Low Bandwidth Infra-Red Networks and Protocols for Mobile Communicating Devices

Andy Harter and Frazer Bennett
Olivetti Research Limited
24a Trumpington Street
Cambridge
CB2 1QA

Telephone: +223 343000

October, 1993

1 Introduction

1.1 Scope

This document is intended as a source of technical reference for the infra-red network developed at Olivetti Research, and in use within Olivetti, Digital, Xerox, Bellcore and elsewhere. The document is restricted in scope to the details of the physical communication medium and formatting of simple data packets over the medium. The ISO Reference Model for Open System Interconnection (the OSI model), is used as a descriptive framework, and within this model the document describes the Physical and Data Link Layers of the IR network. Elements of network architecture which would be described in terms of the Network Layer and above are beyond the scope of this document. Where possible, specific details of actual devices making use of the IR network are included in appendices.

1.2 Historical background

A simple low bandwidth unidirectional IR network was devised in 1989 by Roy Want at Olivetti Research as a component part of the Active Badge system. The Active Badge is personal device which periodically transmits an IR packet. The transmissions are detected by IR base sensors which are in fixed known locations and which relay the information to some central point over a wire network. In this way, the badge is dynamically located. The signaling rate of this system was around 1k baud.

The system was extensively reworked by Roy Want, Andy Harter and Tom Blackie in 1991. A key feature of the redesign was the inclusion of a full bidirectional capability,

with IR transceivers in both badges and base sensors. The signaling rate was increased by approximately one order of magnitude. It was apparent that physically the network was now a more general entity, which other types of cordless or mobile device might use. The protocols were explicitly extended to embrace this concept.

Other mobile devices have been built to use the network. At Xerox Parc, the Parc TAB is a sophisticated mobile personal device with LCD display and touch sensitive screen. At Olivetti Research, a small equipment badge is primarily intended as an asset tag, but has digital inputs to allow cordless and mobile telemetry. Also at Olivetti Research, IR interfaces are being added to portable notebook PC's such as the Olivetti Quaderno and the HP Palmtop.

1.3 Network requirements

The properties of the IR network are targeted on a particular class of object, namely mobile personal devices. These devices have several common characteristics. Most importantly, they are lightweight, small and tetherless. By implication, they have their own power source which might be rechargeable or disposable batteries, or solar cell. Another characteristic of the target devices is that they are simple, cheap and practical to build. This implies the use of simple transceiver circuitry which avoids any complex signal processing.

The power available for such devices to communicate over the IR network is a limiting factor in the achievable signaling rate. Devices need to communicate over a range of distances, and the inverse square law of propagation of electromagnetic radiation rapidly reduces the incident signal energy at the receiver from a distant source. Since receivers must be simple, the margin of the incident signal above ambient noise at the receiver must be easily detectable. By implication, energetic but low rate signaling is needed.

2 IR Network Model

2.1 Topology

The IR network is implicitly formed between mobile devices and fixed base sensors which communicate in the IR spectrum. A third essential component is some form of backbone network over which base sensors relay information to entities managing the IR network. The physical extent of the IR network is determined by the topology of the base sensors which is an important part of the network model.

The properties of IR light greatly influence the topology of base sensor positions. In particular, the property that light is reflected or absorbed by many materials rather than transmitted through them tends to define conveniently bounded and disjoint zones of IR signal. In order to equip a particular environment with an IR network, the space is modelled as a collection of light zones and each zone is spanned with a number of base sensors. The number and position of base sensors in a zone is determined by heuristics involving bidirectional range, zone shape and material composition.

Zoning is a useful property in a wireless network, since the same carrier can be reused in each zone. The spatial diversity which results yields a higher aggregate bandwidth in a collection of zones. In each zone, a modest bandwidth is likely to be sufficient, which corresponds well with the requirements of low power and simple transceiver design. The properties of a spatially indiscriminate carrier such as RF are less able to satisfy these requirements.

2.2 Mobiles

Mobiles must be able to transmit over the IR network, and are obliged to periodically broadcast their identity which should be a globally unique code. This enables a dynamic route to the device to be maintained. For some devices, for example a simple Active Badge, this may be the only information originating from the mobile. Other mobiles with input devices, for example notebooks or the Parc TAB, may originate data of many different forms.

