WELSANDER DE SOUZA PEREIRA

UM MODELO DE INTEGRAÇÃO ENTRE REDES BLUETOOTH E A PILHA DE PROTOCOLOS TCP/IP

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Orientador/Prof. Emerson Rodrigo Alves Tavares

BARBACENA

2003

WELSANDER DE SOUZA PEREIRA

UM MODELO DE INTEGRAÇÃO ENTRE REDES BLUETOOTH E A PILHA DE PROTOCOLOS TCP/IP

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Barbacena – MG, 27 de novembro de 2003.

_____

Prof. Emerson Rodrigo Alves Tavares - Orientador do Trabalho

_____

Prof. Marcelo de Miranda Coelho - Membro da Banca Examinadora

_____

Prof. Eduardo Macedo Bhering - Membro da Banca Examinadora

AGRADECIMENTOS

Agradeço a Deus Pai Criador pela força que me foi dispensada durante todo tempo. Aos meus familiares por serem o alicerce da minha vida. Aos mestres que colaboraram para o meu aprendizado neste período e principalmente ao meu Orientador. E aos meus colegas. A todos muito obrigado.

RESUMO

O presente trabalho propõe a utilização da pilha de protocolos de internet TCP/IP (Protocolo de Controle de Transporte / Protocolo de Internet) integrados com a tecnologia de Rede Bluetooth. Tem-se como finalidade descrever e analisar a integração das tecnologias acima citadas, fazendo com que se integrem e facilitem suas utilizações para que possam fornecer aos seus usuários uma maior e melhor proposta de disponibilização de serviços utilizando a rede convencional. Será verificado também que esta integração se dará de dois modos diferentes: o primeiro através dos protocolos TCP/IP, passando pelo PPP e o RFCOMM até chegar ao L2CAP e o segundo através dos protocolos TCP/IP diretamente com o L2CAP.

Palavras-chave: Bluetooth, TCP, IP, PPP, L2CAP

SUMÁRIO

FIGURAS.....7
TABELAS.....9
SIGLAS.....10
1 INTRODUÇÃO.....13
2 PROTOCOLOS TCP/IP.....15
3 TECNOLOGIA DE REDE BLUETOOTH.....30
4 INTEGRAÇÃO BLUETOOTH E TCP/IP.....55
5 CONCLUSÃO.....67
REFERÊNCIAS BIBLIOGRÁFICAS.....68

FIGURAS

FIGURA 1 - DIVISÃO EM CAMADAS DA ARQUITETURA TCP/IP [4].....16
FIGURA 2 - CONEXÃO DO TCP [4].....20
FIGURA 3 - FASES DE UMA CONEXÃO TCP [4].....20
FIGURA 4 - ESTABELECIMENTO DE CONEXÃO POR MENSAGENS [4].....21
FIGURA 5 - PACOTE TCP [4].....21
FIGURA 6 - DIVISÃO DAS CLASSES DO ENDEREÇO IP [6].....26
FIGURA 7 - MÁQUINAS SITUADAS NA MESMA REDE [6].....27
FIGURA 8 - MÁQUINAS SITUADAS EM REDES DISTINTAS [6].....27
FIGURA 9 - FORMATO DO PACOTE IP [6].....28
FIGURA 10 - EXEMPLO DE PICONET [8].....32
FIGURA 11 - EXEMPLO DE SCATTERNET [8].....32
FIGURA 12 - COMO UM TRANSMISSOR DE RÁDIO FUNCIONA [7].....34
FIGURA 13 - SEQÜÊNCIA DE COMANDOS DE RECONHECIMENTO [7].....37
FIGURA 14 - A ARQUITETURA DE UM DISPOSITIVO BLUETOOTH [7].....39
FIGURA 15 - AS OPERAÇÕES DO RÁDIO BLUETOOTH [7].....40
FIGURA 16 - AS FUNÇÕES DO RADIO MODEM IC BLUETOOTH [8].....42
FIGURA 17 - MICROCHIP PADRÃO BLUETOOTH [9].....43
FIGURA 18 - O GERENCIAMENTO E CONTROLE DO LINK BLUETOOTH[9].....44
FIGURA 19 - A PILHA DE COMPLETA DE PROTOCOLOS BLUETOOTH [7].....47
FIGURA 20 - FORMATO DE UM CABEÇALHO DE PACOTE BLUETOOTH [9].....52
FIGURA 21 - PILHA DE PROTOCOLOS DO PERFIL LAN ACCESS [10].....57
FIGURA 22 - BLUEWINTM [10].....58
FIGURA 23 - CONEXÃO BLUETOOTH COM DOIS NODOS.....59
FIGURA 24 - INTEGRAÇÃO DIRETA TCP/IP E BLUETOOTH (L2CAP) [11].....60
FIGURA 25 - TRANSMISSÃO DE DADOS ENTRE CAMADA DE APLICAÇÃO E TCP [11].....61
FIGURA 26 - TRANSMISSÃO DE DADOS ENTRE TCP, IP E L2CAP [11].....62
FIGURA 27 - TRANSMISSÃO DE DADOS DO L2CAP PARA BASEBAND E VICE-VERSA [11].....62

FIGURA 28 - TRANSMISSÃO DE DADOS ENTRE L2CAP, IP E TCP [11].....63
FIGURA 29 - TRANSMISSÃO DE DADOS ENTRE TCP E A CAMADA DE APLICAÇÃO [11].....63
FIGURA 30 - ESQUEMA GERAL DA INTEGRAÇÃO DIRETA [11].....64
FIGURA 31 - PACOTE NAS CAMADAS BLUETOOTH [11].....64
FIGURA 32 - PACOTE TOTAL [11].....65

TABELAS

TABELA 1 - BANDAS DE FREQÜÊNCIA DE RÁDIO POPULAR [7].....34
TABELA 2 - POTÊNCIA DE SAÍDA PARA CADA CLASSE DE POTÊNCIA BLUETOOTH [7].....41
TABELA 3 - AS CAMADAS DA PILHA DE PROTOCOLOS BLUETOOTH [7].....46
TABELA 4 - MODELO DE PARÂMETROS [11].....65

SIGLAS

ACL – Link Assíncrono Sem-Conexão

AT_COMMANDS - Protocolo de Comandos de Áudio e Telefonia

DAC - Código de Acesso de Dispositivo

DNS - Serviço de Domínio de Nome

FTP - Protocolo de Transferência de Arquivos

GFSK - Troca de Frequência de Teclado de Gaussain

HC - Controlador de Host

HCI - Controlador de Interface de Host

HDI - Dispositivo de Interface do Usuário

HTTP - Protocolo Usado para Buscar Páginas na WEB

IEEE - Instituto de Engenharia Eletrônica e Elétrica

IETF - Força Tarefa de Engenharia da Internet

IP - Protocolo de Internet

IrDA - Associação de Dados Infra-vermelho

IrMC - Protocolo de Comunicações Móveis de Infra-vermelho

ISM - Industrial, Científico e Médio

L2CAP - Protocolo de Controle de Link Lógico e Adoção

LAN - Rede Local

LC - Controlador de Link

LM - Gerenciador de Link

LMP - Protocolo de Gerenciamento de Link

MAC - Camada de Controle de Acesso Médio

MSS - Tamanho Máximo de Segmento

MTU - Unidade de Transferência Máxima

NTTP - Protocolo para Mover Novos Artigos

OBEX - Protocolo de Troca de Objetos

PAN - Rede Pessoal

PDA - Assistente Pessoal Digital

PDU - Protocolo de Unidade de Dados

PPP - Protocolo Ponto a Ponto

RFCOMM - Protocolo de Comunicações de Rádio Freqüência

SCO - Conexão Orientada Síncrona

SDP - Protocolo de Descoberta de Serviço

SIG - Grupo de Interesse Especial

SMTP - Protocolo de Correio Eletrônico

TCP - Protocolo de Controle de Transporte

TCS_ BIN - Protocolo de Especificação de Controle de Telefonia - Binário

TDD - Divisão de Tempo em Duas Direções

UDP - Protocolo de Datagramas do Usuário

WAE - Protocolo de Ambiente de Aplicações sem Fio

WAP - Protocolo de Aplicação sem Fio

1 INTRODUÇÃO

As redes sem fio possuem vários formatos. Um exemplo desse tipo de rede é a tecnologia Bluetooth, usada para acesso sem fio em serviços de curtas distâncias. Este trabalho propõe verificar a possibilidade de integração entre Bluetooth e TCP/IP oferecendo aos usuários o melhor serviço de cada tecnologia.

Na tecnologia TCP/IP novos protocolos foram estruturados e novas técnicas foram desenvolvidas para adaptar protocolos existentes a novas tecnologias de rede [1], daí podermos fazer com que a tecnologia de rede Bluetooth utilize os protocolos TCP/IP para realizar trabalhos ou serviços da Rede Convencional.

O conjunto de protocolos TCP/IP foi projetado especialmente para ser o protocolo utilizado na Internet. Sua característica principal é o suporte direto a comunicação entre redes de diversos tipos. A arquitetura TCP/IP é independente da infra-estrutura de rede física ou lógica empregada. De fato, qualquer tecnologia de rede pode ser empregada como meio de transporte dos protocolos TCP/IP. Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa [2].

Bluetooth é uma tecnologia que promete eliminar os cabos que conectam equipamentos eletrônicos e de computação, e também criar uma gama de aplicações novas para troca de informações. Baseado num chipset conhecido pelo mesmo nome, Bluetooth, possui dispositivos que podem conectar-se ao mesmo tempo, e a esta conexão (rede) denominamos ***piconet*** (picorrede). Possui um máximo de largura de banda de 1 Mbit/seg.

Serão utilizadas juntamente as tecnologias Bluetooth e TCP/IP através de sua integração através de protocolos, utilizando dois perfis sendo que um terá os protocolos PPP e o RFCOMM como ponte para integração entre o Bluetooth e o TCP/IP e o segundo basicamente entre os protocolos TCP e IP da tecnologia TCP/IP e L2CAP do Bluetooth.

