

- Measurement3. Scenario: normal hospital room, daytime with high traffic load.
- Date and time: 23-6-2010 11:00 (busy office with high traffic load generated)
- Conditions: 10 rounds of 2 minutes observing each channel. Netperf generated TCP additional traffic load of 21.14 Mbps.
- Interpretation: Mainly TCP data frames, almost no management frames. Large packet size (more than 500 bytes). High data throughput. See table 7.3.

7.1.4 Interpretation of the results

As it would be expected, in a night-time scenario with low WiFi activity, the observed traffic corresponded to management frames in under-utilized channels in terms of throughput. Meanwhile in a busy daytime scenario, the observed traffic corresponded to high-throughput data frames.

	ch 6
Number of APs in the channel	5
Average packets/s	4536
Average packet size [bytes]	569
Average throughput [MB/s]	20,65
% 802.11 mgmt frames	1%
% 802.11 TCP frames	50%

Table 7.3: *Experiment 1, Measurement 3. Characterization of the environment with additional traffic load*

The less utilized channel was found to be channel 6 at 2.437 GHz. As measures in a less utilized channel would be more accurate, we decided to carry out the following measures of this experiment in the given channel as long as it was possible.

7.2 Experiment 2: Scan parameters analysis

Different wireless NIC implementations by different vendors, result in slightly different behaviours and transmission patterns. Active scanning is a procedure vaguely concredited by the 802.11 standard, implemented in the hardware and software of every wireless NIC.

As different parameters could be specified in active scanning for our implementation's wireless driver tools, we tried to identify different results in an observable scale toggling with parameters as the number of scan probes and the dwell time in every channel.

7.2.1 Description of the experiment

In a quiet Wi-Fi channel in a low activity period (*Mainly management frames, almost no data frames. Small average packet size. Low data throughput*) we repeated an active scanning process sweeping different values for probe request parameters, using the `wl` wireless tool command options, as introduced in the previous chapter's section 6.1.1.

The scanning parameters considered were the following:

Number of probes With the `wl scan_nprobes` command we were able to adjust the number of probes sent in every scan.

Dwell time With the `wl scan_channel_time` command we were able to adjust the dwell time, or time remaining in every channel waiting for probe responses after sending the broadcast probe request when scanning in multiple channels.

With the help of the Wireshark packet-sniffing tool running in a laptop PC, we were able to capture frame timestamps and deduce the probe periodicity, probes spacing and the time taken for processing the scanned data between multiple scans.

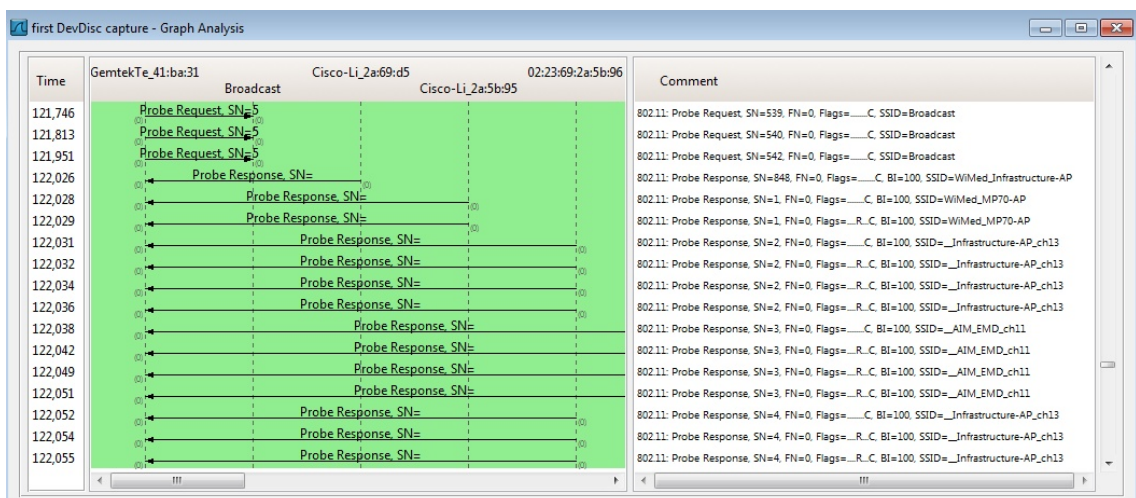


Figure 7.5: Wireshark - Network Protocol Analyzer - Flow graph

We used the X2 portable monitor implementation over one of the WRT54GL router to scan the channel where the MP70's AP and the Hospital AP are operating, as shown in figure 7.6.

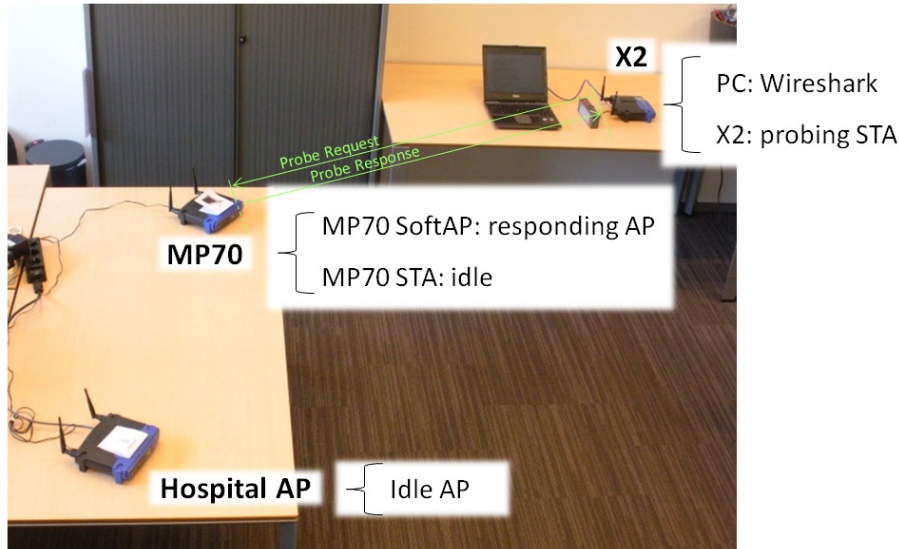


Figure 7.6: *Experiment 2 setup: Scan parameters analysis*

7.2.2 Motivation to carry out the experiment

In order to know more detail of the specific wireless NIC vendor implementation of scanning and probe request/probe response management, we developed the current experiment.

7.2.3 Results of the experiment

We observed the probe request frames for different dwell times and different number of probes configured obtaining the results shown in 7.4.

We defined the **inter-probe time** as the time between probe request frames in a scan (when 2 or more probes were configured). We defined the **inter-scan inter-probe time** as the time between the last probe from a scan and the first probe from the next scan.

It seemed that the **probe requests** were **equidistantly scheduled** to **maximize their separation while staying inside of the dwell time** (as an example: with 2 probes, we measured a consistent inter-probe time of half the dwell time), unless the inter-probe time multiplied by the number of probes was already greater than the dwell time (as an example: with 5 probes and a dwell time of 20 to 80 ms, we measured a constant 10 ms inter-probe time).

Second measurement We performed an scheduled scan, programming multiple scans to statistically infer the time needed for the wireless NIC between different scans, scheduling repetitions of 200 scans with different dwell times and fixing the number of probes to one. We measured

Scan parameters		Wireshark measure [ms]	
n probes	Dwell time [ms]	Inter-probe time	Inter-scan inter-probe time
1	20	-	140
1	40	-	230
1	60	-	230
1	80	-	230
1	100	-	230
1	120	-	320
1	140	-	320
1	200	-	320
2	20	10	130
2	40	20	210
2	60	30	230
2	80	40	190
2	100	50	180
2	120	60	260
2	140	70	250
2	200	100	220
3	20	10	210
3	40	10	210
3	60	20	190
3	80	20	190
3	100	30	170
3	120	40	230
3	140	40	230
3	200	60	200
5	20	10	190
5	40	10	190
5	60	10	190
5	80	10	190
5	100	20	150
5	120	20	150
5	140	20	150
5	200	40	160

Table 7.4: *Experiment 2, Measurement 1. Inter-probe and inter-scan times, varying number of probes and dwell time*

then the total time needed for all the repetitions, obtaining the single repetition time, and basic statistical information (minimum and maximum values, and the mode) on the inter-scan time measuring the probe frames, as shown in 7.5.

Scan parameters		Wireshark measure Inter-scan time [ms]			Measured scan time for 200 repetitions	
Dwell time [ms]	Number of probes	Min.	Mode	Max.	Total scan time (200 rep.) [s]	Single scan time [ms]
20	1	45	50	62	29	145
40	1	47	50	200	45	225
60	1	70	200	210	45	225
80	1	90	190	250	45	225
100	1	110	200	240	45	225

Table 7.5: *Experiment 2, Measurement 2. Inter-scan times, varying dwell time for multiple repetitions*

The dwell time parameter seems to have a lower bound in 20 ms, given that for a value of 10 ms the total scan time for 200 iterations was the same than for 20 ms. Similarly, for longer dwell times up to 100 ms.

The calculated average single scan time figure was always greater than the inter-scan time mode (the most repeated figure for the inter-scan time) for all the dwell time values, and habitually smaller than the maximum measured inter-scan time, except for 80 ms and longer dwell times.

The inter-scan times obtained observing the traces in Wireshark were considerably smaller than the calculated dividing the total scan time by the number of repetitions in the scheduled 200 repetitions scanning. Furthermore, the overhead due to checking for the availability of the driver makes the values to be the same for the different dwell times even if the frame timestamps suggested that the scans could be effectuated way more often.

7.3 Experiment 3: Scanning performance

Taking into account that the scanning process was involved in both the device discovery and the pairing mechanisms in our implementation, it could be considered that it is a fundamental step for our devised solution which makes use of additional SSIDs and information contained on that field of the beacon frames.

For that reason we wanted to have an idea of the scanning accuracy in terms of the reliability on finding a target SSID through active scanning. We based the current experiment in a large number of repetitions to increment the faithfulness of the measure.

We also wanted to study the average time figure of the scanning process, in order to have an estimation of the duration of such a time-consuming step of the implemented mechanisms and to infer an scan optimisation proposal if possible in terms of scan parameters tuning.

7.3.1 Description of the experiment

In a quiet Wi-Fi channel in a low activity period we scheduled 1000 repetitions of an active scanning process sweeping different values for probe request parameters, using the `wl` wireless tool command options, as in the previous experiment but toggling also the channels in which to perform the scan. Afterwards we generated a TCP high load to simulate a not-so-quiet channel environment.

The scanning parameters considered were the following:

Dwell time With the `wl scan_channel_time` command we were able to adjust the dwell time, or time remaining in every channel waiting for probe responses after sending the broadcast probe request when scanning in multiple channels.

Channels With the `wl scan --channels=LIST` command we were able to specify a subset of frequency channels (defined in `LIST`) in which to perform the scanning.

Number of probes With the `wl scan_nprobes` command we were able to adjust the number of probes sent in every scan.

We used the X2 portable monitor implementation over one of the WRT54GL router to perform the scan looking for the MP70's AP SSID, both in a quiet channel and generating a high load TCP stream from the MP70 to the Hospital AP, as shown in figure 7.7.

For obtaining the results we calculated the total scan time in seconds of 1000 repetitions for every combination of parameters. In that way we obtained the average scan time in milliseconds for every one of the thousand of scheduled scans.

Besides, for obtaining the accuracy, we keep a count of the successful scans, taking into account whether the X2 had found the MP70 target SSID in the scan process, obtaining an accuracy

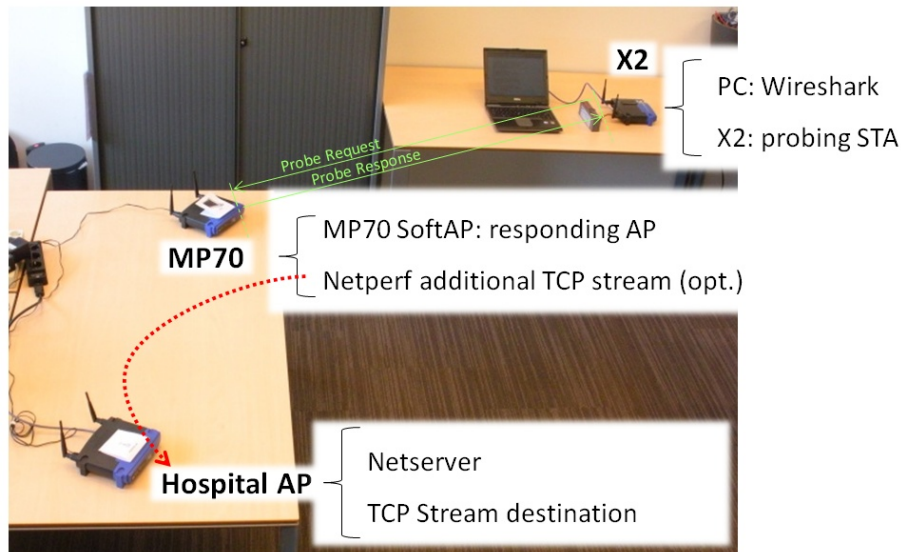


Figure 7.7: Experiment 3 setup: Scanning performance

percentage depending on the scan parameters.

7.3.2 Motivation to carry out the experiment

In order to evaluate the reliability and time-consumption of the scanning process used in the device discovery and pairing mechanisms, we performed the current experiment.

7.3.3 Results of the experiment

The data obtained in this experiment after scheduling 1000 repetitions with different scan parameters combinations is shown in 7.6.

		Additional load			No load	
Dwell time	Channel	n Probes	% MP70 found	Scan time [ms]	% MP70 found	Scan time [ms]
20	6	1	83,3%	295	99,4%	296
40	6	1	83,9%	298	99,4%	298
60	6	1	83,9%	298	99,3%	299
80	6	1	82,5%	298	99,2%	298
100	6	1	83,0%	308	99,4%	309
20	6	2	96,4%	288	99,9%	281
40	6	2	96,8%	300	100,0%	300
60	6	2	96,9%	300	100,0%	300
80	6	2	97,7%	300	100,0%	300
100	6	2	97,8%	304	100,0%	304
20	1,6,11	1	84,2%	397	99,8%	402
40	1,6,11	1	83,7%	397	99,5%	404
60	1,6,11	1	83,5%	487	99,4%	491
80	1,6,11	1	85,0%	574	99,8%	579
100	1,6,11	1	82,4%	574	99,2%	580
20	1,6,11	2	97,7%	396	99,8%	391
40	1,6,11	2	97,8%	400	100,0%	407
60	1,6,11	2	98,3%	488	100,0%	495
80	1,6,11	2	98,5%	577	100,0%	583
100	1,6,11	2	97,9%	577	100,0%	584
20	1,2,3,4,5,6,7,8,9,10,11	1	100,0%	792	100,0%	797
40	1,2,3,4,5,6,7,8,9,10,11	1	100,0%	966	100,0%	975
60	1,2,3,4,5,6,7,8,9,10,11	1	100,0%	1230	100,0%	1239
80	1,2,3,4,5,6,7,8,9,10,11	1	100,0%	1404	100,0%	1418
100	1,2,3,4,5,6,7,8,9,10,11	1	100,0%	1666	100,0%	1681
20	1,2,3,4,5,6,7,8,9,10,11	2	100,0%	794	100,0%	802
40	1,2,3,4,5,6,7,8,9,10,11	2	100,0%	970	100,0%	983
60	1,2,3,4,5,6,7,8,9,10,11	2	100,0%	1232	100,0%	1226
80	1,2,3,4,5,6,7,8,9,10,11	2	100,0%	1408	100,0%	1426
100	1,2,3,4,5,6,7,8,9,10,11	2	100,0%	1670	100,0%	1703

Table 7.6: Experiment 3. Scan performance

7.3.4 Interpretation of the results

There were some interesting points that we deduced from analysing the obtained data in this experiment, shown in 7.6:

- As the scan dwell time parameter increments, the more noticeable this parameter's effect is in the scan time in long scans, as the ones performed in several channels.
- The number of probe requests sent increases the probability of finding the MP70 SSID within the same scan times. The only negative aspect of increment the probes is only that it would generate additional traffic.
- With a fixed dwell time, the probability to find the target MP70 SSID is greater when scanning in several channels, more noticeable the longer the channel list is. The reason is because of channel overlapping, as the device is *over-scanning* in channels over-lapped in frequency detecting neighbour channels activity.
- Even with an additional generated load in the channel, the probability of finding the target SSID was quite high, specially when using a 2 probe request scanning strategy, with an estimated success of 96.4% or higher.
- The average time to successfully find the MP70's SSID was not incremented if using 2 probes instead of just one. And it was considerably incremented in case of enlarging the channel list in which to perform the scan. This average time was not significantly influenced by the optional coexistence of a high load TCP stream in the shared medium.

Our inferred **optimal configuration for the active scan** was considering the following values:

- **Number of probe requests** for active scanning: **2**
- **Dwell time: 20 or 40 ms.** Given that with an adequate number of probe requests, using longer dwell times did not imply a higher probability of finding the MP70's SSID.
- **Channel list:** the **non overlapping channel list (ch1, ch6, ch11)**, taking into account that it represented an increment of just an approximate 33% respect from performing the scan only in the current operating channel.

Considering the obtained figures for the successful scan, one of the longer steps of the pairing process would mean a **fulfilment of the application requirements in terms of time needed for the reconnection** to the MP70 and switching between the X2-MP70 connection and the X2-HospitalAP connection, **both under the *few seconds* requirement.**

7.4 Experiment 4: Delay and delay jitter measurement

Delay in real-time applications, specially in streaming use cases, could translate in a poor performance and degraded user experience. This experiment was about measuring if there was such delay and to study its variation along time, i.e. the delay jitter.

7.4.1 Description of the experiment

In a quiet Wi-Fi channel in a low activity period we performed a very basic test to measure the round trip time between the origin of the data and the other extreme of the wireless dual-link under study, for a number of repetitions. Afterwards we generated a TCP high load to simulate a not-so-quiet channel environment and repeated the experiment to see if it was affected by the channel load.

In the current experiment we used Ping: a basic diagnose tool for checking the communication status between the local host originating the ping (an Echo Request) and a destination host (or multiple hosts) which respond (with an Echo Reply), making use of ICMP messages. It provides measurement of Round Trip Time statistics (min/max/average and standard deviation).

For calculating the jitter and jitter delay, we made use of the ping statistics for 250 repetitions considering that:

- Round-Trip Time (RTT), maximum and average, correspond to maximum and average link delay, in order to check the compliance with the required figure of less than 200 ms as indicated in table 3.2.
- Jitter variability in average corresponds to the RTT standard deviation, in order to check the compliance with the required figure of less than 200 ms.

We used the X2 portable monitor implementation over one of the WRT54GL router to perform the ping with destination the Hospital AP, both in a quiet channel and generating a high load TCP stream from the MP70 to the Hospital AP, as shown in figure 7.8.

7.4.2 Motivation to carry out the experiment

In order to evaluate if the implemented solution met the requirements in terms of delay and the jitter of such delay, we performed the current experiment.

7.4.3 Results of the experiment

The data obtained in this experiment after scheduling 250 ping repetitions both without and with a high generated load is shown in 7.7 and represented graphically in figure 7.9.

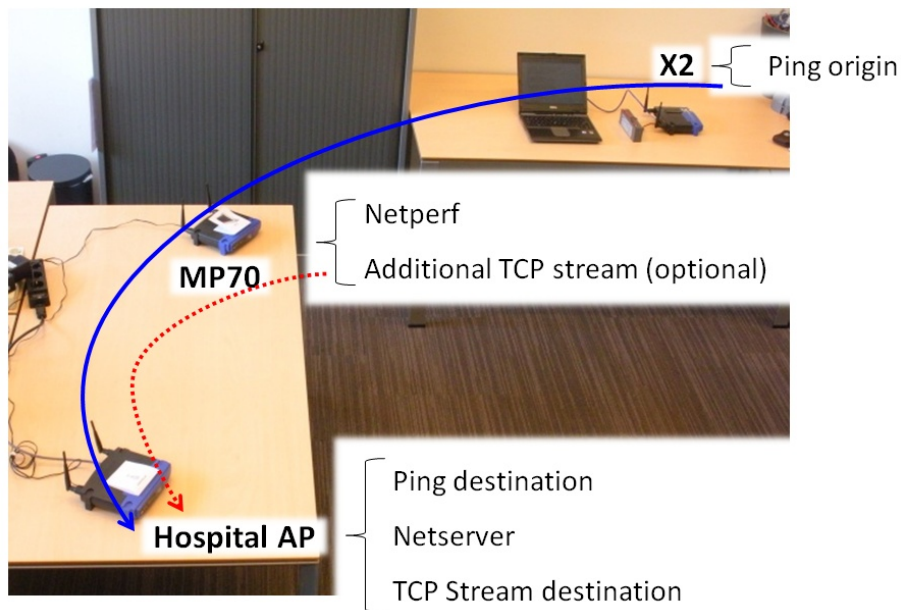


Figure 7.8: Experiment 4 setup: Delay and delay jitter measurement

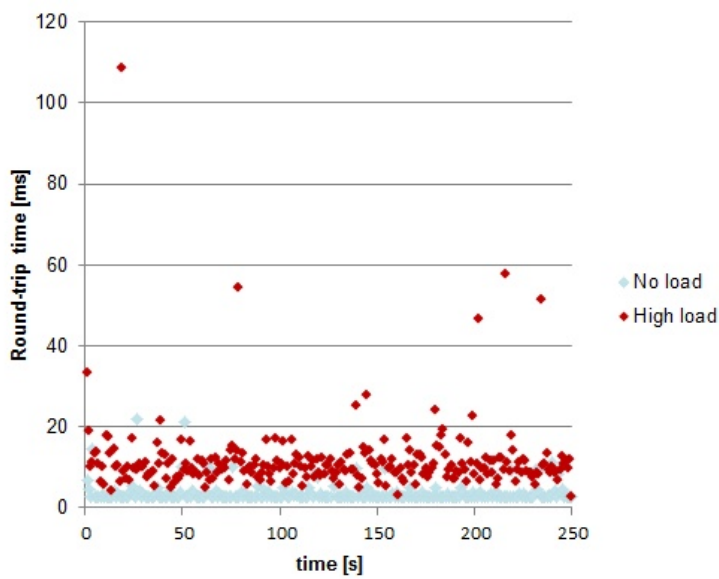


Figure 7.9: Experiment 4 results: RTT for delay and delay jitter requirements

SoftAP Link Delay and Delay jitter		
Number of Iterations	250	250
Load	No load	Max load with Netperf (20 Mbps)
Packet loss	0%	0%
Round-trip time Delay [ms]	Requirement <200 ms	
Min [ms]	2,6	2,7
Average [ms]	3,6	11,6
Max [ms]	21,8	108,6
Jitter [ms]	Requirement <200 ms	
Standard deviation [ms]	2,4	9

Table 7.7: *Experiment 4. Delay and delay jitter measurement*

7.4.4 Interpretation of the results

We obtained promising results indicating that the totality of the ping packets arrived to its destination, together with low average values for the round trip time **delay**, under 4 seconds in a quiet environment and under 12 seconds with high load presence, **fulfilling the requirement of being less than 200 milliseconds**. Even the maximum (worst) values obtained were less than half the requirement figure. And the **delay jitter** figures were also way shorter than the required ones, also **meaning the fulfilment of the requirement** of being under 200 milliseconds too.

7.5 Experiment 5: Throughput measurement

Throughput shortage in high-bandwidth applications could translate in a poor performance and degraded user experience. This experiment was about measuring if the achieved application net throughput was enough to comply with the required figure.

7.5.1 Description of the experiment

To perform an upstream test (*upstream* as from client to server, i.e. from the X2 portable monitor to the Hospital AP to forward patient data to the hospital network, going across the MP70 bedside monitor), we used Netperf and Netserver, as in Experiment 1 (see 7.3) and configured as shown in figure 7.10.

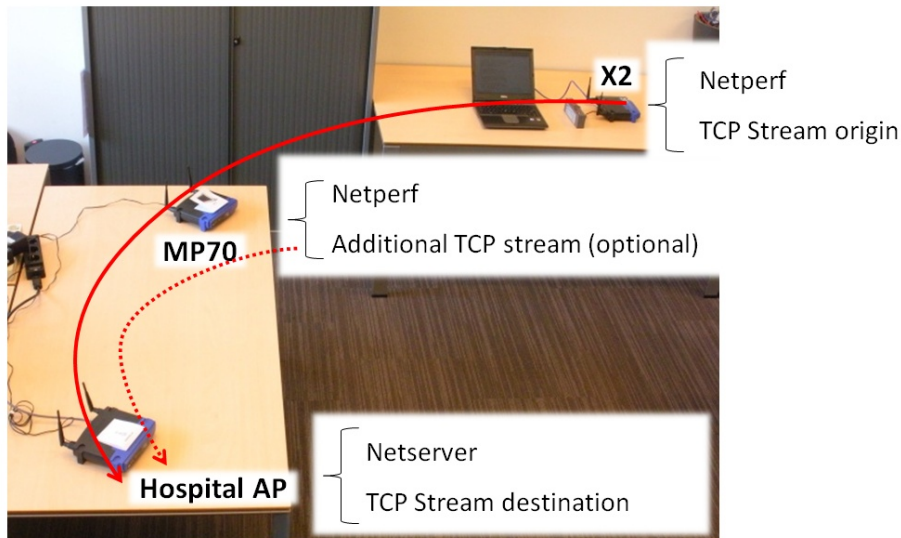


Figure 7.10: Experiment 5 setup: Throughput measurement

7.5.2 Motivation to carry out the experiment

In order to evaluate if the implemented solution met the requirements in terms of throughput, we performed the current experiment.

7.5.3 Results of the experiment

The data obtained in this experiment after running a 2 minute Netperf TCP performance test from the X2 to the Hospital AP, both without and with a high generated load is shown in 7.8.

	SoftAP Link Throughput	
Tool	Netperf and Netserver	
Length	2 min	2 min
Load (forced between MP70 and Hospital AP)	No load	Max load with Netperf
Throughput [Mbps]	Requirement >5 Mbps	
Configured 802.11g data rate [Mbps]	54	
Measured throughput X2-MP70-Hospital AP	10,92	5,32
Measured throughput MP70-Hospital AP	-	10,96
Size of the bulk data transfer [MB]	163,8	79,8
	-	164,4

Table 7.8: Experiment 5. Throughput measurement

7.5.4 Interpretation of the results

Operating at a raw data rate of 54 Mbps, the dual-link solution based on Soft-AP and 802.11g, which in practice delivers a maximum net throughput of 27.9 Mbps due to protocols overhead[35], with 1 Soft-AP hop (i.e. two transmissions over the air) a maximum theoretical throughput of 13.95 Mbps could be obtained.

We obtained an adequate net TCP throughput figure of 10.92 Mbps without additional load. When in presence of a generated high load from the MP70 to the Hospital AP, the available throughput went down to 5.32 Mbps. Being **both figures greater than the 5 Mbps requirement, our implementation fulfilled the throughput requirement.**

Chapter 8

Conclusions and further research

8.1 Conclusions

The results from the experiments carried out, fulfilling all the use case requirements, confirms the suitability of the decisions taken in the different steps of this project, from the choice of applicable technologies –over IEEE 802.11g adopting the SoftAP approach–, to the solution abstract design, and the practical implementation developed.

Having identified the scanning as the most expensive task in terms of time consumption, and given that the duration of the aforementioned task (with the proper adjustment of its parameters) can be bounded by the figure of 400 milliseconds, in both the case of a scenario without apparent load and a fully loaded scenario, we can say that the proposed algorithm designed for the pairing procedure complies with the application requirement of a *few seconds* as the time required to switch the X2-MP70 link to the X2-CSCN AP link.

Taking into account a real-time application like our patient monitoring use case, delay was an important requirement to consider. We could say that our implementation complies more than enough both in terms of delay and its variation, delay jitter, way below the 200 milliseconds requirement.

Considering the available throughput reduction experienced with every packet transmission over the air, we obtained an available throughput above the 5 Mbps requirement, even in one of the worst cases, as the netperf high load was generated by the same wireless NIC of the MP70 that was acting as a SoftAP device, forwarding *patient data* from the X2 to the Hospital AP at the same time and still obtaining a throughput over the requirement figure.

8.2 Further research

Following, we indicate the identified paths on which further research could be done, according to the results and conclusions extracted from our work.

- **Compression and processing algorithms at the origin of patient data.** With more powerful and current processing power available in small devices (like smartphones) every day, it would be interesting to analyse and compress relevant patient data in the X2 portable monitor in real time, prior to just forward it to the MP70 bedside monitor and the Central Monitoring Station through the hospital APs.
- **Enhanced heuristics for pairing and wireless connection.** Involving more parameters in the decision making pairing algorithms will allow a more robust and reality-aware patient monitoring wireless network.
 - **Separation of physical wireless link from patient information flow.** With the use of an intelligent backbone centralised system, integrated into the Hospital Information Systems would allow a more flexible patient monitoring network.
 - **Replace intensive use of SSIDs with the use of IEs:** Further investigation is needed in using the IEEE 802.11 management frame *Information Elements*, with the proper hardware that would allow to use them. To avoid using the SSIDs in such an intense way will mean more privacy, less visibility from the outside of the network and allow faster operation, in terms of discovery and pairing procedures.
- **Implementation over more stable platform,** both in terms of hardware and OS, software.
 - Use of the latest Linux kernel, 2.6.33.

As of June 2010 the latest stable release of the Linux kernel was 2.6.33, while OpenWRT firmware for the WRT54GL routers in its version *Kamikaze 8.09.1* released on June 2009 was based on 2.6.25 and 2.6.26 Linux kernel stable versions.

The 2016 latest stable version of OpenWRT firmware, *Chaos Calmer 15.05.1* released in March 2016, is based in the 3.18.23 LTS Kernel. The most recent release of the Linux kernel is 4.6.3 from June 2016, though.

- Use of a Linux distribution or modules supporting more functional languages where to develop scripts: different shells, diverse languages as python, perl or others.
- Use a more common and up-to-date embedded platform:
 - * **Arduino**¹ is an open-source prototyping platform based on flexible hardware and software, which can be upgraded adding modules communicate wirelessly using any wireless shield module with a compatible footprint (Xbee ZigBee 802.15.4 or Wi-Fi modules). Historically (until 2015) Arduino consisted on an Atmel AVR

¹URL: <https://www.arduino.cc>

microcontroller of 8, 16 or 32 bit, like the one used for our Soft AP implementation as described in section 6.1.1.

- * The **Raspberry Pi** ecosystem would also represent an interesting testbed, although its firmware is closed-source, it is another low-cost, low-consumption single-board computer primarily using Linux-kernel-based operating systems developed with educational purposes.
 - * **Android** devices are nowadays a powerful, flexible and cost-effective alternative for mobile computing, avoiding the need of using traditional PCs in most applications, in a Linux-based OS and battery run, for additional adaptability to different scenarios.
 - * Alternatively, follow the investigations in a **PC-based platform** and then port it to an embedded platform. Consider using *cheap* USB Wireless card sticks that support AP-mode to implement a sub-optimal configuration based in the same exact chipset contained in the Philips monitoring devices, to avoid later compatibility problems when porting the implemented solution from the test platform into production.
- **Test the implementation in a widely-deployed large-scale testbed**, to assure scalability and to test coexistence problems and cross-system interference at the intensely populated 2.4 GHz frequency range.

As an example the *Nitos Facility* is an integrated laboratory facility with heterogeneous testbeds that focuses on supporting experimentation-based research in the area of wired and wireless networks. NITOS is remotely accessible and open to the research community 24/7. It is comprised of three different deployment testbeds: an Outdoor Testbed, an Indoor RF Isolated Testbed and an Office Testbed. Counts on a total of 100 nodes, some of them mobile, with heterogeneous (Wi-Fi, WiMAX, LTE, Bluetooth) wireless technologies².

- Adopt **alternative standards focused in power saving** mechanisms, for improved battery longevity.
 - Wi-Fi HaLow standard IEEE 802.11ah. It extends Wi-Fi into the unlicensed 900 MHz band, enabling low power connectivity necessary for applications including sensor and wearables.

Introduced in January 2016, certifications expected around 2018. At 900 MHz it doubles the range compared to 2.4 GHz thanks to improved radio waves propagation and penetration, and reduced power consumption with an optimized 11ah PHY and MAC featuring a mandatory and globally interoperable 1 and 2 MHz bandwidth modes for sensors and supporting 4, 8, and 16 MHz bandwidths for higher-data rate applications.
 - Wi-Fi low power optimized chips.

²URL: <http://nitlab.inf.uth.gr/NITlab/index.php/testbed>

Example: GainSpan Wi-Fi low power optimized chips
PHY and MAC: 802.11b/g DSSS CSMA-CD
Range: 50-70 m interior, <300 m exterior
Data rates: 1, 2, 5.5, 11 Mbps
Power consumption in normal operation: 60 mW
Power consumption in suspension: 5 microW.

– Bluetooth Low Energy³

Range: >100 m
Data rates: 1 Mbps
Power consumption in normal operation: 1 mW to 500 mW
Peak current consumption: <15 mA.

Envision of the whole system

The ultimate goal of the system has to be to improve the provision of medical services in health-care facilities through the introduction of technology. Specifically by means of the ubiquitous, continuous monitoring of physiological signals, based on the use of Wi-Fi standard wireless devices and sensors. But to reach its main objective should go beyond, incorporating additional features, supported by a backend server, such as: patient management and support for administrative processes (Admission, Discharge and Transfer of patients, with ADT protocol support), dynamic scheduling of appointments, resources, rooms and equipment; and the interaction with other healthcare equipment and their settings (with HL7 protocols support for enhanced compatibility), among others.

Final conclusion

A system such as here conceived, developed and provisionally assessed (as an interim assessment for the suitability of the wireless substitution of previous wired connections) must be supplemented with other subsystems attached to it, in order to form a complete patient management system based on the use of sensors and wireless devices under the Wi-Fi standard.

Its main objective should be to improve the provision of medical services in hospitals, especially the ubiquitous, continuous monitoring of physiological signs. But should go further by incorporating the dynamic management of appointments, assisting medical processes as the diagnostic and medical events detection, facilitating the hospital facilities administration, the interaction with the whole healthcare environment, among others.

The ultimate goal of the system must be to improve the quality of health care through the introduction of solid and reliable wireless technology in the hospital medical field.

³Taking into consideration the use case requirements, specially in terms of bandwidth.