Most mobiles will have receive capabilities, though some will not have permanently enabled receivers for power saving reasons. Such devices will typically have windows of reception surrounding transmission by the mobile. Mobiles which transmit frequently should have a receive capability to enable a collision avoidance scheme to be implemented. This scheme is a period of reception prior to transmission, during which the detection of a modulated signal will prevent the transmission.

Mobiles which transmit infrequently may not need to receive, but their transmission may collide with another transmission particularly in a zone operating near the bandwidth limit. The frequency of transmission can be based on a statistical treatment of assumptions about the density and type of traffic in a zone. This approach is in keeping with the nature of the inherently imperfect medium, and the impossibility of guaranteeing to prevent or detect collisions.

A simple technique to avoid synchronisation is to ensure variation in the periodicity of address broadcasts amongst mobiles of the same type. Furthermore, a particular mobile should have variation in its period. In this way, the number of broadcast collisions can be modelled statistically and will not be prone to locking or beating. In devices capable of attempting to avoid collisions, back-off strategy should be similarly constructed to avoid locking.

2.3 Bases

Bases must be able to transmit and receive over the IR network, and also over the backbone network. Bases require buffering of two types. First, bases require buffers to implement a store and forward capability for outgoing IR messages to mobiles which only have an intermittent receive capability. A transmission from such a mobile represents a rendezvous point when the base can transmit in the knowledge that the mobile is receiving. Bases should also have buffering or memory to provide flexibility in backbone network access method, and to cope with mismatches in communications characteristics between the IR

and backbone networks.

Many aspects of base sensor design are less critical than those for mobiles. Size is less important, and since bases are in fixed locations they are more likely to have an external source of power. However, one disadvantage of the zoning property is that base sensors will be numerous. This implies that base sensors should be cheap, which implies simple and inexpensive backbone network interfaces.

The backbone network might be a dedicated or standard network infrastructure, such as ethernet. The network could be wire based or even a wireless radio local area network. However, a simple, cheap interface probably implies the use of a dedicated wire network with simple protocols requiring the minimum of hardware and software support. Furthermore, it is particularly convenient for low-voltage power distribution to be run in parallel with the network, since the cost and logistics of individually supplying power to base sensors in potentially inaccessible positions must be considered.

3 IR Physical Layer

3.1 Carrier characteristics

The physical layer transmission medium is incoherent radiation in the near IR range with a wavelength of between 880 and 920 nm. Components transmitting and receiving at this wavelength are widely available. A carrier of this wavelength suffers negligible interference from stray sources of higher frequency electromagnetic radiation such as radio frequency emissions.

The necessary power levels of the carrier are determined by a number of factors. The required range between mobile and base is clearly important. The radiometric properties of the emitter and detector are also influential. The power level of the emitter should be such that the radiance of the IR source results in a detectable irradiance at the required range. This will depend on the radiant intensity of the transmitter and the photosensitivity and radiant sensitive area of the detector.

A typical IR photodiode has a photosensitivity such that an irradiance of around $1\mu\mathrm{W/cm}^2$ is detectable. At a distance of 25 metres, this would require a source of radiant intensity 1W/sr, which can be produced by a small number of typical IR emitters in combination. Detectors can also be used in combination to improve receiver sensitivity. This is useful in the detection of reflected signals which are attenuated.

The use of incoherent IR light for signaling is remarkably free from restriction. Equipment operating in the IR spectrum is not believed to be subject to licencing or approval by any regulatory agency. Current health and safety guidelines in a number of countries relate safe *average* levels of IR to those found in bright sunlight.

3.2 Carrier modulation

A baseband modulation scheme is used. Broadband schemes are possible, and are the subject of some interest for higher bandwidth applications. The techniques involved preclude the use of a broadband scheme for simple practical applications requiring low power, low bandwidth mobile communication using currently available optoelectronic technology.