O primeiro perfil será utilizado neste trabalho devido ser ele atualmente o perfil utilizado nos dispositivos Bluetooth e o segundo será utilizado como modelo proposto para ser a integração dessas tecnologias em novas versões do Bluetooth. E também por serem os únicos perfis dessa integração existentes atualmente, sendo que o segundo ainda não está totalmente estabelecido.

2 PROTOCOLOS TCP/IP

O TCP/IP é uma arquitetura flexível, capaz de adaptar a aplicações com necessidades divergentes, como por exemplo a transferência de arquivos e a transmissão de dados de voz em tempo real [3].

Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos então existentes, o que forçou a criação de uma nova arquitetura de referência chamada de Modelo de Referência TCP/IP [3].

A Internet é uma rede pública de comunicação de dados, com controle descentralizado e que utiliza o conjunto de protocolos TCP/IP como base para a estrutura de comunicação e seus serviços de rede. Isto se deve ao fato de que a arquitetura TCP/IP fornece não somente os protocolos que habilitam a comunicação de dados entre redes, mas também define uma série de aplicações que contribuem para a eficiência e sucesso da arquitetura [3].

O conjunto de protocolos TCP/IP foi projetado especialmente para ser o protocolo utilizado na Internet. Sua característica principal é o suporte direto a comunicação entre redes de diversos tipos. Neste caso, a arquitetura TCP/IP é independente da infra-estrutura de rede física ou lógica empregada. De fato, qualquer tecnologia de rede pode ser empregada como meio de transporte dos protocolos TCP/IP, como será visto [4].

A arquitetura TCP/IP, realiza a divisão de funções do sistema de comunicação em estruturas de camadas. A Figura 1 mostra como é a disposição das camadas do TCP/IP:

Aplicação, Transporte, Inter-Rede e Rede

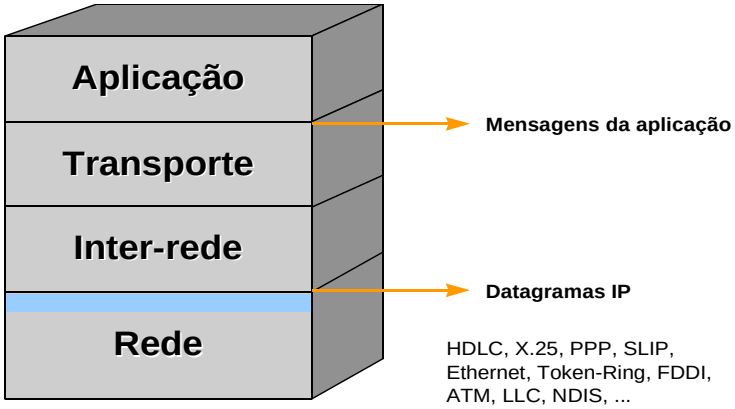


Figura 1 - Divisão em camadas da arquitetura TCP/IP [4]

As camadas da Pilha de Protocolos TCP/IP se dividem em:

1) Aplicação: A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário. Pode-se separar os protocolos de aplicação em protocolos de serviços básicos ou protocolos de serviços para o usuário [4]. Ela contém os protocolos de alto nível. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). [3]

Outros protocolos foram desenvolvidos com o passar dos anos, como o Serviço de Nome de Domínio (DNS, Domain Name Service), que mapeia os nomes de host para seus respectivos endereços de rede, o NTTP é o protocolo usado para mover novos artigos e o HTTP que é o protocolo usado para buscar páginas na WWW (World Wide Web) [3].

2) Transporte: Sua finalidade é permitir que as entidades pares (peer entity) dos hosts de origem e destino mantenham uma conversação [3]. Ela reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos que são o UDP e o TCP [2]:

- **UDP:** é um protocolo sem conexão não confiável para aplicações que não necessitam nem de controle de fluxo, nem da manutenção da seqüência das mensagens enviadas. Ele é amplamente usado em aplicações em que a entrega imediata é mais importante do que a entrega precisa, como a transmissão de dados de voz ou de vídeo [3]. O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente [4].
- **TCP:** é orientado à conexão confiável que permite a entrega sem erros de um fluxo de bytes originado de uma determinada máquina em qualquer computador da inter-rede [4]. Fragmenta o fluxo de bytes de entrada em mensagens e passa cada uma delas para cada camada de inter-redes. No destino, o processo TCP remonta as mensagens recebidas no fluxo de saída. O TCP cuida também do controle de fluxo, impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens muito grande. O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de erro, a sequenciação e a multiplexação de mensagens [3].

3) Inter-redes: Esta camada realiza a comunicação entre máquinas vizinhas através do protocolo IP. Para identificar cada máquina e a própria rede onde esta está situada é definido um identificador, chamado endereço IP, que é independente de outras formas de endereçamento que possam existir nos níveis inferiores. No caso de existir endereçamento nos níveis inferiores é realizado um mapeamento para possibilitar a conversão de um endereço IP em um endereço deste nível [2].

Os protocolos existentes nesta camada são:

- Protocolo de transporte de dados: IP – Protocolo de Internet (Internet Protocol);
- Protocolo de controle e erro: ICMP – Protocolo de Controle de Mensagem da Internet (Internet Control Message Protocol);

- Protocolo de controle de grupo de endereços: IGMP - Grupo de Administração de Protocolo da Internet (Internet Group Management Protocol);
- Protocolos de controle de informações de roteamento [2].

O protocolo IP realiza a função mais importante desta camada que é a própria comunicação inter-redes. Para isto ele realiza a função de **roteamento** que consiste no transporte de mensagens entre redes e na decisão de qual rota uma mensagem deve seguir através da estrutura de rede para chegar ao destino [3].

O protocolo IP utiliza a própria estrutura de rede dos níveis inferiores para entregar uma mensagem destinada a uma máquina que está situada na mesma rede que a máquina origem. Por outro lado, para enviar mensagem para máquinas situadas em redes distintas, ele utiliza a função de roteamento IP. Isto ocorre através do envio da mensagem para uma máquina que executa a função de roteador. Esta, por sua vez, repassa a mensagem para o destino ou a repassa para outros roteadores até chegar no destino [4].

4) Redes: A camada de rede é responsável pelo envio de datagramas construídos pela camada Inter-Rede. Esta camada realiza também o mapeamento entre um endereço de identificação de nível Inter-Rede para um endereço físico ou lógico do nível de Rede. A camada Inter-Rede é independente do nível de Rede [4].

Os protocolos deste nível possuem um esquema de identificação das máquinas interligadas por este protocolo. Por exemplo, cada máquina situada em uma rede Ethernet, Token-Ring ou FDDI possui um identificador único chamado endereço MAC (endereço físico que permite distinguir uma máquina de outra, possibilitando o envio de mensagens específicas para cada uma delas). Tais redes são chamadas redes locais de computadores [4].

As redes ponto-a-ponto, formadas pela interligação entre duas máquinas não possuem, geralmente, um endereçamento a nível de rede (modelo TCP/IP), uma vez que não há necessidade de identificar várias estações [4].

2.1 PROTOCOLO TCP

O protocolo TCP oferece serviços mais complexos, que incluem controle de erros e fluxo, serviço com conexão e envio de fluxo de dados [5].

Cada byte em uma conexão TCP tem seu próprio número de 32 bits. Os números de seqüência são usados tanto para as confirmações quanto para o mecanismo de janela, que utilizam campos de cabeçalho de 32 bits separados. As entidades TCP transmissoras e receptoras trocam dados na forma de segmentos. Um segmento consiste em um cabeçalho fixo de 20 bytes, seguido de zero ou mais bytes. Dois fatores restringem o tamanho do segmento [5]:

- Cada segmento incluindo o cabeçalho do TCP, deve caber na carga útil do IP, que é de 65535 bytes;
- Cada rede tem uma Unidade de Transferência Máxima (MTU, Maximum Transfer Unit), e cada segmento de caber na MTU. Na prática, uma MTU tem alguns milhares de bytes e, portanto, define o limite superior em termos de tamanho do segmento.

O protocolo básico utilizado pelas entidades TCP é o protocolo de janela deslizante. Quando envia um segmento, o transmissor também dispara um temporizador. Quando o segmento chega ao destino, a entidade TCP receptora retorna um segmento com um número de confirmação igual ao próximo número de seqüência que espera receber. Se o temporizador do transmissor expirar antes de a confirmação ser recebida, o segmento será retransmitido [5].

O protocolo TCP oferece as seguintes características:

- Controle de Fluxo e Erro fim-a-fim;
- Serviço confiável de transferência de dados;
- Comunicação full-duplex fim-a-fim;
- A aplicação basta enviar um fluxo de bytes;

- Desassociação entre quantidade de dados enviados pela aplicação e pela camada TCP;
- Ordenação de mensagens;
- Multiplexação de IP, através de várias portas;
- Opção de envio de dados urgentes [2].