Bibliography

- [1] A. SOOMRO, T.J.J. DENTENEER, “Dual-Link Wi-Fi Solution Comparisons and Recommendations”, Philips Research, 2009
- [2] R. AARNINK, “Healthcare today: 2008 Key facts & figures”, Student visit to Philips Healthcare facilities in Best (the Netherlands), April 2010,
URL: http://www.newscenter.philips.com/pwc_nc/main/shared/assets/newscenter/2009_pressreleases/2008_annual_results/Healthcare_facts_figures_2008.pdf
- [3] EUROPEAN COMMISSION. JOINT RESEARCH CENTRE. C. CODAGNONE, I. MAGHIROS., “IDATE 2010, ICT for Health: Remote Monitoring Systems for Chronic Disease Management”, *IDATE 2010, ICT for Health: Remote Monitoring Systems*, Montpellier, November 2010,
URL: <http://www.digiworldsummit.com/2010/UserFiles/File/Ioannis%20Maghiruos%20IPTS%20-%20eHEALTH.pdf>
- [4] EUROPEAN COMMISSION, “Memorandum of Understanding between the European Commission and the United States Department of Health and Human Services on Cooperation Surrounding Health Related Information and Communication Technologies”, December 2010,
URL: http://ec.europa.eu/information_society/activities/health/docs/policy/comm_c_2010_8451ehealth_agreement-en.pdf
- [5] EUROPEAN COMMISSION, “Accelerating the development of the eHealth market in Europe, eHealth Taskforce report 2007”, 2007,
URL: http://ec.europa.eu/information_society/activities/health/docs/publications/lmi-report-final-2007dec.pdf
- [6] EUROPEAN COMMISSION. JOINT RESEARCH CENTRE. F. ABADIE, C. CODAGNONE, I. MAGHIROS ET AL., “Strategic Intelligence Monitor on Personal Health Systems (SIMPHS): Market Structure and Innovation Dynamics”, January 2011,
URL: <http://ftp.jrc.es/EURdoc/JRC62172.pdf>
- [7] EUROPEAN COMMISSION, “Digital Agenda for Europe 2010-2020”, *COM(2010) 245 final/2*, May 2010,
Release URL: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=5826

- Document URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>
- [8] EUROPEAN COMMISSION, “Europe 2020. A strategy for smart, sustainable and inclusive growth”, *COM(2010) 2020 final*, March 2010,
URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF>
- [9] EUROPEAN COMMISSION, “Digital Agenda for Europe. Annual Progress Report 2011”, December 2011,
URL: http://ec.europa.eu/information_society/digital-agenda/documents/dae_annual_report_2011.pdf
- [10] EUROPEAN COMMISSION. INFORMATION SOCIETY AND MEDIA DIRECTORATE-GENERAL. BY DELOITTE & IPSOS BELGIUM, “eHealth Benchmarking III”, April 2011,
Release URL: http://ec.europa.eu/information_society/newsroom/cf/item-detail-dae.cfm?item_id=6952
Document URL: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/ehealth_benchmarking_3_final_report.pdf
- [11] EUROPEAN COMMISSION, “eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century”, *COM(2012) 736 final*, June 2012, Release URL: <http://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century>
Document URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0736:FIN:EN:PDF>
- [12] DRÄGERWERK AG & CO., “Dräger Medical patient monitoring website”, Date accessed: May 2012, URL: http://www.draeger.com/UK/en/applications/patient_monitoring/, 2010
General website URL: http://www.draeger.com/GC/en/products/medical_monitoring/,
Hospital monitoring portfolio URL: http://www.draeger.co.uk/sites/en_uk/Pages/Hospital/ProductSelector.aspx?navID=141
- [13] WELCH ALLYN INC., “Welch Allyn Patient Monitors & Systems website”, Date accessed: June 2010,
Welch Allyn’s patient monitoring website URL: http://www.welchallyn.com/pressroom/media/FlexNet/flexnet_newsroom.htm,
Welch Allyn’s patient monitoring products URL: http://www.welchallyn.com/apps/products/product_category.jsp?catcode=PMS&subcatcode=PMS-NTWK
- [14] LAN/MAN COMMITTEE OF THE IEEE COMPUTER SOCIETY, “IEEE Standard 802.11-2007”, IEEE Xplore Digital Library, vol., no., p.1-1238 June 2007,
URL: <http://standards.ieee.org/findstds/standard/802.11-2007.html>⁴

⁴“Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications” can be accessed at URL: <http://www.ie.itcr.ac.cr/marin/lic/e14515/antenas/802.11-2007.pdf>

- [15] LAN/MAN COMMITTEE OF THE IEEE COMPUTER SOCIETY, “IEEE 802.11 Working Group Project Timelines”, September 2013,
URL: http://www.ieee802.org/11/Reports/802.11_Timelines.htm
- [16] B. O’HARA, A. PETRICK, “IEEE 802.11 Handbook: A Designer’s Companion”, *IEEE standards wireless networks series*, IEEE Standards Association, 2005
- [17] G. ANASTASI, M. CONTI, E. GREGORI, “IEEE 802.11 Ad Hoc Networks: Protocols, Performance and Open Issues”, Chapter 3 in *Mobile Ad Hoc Networking*, IEEE Press and John Wiley and Sons, Inc, New York, 2004
- [18] A. SOOMRO, D. CAVALCANTI, “Opportunities and Challenges in Using WPAN and WLAN Technologies in Medical Environments”, *IEEE Communications Magazine*, Volume 45 Issue 2, p.114-122 , Philips Research North America, February 2007
- [19] H. COSKUN, I. SCHIEFERDECKER AND Y. AL-HAZMI, “Virtual WLAN: Going beyond Virtual Access Points”, *Electronic Communications of the EASST Volume 17*, 2009
- [20] PHILIPS MEDICAL SYSTEMS NEDERLANDS B.V., “Intellivue X2 Multi-Measurement Module Technical Data Sheet”, 2007,
URL: http://media.supplychain.nhs.uk/media/documents/N0889201/Specification/31469_N0889201%20X2%20Tech%20Data%20Sheet.pdf
- [21] PHILIPS MEDICAL SYSTEMS NEDERLANDS B.V., “Intellivue MP60/MP70 Patient Monitor Technical Data Sheet”, 2006,
URL: http://media.supplychain.nhs.uk/media/documents/n0889200/marketing/31990_n0889200.pdf
- [22] R. FRIES, “Reliable Design of Medical Devices, second edition”, Taylor & Francis, 2006
- [23] D. PRUTCHI, M. NORRIS, “Design and Development of Medical Electronic Instrumentation”, Wiley-Interscience, John Wiley and Sons, 2005
- [24] N. J. MULLER, “Bluetooth Demystified”, McGraw-Hill Telecom, 2001
- [25] C. DE M. CORDEIRO, D. P. AGRAMAL, “Ad Hoc & Sensor Networks: Theory and Applications”, World Scientific Publishing Co., 2006
- [26] J. GEIER, “Wireless LANs: Implementing High Performance IEEE 802.11 Networks”, Sams Publishing, 2002
- [27] T. COOKLEV, “Wireless communications standards: a study of IEEE 802.11, 802.15 and 802.16”, Standards Information Network, IEEE Press, 2004
- [28] I.F. AKYILDIZ, W. SU, Y. SANKARASUBRAMANIAM, E. CAYIRCI, “Wireless sensor networks: a survey”, *Computer Networks 38*, Elsevier Science B.V., 2002
- [29] P. S. PANDIAN, K. P. SAFEER, PRAGATI GUPTA, D. T. SHAKUNTHALA, B. S. SUN-

- DERSHESHU AND V. C. PADAKI, “Wireless Sensor Network for Wearable Physiological Monitoring”, *Journal of Networks*, Vol. 3, 2008
- [30] H. BALDUS, K. KLABUNDE, AND G. MÜSCH, “Reliable Set-Up of Medical Body-Sensor Networks”, Philips Research Laboratories Aachen, 2004,
URL: <http://nslab.kaist.ac.kr/courses/2007/cs712/body%20sensor%20networks/Reliable%20Set-Up%20of%20Medical%20Body-Sensor%20Networks.pdf>
- [31] A. VARSHAVSKY, A. SCANNELL, A. LAMARCA, E. DE LARA, J. KRUMM, G. D. ABOWD, A. SENEVIRATNE, T. STRANG, “Amigo: Proximity-based Authentication of Mobile Devices”, Springer-Verlag, *Ubicomp07*, 4717, p.253-270, 2007,
URL: <http://www.cs.washington.edu/education/courses/cse590u/07au/papers/varshavsky.pdf>
- [32] J. KORHONEN AND Y. WANG, “Effect of Packet Size on Loss Rate and Delay in Wireless Links”, 2005 IEEE Wireless Communications and Network Conference (WCNC-05), 2005
- [33] J. MALINEN, “Host AP driver website”, 2002-2007 (date accessed: 2010),
URL: <http://hostap.epitest.fi/>
- [34] PHILIPS MEDIZIN SYSTEME BOÖBLINGEN GMBH,
Conference calls and visit to the customer premises in Böblingen, Germany, where the Patient Monitoring division of Philips Healthcare is based, and for which the project was carried out by Philips Research, Distributed Sensors Systems,
Conference calls: 2009-2010, Customer visit: June 2010
- [35] T.M. NAZMUL HUDA, MD. NUR MOSTOFA, “Throughput Enhancement of IEEE 802.11 WLAN for Next Generation Communications”, Department of Telecommunication Systems, School of Engineering, Blekinge Institute of Technology (BTH), Karlskrona, Sweden, URL: <http://docslide.us/documents/throughput-enhancement-of-ieee-80211-wlan-for-next-generation-communications.html>, 2007 (date accessed: 2016)
- [36] I. RAMANI, S. SAVAGE, “SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks”, Department of Computer Science & Engineering, University of California, San Diego, Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. (Volume:1),
URL: <https://cseweb.ucsd.edu/~savage/papers/Infocom05.pdf>, March 2005
- [37] H. WU, K. TAN, Y. ZHANG, Q. ZHANG, “Proactive Scan: Fast Handoff with Smart Triggers for 802.11 Wireless LAN”, Wireless & Networking Group Microsoft Research Asia, Hong Kong University of Science and Technology, IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications,
URL: https://www.researchgate.net/publication/221243150_Proactive_Scan_Fast_Handoff_with_Smart_Triggers_for_80211_Wireless_LAN, May 2007

- [38] THE LINUX KERNEL ORGANIZATION, “Official Linux Wireless wiki website”, *The main source of Documentation for the Linux wireless (IEEE-802.11) subsystem*
URL: <https://wireless.wiki.kernel.org/en/users/drivers>, 2015-2016 (date accessed: 2016)
- [39] Y. LINM S. CHANG, J. YEH, S. CHENG, “Indoor deployment of IEEE 802.11s mesh networks: Lessons and guidelines”, Department of Computer Engineering, National Chiao Tung University, Taiwan, ROC; Realtek Semiconductor Corp., Taiwan, ROC, Ad Hoc Networks, Elsevier
URL: <http://dx.doi.org/10.1016/j.adhoc.2011.03.003>, 2011
- [40] BLUETOOTH SPECIAL INTEREST GROUP, SIG, “Bluetooth core specification”,
URL: <https://www.bluetooth.com/>, Date accessed: 2010-2016
- [41] WI-FI ALLIANCE, TDLS TASK GROUP, IEEE 802.11z TDLS Task Group documentation: “WFA Scheduled Peer Power Save Mode for TDLS normative, Draft, 2008”, “TDLS Peer Discovery, doc.: IEEE 802.11-09/1218r4, 2009”, “WFA TDLS Use Case Document, version 1.0, 2010”, “TDLS Whitepaper, August 2012”
URL: http://www.wi-fi.org/download.php?file=/sites/default/files/private/20120808_TDLS_White_Paper_FINAL_0.pdf and others WFA confidential, Retrieved from the Wi-Fi Alliance website with Philips account as a WFA member company, from 2010 to 2012

Appendix A

Wireless patient monitoring state of the art

In this appendix, an identification of the available products of the main companies on the market addressing the specific problem of wireless monitoring of vital signs is presented.

Aerotel

Aerotel is an Israel-based, medium-sized company with activities throughout the world. They mostly operate as a product vendor, with devices for the measuring of blood pressure, ECG, blood glucose, weight, SPO2, respiratory rhythm, and remote monitoring software. They provide full-service solutions for telehealth applications, offering an inpatient monitoring system that consists of a medical call centre software and monitoring devices that transfer vital, medical or lifestyle data over the telephone, the Internet or wireless networks. The patient information and the transmitted data can be viewed locally or via the Internet.

URL: <http://www.aerotel.com/es/products-and-solutions/e-cliniq-remote-monitoring.html>

Cardionet Inc. - Agility - Braemar

The US based company CardioNet provides outsourcing services for medical corporations, for instance the possibility to contract the development of medical devices, related software and outsource clinical research through its subsidiary Agility Centralized Research Services Inc.

Through its subsidiary Braemar, it manufactures and markets ambulatory cardiac monitoring devices, a computer based diagnostic monitoring system and a family of patient-worn battery powered diagnostic cardiology devices.

URL: www.cardionet.com

CAS Medical Systems

The United States based CASMED provides medical products and supplies related to remote monitoring to hospitals, emergency medical services, home care providers and original equipment manufacturers (OEMs). Its OEM Services includes the production of blood pressure monitoring and other respiratory monitoring systems including bedside monitors to portable monitors.

URL: www.casmed.com

Dräger Medical AG & Co

The German company is a cooperation between Drägerwerk AG and Siemens AG. It has a comprehensive product portfolio of patient monitoring systems for emergency, perioperative, critical care, perinatal care and homecare. Its portfolio comprises various vital signs monitors, both fixed and to be worn by the patient, as well as solutions for centralized real-time management of non-ambulatory and telemetry patients.



Figure A.1: Dräger's Infinity Delta XL

Dräger's *Infinity Delta XL* (see Figure A.1) serves as both a bedside and transport monitor to continuously monitor patients hospital-wide. Specially designed for monitoring high-acuity patients, has a 12.2" colour display. The wireless operation in this unit is performed by a state-of-the-art wireless card that offers Wi-Fi technology (802.11g) and enhanced security (WPA2).[12]

Infinity Gamma XL is a compact vital signs monitor that can operate as a standalone device or as part of the Infinity Network. It provides a full set of the most commonly used parameters



Figure A.2: *Dräger's* Infinity Gamma XL

for monitoring adult, paediatric and neonatal patients, an 8.4" colour screen and is ideal for low-acuity to mid-acuity care environments.



Figure A.3: *Dräger's* Infinity M300

Dräger's *Infinity M300* (see Figure A.3) is a patient-worn telemetry device, equipped with 802.11b/g technology and WPA2 standard encryption support. Direct communication to the *Infinity CentralStation* through the *Infinity OneNet* facilitates wireless data exchange. It provides continuous standalone monitoring, even if the patient moves out of the wireless network coverage area.

All the Infinity product range relies on the Infinity Docking Stations which can store monitoring settings (waveforms parameters, alarms, etc.) for each patient or each hospital department so all monitors docked on them can reflect the specific configuration schemes automatically. Furthermore the XL bedside monitors incorporate Dräger's Pick and Go technology, which provide seamless wired-to-wireless networking, so surveillance can be continuous, without waiting

for a transport monitor nor disconnecting or reconnecting leads, and therefore without gaps in monitoring or data acquisition.

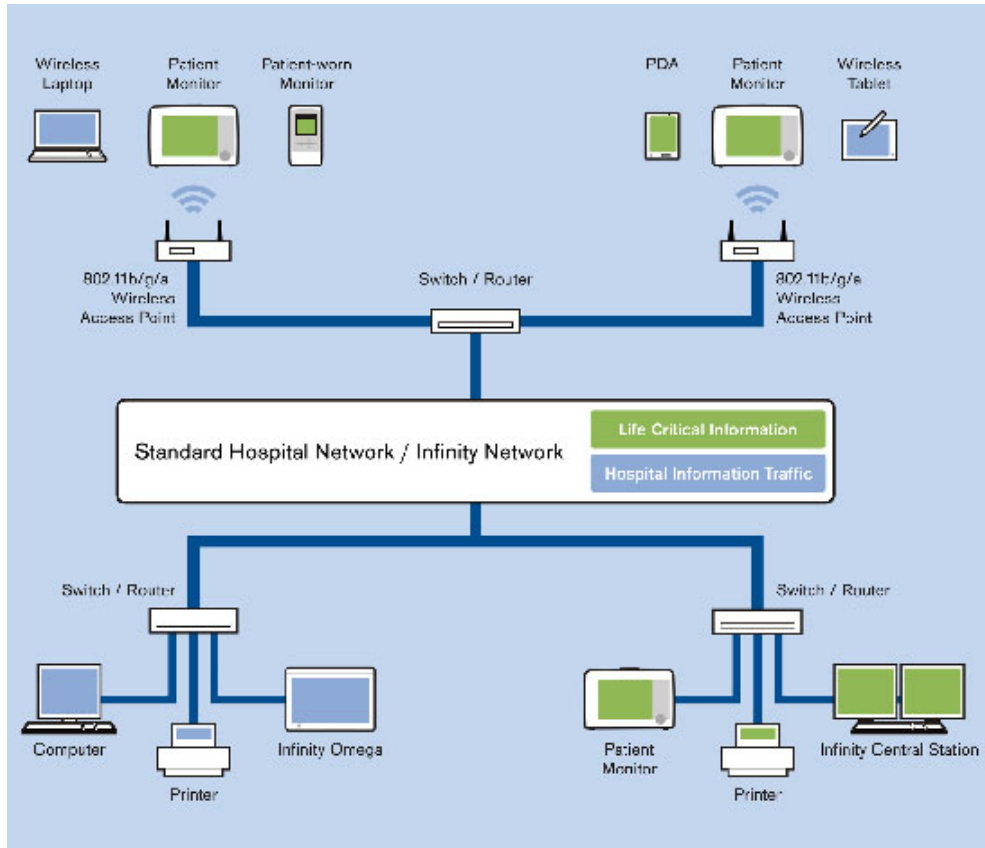


Figure A.4: Dräger's Infinity OneNet architecture

This company's solution is based on the *Infinity OneNet* architecture (see Figure A.4), a shared infrastructure approach that integrates patient monitoring systems into existing hospital-wide wired and wireless networks, rather than requiring a separate network, thanks to Dräger's Infinity gateways which segregate and prioritize life-critical information over hospital information. *Infinity Delta XL* monitors can be networked, moving seamlessly from wired at the bedside to wireless for patient transport. Besides, patient information collected at the bedside and on transport can flow through the Infinity Network to the Infinity CentralStation for central surveillance and to the proprietary *Innovian* patient data management system.

- Allows monitoring devices to share same Wi-Fi access points as hospital's existing network devices.
- QoS by managing network traffic.
- Requires Dräger validated access points, from many of the major network equipment providers that meet industry standards and Dräger's networking requirements.

Conclusions on Dräger's wireless patient monitoring products range:

- Dräger's solution does not contemplate a direct connection between the portable (patient-worn, in this case) device and the bedside monitoring device.
- This solution is available in the market since 2008, in this company's portfolio, and providing QoS management.
- This solution depends on the adoption of the *Infinity OneNet* architecture in the whole hospital network, using compatible Wi-Fi infrastructure equipment from specific validated vendors.

Fukuda Denshi

The Japanese Company Fukuda Denshi produces cardiology instrumentation, patient monitoring and ultrasound technologies, with its main line of product markets catering to the needs for monitoring equipment for critical care and diagnostic ultrasound equipment. Additionally the company produces portable and rugged ECG and digital holter recorder, which is waterproof and can be worn by the patient in their daily life.

URL: www.fukuda.co.jp/english

GE Healthcare

Headquartered in the United Kingdom, GE Healthcare is a worldwide unit of General Electric Company providing medical technologies that are shaping innovations in patient care.

In the field of patient monitoring systems, GE Healthcare offers a comprehensive line of products for different care settings.

Their wireless monitoring systems are mainly based in telemetry systems, conforming the ApexPro family of products which operate in both the 608 to 614 MHz and 1395 to 1400 MHz ranges of WMTS (Wireless Medical Telemetry Service) while the ApexPro FH relies on an access point-based, Frequency-Hopping Spread Spectrum (FHSS) infrastructure which provides with more scalability.

WLAN equipped Monitors: The Dash family of monitors from GE Healthcare provides flexibility in a single platform. With a comprehensive set of clinical parameters, Dash monitors capture vital patient measurements while sophisticated algorithms help prevent false alarms. Dash monitors are highly configurable, enabling to add features and parameters accommodating varying acuity levels for patients across the care continuum. From presentation in the Emergency Department to surgery in the OR to recovery in the PACU, treatment in the ICU and transfer to the Stepdown unit, the Dash monitor is an excellent choice for every point of care.

An integrated wireless LAN option is available for Dash monitors, maintaining a connection

to the CARESCAPE Network and the CARESCAPE CIC Pro central station. Using 802.11b technology, Dash monitors are designed for integration into commonly utilized existing wireless networks, leveraging hospital's investment in current IT infrastructure. Dash monitors in the Combo/Rover mode, combined with the ApexPro telemetry system, enable wireless ECG monitoring.



Figure A.5: *GE Dash patient monitors*

The Dash 5000 is a wireless capable, modular monitor with a full range of clinical parameters. It has a 12.1 inch screen and additional hardkeys for Standby, Admit/Discharge, NIBP Auto, Trend and Main View.



Figure A.6: *GE Dash 5000 patient monitor*

Connectivity and network solutions: To support and provide connectivity for the real-time patient data this company counts with an integrated platform for Clinical Information Logistics, called CARESCAPE Network, which can be whether implemented as a segregated network or as an integrated VLAN on the hospital's infrastructure:

- *VLAN:* A current trend in the marketplace is to utilize VLANs to enable one set of switches to handle multiple networks. With a VLAN configuration, the CARESCAPE Network can share the same switches that the hospital uses to operate all of its other devices including laptops and wired VoIP phones. Advantages: Simplification; Resource sharing (access points for wireless communication, servers for SNMP, DHCP and NTP services and WAN connections for cross-geography data transfers); Networking management.
- *Segregated network:* In a segregated configuration, the CARESCAPE Network is physically separate from the hospital's Enterprise network; it operates on its own switches and

Ethernet cabling. Advantages: Uptime (Since the network operates on its own equipment, other types of enterprise data cannot interrupt the CARESCAPE Network); Performance (uniform performance because it does not share bandwidth with other enterprise data streams); Security (Segregated networks cannot be compromised from other enterprise data VLANs)



Figure A.7: *GE CARESCAPE Network hospital-wide deployment for wireless patient monitoring, WMTS telemetry, two-way radio and VoIP phones*

The CARESCAPE Network conveniently integrates all patient-critical real-time data throughout the enterprise to support informed decision-making. Main features:

- Relies on a hybrid fiber and coax broadband design
- Integrates in a single network all the hospital's communication ecosystem and wireless services together on one comprehensive infrastructure.
- Supports real-time wireless monitoring and alarm notification for continuous patient surveillance, while simultaneously delivering clinical intelligence enterprise-wide, supporting communication devices and technologies such as in-building cellular and public safety communications among others. CARESCAPE Network meets the network specifications of:
 - Wired and wireless patient monitoring systems
 - ApexPro WMTS telemetry systems
 - Fire and Safety communications
 - Cellular viewers
 - Two-way radio

- Cellular and PCS/VoIP phones for voice and data communication
- Standard-based: Ethernet and IP-based network.
- Peer-to-Peer: The CARESCAPE Network does not rely on a central server for data about other servers and monitors.
- Redundancy: Because it is based on Ethernet and utilizes standard network switches, the CARESCAPE Network can be setup in a redundant configuration to help increase uptime.
- QoS: Patient critical data can be given priority over other types of enterprise data.

URL: http://www.gehealthcare.com/eues/patient_monitoring/products/imm-monitoring/index.html

Medic4All/Telcomed

Medic4All is a holding company active in the field of telemedicine, with origins in Israel it is now based in Switzerland, the Irish Telcomed belongs to the holding. Their activities split into two branches: services and technology. The Israel based technology branch develops and manufactures medical monitoring devices, gateways and software applications while it is in Italy that specialised services are developed around their technology to provide complementary telemedicine services for its products.

URL: www.telcomed.ie

Meigaoy

This Chinese company develops, manufactures and sells medical devices. Its portfolio includes Holter System, Multifunction PC-ECG System, Stress Test ECG System, Telemetry ECG Monitoring System, Ambulatory Blood Pressure Monitor and ECG Network Information System.

URL: www.meigaoy.com

Nihon Kohden

Nihon Kohden is a Japan based manufacturer, developer, and distributor of medical electronic equipment. The portfolio includes supplies products for patient monitoring, neurology, sleep assessment, and cardiology. While their products target institutional care, their wireless ECG can be connected through a health hub and record events in case the patient is moving out of the wireless range.

URL: <http://www.nihonkohden.com/products/type/mon/>

OBS Medical

The British company OBS Medical was formed as a merge of two spin-offs from Oxford University and initially developed signal processing solutions for the healthcare sector and algorithms for monitoring jet engines. It offers a range of solutions for integrated in-hospital monitoring, RMT and telecare.

URL: <http://www.obsmedical.com/products/visensia>

Philips Healthcare

Royal Philips Electronics of the Netherlands readjusted its strategic focus on health and wellbeing and as such operates professional and consumer markets through three overlapping sectors: Healthcare, Lighting and Consumer Lifestyle. Its subsidiary Philips Healthcare is among the top global makers of medical imaging equipment, patient monitors, resuscitation products, and telehealth monitoring products and solutions.

See appendix E for further information on the Philips Healthcare's Patient Monitoring division products.

Schiller

The Swiss based company SCHILLER develops, produces and distributes medical devices for cardiopulmonary diagnostics, patient monitoring and emergency medicine. Its product portfolio includes portable ECG device, a pocket defibrillator and multi-functional diagnostic systems.

URL: www.schiller.ch

Smiths Medical PM Inc.

Smiths Medical PM, Inc. is a designer, manufacturer, and distributor of the BCI® brand of patient monitoring equipment and a distributor of the Pneupac® brand of MRI compatible transport ventilators. The RMT related product portfolio of the company comprises both bedside devices for an institutional care and portable RMT devices for the use outside of a hospital.

URL: www.smiths-medical.com/

Sotera Wireless Inc.

The start up Sotera Wireless Inc., formerly Triage, is developing a new method for measuring continuous blood pressure without a cuff and a platform for wireless body-worn patient monitoring, which allows practitioners to follow their patients' body signals throughout all stages of their treatment.

URL: www.soterawireless.com/

Welch Allyn

The United States based Welch Allyn manufactures patient monitoring systems and connected solutions in the health care field for the United States based market and internationally. Their products include also medical diagnostic devices and other general medical electronic equipment for cardiology, physical diagnosis, etc. focusing on blood pressure management products, including sphygmomanometers and home blood pressure management

Welch Allyn's *FlexNet* technology allows to operate real-time patient monitoring on a shared 802.11 a/b/g network along with other hospital applications. This technology offers robust performance and scalability, the highest standards for network security, minimal bandwidth requirements for continuous monitoring data and minimal power consumption for industry-leading monitor battery life.[13]

- Fully shared 802.11 a/b/g network. Patient monitoring limited to 802.11a in the 5GHz band.
- Centralized network management and lower ongoing operating, support and infrastructure costs.
- No proprietary infrastructure components. Standards-based enterprise solution.
- Seamless co-existence with FHSS on the same Welch Allyn *Acuity Central Monitoring System*.
- Supports Wireless Intrusion Detection and Prevention.
- 802.11e Quality of Service (QoS) with 802.1q tagging.

Supported wireless vendors. Although Welch Allyn's solution claims to be based on no proprietary infrastructure components, it is not compatible with all existent wireless network vendors. Its functioning is limited to a list of vendor brands whose wireless equipments are supported by the Welch Allyn's *FlexNet* solution: Aruba Networks Mobility Platform:

- Thin Access Point, Centralized Control Architecture.

- Welch Allyn dedicated networks and shared networks.

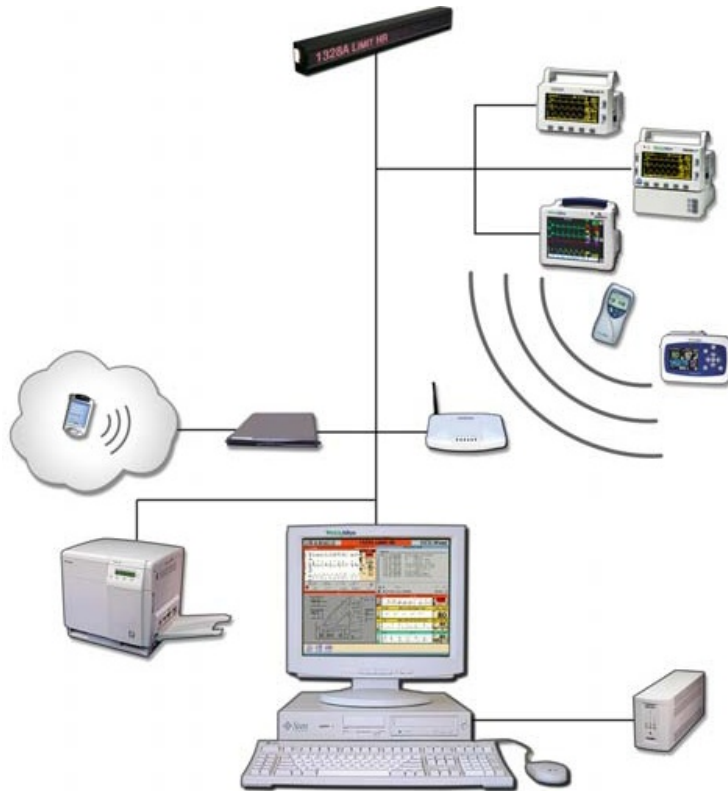


Figure A.8: *Welch Allyn's Acuity System overview*

Welch Allyn's *Acuity Central Monitoring System* (see figure A.8) is a fully integrated system that provides hospital managers with a full solution, including patient admission and discharge management, wireless and wired monitoring management, patient-monitor assignment by room/location, patient-specific alarms and waveform remote monitoring.

Welch Allyn's *Propaq CS* is a base monitor with optional wireless connectivity to *Acuity Central Station*. See figure A.9.



Figure A.9: *Welch Allyn's Propaq CS*

Welch Allyn's *Micropaq Wearable Monitor* (see figure A.10) is a limited monitoring device designed to wirelessly connect to Welch Allyn's *Acuity Central Monitoring System*, that does not work as a standalone monitor.



Figure A.10: *Welch Allyn's Micropaq Wearable Monitor*

Conclusions on Welch Allyn's wireless patient monitoring products:

- Welch Allyn's solution does not contemplate a direct connection between the wearable device and the wall-mounted monitoring device.
- This solution is available in the market since 2008, in this company's portfolio, and providing QoS management.
- The FlexNet solution depends on the adoption of the specific wireless equipment supported in the whole hospital network.

Appendix B

Hardware specifications

This appendix includes the specifications of the hardware utilized for the implementation of the wireless patient monitoring prototypes described in chapter 6.

B.1 WRT54GL Linksys Linux based router by Cisco

The following pages are the WRT54GL specifications. Filename:

Datasheet WRT54GL_V1.1.pdf

Actual /proc/cpuinfo output

```
system type           : Broadcom BCM5352 chip rev 0
cpu model             : BCM3302 V0.8
BogoMIPS              : 199.47
wait instruction      : no
microsecond timers    : yes
tlb\_entries          : 32
extra interrupt vector : no
hardware watchpoint   : no
VCEd exceptions       : not available
VCEI exceptions       : not available
Flash : 4 MB NAND, single chip
System Memory : 16 MB 16-bit DDR SDRAM
Wireless Radio : Broadcom BCM43xx 802.11b/g
Antenna : Dual folding, removable, rotating antennas
Network Switch : (4) 10/100 LAN + (1) 10/100 WAN,
  Auto MDX/MDI-X (Integrated in CPU)
Serial pinout : Yes
JTAG pinout : Yes
```


Linux Wireless

The Linux-based Wireless-G Linux Broadband Router was created specially for hobbyists and wireless aficionados. Add wireless capability to your wired network and enjoy the convenience that comes when you eliminate cables. Add wireless devices to your network. With less wiring, you'll do much more.

Wireless Convenience

You've got the network—now enhance it with Wireless-G access up to 54 Mbps. Now it's easy to grow your network by adding computers, printers and other wireless devices, without stringing cables. Also compatible with Wireless-B devices. Reliable connectivity allows you to move your laptops, or set up your devices all around your home or office. Or add Access Points to two separate networks and create "cable-less cable" connectivity between them.

Easy Configuration

Device and security configuration is a snap with the Browser-based configuration utility.

Complete Security

Work with confidence. Industrial-strength encryption helps keep your communications protected and private. Access filter lets you control who can get on your wireless network.

DATASHEET

Give your wired network wireless connectivity

Easy setup and configuration

128-bit security encryption, access filtering



Wireless-G Linux Broadband Router

Model: WRT54GL

Features

- Complies with 802.11g and 802.11b (2.4 GHz) Standards
- Unsurpassed Wireless Security with Wi-Fi Protected Access™ 2 (WPA2)
- Enhanced Internet Security Management Functions including Internet Access Policies with Time Schedules
- All LAN Ports Support Auto-Crossover (MDI/MDI-X) — No Need for Crossover Cables



Cisco Consumer Business Group
121 Theory
Irvine, CA 92617 USA

www.linksysbycisco.com

Linksys, Cisco and the Cisco Logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Other brands and product names are trademarks or registered trademarks of their respective holders. Copyright © 2009 Cisco Systems, Inc. All rights reserved.

Specifications

Model	WRT54GL
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Ports	Internet: One 10/100 RJ-45 Port Ethernet: Four 10/100 RJ-45 Switched Ports One Power Port
Buttons	One Reset Button
LEDs	Power, DMZ, WLAN, Ethernet (1, 2, 3, 4), Internet
Cabling Type	CAT 5
RF Power (EIRP) in dBm	18
UPnP able/cert	Able
Security Features	Stateful Packet Inspection (SPI) Firewall, Internet Policy
Wireless Security	Wi-Fi Protected Access™ 2 (WPA2), WEP, Wireless MAC Filtering

Environmental

Dimensions	7.32" x 1.89" x 7.87" (186 x 48 x 200 mm)
Weight	17.0 oz (482 g)
Power	12VDC, 1A
Certification	FCC, ICES-003, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 158°F (-20 to 70°C)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Package Contents

- Wireless-G Linux Broadband Router
- Setup Software and User Guide on CD-ROM
- Power Adapter
- Network Cable

Minimum Requirements

- Internet Explorer 6 or Firefox 2 or Higher for Browser-based configuration
- CD-ROM Drive
- Windows XP, Vista, or Vista 64-bit Edition with Latest Updates
- Wired or Wireless Network Adapter.

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

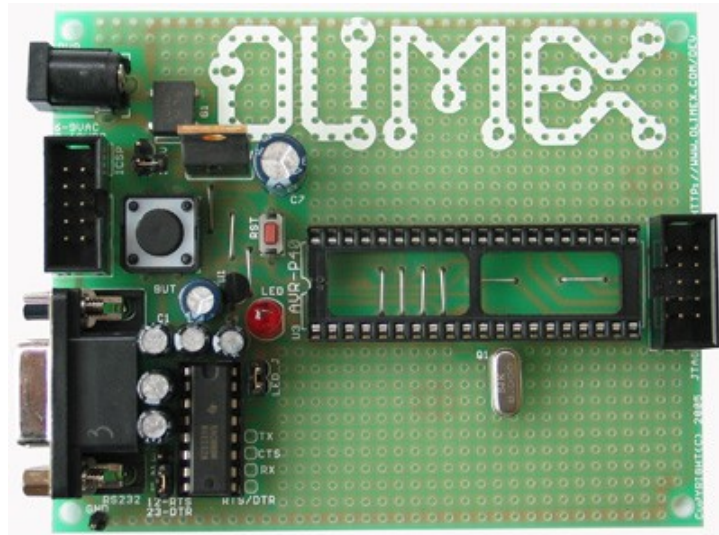
Specifications are subject to change without notice.