A pulse position modulation scheme is used. In this scheme, a sequence of short pulses of carrier are transmitted. The relative timing between the pulses of carrier is used to code information. A binary pulse position modulation is used, where two different relative positions are used to code bit values '0' and '1'. Additional relative positions are used to code synchronisation information.

The carrier is modulated by a transmitter to form discrete sequences of pulses which denote a message. Messages are broadcast without synchronisation or reservation of the carrier, since the level of complexity required to synchronise all potential transmitters within a zone is unwarranted. Furthermore, since the carrier is inherently unreliable, synchronisation is in general not possible. Collision detection at the source is also not possible, because of the hidden terminal problem. The collision avoidance scheme mentioned above is a simple, pragmatic approach to making good use of the carrier.

3.3 Physical Layer Protocol

Table 1 describes the physical format of all messages transmitted over the IR network. The message format is further illustrated in Figure 1. The following notes expand the description.

message	:=	start-sync preamble packet-sync packet
start-sync	:=	125μs gap
preamble	:=	byte
	value	'0x7f'
packet-sync	:=	300μs gap
packet	:=	byte byte-sync byte ... byte-sync byte
byte	:=	bit[7] ... bit[0]
	coding	msb ... lsb
bit	:=	zero | one
byte-sync	:=	200μs gap
zero	:=	150μs gap
one	:=	100μs gap

Table 1: Physical Layer Protocol

Pulse width. In the physical layer protocol of the IR network, pulses of width 3μs are used in the modulation scheme. Pulses of this width are well within the response characteristics of typical emitters and detectors, and are comfortable for manipulation by hardware or software implementing the physical layer.

Figure 1: Physical Layer Protocol

4 IR Data Link Layer

4.1 A connectionless network

In the OSI model, the function of the data link layer can be split into two groups. The lower level Media Access Control (MAC) group takes the transmission system provided by the physical layer and superimposes a scheme for transmitting frames of user data, addressing, and control information. The higher level Logical Link Control (LLC) group adds flow and error control by implementing an end-to-end logical connection.

The data link layer of the IR network has an explicit mechanism for detecting errors and acknowledging the receipt of error-free packets. It does not however, include the necessary addressing information to establish logical end-to-end connections. Network architectures of this kind without the functions of an LLC layer are said to be connectionless.

Figure 2: Data Link Layer Protocol

A Olivetti Research Active Badge

A.1 Description

Active Badges are small mobile devices about 5cm square, weighing about 50g, with internal lithium batteries lasting a year or more. The device transmits and receives over the IR network, and is intended to be worn by personnel in an environment appropriately equipped with base sensors (see Appendix D). The primary function is to behave as a personnel locating tool and to provide an extremely simple ubiquitous means of interacting with the environment.

Each badge has a globally unique device address. Under normal circumstances, a badge periodically broadcasts an IR message containing its address. The period is around 10 seconds, with in-built variation as described earlier. The badge can be stimulated into transmitting at any time by depressing one of two pushbuttons, or by the presence of an external radio frequency field of around 290kHz and appropriate strength. Stimulating radio fields can be simply modulated and the badge is able to distinguish between a small number of patterns (see Appendix C). The cause of the stimulating event is coded in the broadcast message. All external stimuli reset the 10 second interval.

The badge has a receive capability, which for power saving reasons consists of a window of receive opportunity after each address broadcast. Badges receive messages which have been stored and forwarded from a sensor or sensors in the appropriate zone. The window is approximately 1ms wide. Received messages contain commands addressed to the badge, which are decoded and executed. The badge replies to all commands received.

The badge has a small amount of internal state, and there are commands to set and read the state. The badge also has three simple output devices which are a pair of visible LEDs and a piezo-ceramic speaker, and there are commands to light the LEDs and to sound the speaker. Each badge has a private 128 bit key and an encryption algorithm. An authentication command presents a sequence of random bytes which are encrypted by the badge and returned in the reply.