A conexão TCP é ilustrada na Figura 2, partindo de uma porta de algum host, passando pelo TCP e depois pelo IP atingindo a Inter-rede TCP/IP [4]:

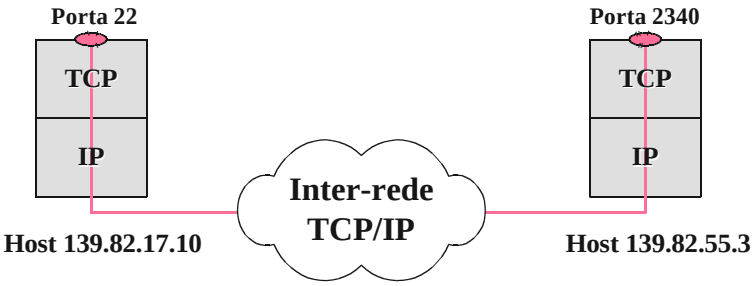


Figura 2 - Conexão do TCP [4]

Uma conexão TCP é formada por três fases: o estabelecimento de conexão, a troca de dados e a finalização da conexão, conforme ilustrado na Figura 3 [4]:

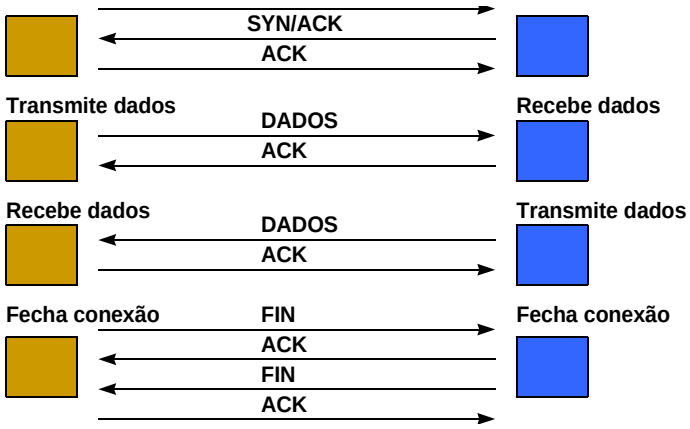


Figura 3 - Fases de uma conexão TCP [4]

A fase inicial de estabelecimento de conexão é formada de três mensagens, conforme a Figura 4 [4]:

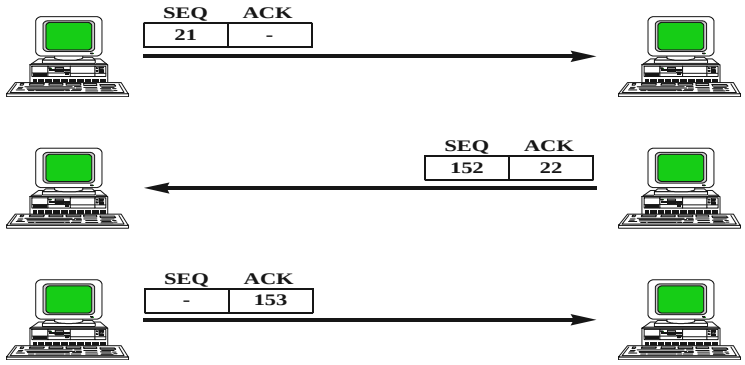


Figura 4 - Estabelecimento de conexão por mensagens [4]

O pacote TCP é formado pela mensagem mostrada abaixo na Figura 5:

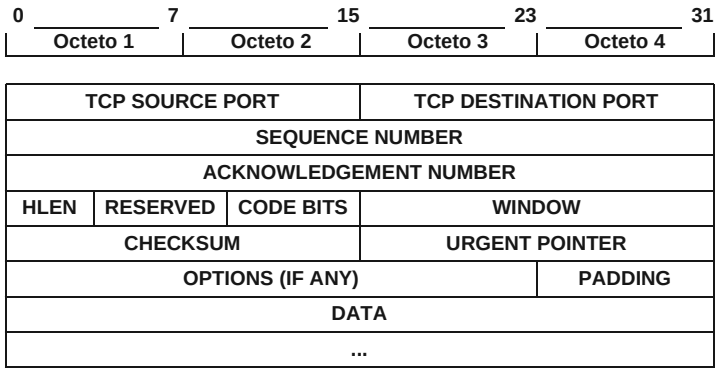


Figura 5 - Pacote TCP [4]

Os campos do pacote são definidos da seguinte forma:

TCP SOURCE PORT: Porta origem da mensagem

TCP DESTINATION PORT: Porta destino da mensagem

SEQUENCE NUMBER: número de sequência dos dados sendo transmitidos face ao conjunto total de dados já transmitidos. Este número indica a posição do primeiro byte de dados sendo transmitido em relação ao total de bytes já transmitidos nesta conexão. O primeiro número de sequência utilizado não é zero ou um, mas começa de um valor aleatório. Logo se um pacote está sendo transmitindo do 1234º byte até o 2000º byte de uma conexão e o SEQUENCE NUMBER inicial utilizado nesta conexão foi 10000, o campo SEQUENCE

NUMBER conterá o valor 11234. O número de sequência em um sentido da conexão (máquina A para B) é diferente do número de sequência do sentido inverso, já que os dados transmitidos por um e outro lado são completamente distintos [4].

ACKNOWLEDGE NUMBER: número que significa o reconhecimento dos dados recebidos até então no sentido inverso. O ACK contém o número do próximo byte do fluxo de dados recebido, que a origem deste pacote espera receber da outra máquina. Este valor leva em consideração o número de SEQUENCE NUMBER inicial praticado pela outra máquina. O valor de ACK informa sempre o próximo byte ainda não recebido do conjunto contíguo de bytes recebidos do transmissor [4].

CODE BITS: São formados por seis bits, URG, ACK, PSH, RST, SYN e FIN, cuja utilização é mostrada abaixo:

- **URG** (bit de Urgência): significa que o segmento sendo carregado contém dados urgentes que devem ser lidos com prioridade pela aplicação. A aplicação origem é responsável por acionar este bit e fornecer o valor do URGENT POINTER que indica o fim dos dados urgentes. Um exemplo da utilização desta facilidade é o aborto de uma conexão (por exemplo por Control-C), que faz com que a aplicação destino examine logo o pacote até o fim da área de urgência, descubra que houve um Control-C e termine a conexão [4].
- **ACK** (bit de Reconhecimento): indica que o valor do campo de reconhecimento está carregando um reconhecimento válido [4].
- **PSH** (bit de PUSH): Este mecanismo que pode ser acionado pela aplicação informa ao TCP origem e destino que a aplicação solicita a transmissão rápida dos dados enviados, mesmo que ela contenha um número baixo de bytes, não preenchendo o tamanho mínimo do buffer de transmissão [4].
- **RST** (bit de RESET): Informa o destino em que a conexão foi abortada neste sentido pela origem [4].
- **SYN** (bit de Sincronismo): é o bit que informa que este é um dos dois primeiros segmentos de estabelecimento da conexão [4].

- **FIN** (bit de Terminação): indica que este pacote é um dos pacotes de finalização da conexão [4].

WINDOW: Este campo informa o tamanho disponível em bytes na janela de recepção da origem deste pacote. Por meio deste valor, o TCP pode realizar um controle adequando de fluxo para evitar a sobrecarga do receptor. Quando este valor é igual a zero, o transmissor não envia dados, esperando receber um pacote com WINDOW maior que zero. O transmissor sempre vai tentar transmitir a quantidade de dados disponíveis na janela de recepção sem aguardar um ACK. Enquanto não for recebido um reconhecimento dos dados transmitidos e o correspondente valor de WINDOW > 0, o transmissor não enviará dados [4].

OPTIONS: O campo de opções só possui uma única opção válida que é a negociação do MSS (Maximum Segment Size) que o TCP pode transmitir [4].

2.1.1 POLÍTICA DE TRANSMISSÃO TCP

Considerando uma conexão TELNET com editor interativo que reage a cada tecla pressionada. Na pior da hipóteses, quando um caractere chegar a entidade TCP receptora, o TCP criara um seguimento TCP de 21 bytes, que será passado ao IP para ser enviado como um datagrama IP de 41 bytes. No lado receptor o TCP envia imediatamente uma confirmação de 40 bytes (20 bytes de cabeçalho TCP e 20 bytes de cabeçalho IP). Mais tarde, quando o editor tiver o lido byte o TCP enviará uma atualização de janela, movendo a janela um byte para a direita. Esse pacote também possui 40 bytes. Por último, quando o editor tiver processado o caracter, ele o ecoará como um pacote de 41 bytes. No total, 162 bytes de largura de banda são utilizados e quatro segmentos são enviados para cada caractere digitado [4].

2.1.2 CONTROLE DE CONGESTIONAMENTO

O primeiro passo para gerenciar o congestionamento é detectá-lo. Antigamente, detectar um congestionamento era difícil. Um *timeout* causado por um pacote perdido podia ter sido provocado por ruído na linha de transmissão ou pelo fato de o pacote ter sido

descartado em um congestionamento do roteador. Era difícil saber a diferença entre os dois casos [4].

Hoje em dia, a perda de pacotes devido o erro de transmissão é relativamente rara porque a maioria dos troncos de longa distância é de fibra (apesar de muitas redes sem fio, a história ser outra). Como conseqüência, a maioria dos *timeouts* de transmissão na internet se deve a congestionamentos. Todos os algoritmos TCP da internet presumem que os *timeouts* são causados por congestionamentos, e monitora os *timeouts* a procura de problemas, da mesma forma que um segurança observa os clientes que entram em um banco [4].

2.1.3 GERENCIAMENTO DE TEMPORIZADORES

O TCP utiliza vários temporizadores para desempenhar seu trabalho. O mais importante deles é temporizador de retransmissão. Quando um segmento é enviado, um temporizador de retransmissão é disparado. Se o segmento foi confirmado antes do temporizador expirar, ele será travado. Se, por outro lado, o temporizador expirar antes de a confirmação chegar, o segmento será retransmitido e o temporizador será disparado mais uma vez [3].

2.2 PROTOCOLO IP

O elemento que mantém a Internet unida é o protocolo de camada de rede, IP. Ao contrário da maioria dos protocolos da camada de rede, o IP foi projetado desde o início tendo como objetivo a ligação inter-redes. A tarefa do protocolo IP é fornecer a melhor forma de transportar datagramas da origem para o destino, independente se as máquinas estão na mesma rede ou em outra [3].

O protocolo IP provê um serviço sem conexão e não-confiável entre máquinas em uma estrutura de rede. Qualquer tipo de serviço com estas características deve ser fornecido pelos protocolos de níveis superiores. As funções mais importantes realizadas pelo protocolo IP são a atribuição de um esquema de endereçamento independente do endereçamento da rede e independente da própria topologia da rede utilizada, além da capacidade de rotear e tomar

decisões de roteamento para o transporte das mensagens entre os elementos que interligam as redes [3].