09021911NC-AI
3415-01458

Model: **WRT54GL**

B.2 AVR-P40-8535 Microcontroller Prototype Board by Olimex

The following pages are the AVR-P40-8535 Olimex development board specifications. Filename:
AVR-P40-8535.pdf



AVR-P40-8535 development board _____ Users Manual



All boards produced by Olimex are ROHS compliant

Revision A, October 2009
Copyright(c) 2009, OLIMEX Ltd, All rights reserved

INTRODUCTION

The **AVR Microcontroller** are low-power CMOS 8-bit controller based on the RISC architecture. The AVR core combines a rich instruction set with general purpose working registers. All the registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

The **AVR-P40-8535** is prototype board for 40 pin AVR microcontrollers with STKxxx compatible 10 pin ICSP connector.

BOARD FEATURES

- STK200 compatible ICSP 5x2 pin connector for in-circuit programming with AVR-PG1 or AVR-PG2
- JTAG 5x2 pin connectr for in-circuit programming and debugging with AVR-JTAG-USB and AVR-JTAG-L
- RS232 Tx, Rx interface with MAX232 IC on socket
- 8 MHz crystal on socket (user can replace with any value)
- reset IC ZM33064
- reset button
- general purpose push button
- status LED connected to PB0 via removable jumper
- DIL40 microcontroller socket
- Power plug-in jack
- selectable +3.3V / +5V power supply voltage regulator
- extension pin headers for each uC pin
- four mounting holes 3.3 mm (0.13")
- GND bus
- Vcc bus
- FR-4, 1.5 mm (0,062"), green soldermask, white silkscreen component print
- dimensions 100x80 mm (3.9x3.15")

ELECTROSTATIC WARNING

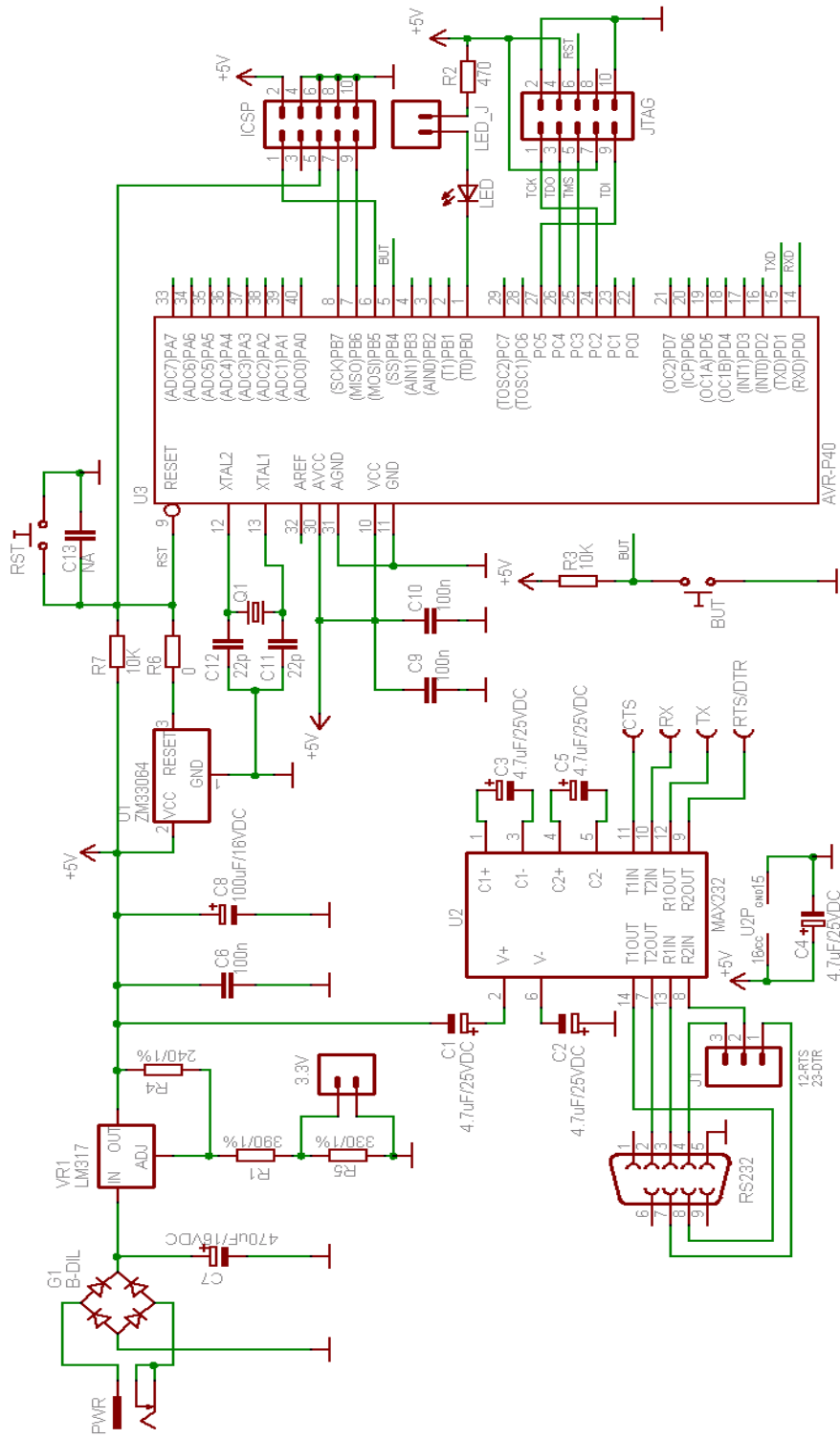
The AVR-P40-8535 board is shipped in protective anti-static packaging. The board must not be subject to high electrostatic potentials. General practice for working with static sensitive devices should be applied when working with this board.

BOARD USE REQUIREMENTS

Cables: The cable you will need depends on the programmer/debugger you use. If you use [AVR-PG1](#), or [AVR-JTAG-L](#), you will need RS232 cable, if you use [AVR-PG2](#), you will need LPT cable, if you use [AVR-ISP500](#), [AVR-ISP500-TINY](#), [AVR-ISP500-ISO](#), or [AVR-USB-JTAG](#) you will need 1.8 meter USB A-B cable.

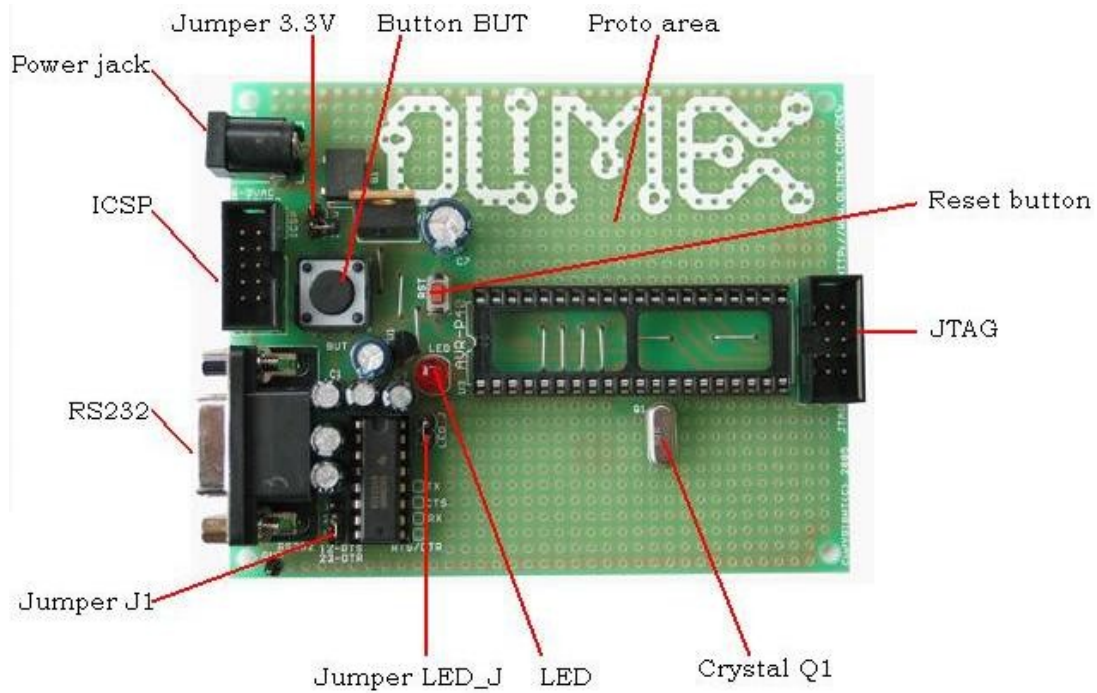
Hardware: Programmer/Debugger - one of the Olimex AVR Programmers: AVR-PG1, AVR-PG2, AVR-ISP500, AVR-ISP500-TINY, AVR-ISP500-ISO, AVR-JTAG-L, AVR-USB-JTAG.

SCHEMATIC



Copyright (C) 2002, OLIMEX Ltd
<http://www.olimex.com/dev>

BOARD LAYOUT



POWER SUPPLY CIRCUIT

AVR-P40-8535 is typically power supplied with min 9.0V DC max 12.0V DC, or min 6.0V AC max 9.0V AC.

RESET CIRCUIT

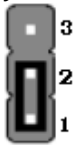
AVR-P40-8535 reset circuit includes pin 5 of ICSP connector, pin 6 of JTAG connector, pin 9 of U3, Reset scheme - U1 and RESET button (RST).

CLOCK CIRCUIT

Quartz crystal 8MHz is connected to AVR Microcontroller pin 12 (XTAL2) and pin 13 (XTAL1).

JUMPER DESCRIPTION

J1



When 1-2 are shorted - RTS is connected to terminal pin RTS/DTR.
 When 2-3 are shorted - DTR is connected to terminal pin RTS/DTR.
Default state is 1-2.

LED_J



When this jumper is open - LED is not connected.
 When this jumper is closed - LED is connected to pin1 (T0/PB0) of the Microcontroller.
Default state is closed.

3.3V



When this jumper is open - LM317 output is 5V DC.
 When this jumper is closed - LM317 output is 3.3V DC.
Default state is open.

WARNINGS!!!

1. The 3.3V jumper selects the power voltage to be 5V (open) or 3.3V (closed). MAX3232 can operate only at 5V power supply so if you are working with 3.3V you should replace it with MAX3232 which works at 3.3V power supply.
2. If you want to operate with 3,3V power supply, remove R6 resistor.

INPUT/OUTPUT

Status Led with name **LED (red)** - this led is connected to PIN1 (T0 / PB0) via jumper LED_J.

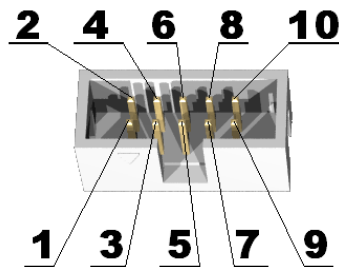
User **button** with name **BUT** - connected to PIN5 (SS / PB4).

Reset **button** with name **RST** - connected to PIN9 (RESET).

CONNECTOR DESCRIPTIONS

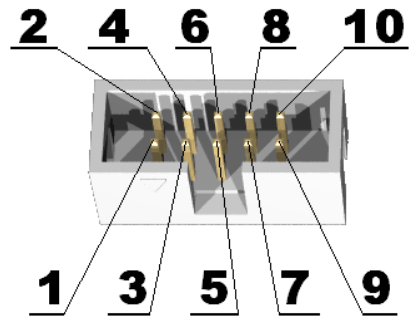
ICSP

PIN #	Signal Name	Functionality
1	MOSI	MOSI / PB5
2	VCC	+5V DC
3	Not connected	-
4	GND	Ground
5	RST	RESET
6	GND	Ground
7	SCK	SCK / PB7
8	GND	Ground
9	MISO	MISO / PB6
10	GND	Ground



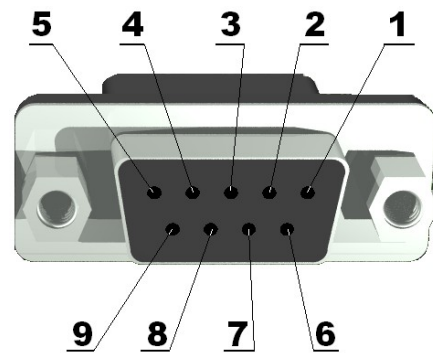
JTAG

PIN #	Signal Name	Functionality
1	TCK	PC2
2	GND	Ground
3	TDO	PC4
4	VREF	+5V DC
5	TMS	PC3
6	NSRST	Reset
7	VCC	+5V DC
8	NTRST	Not connected
9	TDI	PC5
10	GND	Ground



RS232

PIN #	Signal Name
1	CD - Not connected
2	RXD
3	TXD
4	DTR
5	GND
6	DSR - Not connected
7	RTS
8	CTS
9	RI - Not connected

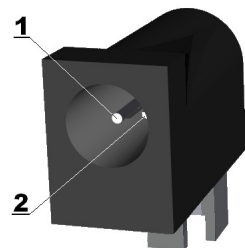


Note1: RTS and DTR is connected to terminal pins via jumper J1, which position is describe bellow.

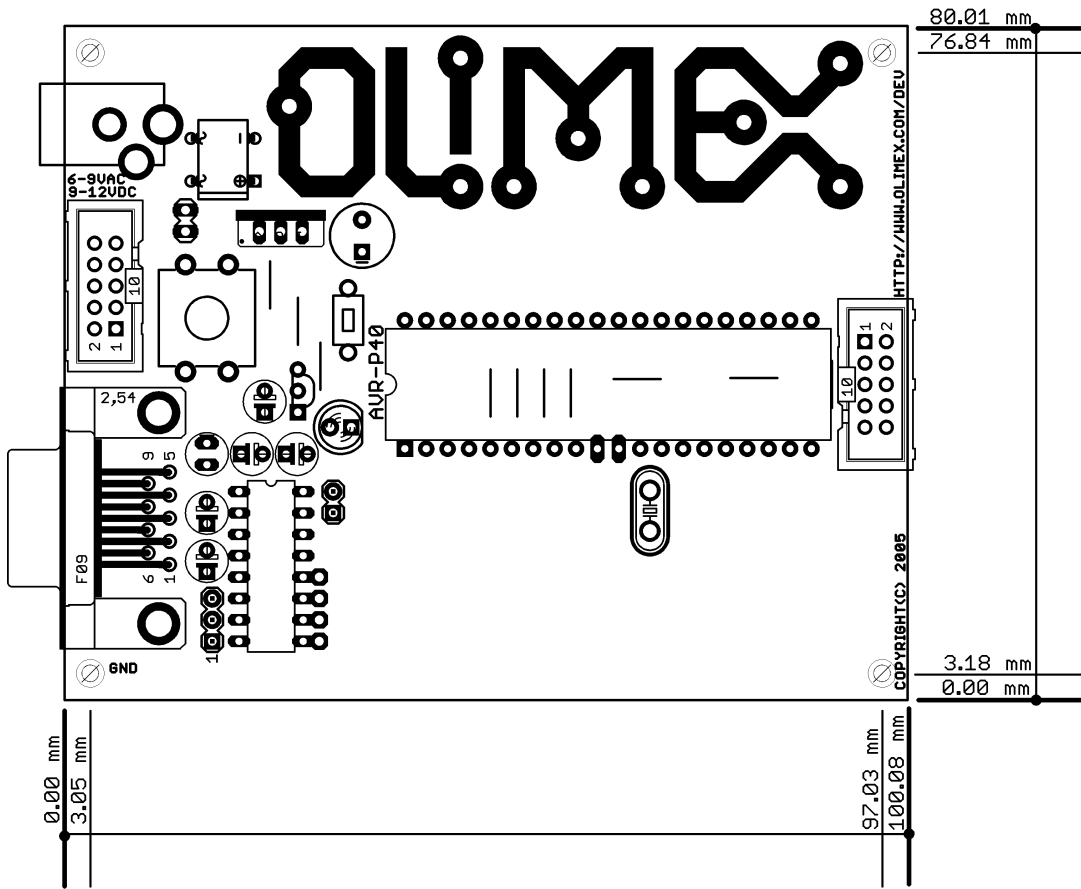
Note2: RX RS232 driver pins have to be connected to AVR microcontroller pin - TXD/PD1 (PIN 15).
TX RS232 driver pins have to be connected to AVR microcontroller pin - RXD/PD0 (PIN 14).

PWR

PIN #	Signal Name
1	Power Input
2	GND



MECHANICAL DIMENSIONS



B.3 ATmega32 40-pin DIP package microcontroller by Atmel

The following pages are the AVR ATmega32 Atmel microcontroller specifications. Filename:

Atmel AVR ATmega32 summary - doc2503s.pdf

Features

- High-performance, Low-power Atmel® AVR® 8-bit Microcontroller
- Advanced RISC Architecture
 - 131 Powerful Instructions – Most Single-clock Cycle Execution
 - 32 x 8 General Purpose Working Registers
 - Fully Static Operation
 - Up to 16 MIPS Throughput at 16 MHz
 - On-chip 2-cycle Multiplier
- High Endurance Non-volatile Memory segments
 - 32Kbytes of In-System Self-programmable Flash program memory
 - 1024Bytes EEPROM
 - 2Kbyte Internal SRAM
 - Write/Erase Cycles: 10,000 Flash/100,000 EEPROM
 - Data retention: 20 years at 85°C/100 years at 25°C⁽¹⁾
 - Optional Boot Code Section with Independent Lock Bits
 - In-System Programming by On-chip Boot Program
 - True Read-While-Write Operation
 - Programming Lock for Software Security
- JTAG (IEEE std. 1149.1 Compliant) Interface
 - Boundary-scan Capabilities According to the JTAG Standard
 - Extensive On-chip Debug Support
 - Programming of Flash, EEPROM, Fuses, and Lock Bits through the JTAG Interface
- Peripheral Features
 - Two 8-bit Timer/Counters with Separate Prescalers and Compare Modes
 - One 16-bit Timer/Counter with Separate Prescaler, Compare Mode, and Capture Mode
 - Real Time Counter with Separate Oscillator
 - Four PWM Channels
 - 8-channel, 10-bit ADC
 - 8 Single-ended Channels
 - 7 Differential Channels in TQFP Package Only
 - 2 Differential Channels with Programmable Gain at 1x, 10x, or 200x
 - Byte-oriented Two-wire Serial Interface
 - Programmable Serial USART
 - Master/Slave SPI Serial Interface
 - Programmable Watchdog Timer with Separate On-chip Oscillator
 - On-chip Analog Comparator
- Special Microcontroller Features
 - Power-on Reset and Programmable Brown-out Detection
 - Internal Calibrated RC Oscillator
 - External and Internal Interrupt Sources
 - Six Sleep Modes: Idle, ADC Noise Reduction, Power-save, Power-down, Standby and Extended Standby
- I/O and Packages
 - 32 Programmable I/O Lines
 - 40-pin PDIP, 44-lead TQFP, and 44-pad QFN/MLF
- Operating Voltages
 - 2.7V - 5.5V for ATmega32L
 - 4.5V - 5.5V for ATmega32
- Speed Grades
 - 0 - 8MHz for ATmega32L
 - 0 - 16MHz for ATmega32
- Power Consumption at 1 MHz, 3V, 25°C
 - Active: 1.1mA
 - Idle Mode: 0.35mA
 - Power-down Mode: < 1µA



**8-bit AVR®
Microcontroller
with 32KBytes
In-System
Programmable
Flash**

**ATmega32
ATmega32L**

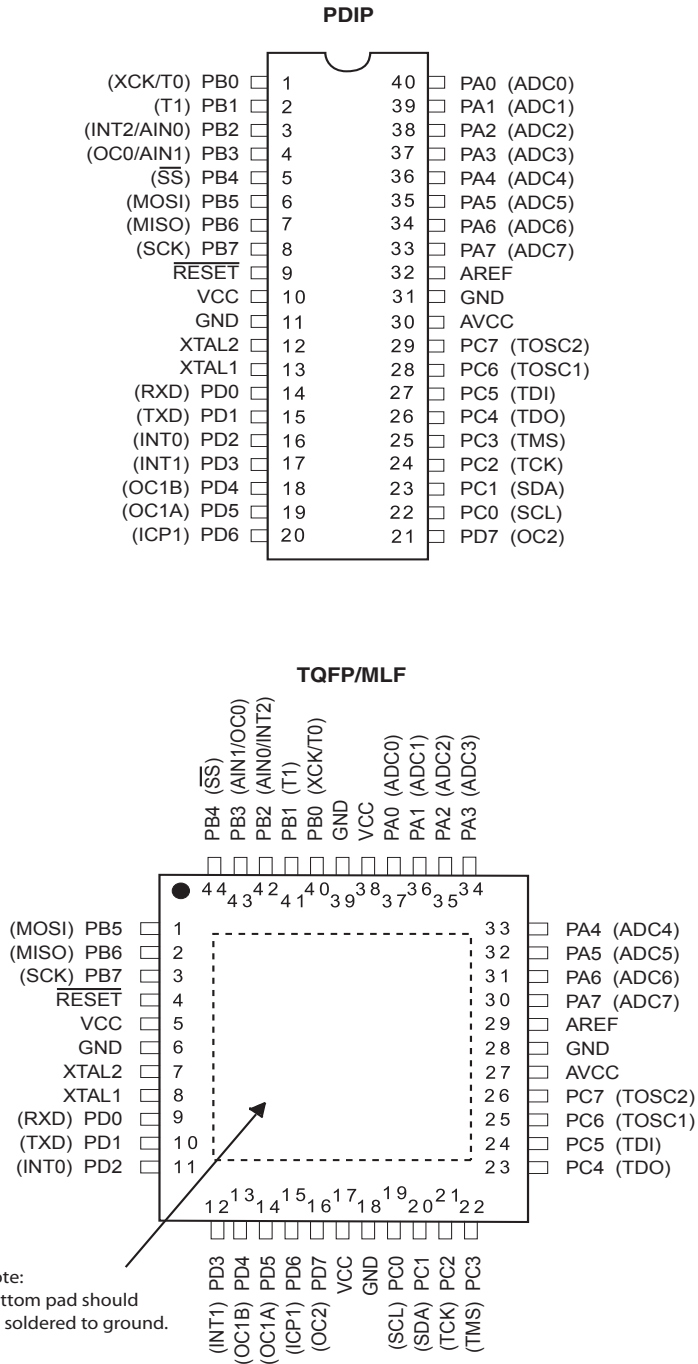
Summary

2503QS-AVR-02/11



Pin Configurations

Figure 1. Pinout ATmega32

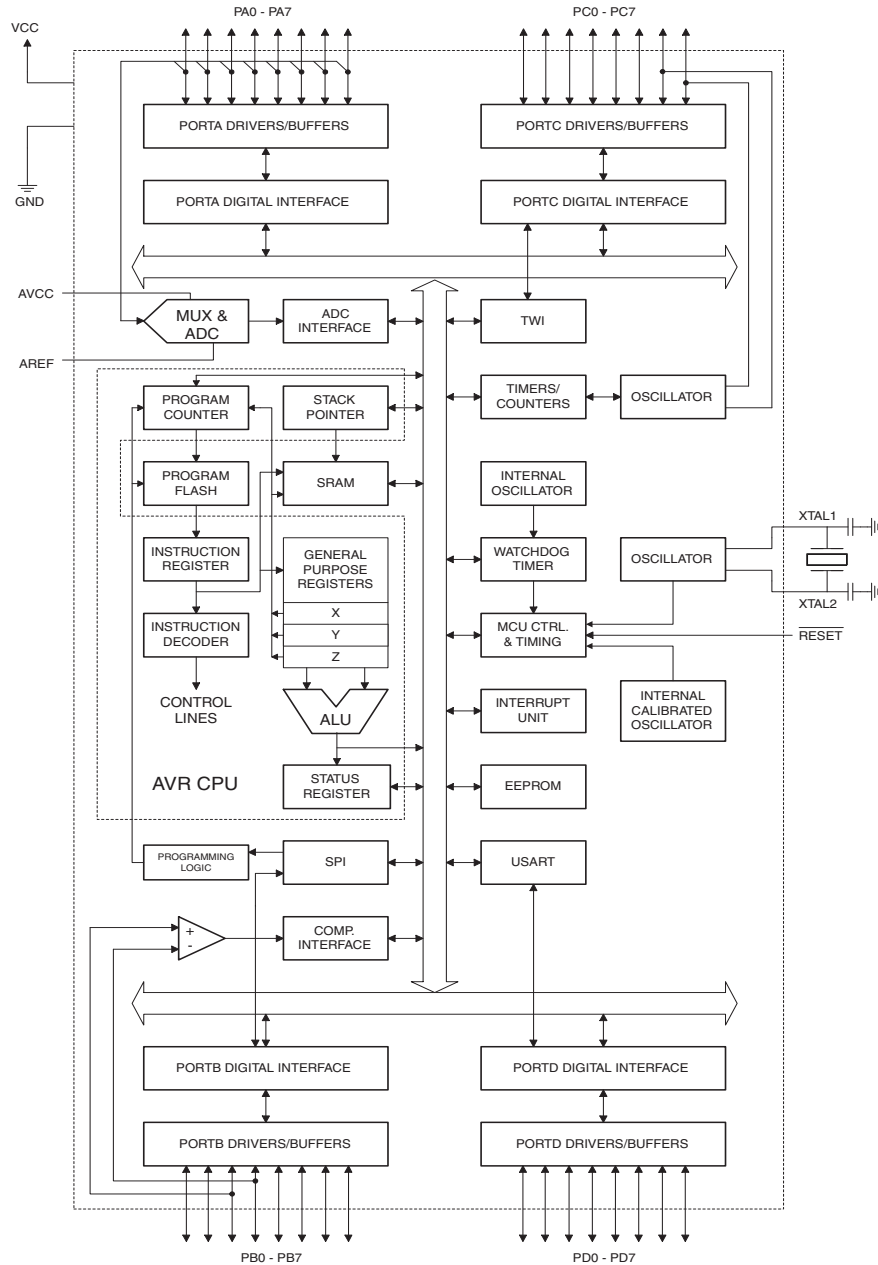


Overview

The Atmel® AVR® ATmega32 is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega32 achieves throughputs approaching 1 MIPS per MHz allowing the system designer to optimize power consumption versus processing speed.

Block Diagram

Figure 2. Block Diagram



The Atmel® AVR® core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

The ATmega32 provides the following features: 32Kbytes of In-System Programmable Flash Program memory with Read-While-Write capabilities, 1024bytes EEPROM, 2Kbyte SRAM, 32 general purpose I/O lines, 32 general purpose working registers, a JTAG interface for Boundary-scan, On-chip Debugging support and programming, three flexible Timer/Counters with compare modes, Internal and External Interrupts, a serial programmable USART, a byte oriented Two-wire Serial Interface, an 8-channel, 10-bit ADC with optional differential input stage with programmable gain (TQFP package only), a programmable Watchdog Timer with Internal Oscillator, an SPI serial port, and six software selectable power saving modes. The Idle mode stops the CPU while allowing the USART, Two-wire interface, A/D Converter, SRAM, Timer/Counters, SPI port, and interrupt system to continue functioning. The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next External Interrupt or Hardware Reset. In Power-save mode, the Asynchronous Timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except Asynchronous Timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the crystal/resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low-power consumption. In Extended Standby mode, both the main Oscillator and the Asynchronous Timer continue to run.

The device is manufactured using Atmel's high density nonvolatile memory technology. The On-chip ISP Flash allows the program memory to be reprogrammed in-system through an SPI serial interface, by a conventional nonvolatile memory programmer, or by an On-chip Boot program running on the AVR core. The boot program can use any interface to download the application program in the Application Flash memory. Software in the Boot Flash section will continue to run while the Application Flash section is updated, providing true Read-While-Write operation. By combining an 8-bit RISC CPU with In-System Self-Programmable Flash on a monolithic chip, the Atmel ATmega32 is a powerful microcontroller that provides a highly-flexible and cost-effective solution to many embedded control applications.

The Atmel AVR ATmega32 is supported with a full suite of program and system development tools including: C compilers, macro assemblers, program debugger/simulators, in-circuit emulators, and evaluation kits.

Pin Descriptions

VCC Digital supply voltage.

GND Ground.

Port A (PA7..PA0) Port A serves as the analog inputs to the A/D Converter.

Port A also serves as an 8-bit bi-directional I/O port, if the A/D Converter is not used. Port pins can provide internal pull-up resistors (selected for each bit). The Port A output buffers have symmetrical drive characteristics with both high sink and source capability. When pins PA0 to PA7 are used as inputs and are externally pulled low, they will source current if the internal pull-up resistors are activated. The Port A pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port B (PB7..PB0)	<p>Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running.</p> <p>Port B also serves the functions of various special features of the ATmega32 as listed on page 57.</p>
Port C (PC7..PC0)	<p>Port C is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port C output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running. If the JTAG interface is enabled, the pull-up resistors on pins PC5(TDI), PC3(TMS) and PC2(TCK) will be activated even if a reset occurs.</p> <p>The TD0 pin is tri-stated unless TAP states that shift out data are entered.</p> <p>Port C also serves the functions of the JTAG interface and other special features of the ATmega32 as listed on page 60.</p>
Port D (PD7..PD0)	<p>Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running.</p> <p>Port D also serves the functions of various special features of the ATmega32 as listed on page 62.</p>
RESET	<p>Reset Input. A low level on this pin for longer than the minimum pulse length will generate a reset, even if the clock is not running. The minimum pulse length is given in Table 15 on page 37. Shorter pulses are not guaranteed to generate a reset.</p>
XTAL1	<p>Input to the inverting Oscillator amplifier and input to the internal clock operating circuit.</p>
XTAL2	<p>Output from the inverting Oscillator amplifier.</p>
AVCC	<p>AVCC is the supply voltage pin for Port A and the A/D Converter. It should be externally connected to V_{CC}, even if the ADC is not used. If the ADC is used, it should be connected to V_{CC} through a low-pass filter.</p>
AREF	<p>AREF is the analog reference pin for the A/D Converter.</p>

B.4 AMC2004A-B-Y6WFDY 4x20 LCD Display Module by Orient Display

The following pages are the AMC2004A-B-Y6WFDY Orient Display LCD specifications. File-name:

AMC2004A-B-Series.pdf

2. Precautions in use of LCD Modules

- (1) Avoid applying excessive shocks to the module or making any alterations or modifications to it.
- (2) Don't make extra holes on the printed circuit board, modify its shape or change the components of LCD module.
- (3) Don't disassemble the LCM.
- (4) Don't operate it above the absolute maximum rating.
- (5) Don't drop, bend or twist LCM.
- (6) Soldering: only to the I/O terminals.
- (7) Storage: please storage in anti-static electricity container and clean environment.