Figure 3: Active Badge Data Link Layer Protocol block

A.3 Data from Active Badge (sssd='1000')

The address broadcast message is the only unsolicited data from the Active Badge. The message consists of the badge address, and event specific data payload. The badge specific codes 'cccc' in the type byte are interpreted as event codes. Table 4 describes the list of possible badge events.

event	cccc	data
periodic broadcast	0000	sequence
side button	0010	sequence
middle button	0001	sequence
badge in field	0100	sequence field
side button in field	0110	sequence field
middle button in field	0101	sequence field
badge in unrecognised field	1000	sequence
side button in unrecognised field	1010	sequence
middle button in unrecognised field	1001	sequence
	where	
sequence	:=	byte
	coding	unsigned integer
field	:=	[byte [byte]]
	coding	see Appendix C

Table 4: Data from Active Badge

Sequence. The sequence number is incremented by 1 for each address broadcast message. 0xff wraps round to 0x01, with value 0x00 reserved. The sequence number provides a simple mechanism for a system to filter duplicate messages propagated by the reception of the same broadcast at more than one base.

Field. A variable length code representing the modulation pattern of the stimulating field. The encoding scheme is described in Appendix C.

A.4 Data to Active Badge (sssd='0000')

For messages from a base to an Active Badge the format of the data portion depends on the value of the badge specific code 'cccc' which is interpreted as a command for the badge to execute. Table 5 describes the list of Active Badge commands.

command	cccc	data	
challenge	0000	random	identifier
sound	0010	tones	identifier
set-state	0011	state	identifier
get-state	0100		
set-home	0001	home	identifier
get-home	0111		
	where		
identifier	:=	[byte]	
	coding	unsigned integer	
random	:=	length byte[0] ... byte[length-1]	
tones	:=	length tone[0] ... tone[length-1]	
tone	:=	byte	
	coding	'dddpppp'	
ddd	:=	bit[7] ... bit[5]	
	value	duration	
ppppp	:=	bit[4] ... bit[0]	
	value	pitch	
state	:=	status tones	
status	:=	byte	
	coding	'xxxxxxrg'	
r	:=	bit[1]	
	value	red LED off ('0') or on ('1')	
g	:=	bit[0]	
	value	green LED off ('0') or on ('1')	
home	:=	length protocol byte[0] ... byte[length-2]	
protocol	:=	byte	
	value	'0x00' (ip address)	
length	:=	byte	
	coding	unsigned integer	

Table 5: Data to Active Badge

Identifier. If included, the command identifier byte allows the badge to execute commands idempotently. A system can arrange for successive commands to contain different identifiers. On receipt, the badge compares the identifier with that of the last command executed. If the identifier is different, the command is executed and the identifier is stored in the badge, otherwise the command is ignored.

Challenge. The system generated random sequence of at most 5 bytes is encrypted by the badge using an algorithm and a private 128 bit key set at manufacture. The encrypted bytes form the data payload of the reply. In this symmetric authentication scheme, both the algorithm and the key are shared secrets with the system, which can therefore verify the identity of the badge.

Sound. A sequence of at most 5 tone bytes are interpreted and sounded on the speaker by the badge. The pitch is coded as a number of semitones from '00001' (low) to '11111' (high). Pitch '00000' is silent, and can be used as a rest. The duration is coded as a number of beats as show in Table 6. where each beat lasts approximately 1/16th of a second

ddd	beats
000	48
001	24
010	12
011	6
100	4
101	3
110	2
111	1

Table 6: Tone duration codes

Set state. The status byte of the badge is set. The status of the visible LEDs will be displayed for the duration of the accompanying sequence of tones which is of maximum length 4. The status of the visible LEDs will be redisplayed for the duration of each subsequent button press. The sequence of tones is not stored and cannot be replayed.

Get state. The value of the status byte is retrieved from the badge.

Set home. Up to five bytes of additional state information is stored in the badge. It is intended that this state is used to contain the address of an agent responsible for the badge at the home organisation of the badge. The first byte is an address protocol character. Value '0x00' denotes an ip address.

Get home. The home address state bytes are retrieved from the badge. This can be used to enable a system to interrogate an unknown badge and contact the agent of the badge to negotiate the exchange of information.