2.2.1 ENDEREÇOS IP

Um endereço IP é um identificador único para certa interface de rede de uma máquina. Este endereço é formado por 32 bits (4 bytes) e possui uma porção de bits de identificação da rede na qual a interface está conectada e outra para a identificação da máquina dentro daquela rede. O endereço IP é representado pelos 4 bytes separados por pontos e representados por números decimais. Desta forma o endereço IP:

11010000 11110101 0011100 10100011 é representado por **208.245.28.63** [6].

Como o endereço IP identifica tanto uma rede quanto a estação a que se refere, fica claro que o endereço possui uma parte para rede e outra para a estação. Desta forma, uma porção de bits do endereço IP designa a rede na qual a estação está conectada, e outra porção identifica a estação dentro daquela rede [6].

Uma vez que o endereço IP tem tamanho fixo, uma das opções dos projetistas seria dividir o endereço IP em duas metades, dois bytes para identificar a rede e dois bytes para a estação. Entretanto isto traria inflexibilidade pois só poderiam ser endereçados 65536 redes, cada uma com 65536 estações. Uma rede que possuísse apenas 100 estações estaria utilizando um endereçamento de rede com capacidade de 65536 estações, o que seria um desperdício [6].

A forma original de dividir o endereçamento IP em rede e estação, foi feita por meio de classes. Um endereçamento de classe A consiste em endereços que tem uma porção de identificação de rede de 1 byte e uma porção de identificação de máquina de 3 bytes. Desta forma, é possível endereçar até 256 redes com 2 elevado a 32 estações. Um endereçamento de classe B utiliza 2 bytes para rede e 2 bytes para estação, enquanto um endereço de classe C utiliza 3 bytes para rede e 1 byte para estação. Para permitir a distinção de uma classe de endereço para outra, foram utilizadas os primeiros bits do primeiro byte para estabelecer a distinção. Nesta forma de divisão é possível acomodar um pequeno número de redes muito grandes (classe A) e um grande número de redes pequenas (classe C) [6].

As classes originalmente utilizadas na Internet são A, B, C, D e E., conforme mostrado na Figura 6. A classe D é uma classe especial para identificar endereços de grupo (multicast) e a classe E é reservada [6].

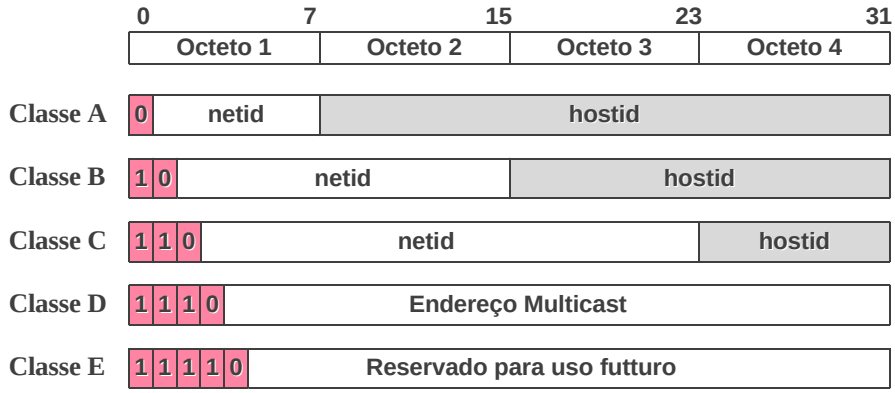


Figura 6 - Divisão das classes do endereço IP [6].

Alguns endereços são reservados para funções especiais:

1) Endereço de Rede: Identifica a própria rede e não uma interface de rede específica, representado por todos os bits de hostid com o valor ZERO [6].

2) Endereço de Broadcast: Identifica todas as máquinas na rede específica, representado por todos os bits de hostid com o valor UM [6].

Desta forma, para cada rede A, B ou C, o primeiro endereço e o último são reservados e não podem ser usados por interfaces de rede [6].

3) Endereço de Broadcast Limitado: Identifica um broadcast na própria rede, sem especificar a que rede pertence. Representado por todos os bits do endereço iguais a UM = 255.255.255.255 [6].

4) Endereço de Loopback: Identifica a própria máquina. Serve para enviar uma mensagem para a própria máquina rotear para ela mesma, ficando a mensagem no nível IP, sem ser enviada à rede. Este endereço é 127.0.0.1. Permite a comunicação inter-processos (entre aplicações) situados na mesma máquina [6].

As Figuras 7 e 8 mostram exemplos de endereçamento de máquinas situadas na mesma rede e em redes diferentes. Pode ser observado que como o endereço começa por 200

(ou seja, os dois primeiros bits são 1 e o terceiro 0), eles são de classe C. Por isto, os três primeiros bytes do endereço identificam a rede. Como na primeira figura, ambas as estações tem o endereço começando por 200.18.171, elas estão na mesma rede. Na segunda figura, as estações estão em redes distintas e uma possível topologia é mostrada, onde um roteador interliga diretamente as duas redes [6].

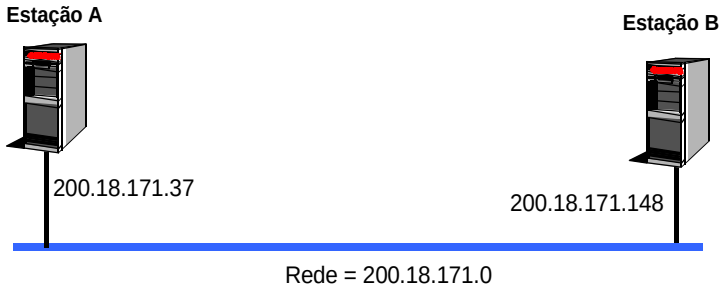


Figura 7 - Máquinas situadas na mesma rede [6]

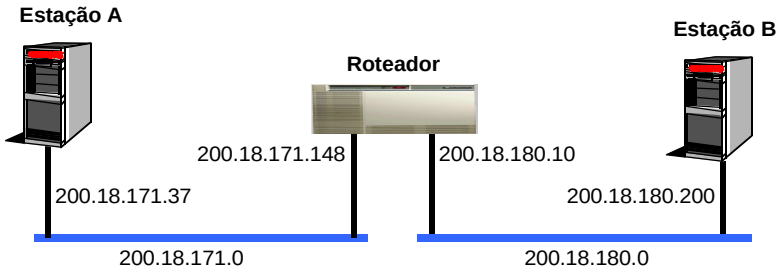


Figura 8 - Máquinas situadas em redes distintas [6]

2.2.2 ROTEAMENTO IP

O destino de uma mensagem IP sendo enviada por uma máquina pode ser a própria estação, uma estação situada na mesma rede ou uma estação situada numa rede diferente. No primeiro caso, o pacote é enviado ao nível IP que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio de ARP e a mensagem é enviada por meio do protocolo de rede [6].

Quando uma estação ou roteador deve enviar um pacote para outra rede, o protocolo IP deve enviá-lo para um roteador situado na mesma rede. O roteador por sua vez irá enviar o pacote para outro roteador, na mesma rede que este e assim sucessivamente até

que o pacote chegue ao destino final. Este tipo de roteamento é chamado de Next-Hop Routing, já que um pacote é sempre enviado para o próximo roteador no caminho [6].

Neste tipo de roteamento, não há necessidade de que um roteador conheça a rota completa até o destino. Cada roteador deve conhecer apenas o próximo roteador para o qual deve enviar a mensagem. Esta decisão é chamada de decisão de roteamento. Uma máquina situada em uma rede que tenha mais de um roteador deve também tomar uma decisão de roteamento para decidir para qual roteador deve enviar o pacote IP [6].

2.2.3 PACOTE IP

O protocolo IP define a unidade básica de transmissão, que é o pacote IP Figura 9. Neste pacote são colocadas as informações relevantes para o envio deste pacote até o destino.

O pacote IP possui o formato descrito abaixo:

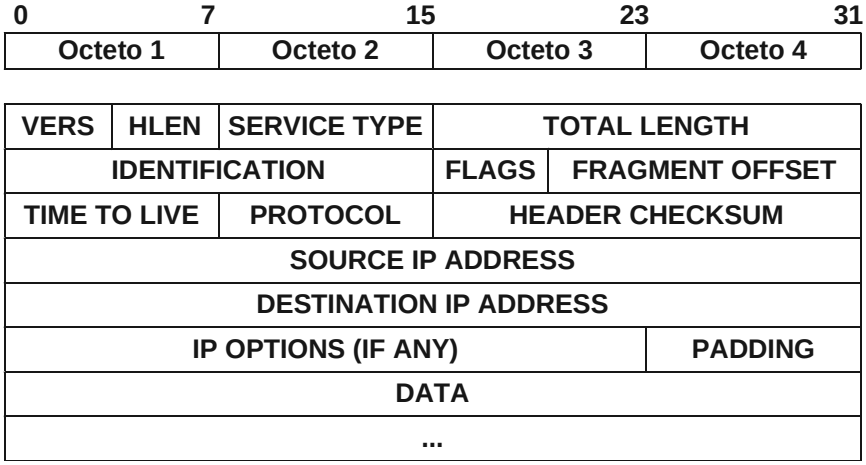


Figura 9 - Formato do Pacote IP [6]

Os campos mais importantes são descritos abaixo:

VERSION - Informa a versão do protocolo IP sendo carregado. Atualmente a versão de IP é 4.

HEADER LENGTH - Informa o tamanho do cabeçalho IP em grupos de 4 bytes.

TYPE OF SERVICE - Informa como o pacote deve ser tratado, de acordo com sua prioridade e o tipo de serviço desejado como Baixo Retardo, Alta Capacidade de Banda ou Alta Confiabilidade. Normalmente este campo não é utilizado na Internet.

IDENTIFICATION - Identifica o pacote IP unicamente entre os outros transmitidos pela máquina. Este campo é usado para identificar o pacote IP no caso de haver fragmentação em múltiplos datagramas.