3. General Specification

Item	Dimension	Unit
Number of Characters	20characters x 4 Lines	—
Module dimension(No Backlight)	98.0 x 60.0 x 10.0 (MAX)	mm
Module dimension(With LED Backlight)	98.0 x 60.0 x 15.0 (MAX)	mm
View area	76.0 x 25.2	mm
Active area	70.40 x 20.80	mm
Dot size	0.55 x 0.55	mm
Dot pitch	0.60 x 0.60	mm
Character size	2.95 x 4.75	mm
Character pitch	3.55 x 5.35	mm
LCD type	TN, Yellow/Gray/Blue STN/FSTN	
Duty	1/16	
View direction	6 o'clock or 12 o'clock	
Backlight Type	None, Yellow Green, Red or White LED backlight	

4. Absolute Maximum Ratings

Item		Symbol	Min	Max	Unit
Input Voltage		V_I	-0.3	VDD+0.3	V
Supply Voltage For Logic		VDD-V _{SS}	-0.3	7.0	V
Supply Voltage For LCD		V _{DD} -V ₀	Vdd-13.5	0	V
Standard Temperature LCM	Operating Temp.	Top	0	50	°C
	Storage Temp.	Tstr	-10	60	°C
Wide Temperature LCM	Operating Temp.	Top	-20	70	°C
	Storage Temp.	Tstr	-30	80	°C

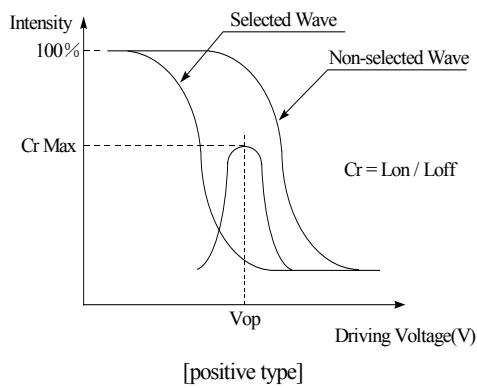
5. Electrical Characteristics

Item	Symbol	Condition	Min	Typ	Max	Unit
Supply Voltage For Logic	V _{DD} -V _{SS}	—	4.5	5.0	5.5	V
Supply Voltage For LCD	V _{DD} -V ₀	Ta=25°C	4.5	5.0	5.5	V
Input High Volt.	V _{IH}	—	0.7 V _{DD}	—	V _{DD}	V
Input Low Volt.	V _{IL}	—	V _{SS}	—	0.3 V _{DD}	V
Supply Current	I _{DD}	V _{DD} =5V	0.7	0.75	1.5	mA
Supply Voltage of Yellow-green backlight	V _{LED}	Forward current =180 mA Number of LED die 2x18= 36	3.8	4.2	4.3	V
Supply Voltage of White backlight	V _{LED}	Forward current =30 mA Number of LED die 2	3.8	4.0	4.2	V

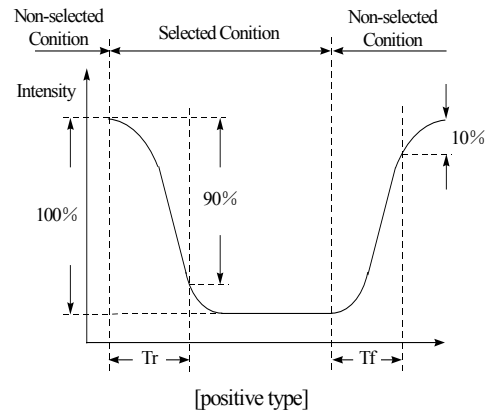
6. Optical Characteristics

Item	Symbol	Condition	Min	Typ	Max	Unit
View Angle	(V) θ	$CR \cong 2$	-20	—	35	deg
	(H) ϕ	$CR \cong 2$	-30	—	30	deg
Contrast Ratio	CR	—	—	3	—	—
Response Time	T rise	—	—	—	250	ms
	T fall	—	—	—	250	ms

Definition of Operation Voltage (Vop)



Definition of Response Time (Tr, Tf)



Conditions :

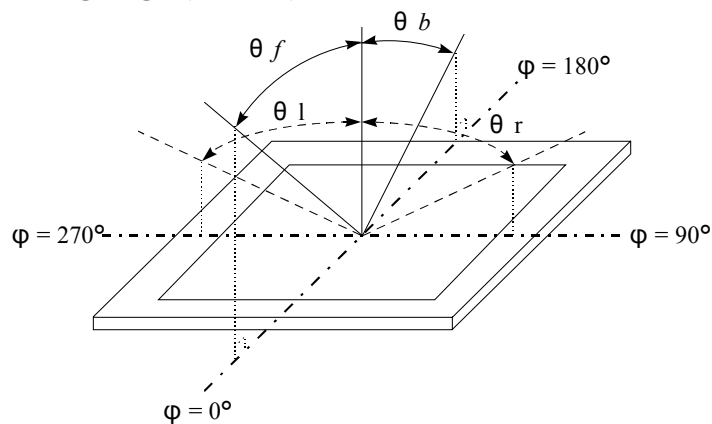
Operating Voltage : Vop

Viewing Angle(θ , ϕ) : 0° , 0°

Frame Frequency : 64 HZ

Driving Waveform : 1/N duty, 1/a bias

Definition of viewing angle($CR \cong 2$)

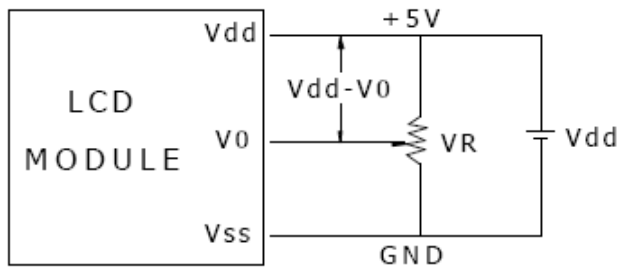


7. Interface Pin Function

Pin No.	Symbol	Level	Description
1	V _{SS}	0V	Ground
2	V _{DD}	5.0V	Supply Voltage for logic
3	V ₀	(Variable)	Operating voltage for LCD
4	RS	H/L	H: DATA, L: Instruction code
5	R/W	H/L	H: Read(MPU→Module) L: Write(MPU→Module)
6	E	H,H→L	Chip enable signal
7	DB0	H/L	Data bit 0
8	DB1	H/L	Data bit 1
9	DB2	H/L	Data bit 2
10	DB3	H/L	Data bit 3
11	DB4	H/L	Data bit 4
12	DB5	H/L	Data bit 5
13	DB6	H/L	Data bit 6
14	DB7	H/L	Data bit 7
15	LED(+)		Anode of LED Backlight
16	LED(-)		Cathode of LED Backlight

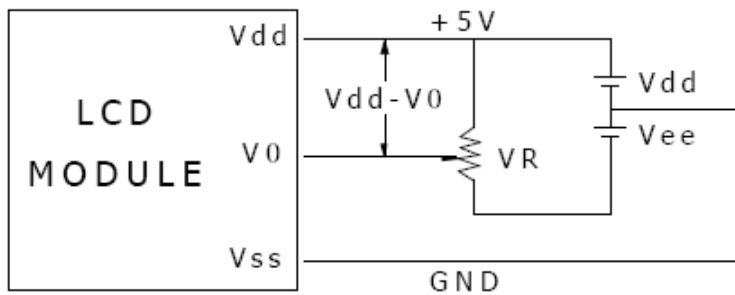
8. POWER SUPPLY

SINGLE SUPPLY VOLTAGE TYPE



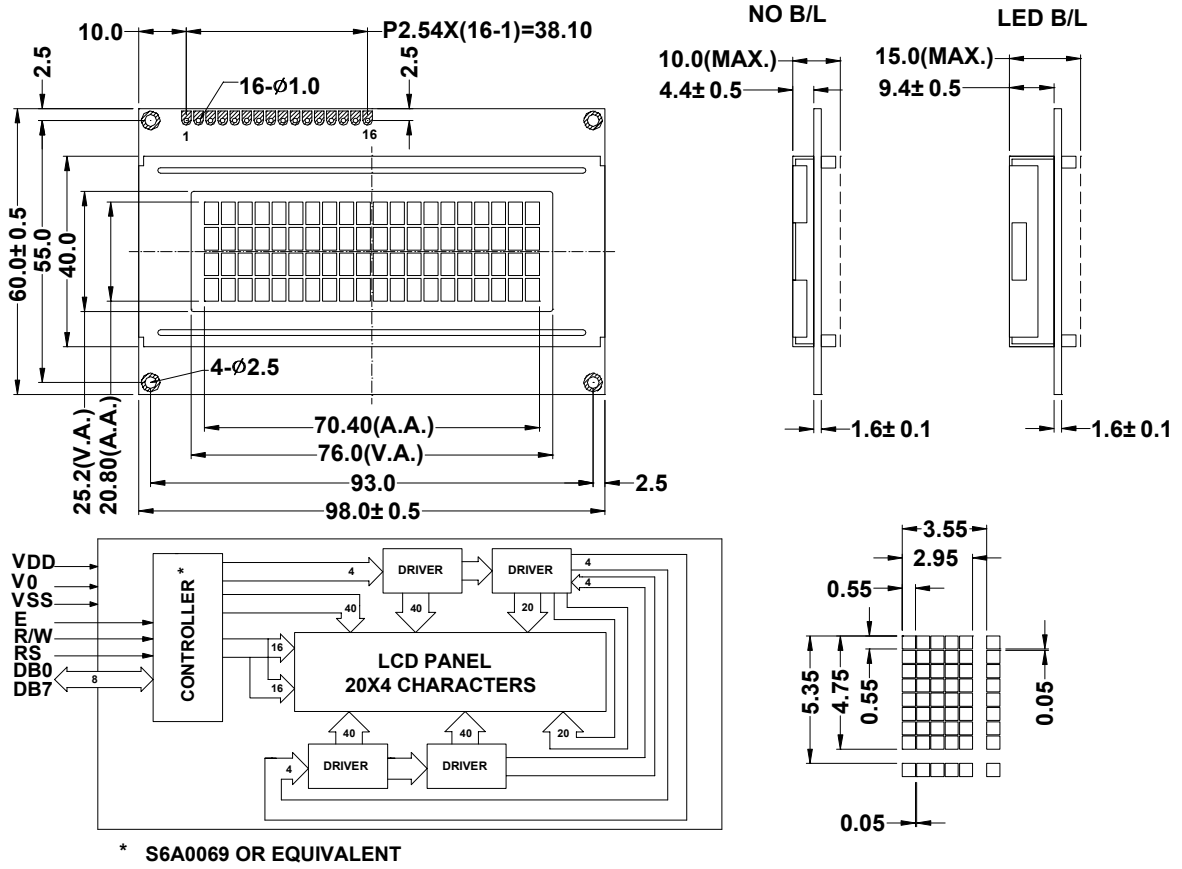
Vdd-V0: LCD Driving Voltage
VR: 10K - 20K

DUAL SUPPLY VOLTAGE TYPE



Vdd-V0: LCD Driving Voltage
VR: 10K - 20K

9. Contour Drawing & Block Diagram



10. Function Description

The LCD display Module is built in a LSI controller, the controller has two 8-bit registers, an instruction register (IR) and a data register (DR).

The IR stores instruction codes, such as display clear and cursor shift, and address information for display data RAM (DDRAM) and character generator (CGRAM). The IR can only be written from the MPU. The DR temporarily stores data to be written or read from DDRAM or CGRAM. When address information is written into the IR, then data is stored into the DR from DDRAM or CGRAM. By the register selector (RS) signal, these two registers can be selected.

RS	R/W	Operation
0	0	IR write as an internal operation (display clear, etc.)
0	1	Read busy flag (DB7) and address counter (DB0 to DB7)
1	0	Write data to DDRAM or CGRAM (DR to DDRAM or CGRAM)
1	1	Read data from DDRAM or CGRAM (DDRAM or CGRAM to DR)

Busy Flag (BF)

When the busy flag is 1, the controller LSI is in the internal operation mode, and the next instruction will not be accepted. When RS=0 and R/W=1, the busy flag is output to DB7. The next instruction must be written after ensuring that the busy flag is 0.

Address Counter (AC)

The address counter (AC) assigns addresses to both DDRAM and CGRAM

Display Data RAM (DDRAM)

This DDRAM is used to store the display data represented in 8-bit character codes. Its extended capacity is 80×8 bits or 80 characters. Below figure is the relationships between DDRAM addresses and positions on the liquid crystal display.

AC
(hexadecimal)

Character Generator ROM (CGROM)

The CGROM generate 5×8 dot or 5×10 dot character patterns from 8-bit character codes. See Table 2.

Character Generator RAM (CGRAM)

In CGRAM, the user can rewrite character by program. For 5×8 dots, eight character patterns can be written, and for 5×10 dots, four character patterns can be written.

Write into DDRAM the character code at the addresses shown as the left column of table 1. To show the character patterns stored in CGRAM.

Relationship between CGRAM Addresses, Character Codes (DDRAM) and Character patterns

Table 1.

11. Character Generator ROM Pattern

Table.2

Lower 4 Bits	Upper 4 Bits	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
xxxx0000	CG RAM (1)			0	@	P	`	P				-	夕	ミ	α	ρ	
xxxx0001	(2)		!	1	A	Q	a	q				。	ア	チ	△	ä	q
xxxx0010	(3)		"	2	B	R	b	r				「	イ	ツ	×	ρ	θ
xxxx0011	(4)		#	3	C	S	c	s				」	ウ	テ	モ	ε	ω
xxxx0100	(5)		\$	4	D	T	d	t				、	エ	ト	カ	μ	Ω
xxxx0101	(6)		%	5	E	U	e	u				・	オ	ナ	1	ε	ü
xxxx0110	(7)		&	6	F	V	f	v				ヲ	カ	ニ	ヨ	ρ	Σ
xxxx0111	(8)		'	7	G	W	g	w				ア	キ	ヌ	ラ	g	π
xxxx1000	(1)		(8	H	X	h	x				ィ	ク	ネ	リ	μ	×
xxxx1001	(2))	9	I	Y	i	y				ウ	ケ	ル		'	γ
xxxx1010	(3)		*	:	J	Z	j	z				エ	コ	ハ	レ	j	¥
xxxx1011	(4)		+	;	K	[k	{				オ	サ	ヒ	ロ	*	¥
xxxx1100	(5)		,	<	L	¥	l					カ	シ	フ	ワ	φ	円
xxxx1101	(6)		-	=	M]	m	}				ユ	ス	ハ	ン	ε	÷
xxxx1110	(7)		.	>	N	^	n	→				ヨ	セ	ホ	”	ñ	
xxxx1111	(8)		/	?	O	_	o	€				ッ	リ	マ	°	ö	■

12. Instruction Table

Instruction	Instruction Code										Description	Execution time (fosc=270Khz)	
	RS	R/W	DB7	DB6	DB5	DB4	DB3	DB2	DB1	DB0			
Clear Display	0	0	0	0	0	0	0	0	0	1	Write "00H" to DDRAM and set DDRAM address to "00H" from AC	1.53ms	
Return Home	0	0	0	0	0	0	0	0	0	1	Set DDRAM address to "00H" from AC and return cursor to its original position if shifted. The contents of DDRAM are not changed.	1.53ms	
Entry Mode Set	0	0	0	0	0	0	0	0	1	I/D	SH	Assign cursor moving direction and enable the shift of entire display.	39μs
Display ON/OFF Control	0	0	0	0	0	0	0	1	D	C	B	Set display (D), cursor (C), and blinking of cursor (B) on/off control bit.	39μs
Cursor or Display Shift	0	0	0	0	0	0	1	S/C	R/L	—	—	Set cursor moving and display shift control bit, and the direction, without changing of DDRAM data.	39μs
Function Set	0	0	0	0	0	1	DL	N	F	—	—	Set interface data length (DL:8-bit/4-bit), numbers of display line (N:2-line/1-line)and, display font type (F:5×11 dots/5×8 dots)	39μs
Set CGRAM Address	0	0	0	1	AC5	AC4	AC3	AC2	AC1	AC0	—	Set CGRAM address in address counter.	39μs
Set DDRAM Address	0	0	1	AC6	AC5	AC4	AC3	AC2	AC1	AC0	—	Set DDRAM address in address counter.	39μs
Read Busy Flag and Address	0	1	BF	AC6	AC5	AC4	AC3	AC2	AC1	AC0	—	Whether during internal operation or not can be known by reading BF. The contents of address counter can also be read.	0μs
Write Data to RAM	1	0	D7	D6	D5	D4	D3	D2	D1	D0	—	Write data into internal RAM (DDRAM/CGRAM).	43μs
Read Data from RAM	1	1	D7	D6	D5	D4	D3	D2	D1	D0	—	Read data from internal RAM (DDRAM/CGRAM).	43μs

* "—" : don't care

13. Timing Characteristics

13.1 Write Operation

Ta=25°C, VDD=5.0± 0.5V

Item	Symbol	Min	Typ	Max	Unit
Enable cycle time	t _{cyE}	1200	—	—	ns
Enable pulse width (high level)	PW _{EH}	140	—	—	ns
Enable rise/fall time	t _{Er} ,t _{Ef}	—	—	25	ns
Address set-up time (RS, R/W to E)	t _{AS}	0	—	—	ns
Address hold time	t _{AH}	10	—	—	ns
Data set-up time	t _{DSW}	40	—	—	ns
Data hold time	t _H	10	—	—	ns

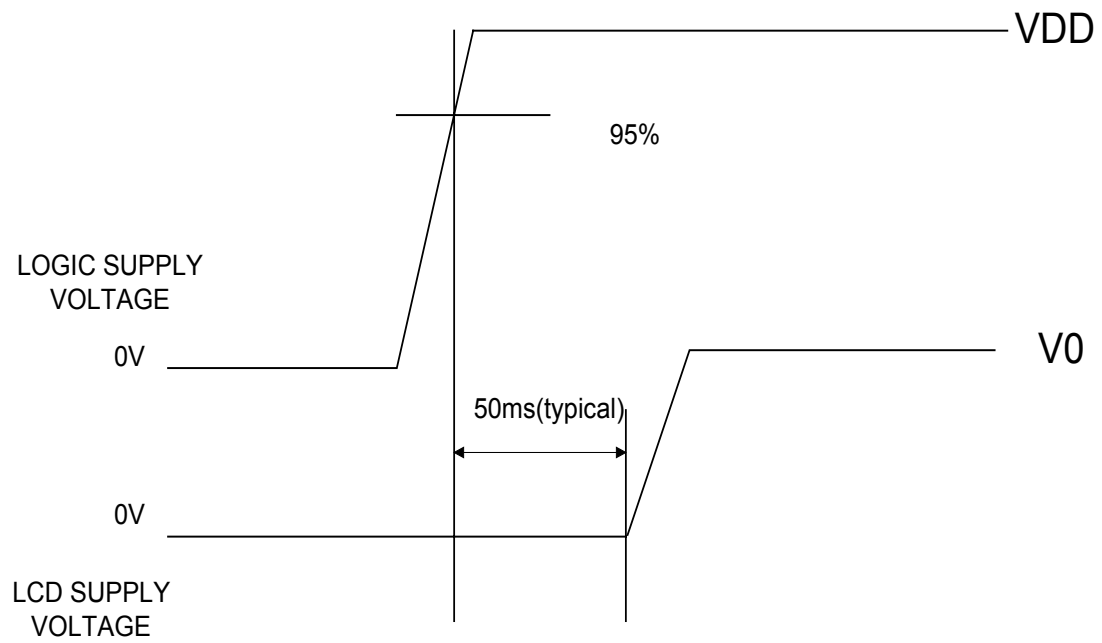
13.2 Read Operation

Ta=25°C, VDD=5.0± 0.5V

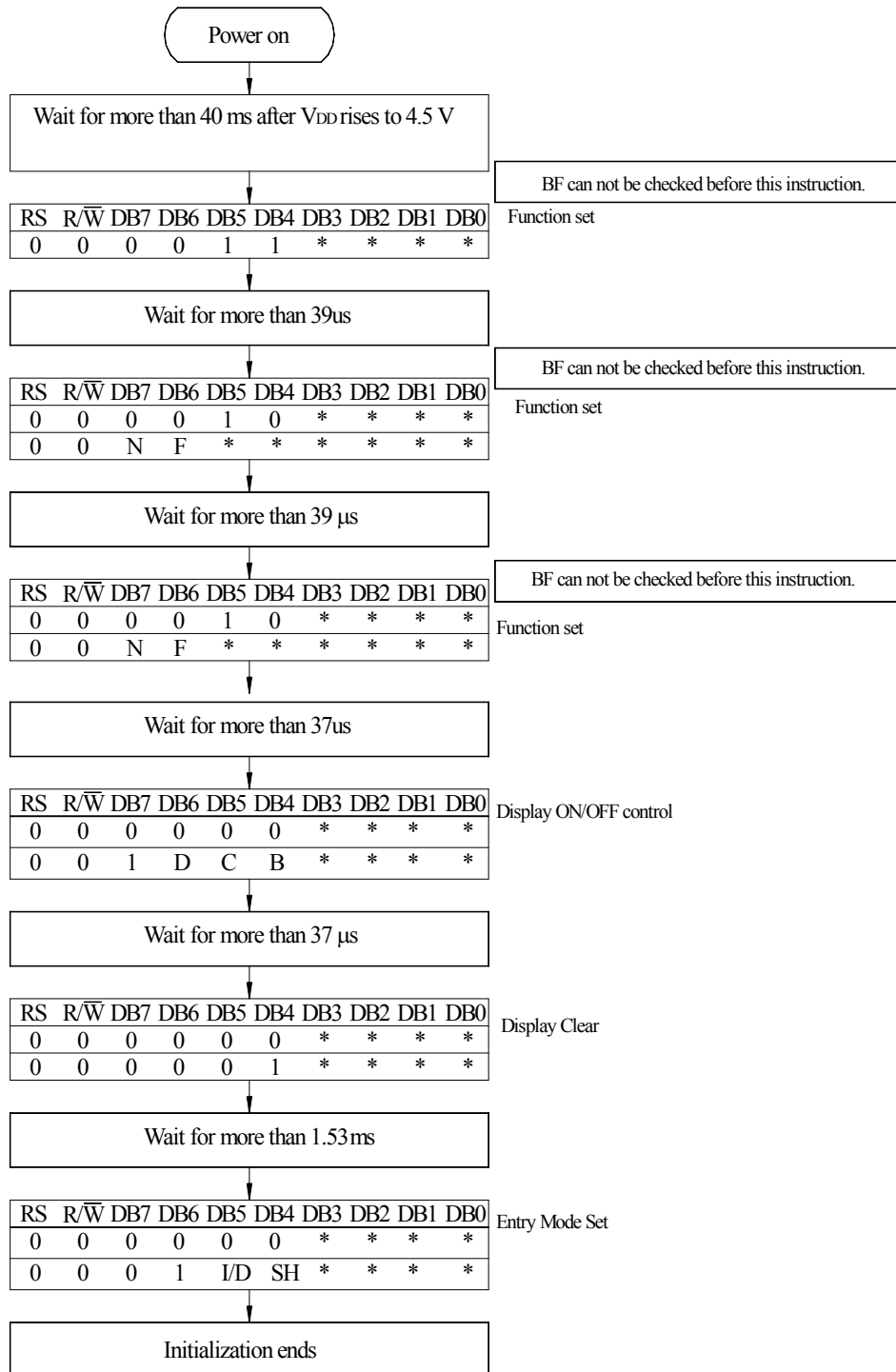
Item	Symbol	Min	Typ	Max	Unit
Enable cycle time	t _{cycE}	1200	—	—	ns
Enable pulse width (high level)	PW _{EH}	140	—	—	ns
Enable rise/fall time	t _{Er} ,t _{Ef}	—	—	25	ns
Address set-up time (RS, R/W to E)	t _{AS}	0	—	—	ns
Address hold time	t _{AH}	10	—	—	ns
Data delay time	t _{DDR}	—	—	100	ns
Data hold time	t _{DHR}	10	—	—	ns

13.3 Timing Diagram of VDD Against V0.

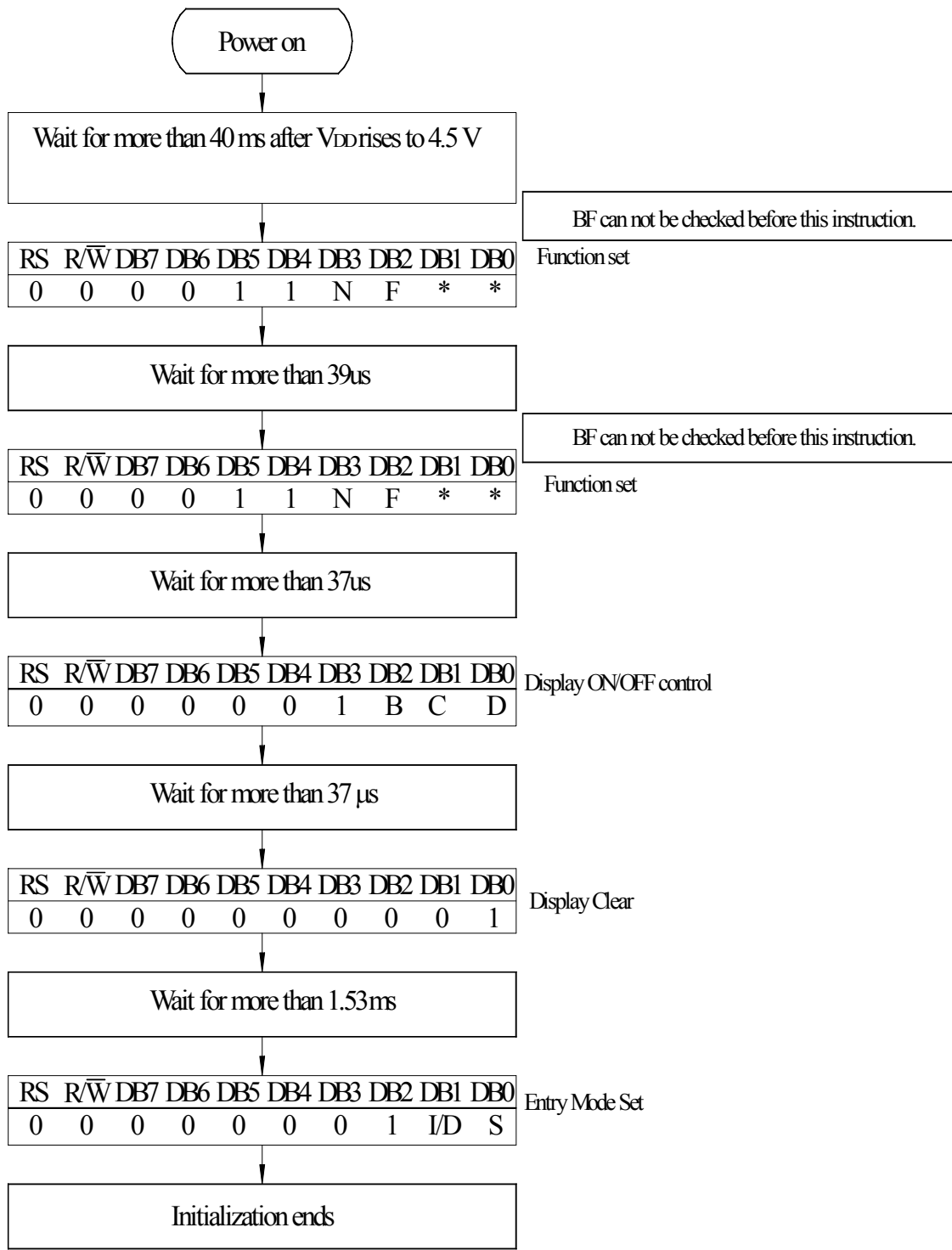
Power on sequence shall meet the requirement of Figure 4, the timing diagram of VDD against V0.



14. Initializing of LCM



4-Bit Ineterface



8-Bit Interface

15. Quality Assurance

Screen Cosmetic Criteria

Item	Defect	Judgment Criterion	Partition																				
1	Spots	<p>A)Clear</p> <table border="1"> <thead> <tr> <th>Size: d mm</th> <th>Acceptable Qty in active area</th> </tr> </thead> <tbody> <tr> <td>$d \leq 0.1$</td> <td>Disregard</td> </tr> <tr> <td>$0.1 < d \leq 0.2$</td> <td>6</td> </tr> <tr> <td>$0.2 < d \leq 0.3$</td> <td>2</td> </tr> <tr> <td>$0.3 < d$</td> <td>0</td> </tr> </tbody> </table> <p>Note: Including pin holes and defective dots which must be within one pixel size.</p> <p>B)Unclear</p> <table border="1"> <thead> <tr> <th>Size: d mm</th> <th>Acceptable Qty in active area</th> </tr> </thead> <tbody> <tr> <td>$d \leq 0.2$</td> <td>Disregard</td> </tr> <tr> <td>$0.2 < d \leq 0.5$</td> <td>6</td> </tr> <tr> <td>$0.5 < d \leq 0.7$</td> <td>2</td> </tr> <tr> <td>$0.7 < d$</td> <td>0</td> </tr> </tbody> </table>	Size: d mm	Acceptable Qty in active area	$d \leq 0.1$	Disregard	$0.1 < d \leq 0.2$	6	$0.2 < d \leq 0.3$	2	$0.3 < d$	0	Size: d mm	Acceptable Qty in active area	$d \leq 0.2$	Disregard	$0.2 < d \leq 0.5$	6	$0.5 < d \leq 0.7$	2	$0.7 < d$	0	Minor
Size: d mm	Acceptable Qty in active area																						
$d \leq 0.1$	Disregard																						
$0.1 < d \leq 0.2$	6																						
$0.2 < d \leq 0.3$	2																						
$0.3 < d$	0																						
Size: d mm	Acceptable Qty in active area																						
$d \leq 0.2$	Disregard																						
$0.2 < d \leq 0.5$	6																						
$0.5 < d \leq 0.7$	2																						
$0.7 < d$	0																						
2	Bubbles in Polarizer	<table border="1"> <thead> <tr> <th>Size: d mm</th> <th>Acceptable Qty in active area</th> </tr> </thead> <tbody> <tr> <td>$d \leq 0.3$</td> <td>Disregard</td> </tr> <tr> <td>$0.3 < d \leq 1.0$</td> <td>3</td> </tr> <tr> <td>$1.0 < d \leq 1.5$</td> <td>1</td> </tr> <tr> <td>$1.5 < d$</td> <td>0</td> </tr> </tbody> </table>	Size: d mm	Acceptable Qty in active area	$d \leq 0.3$	Disregard	$0.3 < d \leq 1.0$	3	$1.0 < d \leq 1.5$	1	$1.5 < d$	0	Minor										
Size: d mm	Acceptable Qty in active area																						
$d \leq 0.3$	Disregard																						
$0.3 < d \leq 1.0$	3																						
$1.0 < d \leq 1.5$	1																						
$1.5 < d$	0																						
3	Scratch	In accordance with spots cosmetic criteria. When the light reflects on the panel surface, the scratches are not to be remarkable.	Minor																				
4	Allowable Density	Above defects should be separated more than 30mm each other.	Minor																				
5	Coloration	Not to be noticeable coloration in the viewing area of the LCD panels. Back-light type should be judged with back-light on state only.	Minor																				

16. Reliability

Content of Reliability Test

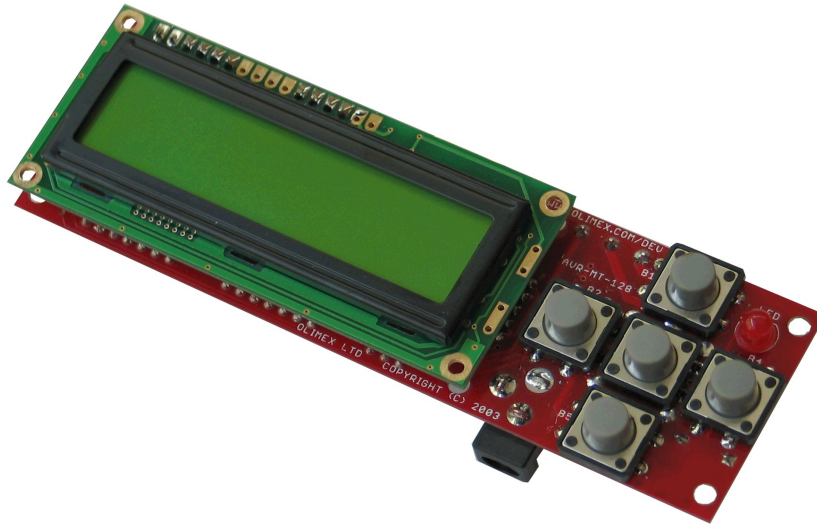
Environmental Test			
Test Item	Content of Test	Test Condition	Applicable Standard
High Temperature storage	Endurance test applying the high storage temperature for a long time.	60°C 96hrs	—
Low Temperature storage	Endurance test applying the high storage temperature for a long time.	-10°C 96hrs	—
High Temperature Operation	Endurance test applying the electric stress (Voltage & Current) and the thermal stress to the element for a long time.	50°C 96hrs	—
Low Temperature Operation	Endurance test applying the electric stress under low temperature for a long time.	0°C 96hrs	—
High Temperature/ Humidity Storage	Endurance test applying the high temperature and high humidity storage for a long time.	60°C, 90%RH 96hrs	—
High Temperature/ Humidity Operation	Endurance test applying the electric stress (Voltage & Current) and temperature / humidity stress to the element for a long time.	50°C, 90%RH 96hrs	—
Temperature Cycle	Endurance test applying the low and high temperature cycle. -10°C 25°C 60°C 30min 5min 30min 1 cycle	-10°C/60°C 10 cycles	—
Mechanical Test			
Vibration test	Endurance test applying the vibration during transportation and using.	10~22Hz→1.5mmp-p 22~500Hz→1.5G Total 0.5hrs	—
Shock test	Constructional and mechanical endurance test applying the shock during transportation.	50G Half sign wave 11 msdc 3 times of each direction	—

***Supply voltage for logic system=5V. Supply voltage for LCD system =Operating voltage at 25°C

B.5 AVR-MT-128 display and interface board

The following pages are the AVR-MT-128 display and interface board specifications. Filename:

AVR-MT-128 DEVELOPMENT BOARD WITH MEGA128.pdf



AVR-MT128 development board

Users Manual

Rev.A, July 2008

Copyright(c) 2008, OLIMEX Ltd, All rights reserved

INTRODUCTION:

AVR-MT128 is simple but powerful board which uses the MCU ATmega128 from Atmel. With its LCD, buttons, relay and variety of interfaces such as RS232 (in two variants – 4 pins and DB9), JTAG, ISCP, Dallas, etc. this board is suitable for different embedded systems applications.

BOARD FEATURES:

- MCU: **ATmega128-16AI** with 128K Bytes Program Flash, 4K Bytes data EEPROM, 4K Bytes RAM
- JTAG connector for in-circuit programming and debugging with AVR-JTAG
- ICSP 5x2 (10) pin STKxxx compatible connector for in-circuit programming with AVR-PG1B or AVR-PG2B
- RS232 connector with TTL levels
- RS232 interface circuit with Tx, Rx signals
- RS232 DB9 female connector
- Dallas touch button port
- Frequency input
- LCD 16x2 display
- Status LED
- Five buttons
- Buzzer
- Power supply circuit +5V, 78L05 with plug-in power jack and diode bridge
- 32 768 Hz oscillator crystal
- 16 MHz crystal oscillator
- Power supply filtering capacitor
- RESET supervisor IC ZM33064
- RELAY with 10A/250VAC NO and NC contacts with screw terminals
- Extension headers for unused in the schematic ports available for external connection
- PCB: FR-4, 1.5 mm (0,062"), green soldermask, white silkscreen component print
- Four mounting holes 3.3 mm (0.13")
- Dimensions: 120x38 mm (4.7x1.5")

ELECTROSTATIC WARNING:

The AVR-MT128 board must not be subject to high electrostatic potentials. General practice for working with static sensitive devices should be applied when working with this board.

BOARD USE REQUIREMENTS:

- Cables:** RS232 straight male-to-female DB9 cable (Note: this is not a null modem cable)
- Hardware:** Programmer: AVR-PG1, AVR-PG2, AVR-ISP500, AVR-ISP500-TINY, AVR-ISP500-ISO or other compatible tool;
Debugger: AVR-JTAG, AVR-JTAG-USB or other compatible tool;

Software: AVR Studio + WinAVR – free C compiler and debugger can be downloaded at avrfreaks.org web site. IAR IW for AVR is a commercial software for development of embedded systems software.