A.5 Replies from Active Badge (sssd='0100')

For reply messages from an Active Badge the format of the data portion depends on the value of the badge specific code 'cccc' which is interpreted as the code of the command which has been executed. Table 7 describes the list of Active Badge command replies.

command	bbbb	data	
challenge	'0000'	response	identifier
sound	'0010'	tones	identifier
set-state	'0011'	set-status	identifier
get-state	'0100'	get-status	
set-home	'0001'	home	identifier
get-home	'0111'	home	
	where		
identifier	:=	[byte]	
	coding	unsigned integer	
response	:=	length byte[0] ... byte[length-1]	
tones	:=	length tone[0] ... tone[length-1]	
tone	:=	byte	
	coding	'dddpppp'	
ddd	:=	bit[7] ... bit[5]	
	value	duration	
ppppp	:=	bit[4] ... bit[0]	
	value	pitch	
set-status	:=	status tones	
status	:=	byte	
get-status	:=	version status	
version	:=	byte	
home	:=	length protocol byte[0] ... byte[length-2]	
protocol	:=	byte	
	value	'0x00' (ip address)	
length	:=	byte	
	coding	unsigned integer	

Table 7: Reply Data from Active Badge

Version. A version number of the Active Badge. The byte is coded as two 4 bit unsigned integers. The most significant 4 bits represent a major version number, and the least significant 4 bits represent a minor revision number.

B Olivetti Research Equipment Badge

B.1 Description

The equipment badge is derived from the Active Badge designed to be attached to pieces of office equipment. The equipment badge is smaller than the Active Badge, about 3cm x 5cm and weighing 25g. The device uses the IR physical layer protocol and periodically transmits a globally unique address.

The interval between transmissions is about six minutes, increasing the battery life of the equipment badge over the Active Badge. The equipment badge may be stimulated into immediate transmission by an external radio field, or by pressing a single pushbutton. The equipment badge is able to decode and report modulated radio fields in the same way as the Active Badge. The equipment badge has no IR receive capability, which helps to improve the battery life.

The equipment badge also monitors two digital inputs which can be connected externally via a small socket. The value of the inputs is reported in each equipment badge transmission.

B.2 Data Link Layer Protocol block

The equipment badge data link layer protocol block is identical to Active Badge data link layer protocol described in Table 3.

B.3 Data from equipment badge (sssdcccc='1001001')

The address broadcast message is the only message from the equipment badge. The message consists of the badge address and the event specific payload, and is described in Table 8.

data	:=	field status
field	:=	[byte [byte]]
	coding	see Appendix C
status	:=	byte
	coding	'000efpqb'
e	:=	bit[4]
		'unrecognized field' bit
f	:=	bit[3]
		'device in field' bit
pq	:=	bit[2] bit[1]
		'input port status' bits
b	:=	bit[0]
		'button press' bit

Table 8: Data from equipment badge

Field. A variable length code representing the modulation pattern of the stimulating field. The encoding scheme is described in Appendix C.

C Proximity Fields

A low-power radio field with a frequency of 290kHz is generated at a fixed location within an IR zone. This field is then pulse-width modulated with a fixed mark/space ratio. The size of the field generator's aerial and the field strength are chosen to give the field an envelope which typically surrounds an office desk. A tuned circuit in the Active Badge and equipment badge is able to detect this field, and the on-board processor will attempt to determine the mark/space ratio of the field that it finds itself in. Once interpreted, the identity of the field is encoded in the periodic address broadcast.

C.1 Olivetti Research Field Generator

The field generator is a stand-alone unit, requiring an external 12v supply. An external aerial is connected, which typically consists of 12m of wire coiled into a 4 turns of a 3m loop. The field strength is adjustable with an internal potentiometer. The modulation pattern is determined by the configuration of an internal 28 pin header as defined in Table 9.