FLAGS (3 bits) - um bit (MF - More Fragments) identifica se este datagrama é o último fragmento de um pacote IP ou se existem mais. Outro bit (DNF - Do Not Fragment) informa aos roteadores no caminho se a aplicação exige que os pacotes não sejam fragmentados.

FRAGMENT OFFSET - Informa o posicionamento do fragmento em relação ao pacote IP do qual faz parte.

TIME-TO-LIVE - Este valor é decrementado a cada 1 segundo que o pacote passa na rede e a cada roteador pelo qual ele passa. Serve para limitar a duração do pacote IP e evitar que um pacote seja roteador eternamente na Internet como resultado de um loop de roteamento.

PROTOCOL - Informa que protocolo de mais alto-nível está sendo carregado no campo de dados. O IP pode carregar mensagens UDP, TCP, ICMP, e várias outras.

HEADER CHECKSUM - Valor que ajuda a garantir a integridade do cabeçalho do pacote IP.

SOURCE ADDRESS - Endereço IP da máquina origem do pacote IP.

DESTINATION ADDRESS - Endereço IP da máquina destino do pacote IP.

OPTIONS - Opções com informações adicionais para o protocolo IP. Consiste de um byte com a identificação da opção e uma quantidade de bytes variável com as informações específicas. Um pacote IP pode transportar várias opções simultaneamente [6].

3 TECNOLOGIA DE REDE BLUETOOTH

No seu aspecto mais básico, a tecnologia Bluetooth apresenta um mundo de conexões sem fio. Usando transmissões de ondas curtas de rádio, essa tecnologia permitirá que todos os dispositivos eletrônicos diferentes se conectem entre si sem o uso de fios e cabos. Entretanto, Bluetooth é mais do que uma tecnologia de substituição de cabos, é também uma tecnologia que permite que qualquer dispositivo eletrônico se comunique automaticamente com outro. Isso significa que, em distâncias curtas (cerca de 10 metros), um computador pessoal pode se conectar, sincronizar e ainda controlar outros dispositivos eletrônicos em casa ou escritório como impressora, televisão e outros [7].

3.1 COMO A TECNOLOGIA BLUETOOTH FUNCIONA

A tecnologia Bluetooth permite comunicação sem fio, tanto de dados quanto de voz, entre dispositivos eletrônicos separados por curtas distâncias. Essa comunicação ocorre sem intervenção manual explícita do usuário. Sempre que um dispositivo compatível com a tecnologia Bluetooth detecta outro dispositivo também compatível, eles são automaticamente sincronizados e uma rede *ad hoc* é criada [7].

O padrão Bluetooth promete fazer o seguinte:

- Eliminar os fios e cabos entre dispositivos fixos e móveis separados por pequenas distâncias;
- Facilitar comunicação de dados e voz;
- Ativar redes *ad hoc* e fornecer sincronização automática entre vários dispositivos compatíveis com esta tecnologia. Numa rede Bluetooth, a transmissão de dados é feita através de pacotes, como na Internet. Para evitar interferências e aumentar a segurança, existem 79 canais possíveis (23 em alguns países onde o governo reservou parte das freqüências usadas). Os dispositivos Bluetooth têm capacidade de localizar dispositivos próximos, formando redes de transmissão. Uma vez estabelecida a rede, os dispositivos determinam um padrão de transmissão, usando os canais possíveis. Isto significa que os pacotes de dados serão transmitidos cada um em um canal diferente, numa ordem que apenas os dispositivos da rede conhecem [8].

3.1.1 ESTRUTURA DE UMA PICONET

Quando um dispositivo Bluetooth percebe outro dispositivo Bluetooth, eles configuram automaticamente uma conexão entre si. Essa conexão é denominada Piconet, um tipo de mini-rede ou uma rede pessoal (PAN) [8].

Esta tecnologia é utilizada tanto para as comunicações ponto-a-ponto como para as comunicações ponto-a-multiponto. Uma piconet é formada no máximo com um dispositivo que denomina-se mestre e no mínimo por outro dispositivo chamado escravo, nela também um dispositivo Bluetooth recebe a função de mestre, enquanto o outro e todos os dispositivos subseqüentes, até um total de oito recebem a função de escravos, como o demonstrado na Figura 10. O dispositivo mestre controla as comunicações incluindo qualquer transferência de dados necessária entre os dispositivos [8].

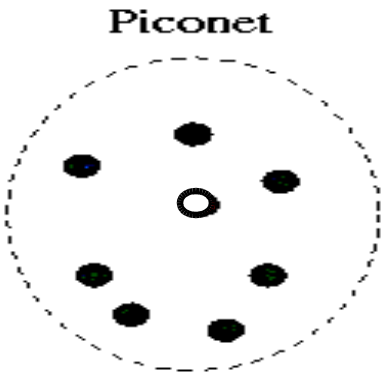


Figura 10 - Exemplo de Piconet [8]

Mestre Escravo

3.1.2 SCATTERNETS

É formada pela interconexão de duas ou mais piconets e facilita a comunicação entre elas. Após ficar em uma piconet por algum tempo o nó comum pode ser ativado para a outra piconet, ele pode enviar e receber pacotes em cada piconet e também transmitir pacotes de uma piconet para outra. Um nó pode ser escravo em uma ou mais piconets ou pode ser mestre em uma e escravo em uma ou mais piconets como demonstrado na Figura 11 [8].

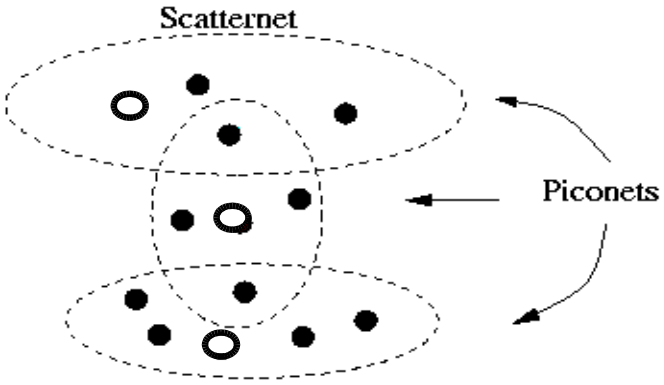


Figura 11 - Exemplo de Scatternet [8]

Mestre Escravo

No domínio do tempo, um canal é dividido em pulsos de duração de 625 micro segundos. De modo a simplificar a implementação, comunicações *full-duplex* são alcançadas aplicando-se um TDD. Neste caso, os slots são utilizados de modo alternado para a transmissão e a para a recepção de pacotes [8].

3.1.3 ONDAS DE RÁDIOS

A tecnologia Bluetooth utiliza um chip com rádio-transmissor pequeno e de baixa voltagem em um dispositivo eletrônico tradicional. Esse rádio (e o software baseado no chip associado a ele) é capaz de transmitir e receber comunicações de dados e de voz de outros dispositivos [7].

Os rádios Bluetooth usam uma banda de rádio denominada banda industrial, científica e médica ou (ISM, Industrial, Scientific and Medic Band) entre 2,4 e 2,48 (GHz). Como os rádios são incorporados em pequenos chips de computador, eles têm dimensões pequenas e podem, eventualmente, ser produzidos com um custo relativamente baixo. A combinação de tamanho pequeno e baixo custo deve ajudar a tornar a tecnologia Bluetooth onipresente em diversos dispositivos eletrônicos, especialmente naqueles com aplicações portáveis [7].

3.1.4 COMO A FREQÜÊNCIA DE RÁDIO FUNCIONA

Para receber um sinal de rádio, precisa-se de um receptor de rádio. O receptor é ajustado para uma freqüência específica para receber sinais oscilando naquela taxa. Se o receptor não estiver ajustado na freqüência correta as transmissões passam sem serem recebidas [7].

Como pode-se ver na Figura 12, as ondas de rádio são geradas quando um transmissor oscila a uma freqüência específica. Quanto mais rápida a oscilação, mais alta a freqüência. Uma antena é usada para ampliar e transmitir o sinal de rádio por longas distâncias [7].

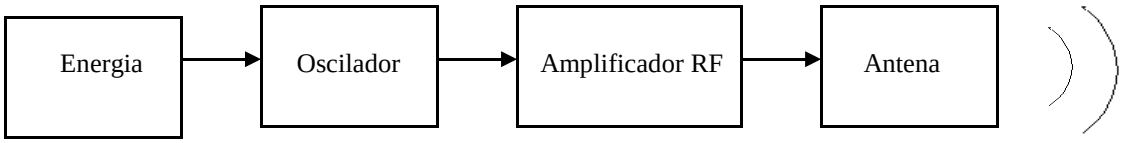


Figura 12 - Como um transmissor de Rádio funciona [7]

Diferentes intervalos de freqüência são utilizados para diferentes tipos de comunicações. Um exemplo é o intervalo de freqüências entre 88MHz e 108MHz que é conhecido como o intervalo de freqüência modulada (FM). A Tabela 1 detalha algumas das bandas de freqüência de rádio mais populares [7].

Tabela 1 - Bandas de freqüência de rádio popular [7].

Alcance de Freqüência	Utilização
535KHz a 1,7MHz	Rádio AM
5,9MHz a 26,1MHz	Ondas curtas de rádio
43,72MHz a 49,97MHz	Telefones sem fios (antigos)
902MHz a 928MHz	Telefones sem fios (mais novos – denominados telefones de 900MHz).
162MHz a 168MHz	Comunicações do FBI (privado)
824MHz a 849MHz	Telefones Celulares
470MHz a 890MHz	Televisões UHF
960MHz a 1,215GHz	Radar de controle de tráfego aéreo
2,40GHz a 2,48GHz	Banda ISM (Bluetooth, Home RF, telefones sem fio de 2,4GHz).

3.2 TRANSMITINDO VOZ E DADOS

Todos os dispositivos compatíveis com a tecnologia Bluetooth devem ser capazes de transmitir sinais de voz e dados. Isso significa que a tecnologia Bluetooth pode ser usada para conectar dispositivos de computação e dispositivos de comunicação [7].