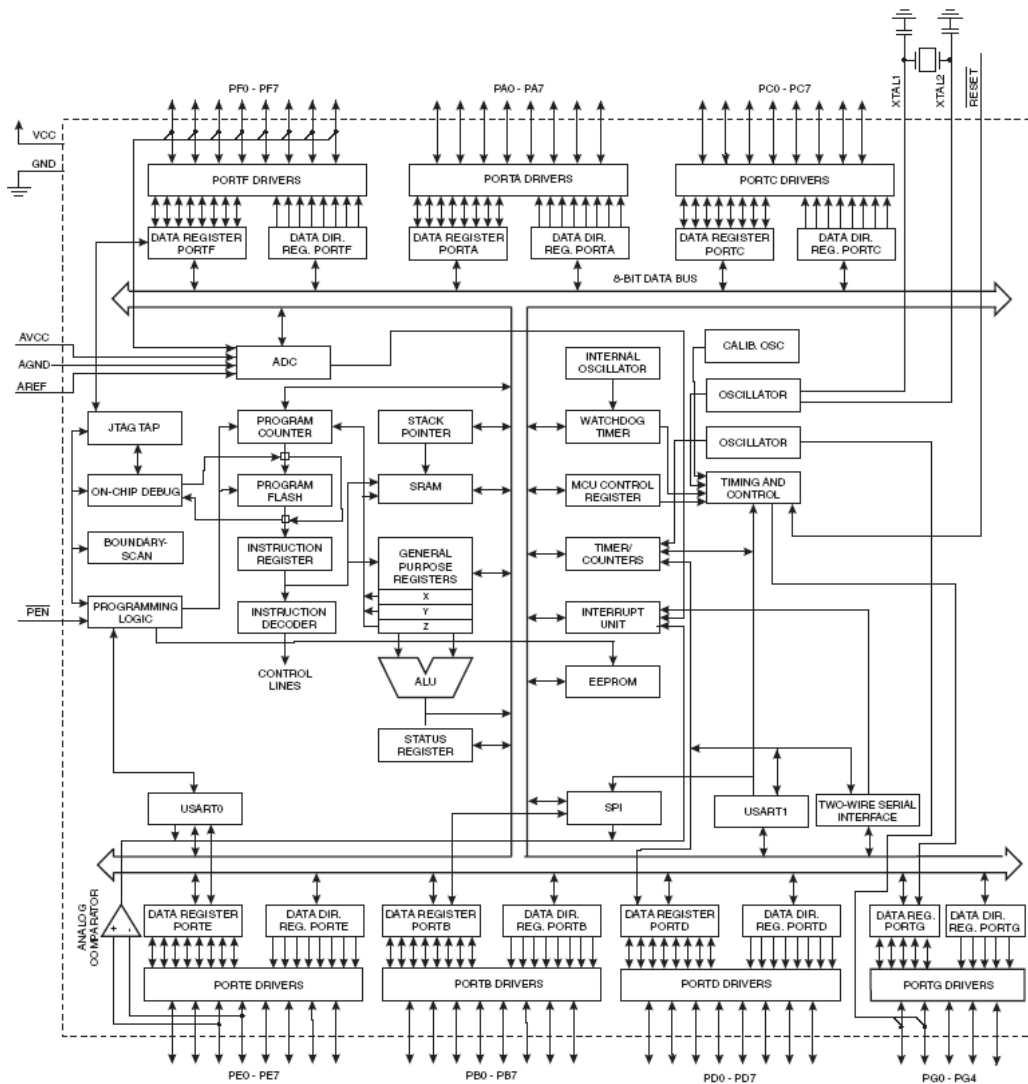
PROCESSOR FEATURES:

AVR-MT128 uses ATmega128 MCU from Atmel with the following features:

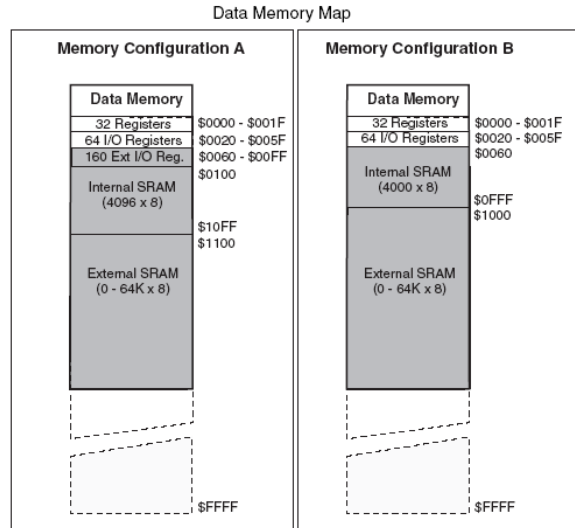
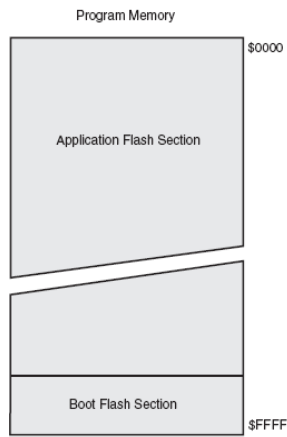
- High-performance, Low-power AVR® 8-bit Microcontroller
- Advanced RISC Architecture
 - o 133 Powerful Instructions – Most Single Clock Cycle Execution
 - o 32 x 8 General Purpose Working Registers + Peripheral Control Registers
 - o Fully Static Operation
 - o Up to 16 MIPS Throughput at 16 MHz
 - o On-chip 2-cycle Multiplier
 - o Nonvolatile Program and Data Memories
 - o 128K Bytes of In-System Reprogrammable Flash
Endurance: 10,000 Write/Erase Cycles
 - o Optional Boot Code Section with Independent Lock Bits
In-System Programming by On-chip Boot Program
True Read-While-Write Operation
 - o 4K Bytes EEPROM
Endurance: 100,000 Write/Erase Cycles
 - o 4K Bytes Internal SRAM
 - o Up to 64K Bytes Optional External Memory Space
 - o Programming Lock for Software Security
 - o SPI Interface for In-System Programming
- JTAG (IEEE std. 1149.1 Compliant) Interface
 - o Boundary-scan Capabilities According to the JTAG Standard
 - o Extensive On-chip Debug Support
 - o Programming of Flash, EEPROM, Fuses and Lock Bits through the JTAG Interface
- Peripheral Features
 - o Two 8-bit Timer/Counters with Separate Prescalers and Compare Modes
 - o Two Expanded 16-bit Timer/Counters with Separate Prescaler, Compare Mode and Capture Mode
 - o Real Time Counter with Separate Oscillator
 - o Two 8-bit PWM Channels
 - o 6 PWM Channels with Programmable Resolution from 2 to 16 Bits
 - o Output Compare Modulator
 - o 8-channel, 10-bit ADC
8 Single-ended Channels
7 Differential Channels
2 Differential Channels with Programmable Gain at 1x, 10x, or 200x
 - o Byte-oriented Two-wire Serial Interface
 - o Dual Programmable Serial USARTs
 - o Master/Slave SPI Serial Interface
 - o Programmable Watchdog Timer with On-chip Oscillator
 - o On-chip Analog Comparator
- Special Microcontroller Features
 - o Power-on Reset and Programmable Brown-out Detection
 - o Internal Calibrated RC Oscillator
 - o External and Internal Interrupt Sources

- Six Sleep Modes: Idle, ADC Noise Reduction, Power-save, Power-down, Standby, and Extended Standby
- Software Selectable Clock Frequency
- ATmega103 Compatibility Mode Selected by a Fuse
- Global Pull-up Disable
- I/O and Packages
 - 53 Programmable I/O Lines
 - 64-lead TQFP and 64-pad MLF
- Operating Voltages
 - 4.5 - 5.5V for ATmega128
- Speed Grades
 - 0 - 16 MHz for ATmega128

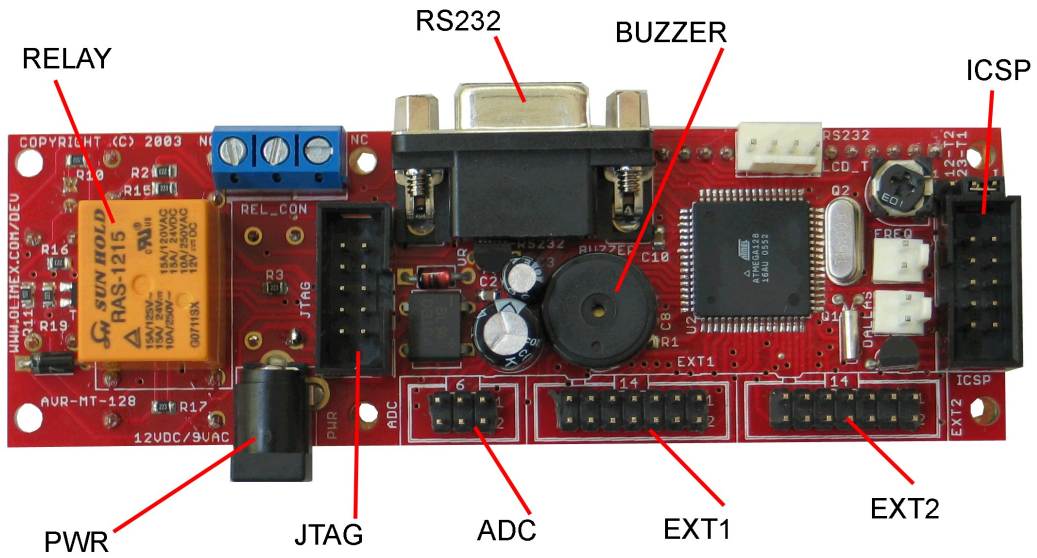
BLOCK DIAGRAM:



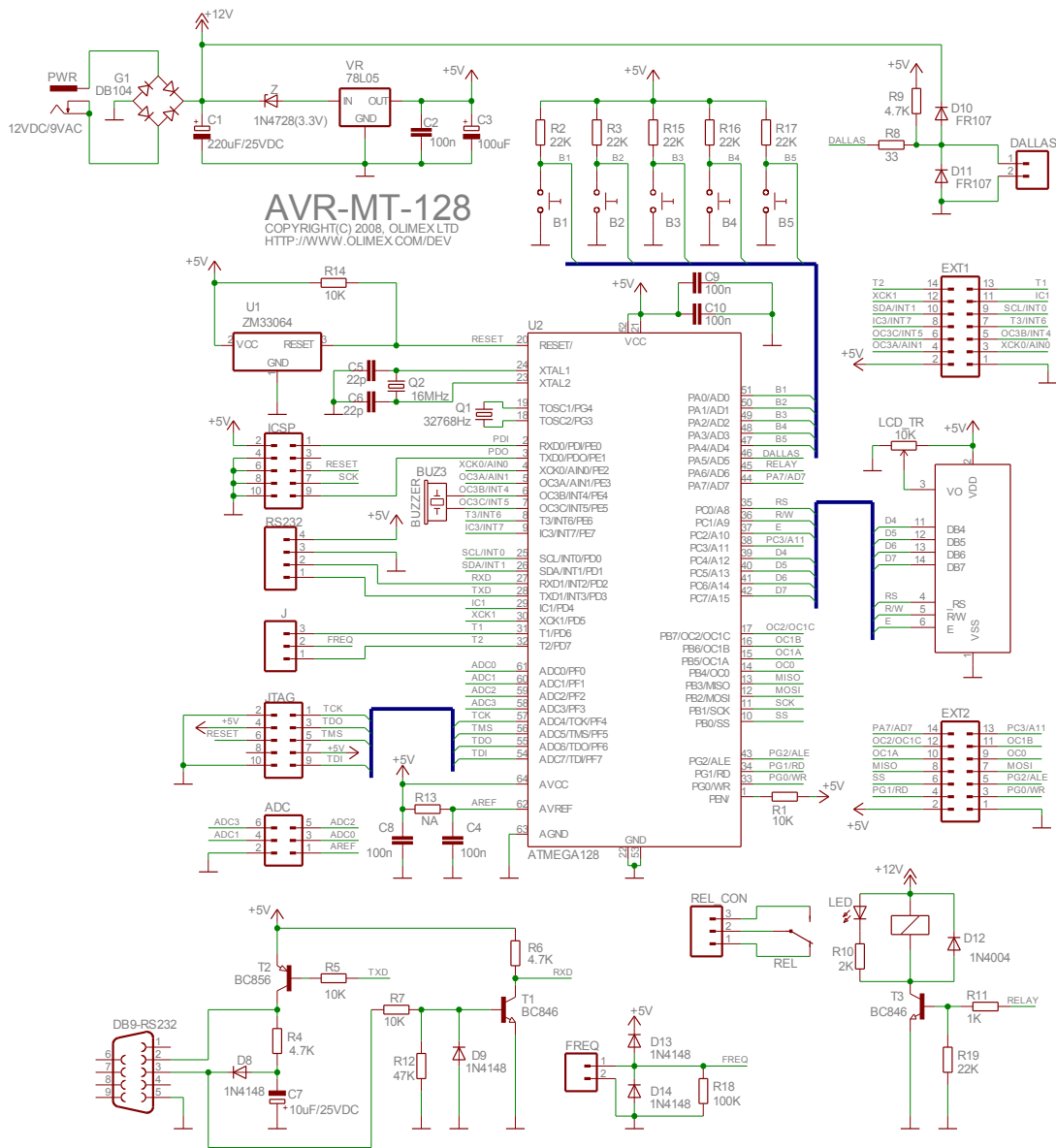
MEMORY MAP:



BOARD LAYOUT:



SCHEMATIC:



POWER SUPPLY CIRCUIT:

The power supply of AVR-MT128 is taken from Power jack connector. You should apply 9 VAC or +12 VDC at the positive central pin. The consumption of the board is about 30 mA.

RESET CIRCUIT:


AVR-MT128 reset circuit is made with ZM33064 with typical threshold 4.5V. When the voltage falls below that minimum, the MSU resets.

CLOCK CIRCUIT:

Quartz crystal 16MHz for maximum performance is connected to ATmega128 pin 23 (XTAL2) and pin 24 (XTAL1). Additional 32 768 Hz tact generator is connected to ATmega128 pin 18 (TOSC2/PG3) and pin 19 (TOSC1/PG4) and supplies the Real Time Clock.

JUMPER DESCRIPTION:

J



pin 31
frequency pin
connected to

This jumper supplies the input user frequency FREQ to either (T1/PD6) or pin 32 (T2/PD7). When 1-2 is shorted the input is connected to T2. When 2-3 is shorted the input frequency pin is T1.

Default state is 1-2 shorted.

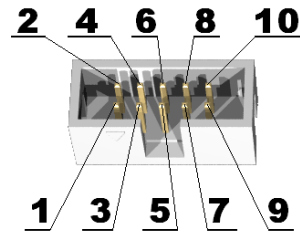
INPUT/OUTPUT:

Status LED (red) connected to the relay.
Relay with name **REL** connected to ATmega128 pin 45 (PA6/AD6).
Trimmer LED_TR connected to the LCD.
Liquid crystal display.
Buzzer with name **BUZZ** connected to ATmega128 pin 6 (OC3B/INT4/PE4) and pin 7 (OC3C/INT5/PE5).
User button B1 connected to ATmega128 pin 51 (PA0/AD0).
User button B2 connected to ATmega128 pin 50 (PA1/AD1).
User button B3 connected to ATmega128 pin 49 (PA2/AD2).
User button B4 connected to ATmega128 pin 48 (PA3/AD3).
User button B5 connected to ATmega128 pin 47 (PA4/AD4).

CONNECTOR DESCRIPTIONS:

JTAG:

Pin #	Signal Name
1	TCK
2	GND
3	TDO
4	+5V
5	TMS
6	RESET
7	+5V
8	NC
9	TDI
10	GND



This connector allows programming and debugging via AVR-JTAG or other compatible tools.

TDI Input **Test Data In**. This is the serial data input for the shift register.

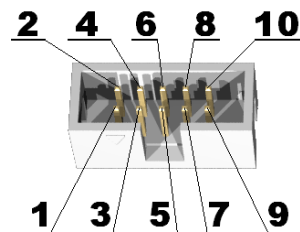
TDO Output **Test Data Out**. This is the serial data output for the shift register. Data is shifted out of the device on the negative edge of the TCK signal.

TMS Input **Test Mode Select**. The TMS pin selects the next state in the TAP state machine.

TCK Input **Test Clock**. This allows shifting of the data in, on the TMS and TDI pins. It is a positive edge triggered clock with the TMS and TCK signals that define the internal state of the device.

ICSP:

Pin #	Signal Name
1	PDI
2	+5V
3	NC
4	GND
5	RST
6	GND



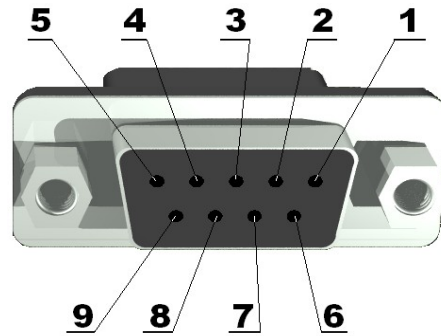
7	SCK
8	GND
9	PDO
10	GND

This connector allows programming via AVR-PG1, AVR-PG2 or other compatible tool.

- PDI** Input **Program Data In.** This pin is serial data input for the MCU.
PDO Output **Program Data Out.** This pin is serial data output from the MCU.
SCK I/O **Serial (Synchronization) Clock.** This is the synchronization signal.

DB9-RS232:

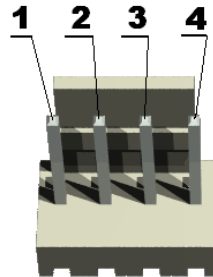
Pin #	Signal Name
1	NC
2	TXD
3	RXD
4	NC
5	GND
6	NC
7	NC
8	NC
9	NC



- TXD** Output **Transmit Data.** This is the asynchronous serial data output for the RS232 interface.
RXD Input **Receive Data.** This is the asynchronous serial data input for the RS232 interface.

RS232:

Pin #	Signal Name
1	TXD
2	RXD
3	GND



4	+5V

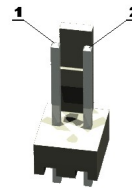
RELAY CONNECTOR:



This connector provides the user with access to the contact plates of the relay.

FREQ:

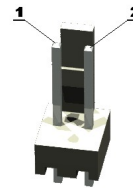
Pin #	Signal Name
1	FREQ
2	GND



External input frequency is applied at pin 1.

DALLAS:

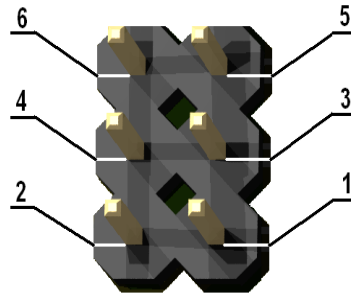
Pin #	Signal Name
1	DALLAS
2	GND



Signal from Dallas chips is applied at pin 1 of the Dallas interface.

ADC:

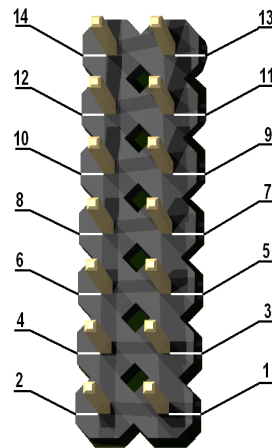
Pin #	Signal Name
1	AREF
2	GND
3	ADC0
4	ADC1
5	ADC2
6	ADC3



Some of the Analog to Digital Converter signals are grouped into an extension.

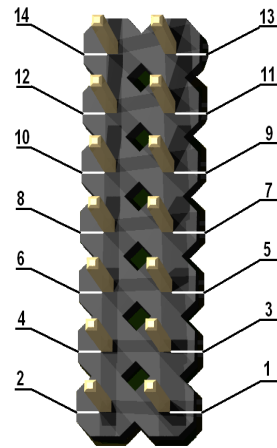
EXT1:

Pin #	Signal Name
1	GND
2	+5V
3	XCK0/AIN0
4	OC3A/AIN1
5	OC3B/INT4
6	OC3C/INT5
7	T3/INT6
8	IC3/INT7
9	SCL/INT0
10	SDA/INT1
11	IC1
12	XCK1
13	T1
14	T2



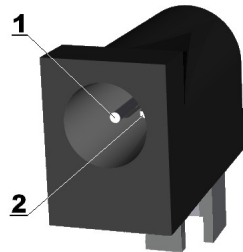
EXT2:

Pin #	Signal Name
1	GND
2	+5V
3	PG0/WR
4	PG1/RD
5	PG2/ALE
6	SS
7	MOSI
8	MISO
9	OC0
10	OC1A
11	OC1B
12	OC2/OC1C
13	PC3/A11
14	PA7/AD7



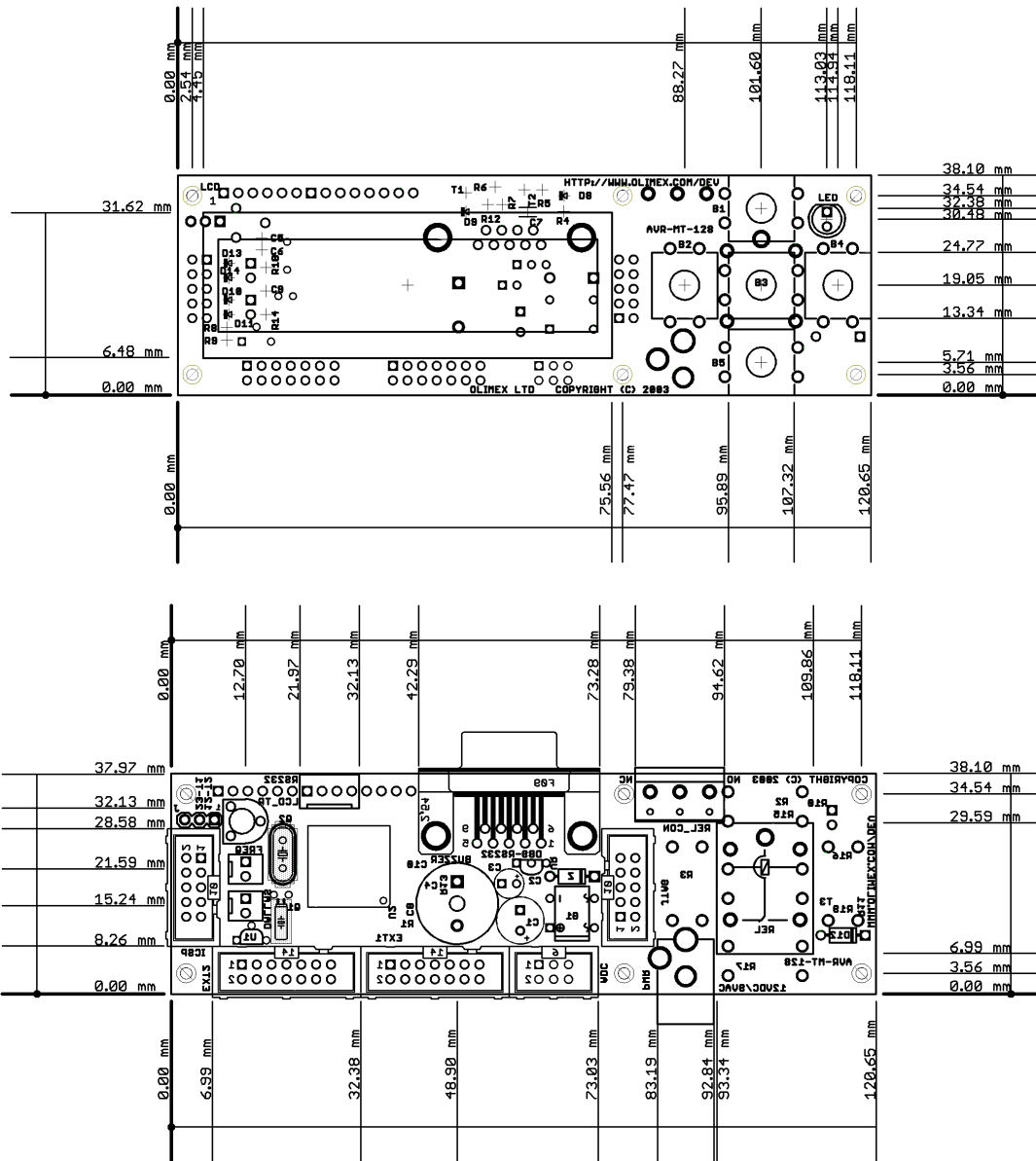
PWR:

Pin #	Signal Name
1	PWR
2	GND



You should apply 9 VAC or +12VDC on pin 1.

MECHANICAL DIMENSIONS:



All measures are in mm.

AVAILABLE DEMO SOFTWARE:

Check for available demo software for **AVR-MT128** on our website:
www.olimex.com/dev.

B.6 AVR-PG1B serial port 10 pin ICSP AVR microcontroller programmer

The following pages are the AVR-PG1B serial port 10 pin ICSP AVR microcontroller programmer specifications. Filename:

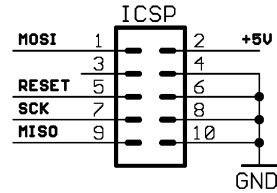
`pdf-AVR-PG1B.pdf`

AVR-PG1B (SERIAL PORT) 10 PIN ICSP AVR MICROCONTROLLER PROGRAMMER

Features:

AVR-PG1B is low cost serial port programmer for AVR microcontrollers with following features:

- Connects to RS232 port
- Uses target board power supply so no need for external power supply



Programming:

AVR-PG1B works with PonyProg software by from Claudio Lanconelli and the latest release may be download for free from <http://www.lancos.com>

RS232 interface:

Your RS232 cable must provide the following signals for properly operation of AVR-PG1B: Tx, Rx, CTS, DTR, RTS, GND.

ICSP interface:

The ICSP connector is 2x5 pin with 0,1" step and Atmel STKxxx compatible layout. The PIN.1 is marked with square pad on bottom and arrow on top. ICSP signals are: 1- MOSI, 2- VCC, 3- NC, 4- GND, 5- RST, 6- GND, 7- SCK, 8- GND, 9- MISO, 10- GND

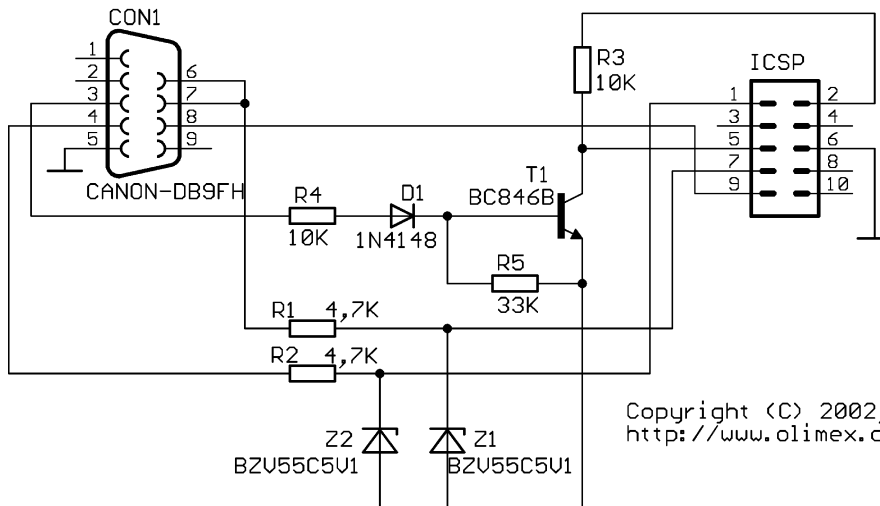
Supported devices:

Current supported devices by PonyProg are:
 AT90S1200, AT90S2313, AT90S2323,
 AT90S2343, AT90S4414, AT90S4434,
 AT90S8515, AT90S8535, AT90S2323,
 AT90S2343, AT90S2333, AT90S4433,
 AT90S4434, AT90S8535, AT90S8534,
 ATmega103, ATmega161, ATmega163,
 ATmega323, ATmega128, ATmega8,
 ATmega16, ATmega64, ATtiny12 and ATtiny15

ICSP TOP view PCB board layout:

Ordering codes:

AVR-PG1B - assembled and tested



Copyright (C) 2002, OLIMEX Ltd
<http://www.olimex.com/dev>

Copyright(c) 2002, OLIMEX Ltd, All rights reserved.
 Development boards for PIC, AVR and MSP430 microcontrollers <http://www.olimex.com/dev>

Appendix C

Preliminary WDS implementation

As a first contact with OpenWrt firmware configuration in WRT54GL routers, we developed a preliminary implementation with the most basic *ad hoc* dual-link approach supported by OpenWrt over the WRT54GL: WDS.

This basic UI X2 implementation with WDS link in the MP70 is presented in this Appendix chapter to complement the final implementation described in chapter 6 section 6.1.1.

Materials

- 2 x Linksys WRT54GL router by Cisco with OpenWRT Linux OS version *Kamikaze 8.09.1*.
- Linksys WRT54GL router by Cisco with Tomato Linux OS v1.25 equipped with external serial ports modification.
- AVR-P40B-8535 AVR Microcontroller Prototype Board.
- Atmel's ATmega32 8-Bit Processor. 32K of program space, 32 I/O lines, 8 of which are 10bit Analog to Digital converter capable. Runs up to 16MHz with external crystal. Package can be programmed in circuit and be debugged with AVR-JTAG.
- Orient Display AMC2004A-B-Y6WFDY 4x20 LCD Display Module. This module is a four-lined 20 characters LCD display¹.
- Custom 12V battery pack.

Methods

For representing the **X2 portable monitor with basic User Interface** we used the Linux-based WRT54GL router loaded with Tomato firmware v1.25, previously modified to incorporate a couple of serial DB9 ports (male and female) in the front, through a simple internally mounted

¹<http://www.eio.com/p-941-orient-display-amc2004a-b-y6wfdy-4x20-character-lcd-display-module.aspx>

Maxim RS233 chip, see schematic in figure C.1. In that way we could connect other serial extensions to it and debrick it easily in case of compatibility problems when flashing the firmware.

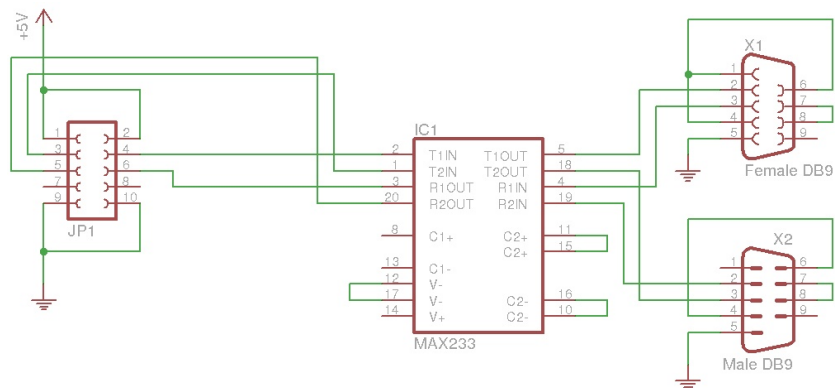


Figure C.1: RS233 schematic for serial ports modification in WRT54GL

We mounted a four-lines 20 characters LCD display in a cardboard box (see figures C.5 and C.8), in order to hold it and at the same time to host the router and a 12-volt battery pack to operate it and thus be able to test it in real battery operation (see figure C.5).

We used a previously assembled prototyping serial-to-JTAG AVR-P40B-8535 AVR Microcontroller Prototype Board and programmed it with the help of the *AVR-JTAG Tool* together with the router to display in a very simple ASCII text-based GUI the reaction to user interaction through the push-button in the front of the router (see figure C.6), used originally to activate/deactivate SES (SecureEasySetup, a Linksys developed kind of WPS to ease the connection process to normal users). In that way we triggered a script to effectuate a wireless scan looking for an specific SSID pattern, thus simulating the Device Discovery process looking for hospital bedside monitors to connect to. This was achieved by adding a hotplug handler which reacts on button press events and a toggle script which triggered the script.

To try a first dual-link implementation, although the WDS approach was discarded in the suitability assessment, we loaded the image of the *Kamikaze 8.09.1* version of OpenWRT OS and connected them as shown in figure C.2 as a simple implementation and trial of the Linux-based embedded router platform.

To do so, we configured an WDS link between the couple of Linksys WRT54GL routers with OpenWRT, hardcoding the other station MAC address in each station. And configured a simultaneous AP in the remote station, representing the MP70 bedside monitor.

Result

We ended up with a functional WDS link between the couple of OpenWrt routers, shown in figure C.7. With it we achieved to share the connection to the wired LAN from the Hospital AP to the MP70, in that case the remote WDS station, which at the same time had an AP running. The X2 was able to run independently on batteries and when the front-button was pressed it was able to scan and detect the presence of the MP70's broadcasted SSID and connect to it, while keeping the user informed of the process through the LCD screen.

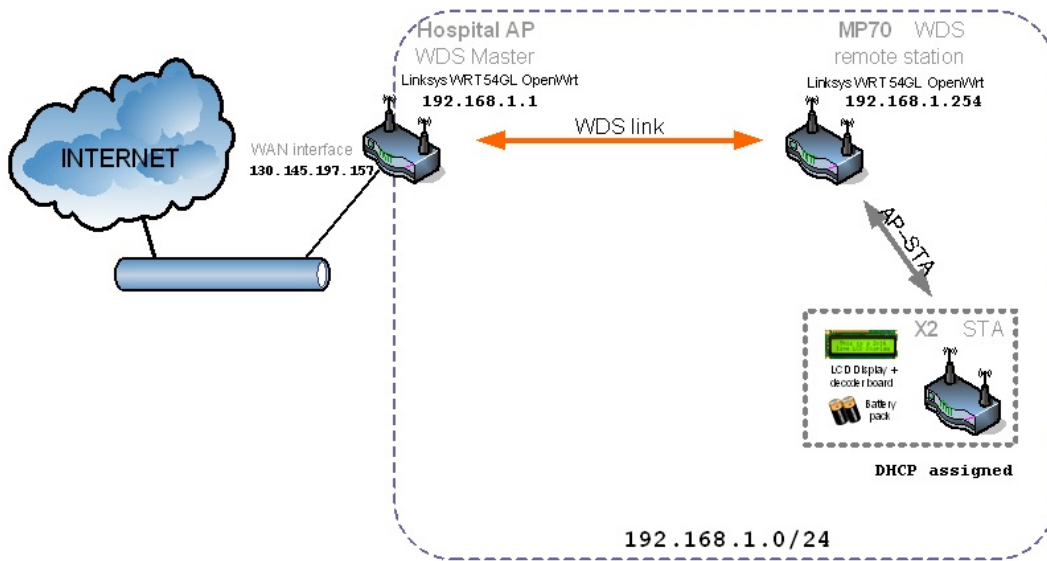


Figure C.2: WDS link implementation schema

See figures C.5 and C.6 showing the physical appearance of the functional implementation representing the X2 portable monitor with a basic User Interface. Some of the User Interface messages are shown in figure C.9.

Link to **demo video** demonstrating the basic User Interface through the front button and the LCD screen in the implementation representing the X2 which detects the SSID of MP70's AP connected through the WDS link to the hospital AP, URL: <https://goo.gl/yDHLtU>².



Figure C.4: QR image link to demonstration video URL <https://goo.gl/yDHLtU>

²The URL can be obtained from scanning the QR code image with an Android app like Google *Google*s available at URL: <https://play.google.com/store/apps/details?id=com.google.android.apps.unveil> or any other barcode scanner app.