pin to be grounded	modulation pattern
2-24-25-26-27	constant field
2	1ms/1ms
2-6-27	2ms/2ms
2-5-26	3ms/3ms
2-5-6-26-27	4ms/4ms
2-4-25	5ms/5ms
2-4-6-25-27	6ms/6ms
2-4-5-25-26	7ms/7ms
2-4-5-6-25-26-27	8ms/8ms
2-3-24	9ms/9ms
2-3-6-24-27	10ms/10ms
2-3-5-24-26	11ms/11ms
2-3-5-6-24-26-27	12ms/12ms
2-3-4-24-25	13ms/13ms
2-3-4-6-24-25-27	14ms/14ms
2-3-4-5-24-25-26	15ms/15ms
2-3-4-5-6-24-25-26-27	16ms/16ms

Table 9: Header configuration for modulation patterns;

C.2 Radio Field Sampling

The Active Badge and equipment badge sample the radio field by monitoring a digital input which indicates whether the radio field is detected or not. The badge samples the input continuously for a period, building an internal representation of the field modulation pattern. The badge will sample for 32ms, or until two mark/space pairs or a field error is detected, whichever is the sooner. A field error is deemed to have occurred if a pulse

shorter than 0.5ms is detected. The internal representation of the modulation pattern is then coded into an IR address broadcast message as described below.

C.3 Radio Field Encoding

The Active Badge and equipment badge will transmit zero, one or two bytes of field code in the payload of the IR address broadcast message. If the field is constant and unmodulated, or a field error was detected, no extra bytes are sent and bit[2] or bit[3] of the badge specific code in the message type byte are set (see Table 4). Otherwise, the mark/space pattern is coded in 2 or 4 nibbles as described in Table 10.

field	:=	byte [byte]
byte	:=	nibble nibble
nibble	coding	'pvvv'
p	:=	bit[3]
	value	'0' (space)
	value	'1' (mark)
vvv	:=	bit[2] ... bit[0]
	value	'000' (1ms)
		'001' (2ms)
		⋮
		'110' (7ms)
		'111' (8ms)

Table 10: Mark/space coding in nibbles

The most significant bit of each nibble distinguishes between mark and space codes. The bottom three bits of each nibble indicate the number of milliseconds, to the nearest millisecond, for which the mark / space was observed. For pulses longer than 8ms, the following nibble continues the count of the pulse length. If the second byte is identical the first byte, then only one byte is encoded in the message.

D Olivetti Research Base Sensor

D.1 Description

The base sensor is a topologically fixed device which receives and transmits over the IR network. The base sensor is also equipped with a backbone network interface, and performs a bridging function between the two networks. Sensors are identified and addressed by a single byte set at manufacture. A red LED on the sensor indicates a message being received over the IR network, and a green LED on the sensor indicates a message being received over the backbone network. Two FIFO memories buffer messages being bridged between networks. The sensor has a single 16 byte buffer for use in store and forward IR communications to intermittently receiving devices, for example the Active Badge. The sensor can also transmit directly over the IR network to devices which are permanently receiving.

The backbone network is constructed using a simple four conductor cable such as twisted pair telephone cable. Two of the conductors are used to supply power to the base sensors, and the remaining two are signal conductors. The topology of the backbone network is an arbitrary rooted acyclic tree where the root or hub is the power source. In practice, the physical extent and topology of the network are constrained by the need to supply power to sensors. Amongst the factors to consider are the voltage and current supply of the source and the power requirements of the sensors. Sensors typically consume 50mA, and require a supply of between 9V and 12V. The resistivity and length of a wire run and the load at the end of the run are important considerations. The optimal topology of the backbone network for a given arrangement of sensors is a star configuration with the hub at a point which minimises the total length of wire. Simple applications of Ohms law are useful in determining whether a topology is practical.

Logically, the signal conductors carry RS232 style signals, and the base sensors are configured to operate at 9600 baud, 8 data bits, no parity, 2 stop bits. Physically, however, the representations of the logic levels are shifted to form a wired-or network. A simple level-shifter at the network hub is used to convert to true RS232 levels. A variant of the base sensor has a true RS232 level interface, and can be used where a single base sensor is required. A dedicated power supply is required for this device.

The RS232 level signal is connected to the serial interface of a network control host. The host can be a standard workstation with the network control function as a background task, or a dedicated system. For applications where access to the IR network is part of a generally available communications infrastructure, the host will have additional networking and further bridging functionality.