3.2.1 COMUTAÇÃO DE CIRCUITO E PACOTE

Os sinais de dados normalmente utilizam uma tecnologia denominada *comutação de pacote.* Com a comutação de pacote, os dados são divididos em grupos pequenos ou *pacotes,* antes de serem transmitidos. Uma única mensagem, fatiada em diversos pacotes, pode, na verdade, ser transmitida por rotas diferentes, em freqüências diferentes ou em uma ordem diferente da original. Uma vez que todos os pacotes de uma mensagem sejam recebidos, eles são recompilados na sua ordem original [7].

Os sinais de voz, por outro lado, utilizam a tecnologia denominada *comutação de circuito.* Com a comutação de circuito, as mensagens *não* são fatiadas em pacotes; em vez disso, um canal dedicado (ou *circuito*) é estabelecido durante a transmissão [7].

A comutação de pacote é uma maneira eficiente para transmitir dados binários (ou de computador); a comutação de circuito é preferível quando as comunicações (como as chamadas de voz) têm de ocorrer em tempo real. Os dispositivos Bluetooth podem funcionar nos dois modos, comutação de pacote e comutação de circuito – simultaneamente, se necessário [7].

3.2.2 DUPLEXAÇÃO

Full duplex refere-se à transmissão de dados em duas direções, simultaneamente. A *half duplex* significa que os dados podem fluir em apenas uma direção de cada vez [8].

As comunicações full-duplex também são denominadas *síncronas* e as comunicações half-duplex são também denominadas *assíncronas*. Na terminologia Bluetooth, as comunicações full-duplex/síncronas são denominadas links SCO e as comunicações half-duplex/assíncronas são denominadas links ACL [8].

Na especificação Bluetooth, a transmissão full duplex utiliza um esquema TDD. O TDD atribui pulsos de tempo subseqüentes para a transmissão e recepção; as unidades mestre transmitem em slots pares, enquanto as escravas respondem em slots ímpares. Alternando de um lado para outro dessa forma em uma única freqüência, duas transmissões diferentes podem compartilhar a mesma freqüência – e permitem comunicações full-duplex [8].

3.3 ESTABELECENDO A CONEXÃO

Serão estabelecidos estados de conexão utilizados na especificação Bluetooth.

3.3.1 ESTADOS DA CONEXÃO

Um dispositivo Bluetooth pode operar em qualquer dos dois estados principais – *Connection* e *Standby*. O dispositivo está no estado Connection se ele está conectado a outro dispositivo e envolvido em atividades correntes. Se o dispositivo não estiver conectado ou se estiver conectado, mas não envolvido ativamente com outros dispositivos, então, ele automaticamente opera no estado Standby [7].

A criação de um estado Standby foi concebida como uma maneira para economizar energia em dispositivos Bluetooth. Se um dispositivo não precisa participar ativamente em determinado momento, não há nenhuma razão para que consuma energia em níveis máximos [7].

Quando um dispositivo está no estado Standby monitora, a cada 1,28 segundos, as mensagens de outros dispositivos. Cada sessão de monitoramento ocorre pelo conjunto de 32 saltos de freqüência definido para aquele tipo de unidade. (A cada tipo de dispositivo Bluetooth é atribuído um grupo diferente de saltos de freqüência) [7].

Uma vez que um dispositivo saia do estado Standby e entre no estado Connection, pode ser colocado em um dos quatro modos possíveis de conexão:

1 - Active: Diz-se que um dispositivo Bluetooth está em modo Active quando está participando ativamente na piconet, transmitindo ou recebendo. Unidades escravas ativas são automaticamente mantidas sincronizadas com a unidade mestre da piconet [7].

2 - Sniff: Quando um dispositivo for colocado em modo Sniff, monitora a piconet a uma taxa reduzida, diminuindo assim seu consumo de energia. A taxa Sniff é programável e varia de uma aplicação para outra [7].

3 - Hold: Dentro de uma piconet, as unidades mestre podem colocar as unidades escravas em modo Hold. Esse modo de economia de energia é utilizado quando nenhum dado precisa ser transmitido. Quando um dispositivo for colocado em modo Hold, apenas um timer

interno permanece ativo. Esse é um modo popular para dispositivos de baixo consumo de energia com necessidades de transferência de dados relativamente simples, como sensores de temperatura [7].

4 - Park: Quando um dispositivo precisa permanecer conectado a uma piconet, mas não necessita participar do tráfego de dados em progresso, esse dispositivo pode ser colocado em modo Park. No modo Park, o dispositivo permanece sincronizado à piconet, mas suspende seu endereço MAC. Ao estacionar dispositivos inativos, uma piconet pode realmente incluir mais de sete unidades escravas. (O número teórico de unidades escravas estacionadas que podem estar conectadas a uma única unidade mestre é 255) [7].

3.3.2 SOLICITAÇÃO E PAGINAÇÃO

Um dispositivo Bluetooth pode emitir dois tipos diferentes de comandos para iniciar um procedimento de conexão. O primeiro comando é denominado um comando de *solicitação*. Um comando de solicitação é emitido quando o número de identificação ou *endereço*, do outro dispositivo ainda não é conhecido. Uma vez que o endereço do dispositivo seja conhecido, um comando *página* é emitido. O comando página serve para "despertar" a outra unidade e estabelecer uma conexão plena entre os dois dispositivos [7].

A Figura 13 mostra a seqüência típica de comandos necessários para estabelecer uma conexão sem fio Bluetooth [7].

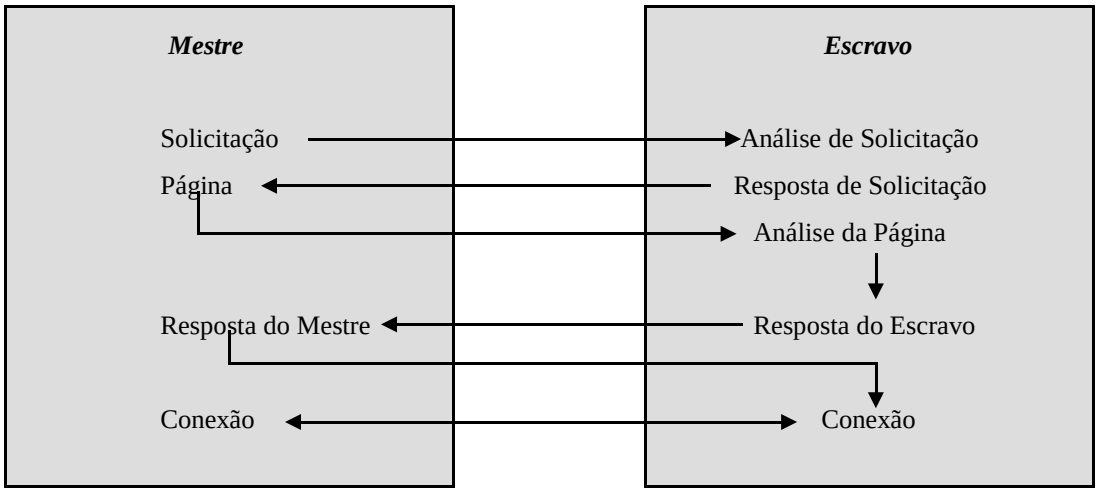


Figura 13 - Seqüência de Comandos de Reconhecimento [7]

3.3.3 CONTROLANDO AS CONEXÕES

Cada chip Bluetooth inclui não apenas o rádio Bluetooth, mas também o que é denominado de Controlador de Link (*Link Controller* - LC). Essa parte do chip é um processador de sinais digitais que manipula, em segundo plano, todas as funções necessárias para estabelecer uma conexão sem fio Bluetooth (também denominado um *link*, daí o nome) [7].

O software em que se baseia o Controlador de Link (Link Controller) é denominado software Gerenciador de Link (*Link Manager* - LM). O software LM utiliza um conjunto de comandos específicos do Protocolo de Gerenciamento de Link (*Link Manager Protocol* ou LMP) que executa funções específicas, incluindo a instalação de link, autenticação e configuração e ainda o envio e recebimento de dados [7].

3.4 A ARQUITETURA BLUETOOTH

A especificação Bluetooth define todos os aspectos da tecnologia Bluetooth, inclusive componentes de hardware e software, processos e procedimentos compartilhados. Antes de detalhar os protocolos e processos técnicos da especificação Bluetooth, é importante entender a arquitetura Bluetooth propriamente dita o que torna um dispositivo compatível com a tecnologia Bluetooth [7].

3.4.1 O DISPOSITIVO BLUETOOTH

Em termos gerais, um dispositivo Bluetooth é qualquer produto eletrônico completo que incorpora um rádio Bluetooth. O rádio propriamente dito (discutido a seguir) não é dispositivo, é apenas um componente do dispositivo [7].

Desde que o produto completo incorpore a tecnologia Bluetooth (na forma de um rádio Bluetooth e do software operacional correspondente, como mostra a Figura 14), o produto pode ser denominado um dispositivo Bluetooth [7].

Na termologia Bluetooth, a parte não Bluetooth de um dispositivo é denominada *host;* todos os componentes Bluetooth (hardware e software) são combinados no *módulo*

Bluetooth. As comunicações entre o host e o módulo Bluetooth são manipulados pelo software Link Manager Bluetooth e pelo Host Controller no módulo Bluetooth [7].

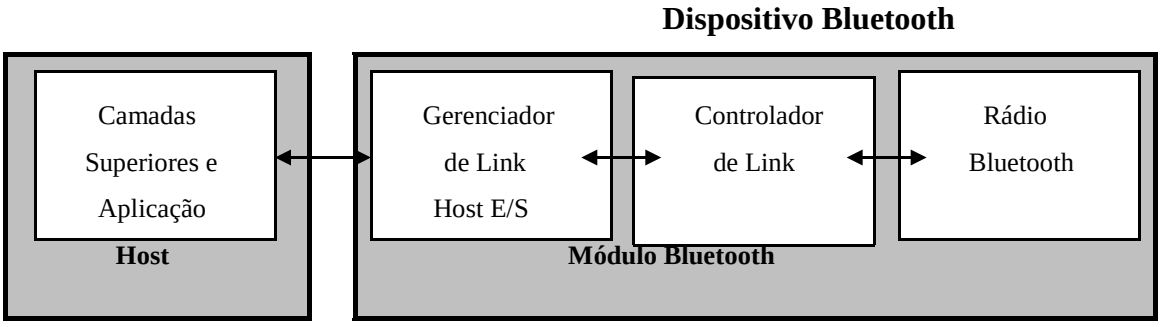


Figura 14 - A arquitetura de um dispositivo Bluetooth [7].