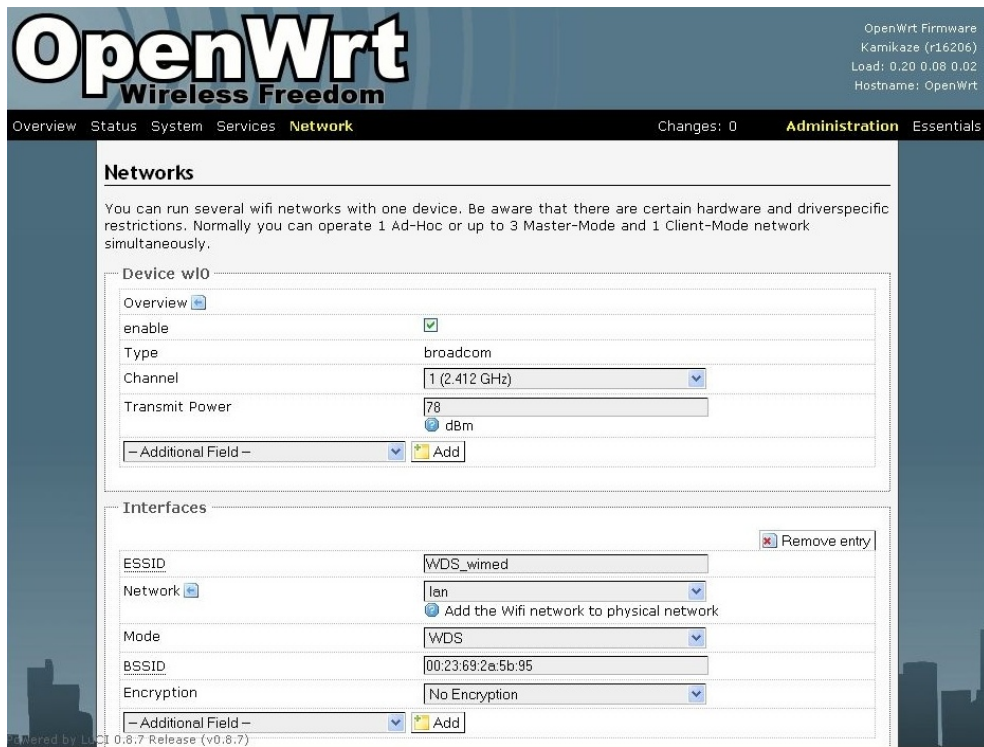


Figure C.3: WDS link setup on OpenWRT configuration web interface



Figure C.5: X2 with basic UI implementation. Overall look and cardboard case assembly detail

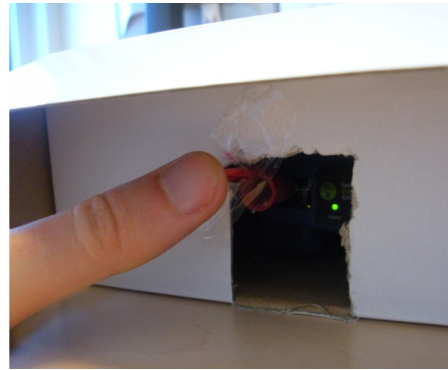


Figure C.6: *X2 with basic UI implementation, LCD display module (back) and UI detail (frontal push-button)*



Figure C.7: *Hospital AP and MP70 connected through WDS link*



Figure C.8: *First implementation. LCD display module detail (front)*

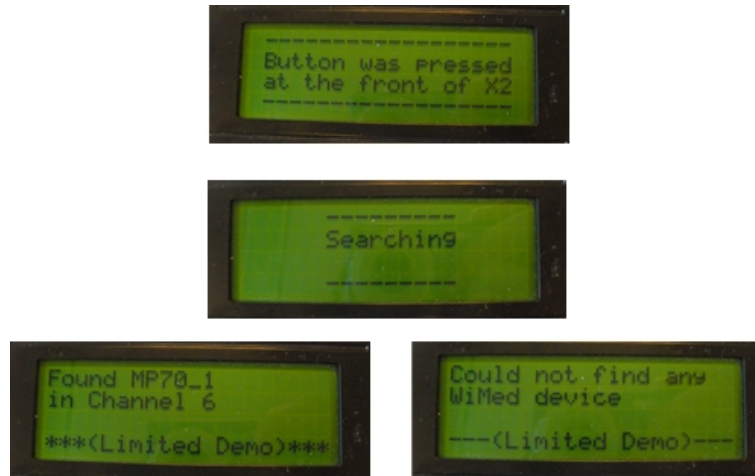


Figure C.9: *First implementation. GUI detail (LCD display)*

C.0.1 Preliminary WDS implementation: X2 portable monitor scripts

The following pages are the X2 portable monitor scripts source code in Linux shell script format, for the preliminary WDS implementation with basic UI over Tomato firmware. Filenames:

pdf_initial_script_tomato_x2_basic.pdf
pdf_button_script_tomato_x2_basic.pdf

```
#!/bin/bash
# Script launched when starting the router
# in the X2 implementation with Basic UI over Tomato OS

# Initialization of the LCD display
cat /jffs/clean_display > /dev/tts/1

# get remote date from NTP server
rdate ntp.xs4all.nl

while [ 1 ]; do
    cat /jffs/clean_display > /dev/tts/1
    # Show date every minute
    /jffs/insert_date /jffs/message_file
    sleep 60
done
```

```

#!/bin/bash
# Script launched when the front button is pressed
# in the X2 implementation with Basic UI over Tomato OS

# Initialization of the LCD display
cat /jffs/clean_display > /dev/tts/1

# Show message "Button was pressed"
cat /jffs/clean_display > /dev/tts/1
cat /jffs/press_display > /dev/tts/1
sleep 2
# Show message "Searching"
cat /jffs/clean_display > /dev/tts/1
cat /jffs/search_display > /dev/tts/1
# Show "Searching" state in the blinking LED light
/jffs/blink 6 0 2 &
wl scan
sleep 1
found=$(wl scanresults | grep -c MP70)
if [ $found = "1" ] ; then
    wl join MP70
    # Show "Success in MP70 found" through the blinking LED light
    /jffs/blink 5 1 3 &
    cat /jffs/clean_display > /dev/tts/1
    # Show message "MP70 found"
    cat /jffs/found_display > /dev/tts/1
else
    # Show "Failure in MP70 found" through the blinking LED light
    /jffs/blink 3 1 1 &
    cat /jffs/clean_display > /dev/tts/1
    # Show message "MP70 not found"
    cat /jffs/notfound_display > /dev/tts/1
fi

```

C.0.2 Preliminary WDS implementation: MP70 bedside monitor WDS link configuration

The following pages show the HospitalAP-MP70 WDS link configuration on the OpenWrt web interface for the preliminary WDS implementation.

The screenshot displays the OpenWrt web interface for configuring a WDS link. The top navigation bar includes 'Overview', 'Status', 'System', 'Services', 'Network', 'Changes: 0', 'Administration', and 'Essentials'. The main content area is titled 'Networks' and contains a section for 'Device wl0'. This section includes an 'Overview' tab and a table of configuration options: 'enable' (checked), 'Type' (broadcom), 'Channel' (1 (2.412 GHz)), and 'Transmit Power' (78 dBm). Below this is an 'Interfaces' section with a 'Remove entry' button and a table of configuration options: 'ESSID' (WDS_wimed), 'Network' (lan), 'Mode' (WDS), 'BSSID' (00:23:69:2a:5b:95), and 'Encryption' (No Encryption). The footer of the interface indicates it is powered by LuCI 0.8.7 Release (v0.8.7).

Figure C.10: WDS link setup on OpenWRT configuration web interface

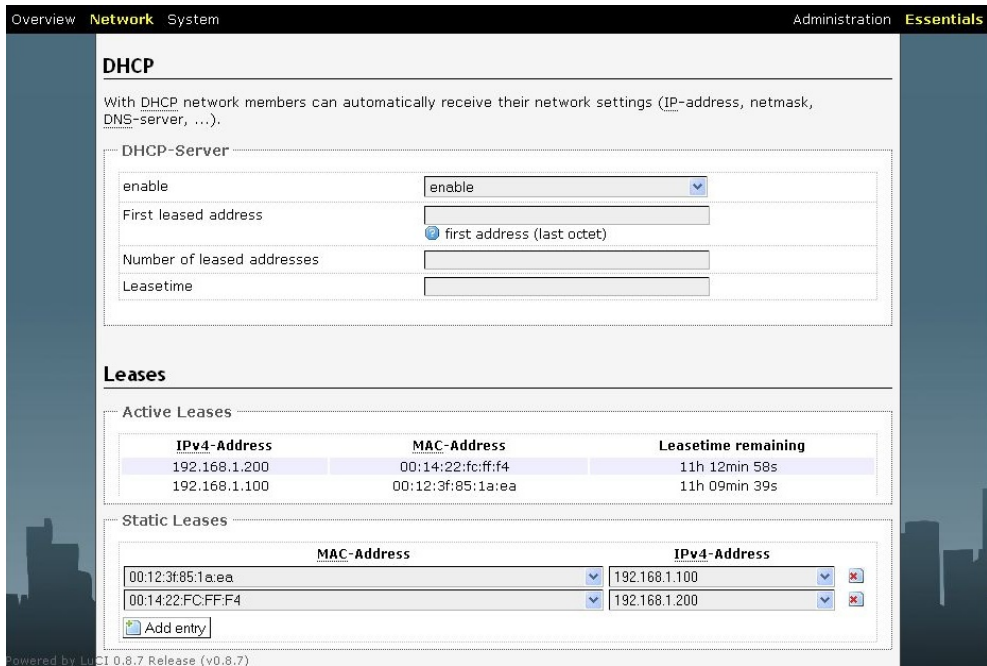


Figure C.11: MP70's DHCP server on OpenWRT configuration web interface

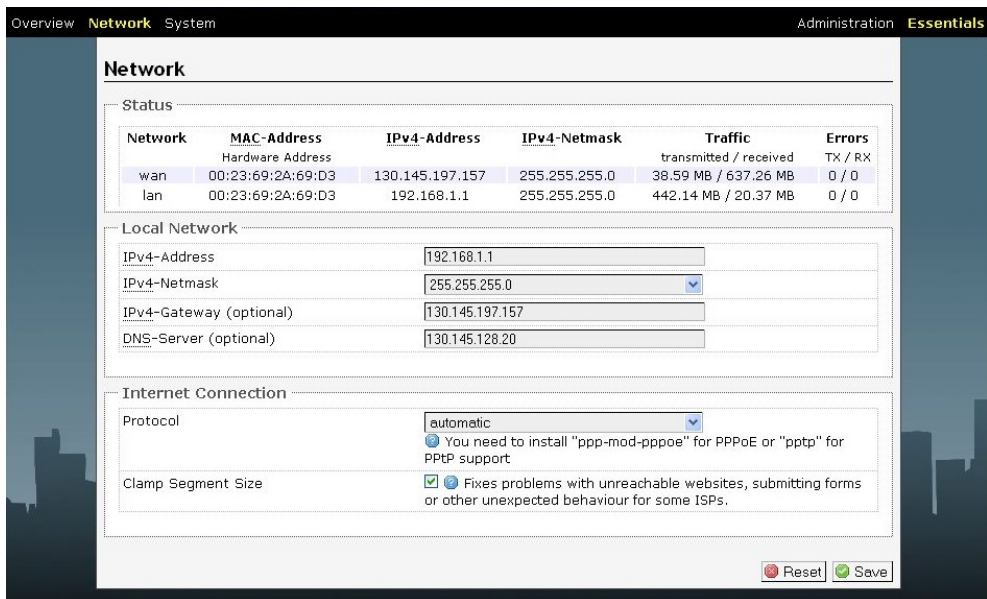


Figure C.12: Hospital AP's DNS and gateway on OpenWRT configuration web interface

Appendix D

Implemented scripts code

This appendix includes the bash shell code of the scripts developed for the final implementation described in chapter 6, the advanced UI X2 embedded implementation with SoftAP MP70.

D.1 X2 portable monitor scripts: advanced UI embedded implementation

The following pages are the X2 portable monitor scripts source code in Linux shell script format.
Filename:

`pdf-script-wimed-X2.pdf`


```

#!/bin/sh
#script_wimed_X2.sh
#####
### Function for checking time passed since initime #####
#####
# Expects a timer as argument $1
# and returns seconds since timer was updated
checktime()
{
    echo $((`date +%s`-$1))
}
#####
### Function for sleeping less than a second #####
#####
sleepin()
#Expects an integer as argument $1, to repeat sleep 0 $1 times
{
    a=0
    while [ $a -lt $1 ] ; do
        sleep 0
        let a=a+1
    done
}
#####
### Function for buzzing the beeper #####
#####
buzz()
{
    echo "bz150_1" > /tmp/commandfile
    sleep $BUZZWAIT
}
buzzmove()
{
    echo "bz200_1" > /tmp/commandfile
    sleep $BUZZWAIT
}
buzzback()
{
    echo "bz400_1" > /tmp/commandfile
    sleep $BUZZWAIT
}
buzzhelp()
{
    echo "bz300_1" > /tmp/commandfile
    sleep $BUZZWAIT
}
buzzselect()
{
    echo "bz050_1" > /tmp/commandfile
    sleep $BUZZWAIT
}
buzzpanic()
{
    echo "bz015_1" > /tmp/commandfile
    sleep $BUZZWAIT
}
#####
### Function for clearing the display #####
#####
cleardisplay()
{
    echo "d_ " > /tmp/commandfile
    sleep $DISPLAYWAIT
}
#####
### Function for sending text to the display #####
#####
display()
{
    echo "d_ "$*" "> /tmp/commandfile
    sleep $DISPLAYWAIT
}
#####

```

```

#### Functions for printing menu top option #####
#####
displaytop()
{
case $state in

    $FREE ) echo "d_Sel[~]      FREE "$*" v"      ">
            /tmp/commandfile
            ;;
    $LINKED)echo "d_Sel[~]      LINKED "$*" v"      ">
            /tmp/commandfile
            ;;
    $ASSIGN)echo "d_Sel[~]      ASSIGNED "$*" v"    ">
            /tmp/commandfile
            ;;
esac
sleep $DISPLAYWAIT
}

#####
#### Functions for printing menu middle option #####
#####
displaymid()
{
case $state in

    $FREE ) echo "d_Sel[~]      FREE^"$*" v"      ">
            /tmp/commandfile
            ;;
    $LINKED)echo "d_Sel[~]      LINKED^"$*" v"      ">
            /tmp/commandfile
            ;;
    $ASSIGN)echo "d_Sel[~]      ASSIGNED^"$*" v"    ">
            /tmp/commandfile
            ;;
esac
sleep $DISPLAYWAIT
}

#####
#### Function for printing menu last option #####
#####
displaylast()
{
case $state in

    $FREE ) echo "d_Sel[~]      FREE^"$*" v"      ">
            /tmp/commandfile
            ;;
    $LINKED)echo "d_Sel[~]      LINKED^"$*" v"      ">
            /tmp/commandfile
            ;;
    $ASSIGN)echo "d_Sel[~]      ASSIGNED^"$*" v"    ">
            /tmp/commandfile
            ;;
esac
sleep $DISPLAYWAIT
}

#####
#### Functions for printing help menus #####
#####
displayhelp()
{
echo "d_[?]" "$*" "      "> /tmp/commandfile
sleep $DISPLAYWAIT
}

#####
menuhelp()
#Expects option number in $1
{
while [ ! -e /tmp/buttonfile2 ]; do

displayhelp $( eval echo \ $help$1 )

```

```

#Back
if [ -e /tmp/buttonfile2 ]; then
    #buzzback
    rm /tmp/buttonfile2
    break
elif [ -e /tmp/buttonfile* ]; then
    echo borrando botones
    rm /tmp/buttonfile*
fi

sleepin $SCROLLWAIT
displayhelp $( eval echo \${addh$1 } )
sleepin $SCROLLWAIT
done

if [ $( ls /tmp | grep -c buttonfile ) -ne 0 ] ; then
    rm /tmp/buttonfile*
fi

}
#####
### Functions for printing status menu #####
#####
displaystatus1()
{
case $state in
    0 )    curr_ssid=$( wl status | grep -c "Not associated" )
           if [ "$curr_ssid" -eq 1 ] ; then
               curr_ssid="Not connected!"
           else
               curr_ssid=$( wl ssid | sed -e 's/Current SSID: //g' | sed -e
's///g' )
               check_fwd
           fi

           echo "d_Menu[~]    FREE"$curr_ssid"           " > /tmp/commandfile
           sleep $DISPLAYWAIT
           ;;

    1 )    echo "d_Menu[~] ASSIGNED                       " >
/tmp/commandfile
           sleep $DISPLAYWAIT
           check_fwd
           echo "d_Patient: "$patID "                       " >
/tmp/commandfile
           sleep $DISPLAYWAIT

           curr_ssid=$( wl status | grep -c "Not associated" )
           if [ "$curr_ssid" -eq 1 ] ; then
               curr_ssid="Not connected!"
               if [ "$link" -eq 0 ] ; then
                   linkedssid=$( (( wl scanresults | sed -ne "/"$ssid"/p" )) | grep
-c "SSID" )
                   echo linkedssid $linkedssid
                   if [ $linkedssid -ge 1 ] ; then
                       wl -a $INTERFACE join $ssid
                       break
                   fi
               fi
           else
               curr_ssid=$( wl ssid | sed -e 's/Current SSID: //g' | sed -e
's///g' )
               check_fwd
           fi
           echo "d_" $curr_ssid "                               " > /tmp/commandfile
           sleep $DISPLAYWAIT
           ;;

    2 )    echo "d_Menu[~]    LINKED"$myMP70"           " > /tmp/commandfile
           sleep $DISPLAYWAIT
           ;;
esac

```

```

#####
menustatus()
{
while [ ! -e /tmp/buttonfile3 ]; do

    displaystatus1

    #Enter
    if [ -e /tmp/buttonfile3 ]; then
        #buzzback
        rm /tmp/buttonfile3
        break
    fi

    check_fwd

done
if [ $( ls /tmp | grep -c buttonfile ) -ne 0 ] ; then
    rm /tmp/buttonfile*
fi
}
#####
### Function for showing the tutorial menu #####
#####
tutorial()
{
if [ -e /tmp/buttonfile* ]; then
rm /tmp/buttonfile*
fi
display "X2 TUTORIAL"
sleepin $SCROLLWAIT
while [ ! -e /tmp/buttonfile* ]; do
display "Press any key to continue      "
sleepin $SCROLLWAIT
display "          or wait  for tutorial:"
if [ -e /tmp/buttonfile* ]; then break; fi
sleepin $SCROLLWAIT
display "Select an optionwith ~ key      "
if [ -e /tmp/buttonfile* ]; then break; fi
sleepin $SCROLLWAIT
display "Read contextual help with ? key "
if [ -e /tmp/buttonfile* ]; then break; fi
sleepin $SCROLLWAIT
display "Press arrows ^to move and  v"
if [ -e /tmp/buttonfile* ]; then break; fi
sleepin $SCROLLWAIT
display "scroll text up ^          and down v"
if [ -e /tmp/buttonfile* ]; then break; fi
sleepin $SCROLLWAIT
display "Go back to previous menu with < "
if [ -e /tmp/buttonfile* ]; then break; fi
sleepin $SCROLLWAIT
if [ -e /tmp/buttonfile* ]; then break; fi
done #any button pressed
echo Button pressed
cleardisplay
rm /tmp/buttonfile*
}
#####
### Functions for implementing menus and UI #####
#####
printtext()
#uses $pos and $state global variables, returns new pos
{
prev=`expr $pos - 1`
next=`expr $pos + 1`

let "textpos=$state+10*$pos"
echo "in printtext textpos: " $textpos

foo=1
while [ 1 ] ; do
    case $pos in

```

```

1 )      displaytop $( eval echo \${text$textpos} )
        ;;
2 )      displaymid $( eval echo \${text$textpos} )
        ;;
3 )      displaylast $( eval echo \${text$textpos} )
        ;;
esac

while [ ! -e /tmp/buttonfile* ]; do
    let foo++
    if [ `expr $foo / 20` -eq 1 ] ; then
        check_fwd
        foo=1
    fi
done

#Select
if [ -e /tmp/buttonfile3 ]; then
    rm /tmp/buttonfile3
    #buzzselect
    return $pos
fi

#Help
if [ -e /tmp/buttonfile4 ]; then
    rm /tmp/buttonfile4
    #buzzhelp
    menuhelp $textpos
fi

#Down
if [ -e /tmp/buttonfile5 ]; then
    rm /tmp/buttonfile5
    #buzzmove
    if [ "$pos" -ne 3 ] ; then
        pos=$next
        return $next
    fi
fi

#Up (previous option)
if [ -e /tmp/buttonfile1 ]; then
    rm /tmp/buttonfile1
    #buzzmove
    if [ "$pos" -ne 1 ] ; then
        pos=$prev
        return $prev
    fi
fi

#back
if [ -e /tmp/buttonfile2 ]; then
    #buzzback
    rm /tmp/buttonfile2
    return 0
fi

done #while 1
}
#####
printlist()
#uses $poslist and global variables, returns new pos
{
    maxlist=$1

    prev=`expr $poslist - 1`
    next=`expr $poslist + 1`
}

```

```

while [ 1 ] ; do
    case $poslist in

        1 )      displaytop $( eval echo \${list}${poslist} )
                ;;
        2 )      displaymid $( eval echo \${list}${poslist} )
                ;;
        $maxlist )
                displaylast $( eval echo \${list}${poslist} )
                ;;
    esac

    #Select
    if [ -e /tmp/buttonfile3 ]; then
        rm /tmp/buttonfile3
        #buzzselect
        return $poslist
    fi

    #Help
    if [ -e /tmp/buttonfile4 ]; then
        rm /tmp/buttonfile4
        #buzzhelp
        menuhelp "Select an element of the list"
    fi

    #Down
    if [ -e /tmp/buttonfile5 ]; then
        rm /tmp/buttonfile5
        #buzzmove
        if [ "$poslist" -ne "$maxlist" ] ; then
            poslist=$next
            return $next
        fi
    fi

    #Up (previous option)
    if [ -e /tmp/buttonfile1 ]; then
        rm /tmp/buttonfile1
        #buzzmove
        if [ "$poslist" -ne 1 ] ; then
            poslist=$prev
            return $prev
        fi
    fi

    #back
    if [ -e /tmp/buttonfile2 ]; then
        #buzzback
        rm /tmp/buttonfile2
        return 0
    fi

done #while 1
}
#####
### Function for showing the list menu #####
#####
menulist()
#Returns code of the choosen option in return code variable $?
{
    echo "in menulist function current list pos:" $poslist
    if [ $( ls /tmp | grep -c buttonfile ) -ne 0 ] ; then
        rm /tmp/buttonfile*
    fi
    oldposlist=$poslist
}

```

```

printlist $1
case $? in
    $oldposlist ) let "poslist=1"
                  return $oldposlist
                  ;;
    0 )          return 0
                  ;;
    * )          echo new pos: $poslist
                  return 999
                  ;;
esac

echo "problems in menu!"
}

#####
### Function for showing the main menus #####
#####
menu()
#Returns code of the choosen option in return code variable $?
{
echo "in menu function current state:" $state current menu pos: $pos
if [ $( ls /tmp | grep -c buttonfile ) -ne 0 ] ; then
    rm /tmp/buttonfile*
fi
let "textpos=$state+10*$pos"
echo $textpos
oldpos=$pos

printtext
case $? in
    $oldpos ) let "pos=1"
              return $textpos
              ;;
    0 )      return 0
              ;;
    * )      echo new pos: $pos
              let "textpos=$state+10*$pos"
              echo new textpos: $textpos
              return 999
              ;;
esac

echo "problems in menu!"
}

#####
### Function for Connecting to Hospital AP #####
#####
connect_hospital()
{
#RESET WL
wl -a eth1 down
wl -a eth1 up
wl status

initime=$( date +%s )
while [ `checktime $initime` -lt $MAXSCANTIME ] ; do
    display "Scanning..."
    wl -a $INTERFACE ap 0
    wl -a $INTERFACE scan -t active -n $n_probes -a $dwell_t
    freemps=0
    while [ $( wl channel | grep -c No ) -eq 0 ] ; do
        a=1 #don't run the rest of the script until scan is complete
    done
    wl channel
    wl scanresults | grep Hospital
    freemps=$(( ( wl scanresults | sed -ne "/$nameHospitalAP/p" )
                | wc -l )
    if [ $freemps -ge 1 ] ; then
        break
    fi
fi
}

```

```

        display "Not found. Scanning again...  "
        sleepin $INTERSCANWAIT
done #WHILE MAXSCANTIME

if [ $freemps -ge 1 ] ; then
    AP=$( wl scanresults | sed './.{H;$!d};x;/'$nameHospitalAP'/'!d' |
    awk 'BEGIN {} /^SSID/ {name=$2} /^Mode/ {signal[name]=$4} END {
    max=-100; for (i in signal) {if (signal[i] > max) { max=signal[i]
    ; maxname=i } }; print maxname }' | sed -e 's/"//g' )

    chan=$( wl scanresults | sed './.{H;$!d};x;/'$nameHospitalAP'/'!d'
    | awk 'BEGIN {} /^SSID/ {name=$2} /^Mode/ {signal[name]=$4 ;
    chan[name]=$10 } END {max=-100; for (i in signal) {if (signal[
    i] > max) { max=signal[i]; maxchan=chan[i] } }; print maxchan }
    ' | sed -e 's/"//g' )

    wl -a $INTERFACE channel $chan
    display "Connect to ch:"$chan $AP
    wl join $AP
    sleepin $SCANRESULTSWAIT
    #wl status

    return 1 #OK

else
    return 0 #Error, not found
fi

}
#####
#### Function for Checking data forwarding to Hospital_AP ####
#####
check_fwd()
{
led white on
con=$( wl status | grep -c "Not" )
if [ "$con" -ne 1 ] ; then
    pingres=$( ping -c 1 $patientdata_dest_IP | grep -c "ms")
fi
if [ "$pingres" -ge 1 ] ; then
    if [ "$state" -ge 1 ] ; then
        led amber on
        buzzselect
        echo "Forwarding patient physiological data"
        sleep 1
        led amber off
    fi
fi
led white off
}
#####
#### Function for pairing with MP70 #####
#####
pairing()
{
pairtime=$( date +%s )
while [ `checktime $pairtime` -lt $MAXPAIRINGTIME ] ; do

    while [ `checktime $pairtime` -lt $MAXSCANTIME ] ; do
        display "Scanning..."
        wl -a $INTERFACE ap 0
        wl -a $INTERFACE scan -t active -n $n_probes -a $dwell_t
        freemps=0
        while [ $( wl channel | grep -c No ) -eq 0 ] ; do
            freemps=0
        done
        freemps=$( (( wl scanresults | sed -ne
        "$nameMP70_wildcard_FREE"/p" )) | grep -c "SSID" )
        echo mps $freemps
        if [ $freemps -ge 1 ] ; then
            break
        fi
    done
done
}

```



```

        display "Not found. Scanning again..."
        sleepin $INTERSCANWAIT
done #WHILE MAXSCANTIME

if [ $freemps -ge 1 ] ; then
    display "$freemps free MP70s found"

    scanres=$( wl scanresults | sed './.{H;$!d};x;
/'$nameMP70_wildcard_FREE'!/d' | awk 'BEGIN {} /^SSID/ {
print $2} /^Mode/ {print $4,$10} /^BSSID/ {print $2; print
""} END {}' | sed -e 's/"//g' )

    chan=$( wl scanresults | sed './.{H;$!d};x;
/'$nameMP70_wildcard_FREE'!/d' | awk 'BEGIN {} /^Mode/ {canal[
$10]++} END { max=0; for (i in canal) {if (canal[i] > max) {
max=canal[i]; maxcanal=i} } ; print maxcanal }' | sed -e
's/"//g' )

    #echo resultados $scanres
    echo canal $chan

    wl -a $INTERFACE channel $chan
    wl -a $INTERFACE channel
    wl -a $INTERFACE ap 1
    wl -a $INTERFACE ap
    wl -a $INTERFACE ssid X2_FREE_${patID}

    sleepin $X2APWAIT
    wl -a $INTERFACE ap 0
    wl -a $INTERFACE ap

    wl -a $INTERFACE scan -t active -c $chan -n $n_probes -a $dwell_t

    while [ $( ( wl channel | grep -c No ) -eq 0 ) ; do
        a=0
    done
    candidatenum=$( ( wl scanresults | sed -ne "/"${
nameMP70_wildcard_FREE}_${patID}"/p" ) | grep -c
"SSID" )

    candidateres=$( wl scanresults | sed './.{H;$!d};x;
/'$nameMP70_wildcard_FREE'!/d' | awk 'BEGIN {}
/^SSID/ {print $2} END {}' | sed -e 's/"//g' )

    display "Select an MP70"
    ssid=""

    if [ $candidatenum -ge 1 ] ; then

        primaryssid=$( echo $candidateres | sed -e 's/_FREE//g' )
        echo prima $primaryssid
        eval list${ord}="$primaryssid"
        echo eva list
        eval echo \${list}${ord}
        let ord++

        echo ord $ord
        echo candidats $candidatenum

        while [ 1 ] ; do
            menulist $candidatenum
            optionlist=$?
            echo Option from the list: $optionlist
            case $optionlist in
                0 )      return 0 #back to menu
                        ;;
                999)    echo menu again
                        ;;
                * )      break
                        ;;
            esac
        done
    fi
done

```

```

#                ssid="MP_0.7" #for testing purposes use fixed ssid="MP_0.7"

echo You have selected $ssid

wl -a $INTERFACE join $ssid

wl -a $INTERFACE scan -t active -c $chan -n $n_probes -a $dwell_t

while [ $( wl channel | grep -c No ) -eq 0 ] ; do
    a=0
done
candidatenum=$( ( wl scanresults | sed -ne "/"${
nameMP70_wildcard_ASSIGNED}_${patID}"/p" )) | wc -l )
#found matching candidates
return 1

else
    display "Standalone monitor"
    #Scenario 4
    echo "Suggestion: connect to Hospital_AP"
fi
done #pairingtime
}
#####
##### X2 SCRIPT #####
#####
#####
=====
# Parameters #
=====
export INTERFACE=eth1
export nameMP70_wildcard_FREE="MP_*_F"
export nameMP70_wildcard_ASSIGNED="MP_*_A"
export MAXSCANTIME=4
export MAXPAIRINGTIME=10
export MAXPINGTIME=1
export INTERSCANWAIT=7
export SCANRESULTSWAIT=10
export X2APWAIT=20
export SCROLLWAIT=8
export TOTALOPTIONS=3
export DIR="/jffs/wimed_diego/"
export BUZZWAIT=0
export FREE=0
export ASSIGN=1
export LINKED=2
export DISPLAYWAIT=2
export nameHospitalAP="Hospital.*"
export patientdata_dest_IP=192.168.1.1
export list='list'

====Default arguments=====
export verbose=1
export dwell_t=20
export n_probes=2
export ssid=""
=====

#####
##### Menu Text #####
#####
#----- FREE -----
#-----
text10="Create patient          "
help10="Create a new PatientID for  "
addh10="this X2 and its patient    "

text20="Replacement X2          "
help20="X2 replacement with already "
addh20="assigned MP70 and PatientID  "

```

```

text30="Connect to AP          "
help30="Connect to Hospital network "
addh30=" directly              "

#-----
#-----  ASSIGN  -----
#-----
text11="Start pairing          "
help11="Pair the X2 with a free MP70 "
addh11="Choose between available MP70"

text21="Unassign patID        "
help21="Unassign the patientID  "
addh21="from this X2         "

text31="Connect to AP          "
help31="Connect to Hospital network "
addh31=" directly              "

#-----
#-----  LINKED  -----
#-----
text12="Unlink from MP70      "
help12="Pause the connection between "
addh12="this X2 and its MP70    "

text22="Unpair from MP70      "
help22="Break the pairing       "
addh22="between this X2 and its MP70 "

text32="Unassign patient      "
help32="Unassign the patientID  "
addh32="from this X2          "

#=====

#=====
# Initial global variables      ==
#=====
export state=$FREE
export pos=1
export link=0
export poslist=1
export patID
export myMP70
#=====

#=====
# Clean initialization          ==
#=====
cleardisplay
wl -a $INTERFACE ap 0
#=====

#=====
#===== Processing arguments =====
#=====
echo args $# ":" $1 $2 $3 $4

if [ "$#" -ge 1 ] ; then
    case $1 in
        "-s" ) verbose=0
                echo Silent mode
                ;;
        "-n" ) n_probes=$2
                echo $2 probes per scanned channel
                ;;
        "-d" ) dwell_t=$2
                echo $2 "ms of dwell time per channel (active scanning)"
                ;;
        * )      printf "Usage: %s: [-s] Silent mode [-n n_probes] number of
                probes per scanned channel [-d dwell_t] dwell time per channel (

```

```

        active scanning) \n" $0 >&2
            exit 2
            ;;
        esac
fi
if [ "$#" -ge 2 ] ; then
    case $1 in
        "-s" ) case $2 in
                "-n" ) n_probes=$3
                        echo $3 probes per scanned channel
                        ;;
                "-d" ) dwell_t=$3
                        echo $3 "ms of dwell time per channel (active scanning)"
                        ;;
                * ) printf "Usage: %s: [-s] Silent mode [-n n_probes] number of
                probes per scanned channel [-d dwell_t] dwell time per channel (
                active scanning)\n" $0 >&2
                exit 2
                ;;
            esac
            ;;
        "-n" ) case $3 in
                "-s" ) verbose=0
                        echo Silent mode
                        ;;
                "-d" ) dwell_t=$4
                        echo $4 "ms of dwell time per channel (active scanning)"
                        ;;
                * ) printf "Usage: %s: [-s] Silent mode [-n n_probes] number of
                probes per scanned channel [-d dwell_t] dwell time per channel (
                active scanning) \n" $0 >&2
                exit 2
                ;;
            esac
            ;;
        "-d" ) case $3 in
                "-s" ) verbose=0
                        echo Silent mode
                        ;;
                "-n" ) n_probes=$4
                        echo $4 probes per scanned channel
                        ;;
                * ) printf "Usage: %s: [-s] Silent mode [-n n_probes] number of
                probes per scanned channel [-d dwell_t] dwell time per channel (
                active scanning) \n" $0 >&2
                exit 2
                ;;
            esac
            ;;
        * ) printf "Usage: %s: [-s] Silent mode [-n n_probes] number of
        probes per scanned channel [-d dwell_t] dwell time per channel (
        active scanning) \n" $0 >&2
        exit 2
        ;;
    esac
fi

if [ "$#" -gt 4 ] ; then
    case $1 in
        "-n" ) n_probes=$5
                echo $5 probes per scanned channel
                ;;
        "-d" ) dwell_t=$5
                echo $5 "ms of dwell time per channel (active scanning)"
                ;;
        * ) printf "Usage: %s: [-s] Silent mode [-n n_probes] number of
        probes per scanned channel [-d dwell_t] dwell time per channel (
        active scanning) \n" $0 >&2
        exit 2
        ;;
    esac
fi

```

```

=====

if [ "$verbose" -ne 0 ] ; then
    display "Philips ResearchPatient Monitor"
    echo Salutation message displayed
    sleep $DISPLAYWAIT

    tutorial
fi

#RESET WL
wl -a $INTERFACE down
wl -a $INTERFACE up

pos=1
while [ true ] ; do

echo current state: $state current menu pos: $pos

menu
option=$?
echo Option: $option

case $state in
    $FREE )
        case $option in
            10)    echo Generate PatientID
                    patID=$( ./X2_genPatientID.sh )
                    state=$ASSIGN
                    #if [ "$link" -eq 0 ] ; then
                    #    connect_hospital
                    #fi
                    ;;
            20)    echo Replace X2
                    #assuming it was succesful, the X2 will be assigned and linked
                    state=$LINKED
                    menustatus
                    ;;
            30)    echo Connect to Hospital_AP
                    connect_hospital
                    if [ "$?" -eq 0 ] ; then
                        buzz
                        display "Unable to connect"
                        display "to Hospital AP"
                    else
                        menustatus #show status connection to AP
                    fi
                    ;;
            0)    echo Back to status
                    menustatus
                    ;;
            999)  echo menu again
                    ;;
        esac
        ;;
    $ASSIGN )
        case $option in
            11 )    echo Pairing
                    pairing
                    if [ "$?" -eq 0 ] ; then
                        buzz
                        display "Unable to pair MP70"
                    else
                        #if it was succesful, the X2 will be assigned and linked
                        state=$LINKED
                        myMP70=$( wl ssid | sed -e 's/Current SSID: //g' | sed -e
's///g' )
                        menustatus

```

```

        fi
        ;;
21) echo Unassign Patient
    #assuming it was succesful, the X2 will be unassigned
    state=$FREE
    patID=""
    menustatus
    ;;
31) echo Connect to Hospital_AP
    connect_hospital
    if [ "$?" -eq 0 ] ; then
        buzz
        display "Unable to connect"
        display "to Hospital AP"
    else
        menustatus #show status connection to AP
    fi
    ;;
0) echo Back to status
    menustatus
    ;;
999) echo menu again
    ;;

    esac
    ;;

$LINKED ) case $option in

12 ) echo Unlink MP70
    #assuming it was succesful, the X2 will be assigned and unlinked
    state=$ASSIGN
    ssid=$( wl ssid | sed -e 's/Current SSID: //g' | sed -e 's//g'

)

    link=0
    #wl -a $INTERFACE join $ssid
    menustatus
    ;;
22) echo Unpairing MP70
    #assuming it was succesful, the X2 will be unassigned
    state=$FREE
    ssid=" _ "
    #note
    wl -a $INTERFACE join $ssid
    menustatus
    ;;
32) echo Unassign Patient
    #assuming it was succesful, the X2 will be unassigned
    state=$FREE
    patID=""
    ssid=" _ "
    #note
    wl -a $INTERFACE join $ssid
    menustatus
    ;;
0) echo Back to status
    menustatus
    ;;
999) echo menu again
    ;;

    esac
    ;;

esac

done

display "#####"
echo
echo END OF THE SCRIPT
echo

##### END #####