D.2 Backbone network host to sensor protocol

The host to sensor protocol is described in Table 11.

message	:=	preamble address [packet]
preamble	:=	byte
	value	'0xff'
address	:=	byte
	value	'0x00' to '0xfe'
packet	:=	type length block
type	:=	byte
	coding	'sssccccc'
sss	:=	bit[7] ... bit[5]
	value	'000' (data for immediate ir transmission)
	value	'110' (data for buffered ir transmission)
	value	'111' (data to base sensor)
ccccc	:=	bit[4] ... bit[0]
	value	base sensor specific code (sss='111')
	value	mobile device specific code (otherwise)
length	:=	byte
	coding	unsigned integer
block	:=	byte[0] ... byte[length - 1]

Table 11: Backbone network host to sensor protocol

Message. There are three types of message. First, a control message can be issued to a sensor. Second, a message for relay over the IR network can be transmitted. Third, a message can be issued to effect a poll of a sensor which results in received buffered IR packets being relayed back to the host. Sensors do not transmit unsolicited data, and every byte received over the IR and buffered in the sensor, or reply to a control message, must be extracted by explicit polling.

Preamble. The preamble is an escape sequence to delimit address bytes. All instances of byte values '0xff' in the packet are transmitted twice over the backbone network.

Address. In the protocol between the host network controller and base sensors, all messages from the host contain the explicit address of a sensor. There are 255 possible sensor addresses in the range '0x00' to '0xfe' inclusive, which determines the maximum logical size of any one backbone network.

Packet. The optional packet is one of three types. Type codes sss='000' and sss='110' indicate messages directed at mobiles intended for relay over the IR network. Type code sss='111' indicates a control message for the sensor.

Block. The format of the block is dependent on the type of the message. For messages intended for mobiles, the format is as described in the generic data link layer protocol, Table 2. In particular, for messages intended for Active Badges the format of the block is as described in Tables 3 and 5. Messages intended for the sensor itself are described below.

D.3 Control commands from host to sensor

For backbone network host to sensor control messages, the format of the block is as described in Table 12.

command	ccccc	block
reset-buffer	00000	null
reset-fifos	00001	null
get-state	00010	null
output-on	00011	null
output-off	00100	null
persistence-on	00101	null
persistence-off	00110	null
	where	
null	:=	byte
	value	'0x00'

Table 12: Control commands to sensor

Reset buffer. Cause any data in the 16 byte store and forward buffer to be discarded.

Reset fifo's. Cause any data in the FIFO's bridging the IR and backbone networks to be discarded. Useful at sensor initialisation.

Get state. Retrieve internal sensor status.

Output on. The base sensor has a single digital output, which is turned on by this command. Typically, the digital output is connected to a circuit generating the radio frequency field which can stimulate the Active Badge.

Output off. Turn the digital output off.

Persistence on. Do not automatically flush the 16 byte store and forward buffer when the buffered message has been transmitted. In this mode, the message is eligible for repeated transmission.

Persistence off. Automatically flush the 16 byte store and forward buffer when the buffered message has been transmitted.

Figure 4: Backbone network protocol interleaving

Packet. The packet is one of three types. Type codes sss='100' and sss='010' indicate messages received from mobiles being relayed over the backbone network. Type code sss='011' indicates a reply to a sensor control message.

Block. The format of the block is dependent on message type. For messages received from mobiles, the format is as described in the generic data link layer protocol, Table 2. In particular, for messages received from Active Badges the format of the block is as described in Tables 3, 4 and 7. Messages generated by the sensor are described below.

D.5 Control replies from sensor to host

For backbone network sensor to host control replies, the format of the block is as described in Table 14.

command	ccccc	block
get-state	00010	status
	where	
status	:=	length version status[0] status[1]
length	:=	byte
	coding	unsigned integer
	value	'0x03'
version	:=	byte
status[0]	:=	byte
status[1]	:=	byte

Table 14: Control replies from sensor

Version. A version number of the base sensor. The byte is coded as two 4 bit unsigned integers. The most significant 4 bits represent a major version number, and the least significant 4 bits represent a minor revision number.