3.4.2 O HOST CONTROLLER

O Controlador de Host (Host Controller - HC) é a parte do módulo Bluetooth que gerencia toda a comunicação e interação entre o módulo Bluetooth e o dispositivo host. A conexão entre as duas partes pode ser *hardwired* (isto é, o módulo Bluetooth pode ser construído na placa de circuito principal do dispositivo host) ou modular (com o módulo Bluetooth anexado ao dispositivo host como um acessório complementar ou uma placa conectada) [7].

O Host Controller interpreta os dados recebidos do host e os direciona ao(s) componente(s) apropriado(s) do módulo Bluetooth. Também interpreta os dados vindos do módulo Bluetooth e os envia a seu destino para a função apropriada no dispositivo host [7].

Para assegurar a interoperabilidade de módulos Bluetooth procedentes de vários fabricantes, a especificação Bluetooth define uma interface padrão (e protocolo de comunicações) que pode ser usada por todos os módulos Bluetooth e por todos os dispositivos host que incorporam a tecnologia Bluetooth. Esse Controlador de Interface de Host (HCI), embora não seja um componente obrigatório da especificação Bluetooth (não é absolutamente necessário se o módulo Bluetooth estiver completamente integrado no projeto do dispositivo host), é útil para aqueles dispositivos Bluetooth que pretendem ser usados em um modo complementar ou acessório. Dentro do módulo Bluetooth, o Controlador de Host faz uma interface diretamente com o hardware do Controlador de Link [7].

3.4.3 O RÁDIO BLUETOOTH

O rádio Bluetooth transmite pela banda de freqüência de rádio de 2,4GHz, utilizando as tecnologias do salto de freqüência de alargamento da banda e a Time Division Duplexing (TDD). Um rádio Bluetooth Class 3 (o tipo mais comum de dispositivo) pode funcionar com um alcance de cerca de 10 metros (aproximadamente 30 pés) [1]. Ele faz uma interface diretamente com o Link Controller (por meio do Link Manager do protocolo Link Manager), o qual, em seguida, faz uma interface com o Host Controller, que faz uma interface (por meio do HCI) com dispositivo host [7].

3.4.3.1 Operações de Rádio

Ao contrário do rádio em seu sistema de áudio, o rádio Bluetooth funciona como um transmissor e um receptor. As operações de transmissão de rádio incluem a geração e a modulação da onda portadora, como também o controle da potência de transmissão e da intensidade do sinal. As operações de recepção incluem a habilidade de ajustar a freqüência portadora adequada e adaptar a intensidade do sinal recebido [7].

A Figura 15 detalha as operações principais do rádio Bluetooth.

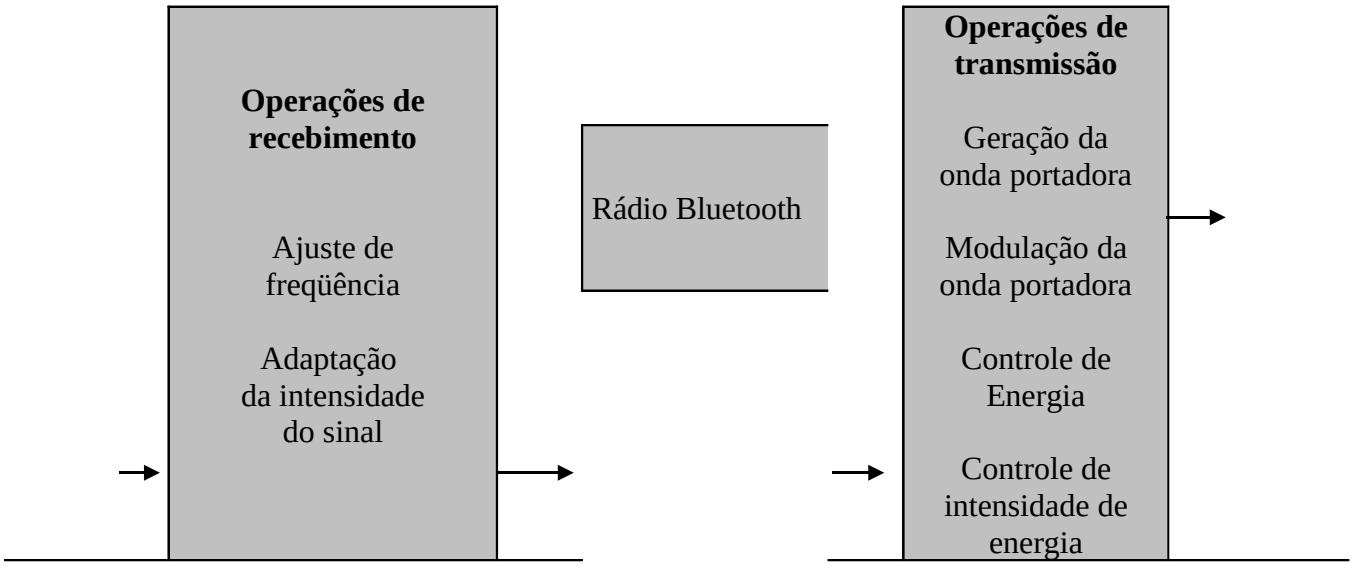


Figura 15 - As operações do rádio Bluetooth [7]

Como você pode ser visto na Tabela 2, há realmente três classes diferentes de rádio Bluetooth definidas na especificação Bluetooth; a potência de saída (e, consequentemente, o alcance de transmissão/recepção) é o diferencial entre as classes. A

Class 3, que define uma saída de um miliwatt (mW) (e um alcance de 10 metros), é a classe "padrão" para dispositivos Bluetooth [7].

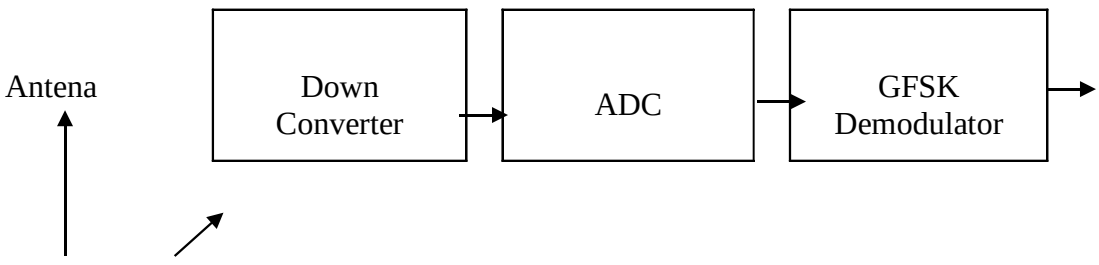
Tabela 2 - Potência de saída para cada classe de potência Bluetooth [7].

CLASSE DE POTÊNCIA	POTÊNCIA DE SAÍDA MÁXIMA	POTÊNCIA DE SAÍDA MÍNIMA
1	100mW (20dBm)	1mW (0dBm)
2	2,5mW (4dBm)	0,25mW (-6dBm)
3	1mW (0dBm)	N/Disp.

3.4.3.2 Os Chips Radio e Controller

As implementações iniciais de tecnologia Bluetooth utilizam dois chips de circuito integrado (IC, Integrated Circuit) separados. O primeiro chip, mostrado na Figura 16, é o Radio Modem. Esse chip é a essência do rádio, e – além de ser um transceptor de rádio completamente integrado – desempenha as funções de modulação/demodulação, recuperação da sincronização de quadro e saltos de freqüência. Como você pode ser visto na Figura 16, ele também se conecta diretamente à pequena antena, que é necessária para transmitir e receber os sinais sem fio Bluetooth [8].

O segundo dos dois chips no conjunto de chips inicial Bluetooth é o Controller IC Bluetooth. Esse chip implementa o protocolo e funções Baseband – e contém o Link Controller, que executa a conexão básica e atividades de configuração [8].



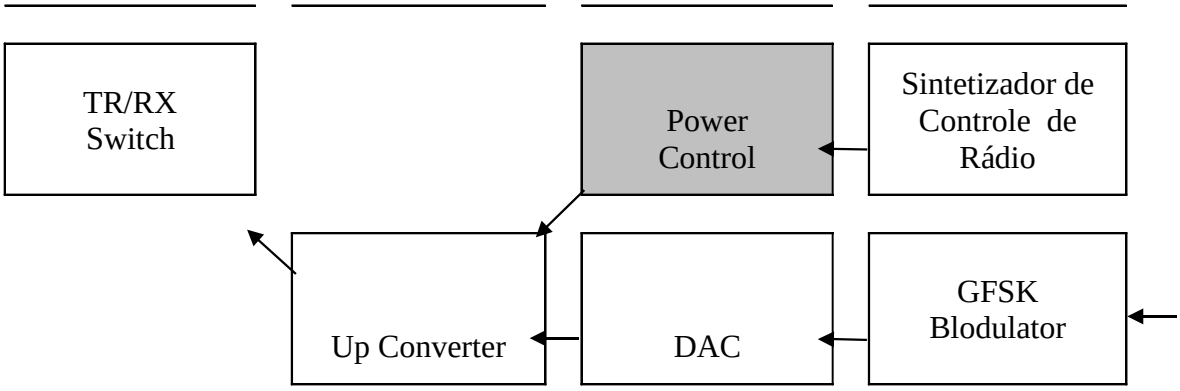


Figura 16 - As funções do Radio Modem IC Bluetooth [8].