```

The following page is the X2 portable monitor script for creating a new PatientID in Linux shell script format. Filename:

`pdf-X2_genPatientID.pdf`

```

#!/bin/sh
#X2_genPatientID.sh
##### VARIABLES #####
interface=eth1
DIR="/jffs/"
#####

#GET MAC
macsp=$( ifconfig $interface | sed -ne "s/${interface}.*Link encap:Ethernet HWaddr //p" )

#CLEAN EXTRA SPACE AT THE END
mac=$( echo $macsp | sed -ne "s/:/:/p" )

#CHECK COUNTER EXISTENCE
occur=$( ls $DIR | grep -c patient_counter )
if [ $occur -ne "1" ] ; then

    #CREATE IF DOESN'T EXIST
    patient_count=$( wl rand | sed -ne "s/ (.*)//p" )
    echo $patient_count > `echo ${DIR}patient_counter`
fi

#INCREMENT COUNTER IN 1
patient_count=$( cat patient_counter )
if [ $patient_count -lt 99999 ] ; then
    patient_count=$( expr $patient_count + 1 )
    echo $patient_count > `echo ${DIR}patient_counter`
else
    patient_count=1
    echo $patient_count > `echo ${DIR}patient_counter`
fi

#CONCATENATE MAC AND COUNTER
patID="${mac}"_"${patient_count}"

#RETURN RESULT
echo $patID

```


D.2 MP70 bedside monitor script: SoftAP implementation

The following pages are the MP70 bedside monitor scripts source code in Linux shell script format. Filename:

`pdf-script_wimed_MP70.pdf`

```

#!/bin/sh
#script_wimed_MP70.sh
#####
####  Function for checking time passed since initime #####
#####
# Expects a timer as argument $1
# and returns seconds since timer was updated
checktime()
{
    echo $((`date +%s`-$1))
}
#####
####  Function for sleeping less than a second #####
#####
sleepin()
#Expects an integer as argument $1, to repeat sleep 0 $1 times
{
    a=0
    while [ $a -lt $1 ] ; do
        sleep 0
        let a=a+1
    done
}
#####
#####
#####  MP70 SCRIPT #####
#####
#####
#====
# Parameters #
#====
export prim="wl0.1"
export secon="wl0.2"
export IP="0.7"
export chan=6
export state=0
export MAXSCANTIME=4
export MAXPAIRINGTIME=20
export MAXPINGTIME=1
export INTERSCANWAIT=7
export SCANRESULTSWAIT=10
export FREE=0
export LINKED=1
export UNLINKED=2
export INTERFACE=$secon
export nameX2_FREE_wildcard="X2_FREE_.*"

#====Default arguments=====
export dwell_t=20
export n_probes=2
#====

wl -a $prim ssid "MP_">${IP}
wl -a $secon ssid "MP_">${IP}"_F"

echo 0 > /proc/diag/led/ses_orange
echo 0 > /proc/diag/led/ses_white

while [ 1 ] ; do

    while [ 1 ] ; do

```

```

echo 1 > /proc/diag/led/ses_white #white led on
echo -n "."
wl -a $INTERFACE scan -t active -n $n_probes -a $dwell_t -c $chan
freex2s=0
while [ $( wl -a $INTERFACE channel | grep -c No ) -eq 0 ] ; do
    freex2s=0
done
freex2s=$( ( wl scanresults | sed -ne
"/"$nameX2_FREE_wildcard"/p" ) | wc -l )
if [ $freex2s -ge 1 ] ; then
    echo "Free X2 found!"
    echo 1 > /proc/diag/led/ses_orange #orange led on
    break
fi
echo 0 > /proc/diag/led/ses_white #white led off
done
candidateres=$( wl scanresults | sed '/./{H;$!d};x;
/'$nameX2_FREE_wildcard'!/d' | awk 'BEGIN {} /^SSID/ {
print $2} /^Mode/ {print $4,$10} /^BSSID/ {print $2;
print ""} END {}' | sed -e 's//g' )

X2_MAC=$( wl scanresults | sed '/./{H;$!d};x;
/'$nameX2_FREE_wildcard'!/d' | awk 'BEGIN {} /^SSID/ {print
$2} END {}' | sed -e 's//g' | sed -e 's/_/ /g' | awk
'BEGIN {} {print $3} END {}' )

patID=$( wl scanresults | sed '/./{H;$!d};x;
/'$nameX2_FREE_wildcard'!/d' | awk 'BEGIN {} /^SSID/ {print
$2} END {}' | sed -e 's//g' | sed -e 's/_/ /g' | awk 'BEGIN
{} {print $4} END {}' )

wl -a $secon ssid "MP_">${IP}"_F_">${X2_MAC}"_">${patID}

wl -a $prim macmode 2
wl -a $prim mac none
wl -a $prim mac $X2_MAC

pairtime=$( date +%s )
while [ `checktime $pairtime` -lt $MAXPAIRINGTIME ] ; do
myX2=$( wl -a $prim assoclist | grep -c $X2_MAC )
if [ "$myX2" -eq 1 ] ; then
    break
fi

wl -a $INTERFACE scan -t active -n $n_probes -a $dwell_t

while [ $( wl channel | grep -c No ) -eq 0 ] ; do
    a=0
done

MP70_wildcard_patID="MP_.*A_">${patID}
otherMP70=$( wl scanresults | grep -c $MP70_wildcard_patID )
if [ "$otherMP70" -ge 1 ] ; then
    myX2=0
    break
fi

done

if [ "$myX2" -eq 1 ] ; then
    wl -a $secon ssid "MP_">${IP}"_A_">${patID}
    echo 1 > /proc/diag/led/ses_orange

```

```
while [ "$myX2" -eq 1 ] ; do
    myX2=$( wl -a $prim assoclist | grep -c $X2_MAC )
done
echo 0 > /proc/diag/led/ses_orange

else
    wl -a $secon ssid "MP_">${IP}"_F"
    wl -a $prim mac none
fi

done

##### END OF THE SCRIPT #####
```

The following pages are the MP70 bedside monitor SoftAP configuration. Filename:

pdf_etc_config_MP70.pdf

```

#####
# Network interfaces configuration
#####
root@OpenWrt:/etc/config# ifconfig
br-lan    Link encap:Ethernet  HWaddr 00:1D:7E:30:A6:56
          inet addr:192.168.0.7 Bcast:192.168.0.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:6892 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6823 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:384857 (375.8 KiB)  TX bytes:3539783 (3.3 MiB)

eth0      Link encap:Ethernet  HWaddr 00:1D:7E:30:A6:56
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:6642 (6.4 KiB)
          Interrupt:4

eth0.0    Link encap:Ethernet  HWaddr 00:1D:7E:30:A6:56
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:6214 (6.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436 Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2714 (2.6 KiB)  TX bytes:2714 (2.6 KiB)

w10       Link encap:Ethernet  HWaddr 00:1D:7E:30:A6:58
          inet addr:192.168.1.7 Bcast:192.168.1.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:10439 errors:0 dropped:0 overruns:0 frame:67442
          TX packets:12125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3463481 (3.3 MiB)  TX bytes:4054492 (3.8 MiB)
          Interrupt:2 Base address:0x5000

w10.1     Link encap:Ethernet  HWaddr 02:1D:7E:30:A6:59
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

#####
# Wireless interfaces configuration
#####
root@OpenWrt:/etc/config# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth0.0    no wireless extensions.

br-lan    no wireless extensions.

w10       IEEE 802.11-DS  ESSID:"Hospital_AP"
          Mode:Master  Frequency:2.437 GHz  Access Point: 00:23:69:2A:69:D5
          Bit Rate=54 Mb/s   Tx-Power:32 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Link Quality:5  Signal level:0  Noise level:163
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0

```

Tx excessive retries:2 Invalid misc:0 Missed beacon:0

wl0.1 IEEE 802.11-DS ESSID:"MP70"
Mode:Master Channel:6 Access Point: 02:1D:7E:30:A6:59
Bit Rate=54 Mb/s
RTS thr:off Fragment thr:off

Wireless configuration

#####

root@OpenWrt:/etc/config# cat wireless

```
config wifi-device wl0
    option type      broadcom
    option channel   6

    # REMOVE THIS LINE TO ENABLE WIFI:
    option disabled 0
```

```
config wifi-iface
    option device    wl0
    option network   lan
    option mode      ap
    option ssid      MP70
    option encryption none
```

```
config wifi-iface
    option device    wl0
    option mode      sta
    option ssid      Hospital_AP
    option encryption none
```


Network configuration

#####

root@OpenWrt:/etc/config# cat network

```
config 'switch' 'eth0'
    option 'vlan0' '1 2 3 4 5*'
    option 'vlan1' '0 5'
```

```
config 'interface' 'loopback'
    option 'ifname' 'lo'
    option 'proto' 'static'
    option 'ipaddr' '127.0.0.1'
    option 'netmask' '255.0.0.0'
```

```
config 'interface' 'lan'
    option 'type' 'bridge'
    option 'ifname' 'eth0.0'
    option 'proto' 'static'
    option 'ipaddr' '192.168.0.7'
    option 'netmask' '255.255.255.0'
```

```
config 'interface' 'wan'
    option 'ifname' 'wl0'
    option 'proto' 'static'
    option 'ipaddr' '192.168.1.7'
    option 'netmask' '255.255.255.0'
    option 'gateway' '192.168.1.1'
    option 'dns' '192.168.1.1'
```

```
config 'route'
    option 'interface' 'lan'
    option 'target' '192.168.1.0'
    option 'netmask' '255.255.255.0'
    option 'gateway' '192.168.1.1'
```

#####

```

# DHCP configuration
#####
root@OpenWrt:/etc/config# cat dhcp
config dnsmasq
    option domainneeded      1
    option boguspriv         1
    option filterwin2k       '0' #enable for dial on demand
    option localise_queries  1
    option local             '/lan/'
    option domain            'lan'
    option expandhosts        1
    option nonegcache        0
    option authoritative     1
    option readethers        1
    option leasefile         '/tmp/dhcp.leases'
    option resolvfile        '/tmp/resolv.conf.auto'
    #list server              '/mycompany.local/1.2.3.4'
    #option nonwildcard      0
    #list interface          br-lan

config dhcp lan
    option interface         lan
    option start             100
    option limit             150
    option leasetime         12h

config dhcp wan
    option interface         wan
    option ignore            1

#####
# Firewall configuration
#####
root@OpenWrt:/etc/config# cat firewall
config defaults
    option syn_flood        1
    option input             ACCEPT
    option output            ACCEPT
    option forward           ACCEPT

config zone
    option name              lan
    option input             ACCEPT
    option output            ACCEPT
    option forward           ACCEPT

config zone
    option name              wan
    option input             ACCEPT
    option output            ACCEPT
    option forward           ACCEPT
    option masq              1

config forwarding
    option src               lan
    option dest              wan
    option mtu_fix          1

```


The following pages are the Hospital AP configuration. Filename:

pdf_etc_config_HospitalAP.pdf

```

#####
# Network interfaces configuration
#####
root@OpenWrt:/etc/config# ifconfig
br-lan    Link encap:Ethernet  HWaddr 00:23:69:2A:69:D3
          inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:20115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28851 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1758073 (1.6 MiB)  TX bytes:31838127 (30.3 MiB)

eth0      Link encap:Ethernet  HWaddr 00:23:69:2A:69:D3
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:436649 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21723 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:74168110 (70.7 MiB)  TX bytes:2370189 (2.2 MiB)
          Interrupt:4

eth0.0    Link encap:Ethernet  HWaddr 00:23:69:2A:69:D3
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:6826 (6.6 KiB)

eth0.1    Link encap:Ethernet  HWaddr 00:23:69:2A:69:D3
          inet addr:130.145.197.176 Bcast:130.145.197.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:436611 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21581 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:66304899 (63.2 MiB)  TX bytes:2241902 (2.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wl0       Link encap:Ethernet  HWaddr 00:23:69:2A:69:D5
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:20112 errors:0 dropped:0 overruns:0 frame:1918079
          TX packets:28960 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2039623 (1.9 MiB)  TX bytes:32074385 (30.5 MiB)
          Interrupt:2 Base address:0x5000

#####
# Wireless interfaces configuration
#####
root@OpenWrt:/etc/config# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth0.0    no wireless extensions.

eth0.1    no wireless extensions.

br-lan    no wireless extensions.

wl0       IEEE 802.11-DS  ESSID:"Hospital_AP"
          Mode:Master  Frequency:2.437 GHz  Access Point: 00:23:69:2A:69:D5
          Bit Rate=54 Mb/s   Tx-Power:0 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off

```

```
Link Quality:5 Signal level:0 Noise level:161
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:64 Invalid misc:0 Missed beacon:0
```

```
#####
# Wireless configuration
#####
root@OpenWrt:/etc/config# cat wireless
```

```
config 'wifi-device' 'wl0'
  option 'type' 'broadcom'
  option 'disabled' '0'
  option 'channel' '6'
  option 'txpower' '0'

config 'wifi-iface'
  option 'device' 'wl0'
  option 'network' 'lan'
  option 'mode' 'ap'
  option 'encryption' 'none'
  option 'ssid' 'Hospital_AP'
```

```
#####
# Network configuration
#####
root@OpenWrt:/etc/config# cat network
```

```
config 'switch' 'eth0'
  option 'vlan0' '0 1 2 3 5*'
  option 'vlan1' '4 5'

config 'interface' 'loopback'
  option 'ifname' 'lo'
  option 'proto' 'static'
  option 'ipaddr' '127.0.0.1'
  option 'netmask' '255.0.0.0'

config 'interface' 'lan'
  option 'type' 'bridge'
  option 'ifname' 'eth0.0'
  option 'proto' 'static'
  option 'ipaddr' '192.168.1.1'
  option 'netmask' '255.255.255.0'
  option 'dns' '130.145.128.20'
  option 'gateway' '130.145.197.1'

config 'interface' 'wan'
  option 'ifname' 'eth0.1'
  option 'proto' 'dhcp'
```

```
root@OpenWrt:/etc/config# cat dhcp
```

```
#####
# DHCP configuration
#####
```

```
config 'dnsmasq'
  option 'domainneeded' '1'
  option 'boguspriv' '1'
  option 'filterwin2k' '0'
  option 'localise_queries' '1'
  option 'local' '/lan/'
  option 'domain' 'lan'
  option 'expandhosts' '1'
  option 'nonegcache' '0'
  option 'authoritative' '1'
  option 'readethers' '1'
  option 'leasefile' '/tmp/dhcp.leases'
  option 'resolvfile' '/tmp/resolv.conf.auto'
```

```

config 'dhcp' 'lan'
    option 'interface' 'lan'
    option 'leasetime' '12h'
    option 'ignore' '0'
    option 'start' '200'
    option 'limit' '49'

config 'dhcp' 'wan'
    option 'interface' 'wan'
    option 'ignore' '1'

#####
# Firewall configuration
#####
root@OpenWrt:/etc/config# cat firewall
config defaults
    option syn_flood      1
    option input          ACCEPT
    option output         ACCEPT
    option forward        REJECT

config zone
    option name           lan
    option input          ACCEPT
    option output         ACCEPT
    option forward        REJECT

config zone
    option name           wan
    option input          REJECT
    option output         ACCEPT
    option forward        REJECT
    option masq           1

config forwarding
    option src            lan
    option dest           wan
    option mtu_fix       1

```


Appendix E

Philips Patient Monitoring products

This appendix includes the specifications brochures and data sheets of the main products of the Patient Monitoring division of Philips Healthcare.

The Philips IntelliVue Patient Monitor series offers a complete monitoring solution that is flexible and modular, designed to suit a broad spectrum of monitoring needs. It comprises a whole range of multi-parameter patient monitor models: MP2/X2, MP5, MP20, MP30, MP40, MP50, MP60, MP70, MP80 and MP90 among other IntelliVue Patient Monitors that consist of display units including built-in or separate flat panel displays, central processing units (CPU) and physiological measurement modules. All monitors share the same system architecture and the same software is executed on each monitor.

The IntelliVue Patient Monitors measure multiple physiological parameters such as surface ECG electrocardiogram, arrhythmias, invasive and non-invasive blood pressure, respiration parameters, SPO2 oxygen saturation of arterial blood, temperature, EEG electroencephalogram, etc., generate alarms, record physiological signals, store derived data, and communicate derived data and alarms to central stations via the IntelliVue Clinical Network.

Filename:

Intellivue_family-ES.pdf [in Spanish]

Cuidado Trascendencia

la familia de monitores de paciente IntelliVue



Presentación de la información IntelliVue: Un antídoto para la sobrecarga de información

Al proporcionar una imagen mental de la información del paciente, las pantallas extraordinariamente configurables y las herramientas de ayuda a la toma de decisiones clínicas de IntelliVue reflejan procesos pensados clínicamente.

Los monitores IntelliVue recogen, combinan y establecen referencias cruzadas de los datos fisiológicos para facilitar una imagen coherente del estado del paciente. Las aplicaciones oscilan desde la detección de sucesos basada en reglas y las alarmas inteligentes a los algoritmos sofisticados que asignan

categorías y crean tendencias de la información de forma lógica y útil.

Las mediciones más relevantes clínicamente que necesita

Con mediciones innovadoras y “estándar de cuidados”, Philips ofrece una amplia gama de las mediciones más destacadas del mercado enfocando en la presentación práctica de la información de todas las mediciones.

Los módulos de medición son compatibles con las diversas plataformas.



1967

Hewlett-Packard entra en el sector médico con la adquisición de Sanborn Company de Waltham, Massachusetts.



1968

HP presenta el primer monitor fetal no invasivo disponible comercialmente con monitorización externa de las contracciones uterinas, fonocardiografía y ECG directo.



Década de los 80

Hewlett-Packard ofrece el primer sistema de monitorización modular del sector médico, diseñado con módulos de medición.

continuo. clínica.



La familiaridad aporta eficacia

Cuando se conoce un monitor IntelliVue, se conocen todos. Una interfase de usuario común ahorra tiempo de formación del personal y contribuye a aumentar el flujo de trabajo y la eficacia del funcionamiento. Además, los fungibles se pueden compartir entre todos los monitores IntelliVue.

Un IntelliVue para cada servicio

Elija el modelo que se adapte a sus pacientes y a su presupuesto. La familia IntelliVue abarca todos los entornos de cuidados, los niveles de gravedad de los pacientes y los requisitos clínicos con características diseñadas según sus necesidades.



Una red clínica sólida

Con la Red Clínica IntelliVue, la información crítica de monitorización del paciente y las alarmas recorren una red aislada física o lógicamente que también está abierta a otros sistemas de información hospitalaria.

Configuración de pantalla adaptable y sencilla

Elija entre cientos de visualizaciones de pantalla estándar o diseñe la suya propia mediante los servicios de personalización de Philips. Los perfiles de usuario permiten la adaptación precisa a los requisitos específicos del caso clínico y permiten presentar la información en el formato más práctico.



Década de los 90

Con los modelos especializados de monitorización de pacientes para anestesia y cuidados intensivos neonatales, Hewlett-Packard ofrece monitores y mediciones en un espectro de cuidados aún más amplio.



2002









Philips Medical Systems desvela el primer monitor de paciente IntelliVue.



2005

La flexibilidad de la Red Clínica IntelliVue unifica la monitorización alámbrica e inalámbrica para lograr un flujo ininterrumpido de los datos clínicos.



IntelliVue	MP20	MP30	MP40	MP50	MP60	MP70	MP80	MP90
Tipo de paciente	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal	Adulto, pediátrico, neonatal
Formas de onda	3 (4 opcional) (13 para ECG convencional y EASI)	3 (4 opcional) (13 para ECG convencional y EASI)	Hasta 6** (13 para ECG convencional y EASI)	Hasta 6** (13 para ECG convencional y EASI)	Hasta 6** (13 para ECG convencional y EASI)	Hasta 8 (13 para ECG convencional y EASI)	Hasta 8 (13 para ECG convencional y EASI)	Hasta 12 para pantalla independiente (13 para ECG convencional y EASI)
Parámetros	ECG, Resp, SpO ₂ , PNI, PSI (3), Temp (2), GC, GCC, CO ₂ , PCP, OxiCRG, ST, arritmias, Módulo de gases esenciales, BIS	ECG, Resp, SpO ₂ , PNI, PSI (3), Temp (2), GC, GCC, CO ₂ , PCP, OxiCRG, ST, arritmias, Módulo de gases esenciales, BIS	ECG, Resp, SpO ₂ (2), PNI, PSI (4), Temp (2), GC, GCC, CO ₂ , PCP, BIS, OxiCRG, ST, arritmias, GasTc, ID de 5 agentes en gases anestésicos, EEG, VueLink (2)	ECG, Resp, SpO ₂ (2), PNI, PSI (4), Temp (2), GC, GCC, CO ₂ , PCP, BIS, OxiCRG, ST, arritmias, GasTc, ID de 5 agentes en gases anestésicos, EEG, VueLink (2)	ECG, Resp, SpO ₂ (2), PNI, PSI (6), Temp (4), GC, GCC, CO ₂ , PCP, BIS, OxiCRG, ST, arritmias, SvO ₂ , GasTc, ID de 5 agentes en gases anestésicos, EEG, VueLink (4)	ECG, Resp, SpO ₂ (2), PNI, PSI (6), Temp (4), GC, GCC, CO ₂ , PCP, BIS, OxiCRG, ST, arritmias, SvO ₂ , GasTc, ID de 5 agentes en gases anestésicos, EEG, VueLink (4)	ECG, Resp, SpO ₂ (2), PNI, PSI (6), Temp (4), GC, GCC, CO ₂ , PCP, BIS, OxiCRG, ST, arritmias, SvO ₂ , GasTc, ID de 5 agentes en gases anestésicos, EEG, VueLink (4)	ECG, Resp, SpO ₂ (2), PNI, PSI (6), Temp (4), GC, GCC, CO ₂ , PCP, BIS, OxiCRG, ST, arritmias, SvO ₂ , GasTc, ID de 5 agentes en gases anestésicos, EEG, VueLink (4)
Pantalla del monitor	Integrada: SVGA de 10,4" en color (800 x 600)	Integrada: SVGA de 10,4" en color (800 x 600)	Integrada: SVGA de 12" en color (800 x 600)	Integrada: SVGA de 12" en color (800 x 600)	Integrada: XGA de 15" en color (1.024 x 768)	Integrada: XGA de 15" en color (1.024 x 768)	Elección del usuario: XGA (1.024 x 768) o SXGA (1.280 x 1.024)	Elección del usuario de hasta 2 pantallas independientes: XGA (1.024 x 768) o SXGA (1.280 x 1.024)
Pantallas esclavas admitidas	Una	Una	Una	Una	Una	Una	Una	Dos
Peso	5,8 kg (13 lbs) con una batería y MMS	5,8 kg (13 lbs) con una batería y MMS	8,6 kg (19 lbs) con batería	8,6 kg (19 lbs) con batería	11 kg (25 lbs)	11 kg (25 lbs)	11 kg (25 lbs) Solo CPU	11 kg (25 lbs) Solo CPU
Funcionamiento con batería	2 ión-litio de 'intercambio en caliente' 5 horas*	2 ión-litio de 'intercambio en caliente' 5 horas*	2 ión-litio de 'intercambio en caliente' 5 horas*	2 ión-litio de 'intercambio en caliente' 5 horas*	No	No	No	No
Navegación por la pantalla	Control de navegación	Control de navegación, Pantalla táctil	Control de navegación; SpeedPoint remoto; Ratón; cualquier dispositivo PS/2	Control de navegación; pantalla táctil; SpeedPoint remoto; Ratón; cualquier dispositivo PS/2	Control de navegación; SpeedPoint remoto; Ratón; cualquier dispositivo PS/2	Pantalla táctil; SpeedPoint; (opcional) SpeedPoint remoto; Ratón; cualquier dispositivo PS/2	Pantalla táctil; SpeedPoint; SpeedPoint remoto; Ratón; cualquier dispositivo PS/2	Pantalla táctil; SpeedPoint; SpeedPoint remoto; Ratón; cualquier dispositivo PS/2
Servidor de mediciones multiparamétricas	Si 	Si 	Si 	Si 	Si 	Si 	Si 	Si 
Servidor de módulos flexibles, 8 módulos	No aplicable	No aplicable	No aplicable	No aplicable	1	1	1	Hasta 2
Ranuras integradas para módulos de medición	No aplicable	No aplicable	4 (opcional)	4 (opcional)	2 (opcional)	2 (opcional)	No aplicable	No aplicable
Capacidades de interconexión	RS232/MB, impresora, llamada a la enfermera, PS/2, VGA	RS232/MB, impresora, llamada a la enfermera, PS/2, VGA	Módulo VueLink para dispositivos externos, RS232/MB, impresora, llamada a la enfermera, PS/2, VGA	Módulo VueLink para dispositivos externos, RS232/MB, impresora, llamada a la enfermera, PS/2, VGA	Módulo VueLink para dispositivos externos, RS232/MB, impresora, llamada a la enfermera, PS/2, VGA	Módulo VueLink para dispositivos externos, RS232/MB, impresora, llamada a la enfermera, PS/2, VGA	Módulo VueLink para dispositivos externos, RS232/MB, impresora, llamada a la enfermera, PS/2, VGA/DVI	Módulo VueLink para dispositivos externos, RS232/MB, impresora, llamada a la enfermera, PS/2, VGA/DVI
Capacidad de conexión en red	LAN opcional	LAN estándar	Listo para conectar a la LAN	LAN estándar	LAN opcional	LAN estándar	LAN estándar	LAN estándar
Tecnología portal	No	No	Si, ventana de 640 x 420	Si, ventana de 640 x 420	Si, ventana de 800 x 540	Si, ventana de 800 x 540	Si, ventana de 800 x 540	Si, ventana de 800 x 540 o superior
Almacenamiento local de tendencias	De 4 a 48 horas a 12 s, 1 ó 5 min	De 4 a 48 horas a 12 s, 1 ó 5 min	De 4 a 48 horas a 12 s, 1 ó 5 min	De 4 a 48 horas a 12 s, 1 ó 5 min	De 4 a 72 horas a 12 s, 1 ó 5 min	De 4 a 72 horas a 12 s, 1 ó 5 min	De 4 a 72 horas a 12 s, 1 ó 5 min	De 4 a 72 horas a 12 s, 1 ó 5 min
Almacenamiento central de tendencias	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas	De 24 a 96 horas 4 ondas, 30 parámetros, segmentos ST, sucesos; de 50 a 150 alarmas
Captura/análisis de 12 derivaciones	Si, 10 almacenados en la central	Si, 10 almacenados en la central	Si, 10 almacenados en la central	Si, 10 almacenados en la central	Si, 10 almacenados en la central	Si, 10 almacenados en la central	Si, 10 almacenados en la central	Si, 10 almacenados en la central
Inalámbrico	Si	Si	Si	Si	Si	Si	Si	Si
Registrador	Integrado o central	Integrado o central	Modular o central	Modular o central	Modular o central	Modular o central	Modular o central	Modular o central
Montaje	Montaje rápido/GCX	Montaje rápido/GCX	Montaje rápido/GCX	Montaje rápido/GCX	Varios	Varios	Varios	Varios

M8001A MP20
M8002A MP30
M8003A MP40

M8004A MP50
M8005A MP60
M8007A MP70

M8008A MP80
M8010A MP90

M3001A Servidor de mediciones multiparamétricas

* La estimación de la duración de la batería se basa en las condiciones de funcionamiento anticipadas. Para obtener información detallada, consulte los folletos del producto.

** Hasta 8 formas de onda en China, Hong Kong y Taiwán.



Philips Medical Systems forma parte de Royal Philips Electronics
www.medical.philips.com
medical@philips.com
fax: +31 40 27 64 887

Philips Medical Systems
3000 Minuteman Road
Andover, MA 01810-1085
(800) 934-7372

© Koninklijke Philips Electronics N.V. 2005
Reservados todos los derechos. Prohibida la reproducción total o parcial sin el consentimiento previo por escrito del propietario de los derechos de autor.

Philips Medical Systems Nederland B.V se reserva el derecho de realizar cambios en las especificaciones o de dejar de fabricar cualquier producto en cualquier momento sin previo aviso ni obligaciones y no se considera responsable de las

consecuencias derivadas de la utilización de esta publicación.
Impreso en los Países Bajos
4522 962 03364/862 * JUN 2005

E.1 IntelliVue MP2/X2 Multi-Measurement Module and transport monitor

The MP2/X2 monitors are indicated for use by healthcare professionals whenever there is a need for monitoring the physiological parameters of patients.

Both monitors are intended to be used for monitoring and recording of, and to generate alarms, for, multiple physiological parameters of adults, pediatrics, and neonates.

The monitors are intended for use by trained healthcare professionals in a hospital environment. The ECG measurement is intended to be used for diagnostic recording of rhythm and detailed morphology of complex cardiac episodes.

	IntelliVue MP2/X2
<i>Weight</i>	1.5 kg [3.3 lbs] (MP2 monitor) 1.2 kg [2.7 lbs] (MMS X2 monitor)
<i>Waveforms</i>	Configurable flexible display of up to 3 waveforms
<i>Battery</i>	User replaceable 3-hour battery 10.8 V 1000mAh
<i>Power consumption</i>	<40 W average <65 W peak
<i>Measurement functions</i>	12-lead ECG, SpO_2 , and NBP with industry-leading measurements
<i>Monitor screen display</i>	3.5" LCD TFT touchscreen with 320 x 240 resolution

Table E.1: *MP2/X2 portable patient monitors specifications*

For further technical specification details, see the “Intellivue X2 Multi-Measurement Module Technical Data Sheet” [20].

Filename:

IntelliVue_MMS_X2-brochure.pdf



IntelliVue MMS X2

Combined multi-measurement module and transport monitor

asimpleswitch.com

PHILIPS

The first transp to take

Trust Philips to lighten the load when it comes to patient transport. At just 2.7 lbs (1.2 Kg), the IntelliVue MMS X2 is designed to push the boundaries of what you thought possible. It's small in size and large in capability, offering truly seamless transport across all levels of patient monitoring. Just a single step allows you to unplug and go, helping to reduce error and improve patient safety. IntelliVue MMS X2 is a transport monitor that's also a measurement module, with the clarity of exclusive integrated Clinical Decision Support features that help make it extremely easy to focus on the patient at every point. Trust Philips, a worldwide leader in patient monitoring, to bring you the advances that matter day to day.

port solution
you someplace entirely new



Continuous across the



Provides comprehensive transport monitoring, including options for invasive pressure or CO₂, helping clinicians to immediately focus on the patient in every setting.



Connects to IntelliVue patient monitor for continuous capture of pre-operative patient data and settings.

Small enough
to go anywhere.

Powerful enough
to go everywhere.



Flexible enough to be used as an induction monitor as well as a transport monitor.

information continuum of care

Extremely light yet rugged

IntelliVue MMS X2 is the lightest, smallest, and most rugged advanced transport monitor available (at just 2.7 lbs, 1.2 Kg).

Extremely easy to use

Features the intuitive IntelliVue colorful and clear touch screen with 3.5" display, as well as seamless electronic recording. Just plug and play to transport to other IntelliVue monitors.

Extremely effective in transport

Now getting from Point A to point B is as easy as 1, 2, 3 with the fastest and simplest way to transport a patient. In or out of the hospital, it's just one step to unplug and go. An MMS with a display, alarm capability, battery and extended trends, IntelliVue MMS X2 is part of a seamlessly integrated hospital transport solution and features a 3-hour removable battery.

Extremely effective for patient mobility

So compact, it's easily carried by patients in low-acuity settings, allowing patients the freedom to roam, and the clinician the freedom to provide the best quality of care.

Extremely sustainable

IntelliVue MMS X2 is also a Philips Green Flagship product, meeting rigorous environmental standards in manufacturing and use.



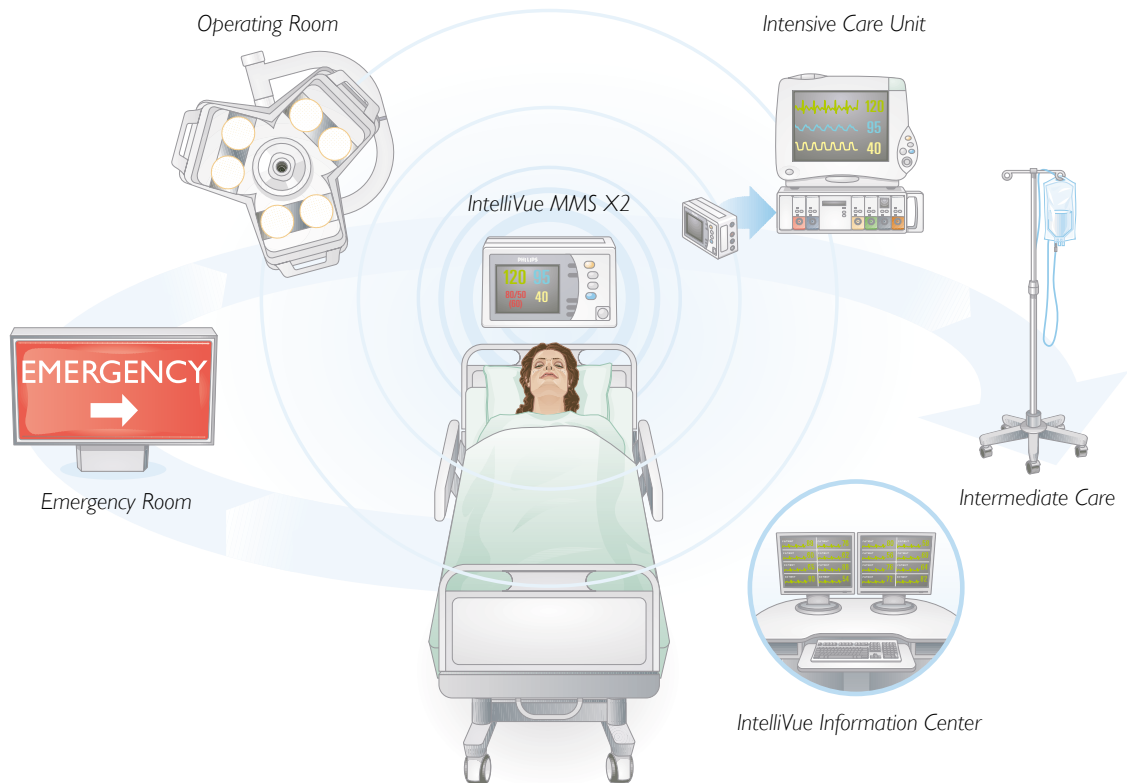
Clearly keeps vital information in front of the anesthesiologist in the OR.



Captures all monitoring information in every environment from the first moment through post-operative care.

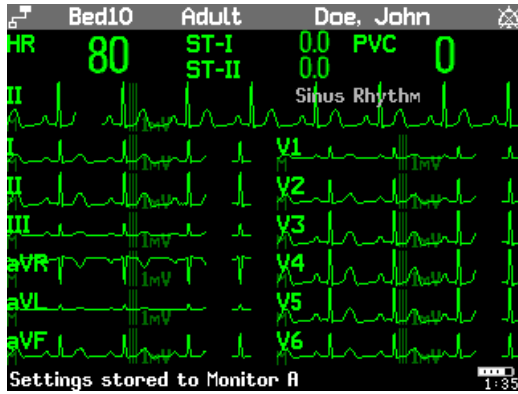
No matter where they go, IntelliVue MMS X2 goes too

The IntelliVue MMS X2: the center of smooth workflow

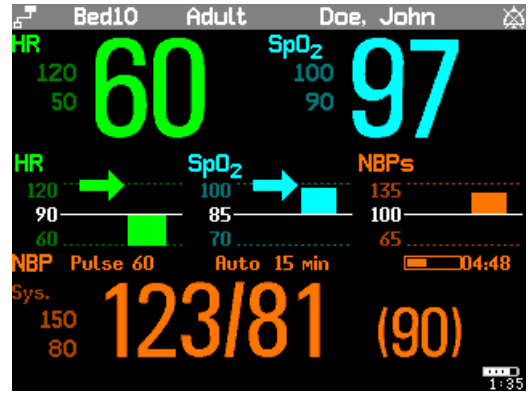


Continuity of data everywhere

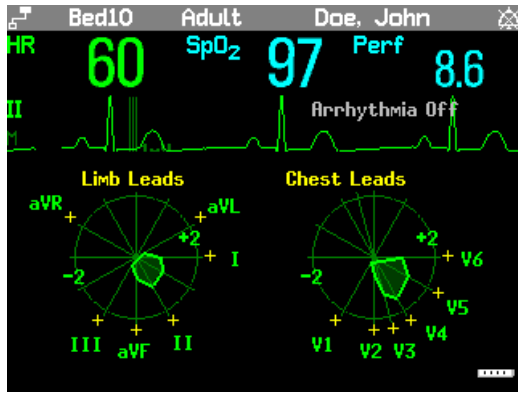
ER, OR, ICU, intermediate care... now it's easier to focus on the patient with this transport monitor and MMS module in one. IntelliVue MMS X2 gives you clearly actionable information to make the best decisions for patients moment to moment.



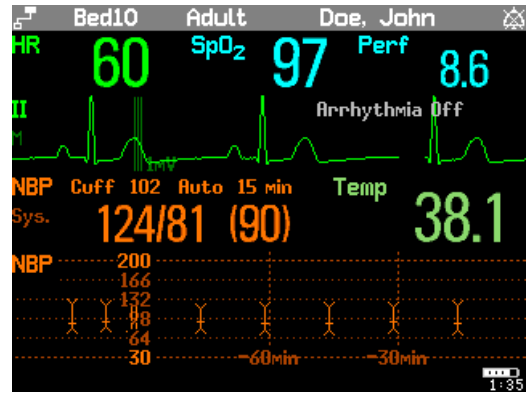
Provides both derived and diagnostic 12-lead ECG measurements.



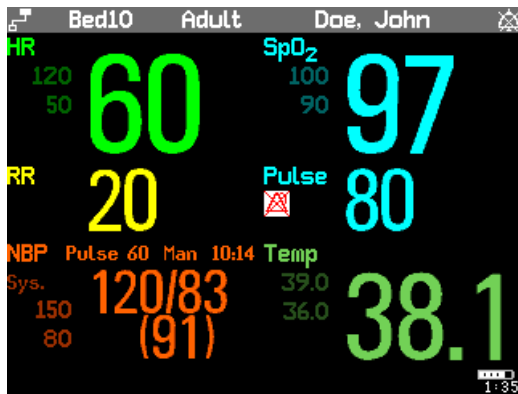
Advanced Horizon Trends feature focuses on deviations from baseline to give a more accurate clinical picture at a glance.



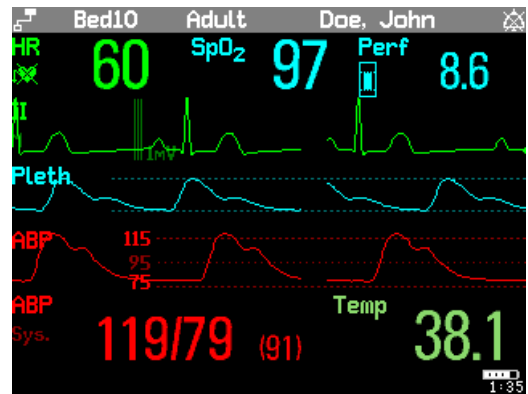
Proprietary ST Map gives a graphical display of ST segment data to quickly view perfusion changes.



Access trending up to 48 hours in 5-minute resolution or 24 hours in 1-minute resolution. Graphical trends are also available on screen.



Immediately view all important data, even from a distance.



Three-waveform display captures most important information for display to support quick, clear decision-making.

IntelliVue MMS X2 takes your patients anywhere they need to go



Philips offers a wide range of supplies, including NIBP cuffs, SpO₂ sensors, and a variety of cables and leads to meet your needs.

M3002A MMS X2

For more information, visit: www.medical.philips.com/IntelliVueMMSX2



© 2007 Koninklijke Philips Electronics N.V.
All rights are reserved.

Philips Medical Systems Nederland B.V. reserves the right to make changes in specifications and/or to discontinue any product at any time without notice or obligation and will not be liable for any consequences resulting from the use of this publication.

Philips Medical Systems is part of Royal Philips Electronics

www.medical.philips.com
medical@philips.com
fax: +31 40 27 64 887

Printed in The Netherlands
4522 962 25581/862 * SEP 2007

Philips Medical Systems
Global Information Center
P.O. Box 1286
5602 BG Eindhoven
The Netherlands

Both MP2 and X2 monitors are also intended for use during patient transport inside and outside of the hospital environment, specially the MP2 monitor, which is more rugged and has been designed to withstand the harsh conditions and exigencies of medical transport and emergencies.

Built to perform under harsh conditions, the MP2 is compliant with out-of-hospital transport standards¹ for both land and air transport. Cleared for use in road ambulance, aircraft and helicopter transport, it is designed to withstand harsh out-of-hospital environments, including rain, shock, vibration, high humidity, and temperature.

Filename:

IntelliVue_MP2-brochure.pdf [in Spanish]

¹The MP2 patient monitor with ECG/Resp, NBP, SpO₂, Pressure, Temp, CO₂ (only Mainstream Sensor M2501A), LAN and battery can be used in a transport environment such as road ambulance, airplane or helicopter. U.S. Army Airworthiness Certification and Evaluation (ACE) program of the U.S. Army Aeromedical Research Laboratory (USAARL). Tests performed in accordance with the following standards: MIL-STD-461E, MIL-STD-810F, MIL-STD-1472F, ANSI/AAMI HE48-1993 HF, ANSI/AAMI ES1.



Monitores de paciente



IntelliVue MP2

Monitor de paciente extremadamente compacto y fácil de usar

PHILIPS

Suficientemente pequeño para Suficientemente grande para

El IntelliVue MP2 es un monitor para traslados increíblemente resistente, versátil y ligero, a la par que fácil de usar. Es un dispositivo asequible, de pequeño tamaño y gran capacidad, que le permitirá monitorizar a sus pacientes en cualquier momento y en cualquier lugar. Un simple paso le permite desconectar y ponerse en marcha a la vez que le ayuda a evaluar, diagnosticar y tratar a sus pacientes en cualquier parte.

Y lo mejor de todo: es Philips, por lo que gozará de un dispositivo de calidad e innovador con una tecnología sencilla para que pueda dedicarse plenamente a la atención al paciente, en lugar de al uso del monitor.

Diseñado específicamente para traslados

Ahora, llegar desde un punto A hasta un punto B es tan sencillo como contar hasta 3 gracias a la continuidad de la monitorización durante el traslado de forma rápida y sencilla. Dispone de un diseño de pantalla flexible perfectamente adaptable a su entorno con una visualización de hasta 3 formas de onda. Este dispositivo también incluye una batería extraíble con 3 horas de duración.

Disponible con las mediciones estándar del sector

Dispone de una pantalla táctil nítida y en color de 3,5 pulgadas, además de una capacidad de registro electrónico sin precedentes de los principales signos vitales. IntelliVue MP2 también cuenta con una versión opcional de mediciones de monitorización completa.

Extremadamente eficaz para la movilidad de pacientes

Gracias a su diseño compacto, los pacientes pueden transportar cómodamente el monitor en entornos de baja gravedad, ofreciendo a los pacientes una gran libertad de movimiento y al personal sanitario la oportunidad de ofrecerles la mejor atención.

Sostenibilidad

IntelliVue MP2 es un producto Philips Green Flagship, que cumple los estrictos requisitos de respeto al medioambiente tanto en términos de fabricación como de uso.



llevarlo a cualquier lugar.
monitorizar a cualquier paciente.



IntelliVue MP2 monitoriza fácilmente desde cualquier lugar y en cualquier momento



Philips ofrece una amplia gama de fungibles, incluidos manguitos de PNI, sensores de SpO₂ y una variedad de cables y latiguillos para satisfacer todas sus necesidades de monitorización.

Para obtener más información, visite: www.medical.philips.com/IntelliVueMP2

M8102A MP2

asimpleswitch.com



© 2008 Koninklijke Philips Electronics N.V.
Reservados todos los derechos.

Philips Medical Systems Nederland B.V. se reserva el derecho de realizar cambios en las especificaciones y/o de dejar de fabricar cualquier producto en cualquier momento sin previo aviso ni obligaciones y no se considera responsable de las consecuencias derivadas de la utilización de esta publicación.

SureTemp es una marca comercial registrada de Welch Allyn, Inc.

Philips Healthcare forma parte de
Royal Philips Electronics

www.philips.com/healthcare
healthcare@philips.com
fax: +31 40 27 64 887

Impreso en los Países Bajos
4522 962 25574/862 * FEB 2008

Philips Healthcare
Global Information Center
P.O. Box 1286
5602 BG Eindhoven
Países Bajos

E.2 IntelliVue MP70 bedside patient monitor

IntelliVue MP70 patient monitors are designed to match the pace and unique needs of adult, pediatric, and neonatal intensive care; anesthesia and peri-operative care; and cardiac care environments.

Built on Philips strong heritage in patient monitoring, IntelliVue MP70 has highly flexible screen configuration; an extensive clinical measurements menu; built-in clinical support tools such as Event Surveillance, conventional diagnostic 12-lead ECG, and multi-lead arrhythmia analysis; and many other powerful features.

	IntelliVue MP70
<i>Weight</i>	<10 kg [<22.05 lbs]
<i>Waveforms</i>	4, 6, 8 (13 ECG)
<i>Monitor screen display</i>	Integrated 38 cm (15") color XGA display with 1024 x 768 resolution
<i>Screen navigation</i>	Touchscreen SpeedPoint Remote SpeedPoint Mouse PS2-compatible user's choice
<i>Power consumption</i>	<145 W
<i>Applications for specific care settings</i>	Anesthesia Critical cardiac care Neonatal monitoring
<i>Multi-Measurement Server support</i>	Compatible
<i>Flexible Module Server support</i>	One supported Flexible Module Server (8 measurement slots)
<i>Internal measurement slots</i>	2
<i>Networking capability</i>	Standard Ethernet wired LAN and wireless LAN
<i>Portal technology</i>	Compatible

Table E.2: *MP70 bedside patient monitor specifications*

For further technical specification details, see the “Intellivue MP60/MP70 Patient Monitor Technical Data Sheet” [21]

Filename:

IntelliVue_MP70-brochure.pdf



Networked versatility

IntelliVue MP60 and MP70 patient monitors

PHILIPS
sense and simplicity

Critical performance

The IntelliVue family of networked patient monitors gives care teams throughout the hospital more of the information they need right at the patient's side. All share a common user interface and outstanding industrial design. Philips innovative portal technology is available on the portable MP40 and MP50, the versatile MP60, MP70, and MP80¹ for intermediate and critical care, and the MP90 for the highest acuity patients. The IntelliVue series also includes the compact, networked MP20 and MP30 for flexible care and patient transfer. Multi-Measurement Servers enable data continuity between monitors throughout the patient's stay.



High-performance monitoring for critical and intermediate care settings

IntelliVue MP60 and MP70 patient monitors are designed to match the pace and unique needs of adult, pediatric, and neonatal intensive care; anesthesia and peri-operative care; and cardiac care environments.

The monitors are easy to use, operate on a networked platform that can span the hospital enterprise, and can be configured to suit patient acuity, department protocols, or specific procedure requirements.

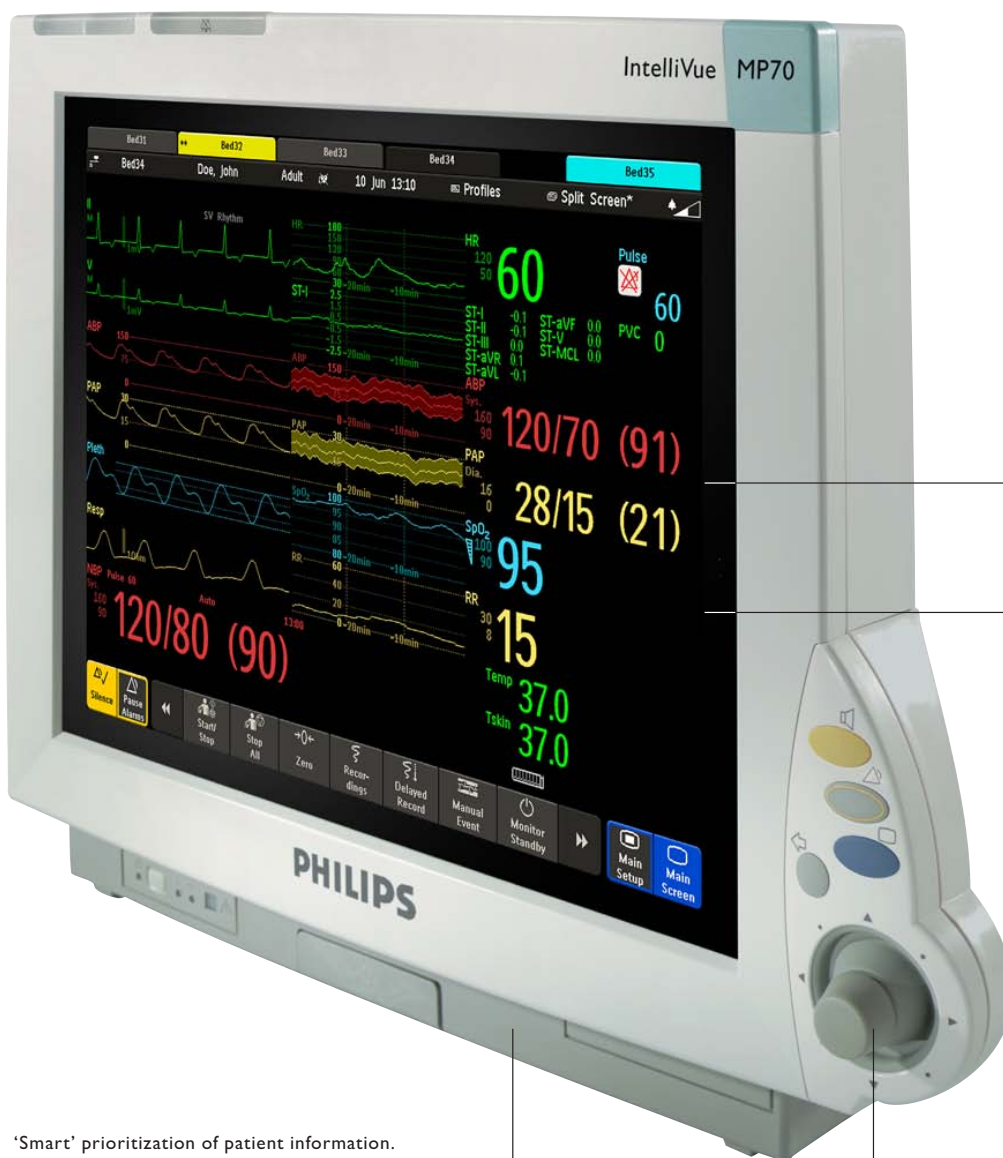
A clearer view

We've redesigned the user interface to improve visibility of patient data, make it easier to use, and to enhance compatibility with standard software. You can also locally print in a harmonized layout. Each NBP measurement now generates a column in the vital signs trend table. Measurements for other values are added to provide a comprehensive vital signs data set for the NBP measurement time, offering a more complete picture.

1. Not available in the US.

for critical needs

Comprehensive and connected



Customized viewing options

let you view and analyze data in graphical or numerical formats, juxtapose real-time measurements and trended data, and organize every onscreen element – from waveforms to data labels – as desired.

IntelliVue comes with **10 pre-set screen configurations.**

38cm (15") color XGA monitor display with 4, 6 or 8 waveforms is bright and easy to read.

Touchscreen operation makes many functions accessible through simple, one-touch commands. (Touchscreen is available on MP70 only.)

Dynamic Wave area features waves that automatically adjust in size depending on the number of waves configured.

'Smart' prioritization of patient information.

Portal technology uses Philips Tunneling Control Engine to prioritize physiologic measurements, monitoring information, and alarm notifications – regardless of the amount of network traffic. IntelliVue offers uninterrupted patient monitoring without the risk of system overload or additional network connections.

No separate hard drive and no fan. IntelliVue is space-saving, quiet, stable, and starts quickly.

SpeedPoint operation designed for easy information input and onscreen navigation (optional on MP70).

Best in class for you

Philips is committed to providing best-in-class standard measurements, such as oximetry with the Philips FAST SpO₂, Masimo® SET®, or Nellcor® OxiMax™ algorithms, and the Philips ST/AR algorithm to support clinicians' decisions at the patient's side. Our goal is to provide crucial measurement information in the forms that will best serve clinical need by:

- Maintaining and advancing the performance of existing, widely used standard-of-care measurements
- Investing heavily in research, development, and clinical validation of new, innovative parameters and algorithms
- Working with strategic partners to integrate next-generation measurements and technology
- Providing interfaces to more than 100 third-party specialty measurement devices – mechanical ventilators, gas analyzers, anesthesia machines – through the Philips VueLink and IntelliBridge modules.



Multi-Measurement Server

Multi-Measurement Server Extension

2. Continuous cardiac output and PiCCO technology not available in the US.

The Multi-Measurement Server includes a collection of the most consistently required parameters in a single unit, which saves valuable space.

- Lightweight and compact
- Stores up to 8 hours of data
- For patient transport and transfer, the Multi-Measurement Server detaches and inserts into any other Philips IntelliVue monitor or Philips M3 and M4 transport monitors
- Upon return to the patient's bed, reconnects to IntelliVue and uploads stored transfer data without recabling or reconfiguring
- Can remain with a patient throughout the hospital stay

Standard Multi-Measurement Server includes SpO₂, ECG and arrhythmia, non-invasive blood pressure, and an optional invasive blood pressure/temperature port.

Microstream CO₂ Extension also includes an optional invasive blood pressure/temperature port.

Capnography Extension with a choice of mainstream or sidestream CO₂ measurement is available in a variety of configurations and can include additional pressures, temperature, cardiac output, or continuous cardiac output using PiCCO® technology.²

Hemodynamic Extension includes cardiac output, continuous cardiac output using PiCCO technology,² invasive blood pressure, and temperature. An additional invasive blood pressure/temperature port is optional.

Individual clinical measurement modules expand Philips clinical measurement offering. Choose from a wide variety of measurement parameters that integrate within IntelliVue. Patient monitoring capabilities evolve as new measurements become available.

Modules fit conveniently into a Flexible Module Server. Most modules are interchangeable with Philips CMS 2002 monitors.



4 IntelliVue MP60 and MP70 patient monitors



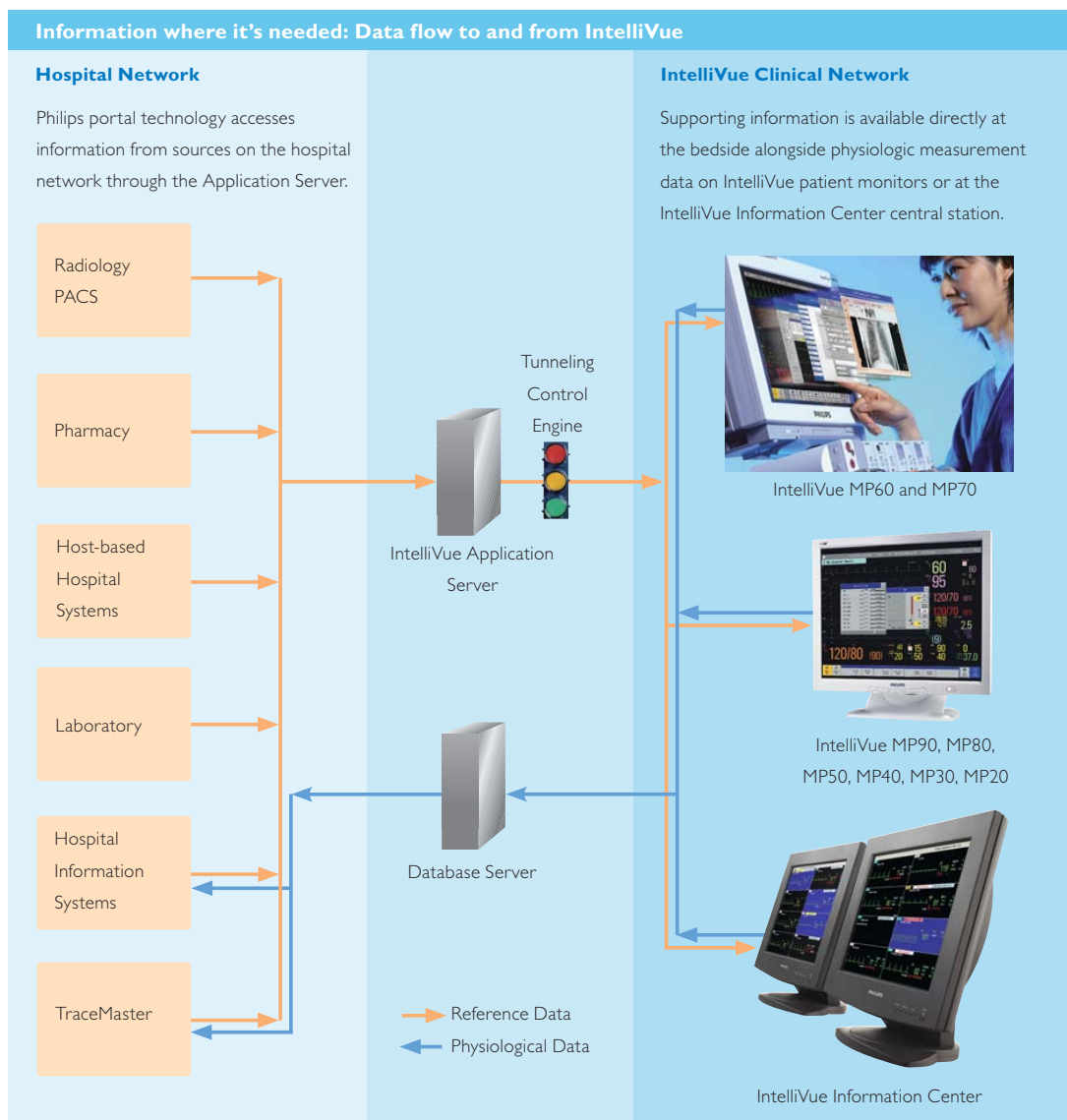
See more to do more



Capture, review, and store diagnostic 12-lead ECGs at the monitor before sending them to the IntelliVue Information Center. The Smart Alarm Delay algorithm helps reduce the number of pulse oximetry nuisance alarms, allowing you to focus your attention where needed.³ IntelliVue offers highly flexible screen configurations, an extensive clinical measurements menu, and built-in Clinical Decision Support tools.

3. Not available in the US.

Information where you



Seamless information flow within the clinical network

Offering outstanding information access and decision support, Philips innovative clinical network includes portal technology, which allows care teams to view real-time physiologic data on the same screen with clinical review applications, digital radiology images, archived data, lab results, medication guidelines, and hospital protocols, for example.

Information flows and converges where it's needed most, contributing to quicker therapeutic turnaround times, a more comprehensive set of information upon which to base clinical decisions, and efficient information sharing among multidisciplinary teams.

need it

Product specifications

	MP60	MP70
Portal technology	Compatible	Compatible
Waveforms	4, 6, 8 ⁴ (13 ECG)	4, 6, 8 (13 ECG)
Monitor screen display	One integrated 38cm (15") color XGA	One integrated 38cm (15") color XGA
Screen navigation	<ul style="list-style-type: none"> • SpeedPoint • Remote SpeedPoint • Mouse • PS/2-compatible user's choice 	<ul style="list-style-type: none"> • Touchscreen • SpeedPoint • Remote SpeedPoint • Mouse • PS/2-compatible user's choice
Multi-Measurement Server (MMS) and extensions	Compatible	Compatible
Flexible Module Server (8 measurement slots)	One supported Flexible Module Server	One supported Flexible Module Server
Two internal measurement slots	Optional	Optional
Networking capability	Optional	Optional

4. 8-wave option not available in the US.

Actionable information through Clinical Decision Support



Available through portal technology, On-line Electronic Help (OLEH) is a complete point of care reference system for the anesthesiologist in the operating room.



Advanced Event Surveillance correlates up to four parameters from the IntelliVue patient monitor.

**Philips Healthcare is part of
Royal Philips Electronics**

How to reach us

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

Asia

+49 7031 463 2254

Europe, Middle East, Africa

+49 7031 463 2254

Latin America

+55 11 2125 0744

North America

+1 425 487 7000

800 285 5585 (toll free, US only)

M8007A MP70
M8005A MP60
M3001A Multi-Measurement Server

Nellcor is a registered trademark and OxiMax is a trademark of Nellcor Puritan Bennett, Inc. Masimo and SET are registered trademarks of Masimo Corporation. Microstream is a registered trademark of Oridion Medical, Ltd.

Please visit www.philips.com/IntelliVueMP70



© 2010 Koninklijke Philips Electronics N.V.
All rights are reserved.

Philips Healthcare reserves the right to make changes in specifications and/or to discontinue any product at any time without notice or obligation and will not be liable for any consequences resulting from the use of this publication.

Printed in The Netherlands.
4522 962 63981 * AUG 2010

E.3 IntelliVue Information Center

The Philips IntelliVue Information Center combines the real-time monitoring surveillance of a central station with sophisticated clinical decision support tools and the ease of touchscreen operation.

Capture complete waveforms, trends, alarms, and numerics from wired and wireless networked Philips patient monitors and other telemetry systems.

- Clinical decision support tools, including real-time trend display and retrospective review applications
- Secure web access with multi-patient views
- Scalable to support 4 to 3840 patients with up to 96-hour Full Disclosure for review of physiologic data
- HL7 data export to the IntelliVue Clinical Information Portfolio and other clinical information systems
- Inbound ADT² interface
- Direct ECG export to cardiology management systems
- Integrated paging controls, including waveform paging
- Portal technology to access hospital applications such as PACS³ and LIS⁴
- Research data export

Because it uses familiar Microsoft Windows screens, menus, and navigation commands, working with the IntelliVue Information Center requires no special computer expertise. The convenient Help application provides contextual information and instructions from any screen.

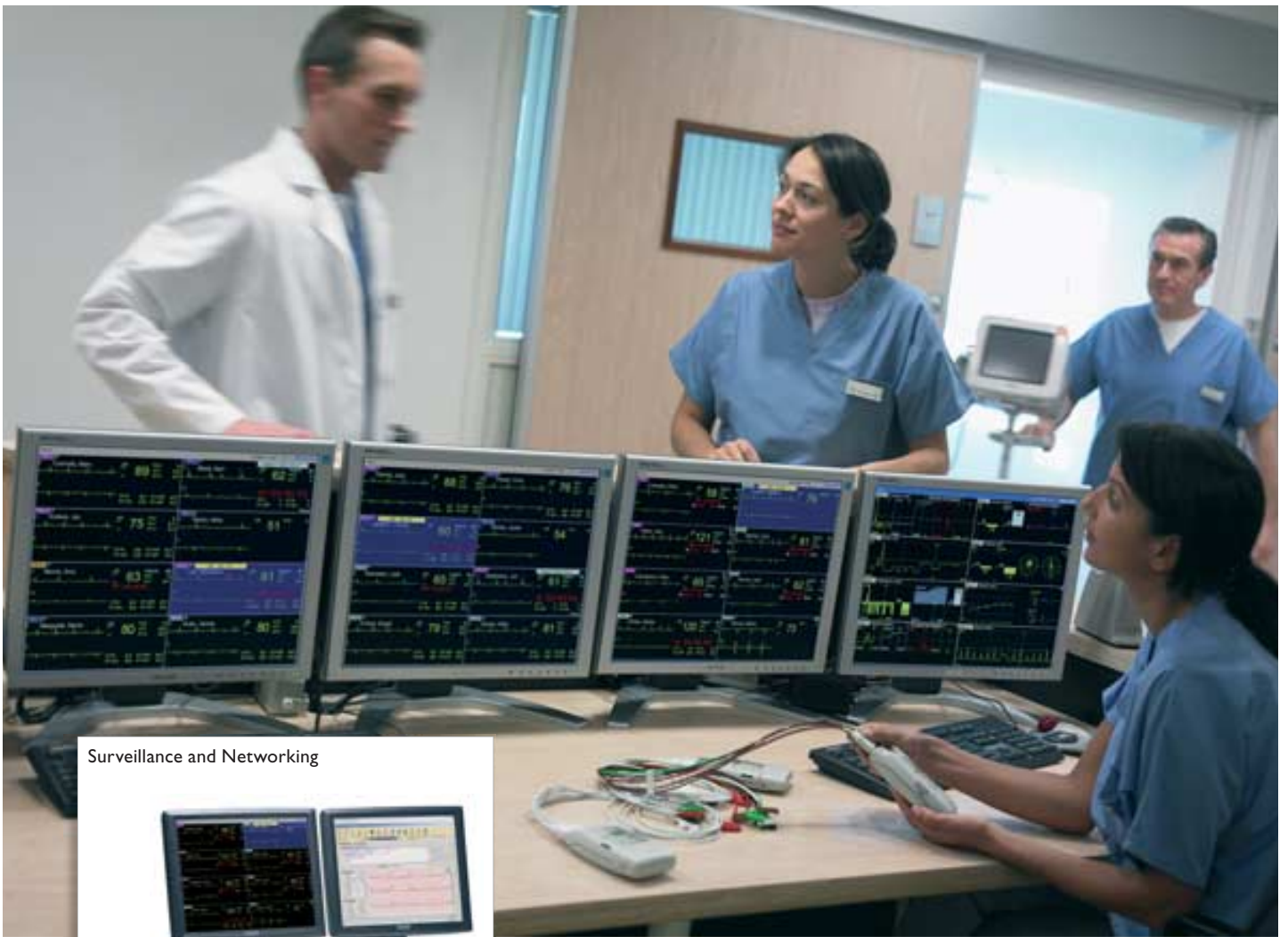
Filename:

IntelliVue_Information_Center_Brochure.pdf

²Admission Discharge Transfer: synchronized patients database, with admitted and discharged status, patient demographic data. It also allows tracking workload, recording the elements used in providing services, diagnosis, referring physician and costs data.

³Picture archiving and communication system for medical imaging.

⁴Laboratory Information Systems, for improved laboratory productivity, reduced occurrence of wrong diagnosis, as well as billing capabilities that directly update the electronic health record (EHR).



IntelliVue Information Center

Central surveillance and clinical decision support



Surveillance plus advanced

IntelliVue Information Center combines the real-time monitoring surveillance of a central station with sophisticated clinical decision support tools. The Information Center can capture complete waveforms, trends, alarms, and numerics from networked Philips patient monitors and telemetry systems, as well as the HeartStart MRx Monitor/Defibrillator.*

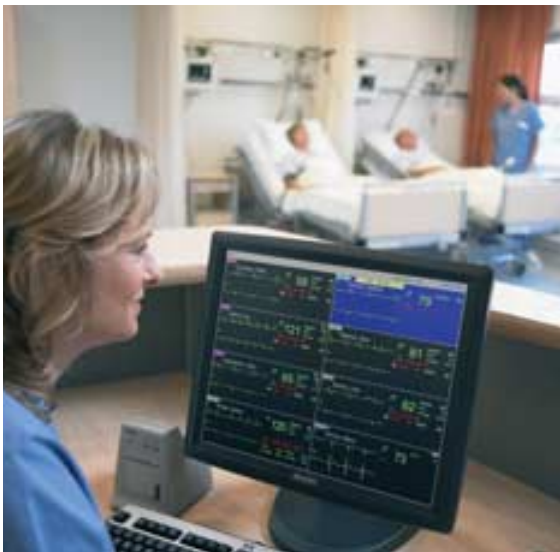
The Information Center is equipped with innovative Philips portal technology, which provides ready access to data from web-enabled applications on the hospital network. Monitoring data can be viewed together with digital radiology images, archived data, lab results, reports, protocols, and other information conveniently and logically on the display.

Intuitive user interface

No special computer expertise is needed to work with the Information Center since it uses familiar Microsoft Windows® screens, menus, and navigation commands. Our Help application provides contextual information and instructions from any screen.

Key features of the IntelliVue Information Center

- Continuous surveillance monitoring of wired, wireless, and telemetry beds
- Clinical decision support tools, including real-time trend display and retrospective review applications
- Secure web access with multi-patient views
- Scalable to support 4 to 1,920 patients with up to 96 hour Full Disclosure
- HL7 data export to the IntelliVue Clinical Information Portfolio and other clinical information systems
- Inbound ADT interface
- Direct ECG export to Philips Holter System, TraceMasterVue, and other cardiology management systems
- Integrated paging controls, including waveform paging
- Portal technology for access to web-enabled hospital applications, such as PACS and LIS
- Research data export



* Wireless HeartStart MRx networking available only with the IntelliVue 1.4 GHz wireless network. Wired MRx networking available only in the US.

clinical decision support

Main screen displays real-time waveforms and parameters for up to 16 patients.

Patented back-lighting makes it easy to recognize alarms by highlighting the entire patient sector. Blue, yellow, and red alarms indicate the level of urgency.

Volume indicator now on main screen.

ST/AR is a gold-standard algorithm from Philips that provides continuous multi-lead analysis of ST segments and arrhythmia detection with highly accurate, proven performance.

Pair **telemetry transceiver with a bedside monitor** to view all parameters in same window.

Battery gauge appears in patient sector for telemetry devices and transport monitors.

Touchscreen operation makes many functions directly accessible through simple commands.

Portal technology opens a window for access to hospital applications, such as PACS and LIS.

Trend display brings ST Map, horizon display, and other screen trends available on the bedside to the central station.

USB 2-channel recorder is designed to be environmentally friendly. A 4-channel serial recorder is also available.

Contextual online help for every screen and function, plus a quick start tutorial that covers all the basic functionality in approximately 15 minutes.

Device location helps staff track down missing telemetry transceivers.

ST Contour displays ST measurements in a very compact graphical format.