3.4.4 HARDWARE BLUETOOTH

A placa com Bluetooth inclui um sistema de desenvolvimento de software com a camada de controle de acesso médio (Medium Access Control Layer - MAC). Esta tecnologia permite dígitos binários de 730kbps, trabalhando a 2.4GHz em 79 canais da banda ISM e taxa de transferência de 1 Mbps. Bluetooth é incompatível com o padrão para bandas ISM IEEE 802.11. O Bluetooth suporta os principais protocolos como: TCP/IP, e RFCOMM [9].

Todo o padrão é implementado em um único microchip de 9 x 9 milímetros como é mostrado na Figura 17. Qualquer sistema que utiliza a tecnologia Bluetooth pode ser visualizado em termos de quatro componentes:

- Uma unidade de rádio (“Radio Unit”);
- Uma unidade de banda básica (“Baseband Unit”);
- Uma pilha ou camada de software (“Software Stack”) e
- Um programa aplicativo (“Aplication Software”) [9].

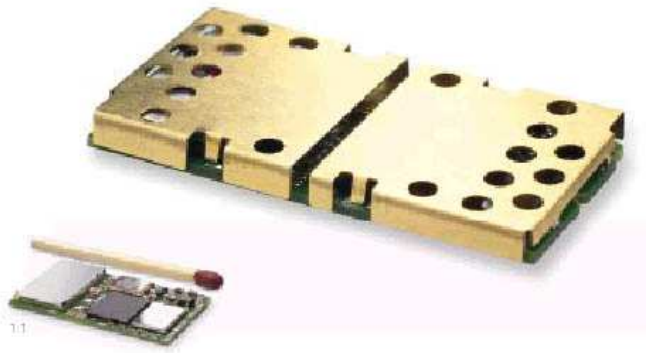


Figura 17 - Microchip padrão Bluetooth [9]

3.4.5 CRIANDO E CONTROLANDO A CONEXÃO

Em linguagem Bluetooth, uma conexão entre dois dispositivos é denominada um link. O gerenciamento e controle de link – o gerenciamento das conexões Bluetooth – é uma função essencial de qualquer dispositivo Bluetooth. Esta seção fornecerá alguns detalhes sobre como os dispositivos Bluetooth estabelecem links e como eles controlam os diversos links inerentes em uma piconet com vários dispositivos [9].

3.4.5.1 O Link Manager e o Link Controller

As conexões entre dispositivos Bluetooth são manipulados por uma combinação de software e hardware. O software é denominado Link Manager (LM); o hardware associado é denominado Link Controller (LC) [9].

O software LM executa a instalação do link, autenticação, configuração e outras atividades necessárias para estabelecer um link entre dois dispositivos Bluetooth. Em essência o LM detecta outros dispositivos que executam um mesmo software LM e, em seguida, se comunica com eles por meio do protocolo Link Manager (LMP, Link Manager Protocol) da tecnologia Bluetooth [9].

Para desempenhar essa função, o software LM deve utilizar os serviços fornecidos pelo hardware LC subjacente. O LC facilita enviando e recebendo dados, configurando conexões e outras atividades relacionadas [9].

É fácil confundir o Link Manager com o Link Controller, embora, na realidade eles sejam totalmente interdependentes. Como você pode ser visto na Figura 18, o software LM é executado no hardware LC, utilizando o LMP ele se comunica com o Baseband e estabelece a comunicação [9].

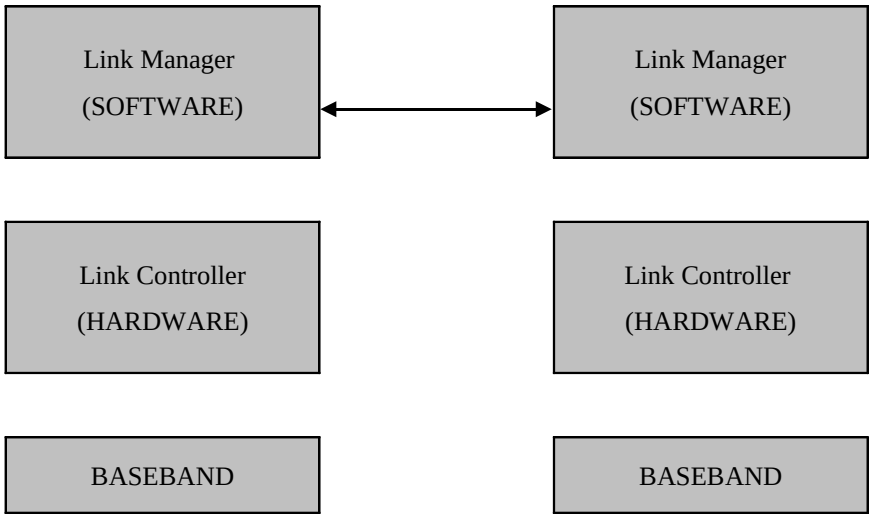


Figura 18 - O gerenciamento e controle do link Bluetooth[9]

Uma vez que o link seja estabelecido entre dois dispositivos Bluetooth, os Links Managers de cada unidade comunicam-se entre si pelo Protocolo Link Manager. As mensagens enviadas entre essas duas unidades adotam a forma do que a tecnologia Bluetooth denomina o Protocolo de Unidades de Dados (PDUs). Considerando que essas pequenas mensagens em nível de sistema sejam fundamentais para manter o link entre os dois dispositivos, elas têm uma prioridade mais alta do que as comunicações de dados ou voz do usuário [9].

3.4.5.2 Controle de Alto Nível

Além das informações de link básico transmitidas por meio do protocolo Link Manager, o Bluetooth define um nível mais alto de controle denominado Protocolo de Controle de Vínculo Lógico e Adoção (Logical Link Control and Adaptation Protocol -L2CAP). Este protocolo entra em atividade uma vez que o link inicial entre dois dispositivos tenha sido estabelecido por meio do Protocolo de Gerenciamento de Link [7].

O L2CAP manipula uma variedade de funções de nível mais alto entre dois dispositivos Bluetooth, inclusive a multiplexação de protocolo, a segmentação e reconstrução de pacote e informações da qualidade de serviço (QoS, Quality of Service). Além disso, o L2CAP se comunica com outros protocolos de comunicação, inclusive o SDP, o RFCOMM e o TCS-BIN [7].

Da mesma maneira que os LMPs comunicam-se entre si por meio de PDUs, as camadas L2CAP em unidades conectadas comunicam-se por meio de suas próprias séries de mensagens, denominadas eventos. As mensagens de eventos se parecem muito com PDUs (por exemplo, ***L2CAP_DisconnectReq*** indica que um pacote de solicitação de desconexão foi recebido), mas representam sua própria linguagem distinta [7].

3.5 DEFININDO OS PROTOCOLOS

Na especificação Bluetooth, o software adota a forma de protocolos padronizados que são utilizados para implementar vários procedimentos e processos. Alguns desses protocolos são exclusivos para a tecnologia Bluetooth; outros são protocolos existentes usados por outras tecnologias e aplicações. Compreender quais protocolos são usados e como é essencial para entender como a tecnologia Bluetooth funciona [7].

3.5.1 A PILHA DE PROTOCOLOS BLUETOOTH

Na maioria das vezes, os diferentes protocolos utilizados em uma tecnologia específica seguem uma hierarquia predefinida. A camada básica de hierarquia normalmente contém protocolos que são usados em todas as aplicações da tecnologia. Outras camadas são empilhadas sobre essa camada básica e contém protocolos que definem cada vez mais funções verticais [7].

A pilha de protocolos Bluetooth pode ser dividida em quatro camadas principais, de acordo com a função. A Tabela 3 detalha as diferentes camadas de protocolos e os protocolos específicos incluídos em cada camada [7].

Tabela 3 - As Camadas da Pilha de Protocolos Bluetooth [7]

CAMADA DE PROTOCOLOS	PROTOCOLOS UTILIZADOS
Protocolos Principais	Baseband Link Manager Protocol (LMP) Logical Link Control and Adoption Protocol (L2CAP) Service Discovery Protocol (SDP)
Protocolo de Substituição de Cabos	RFCOMM
Protocolos de Controle de Telefonias	Telephony Control Specification – Binary (TCS-BIN) AT – Commands
Protocolos Adotados	Point-to-Point Protocol (PPP) Transport Control Protocol / Internet Protocol / User Datagram Protocol (TCP/IP/UDP) Object Exchange Protocol (OBEX) Infrared Móbile Communications (IrMC) Wireless Application Protocol (WAP) Wireless Application Environment (WAE) VCard, vCalendar, vMessage e vNote (formatos de conteúdo)

A pilha de protocolos Bluetooth completa é mostrada na figura 19. Naturalmente, nem todas as aplicações utilizam todos os protocolos da pilha principal; em vez disso as aplicações individuais executam o mais das fatias verticais dentro da pilha [7].

A pilha completa de protocolos inclui os protocolos específicos Bluetooth (como a LMP e o L2CAP) e os protocolos não específicos da tecnologia Bluetooth (como o OBEX e o PPP). Como é normal durante o desenvolvimento de uma nova tecnologia, não apenas é mais eficiente trabalhar com os protocolos existentes, como também serve para garantir algum grau de interoperabilidade entre a tecnologia Bluetooth e as outras tecnologias de comunicação [7].

Em geral, a camada de protocolos principal inclui os protocolos específicos Bluetooth desenvolvidos pelo Grupo Bluetooth SIG (Ericsson, Nokia, Toshiba, IBM, Intel, 3Com, Lucent Technologies, Microsoft e Motorola). As outras três camadas de protocolos – Substituição de Cabos, Controle de Telefonia e Adotados – incluem protocolos que permitem que aplicações específicas sejam executadas pelos protocolos principais da tecnologia Bluetooth. Além disso, a especificação Bluetooth é aberta para que protocolos adicionados

possam ser acomodados em um modo interoperável na parte superior dos protocolos principais específicos da tecnologia Bluetooth e dos protocolos orientados a aplicação [7].

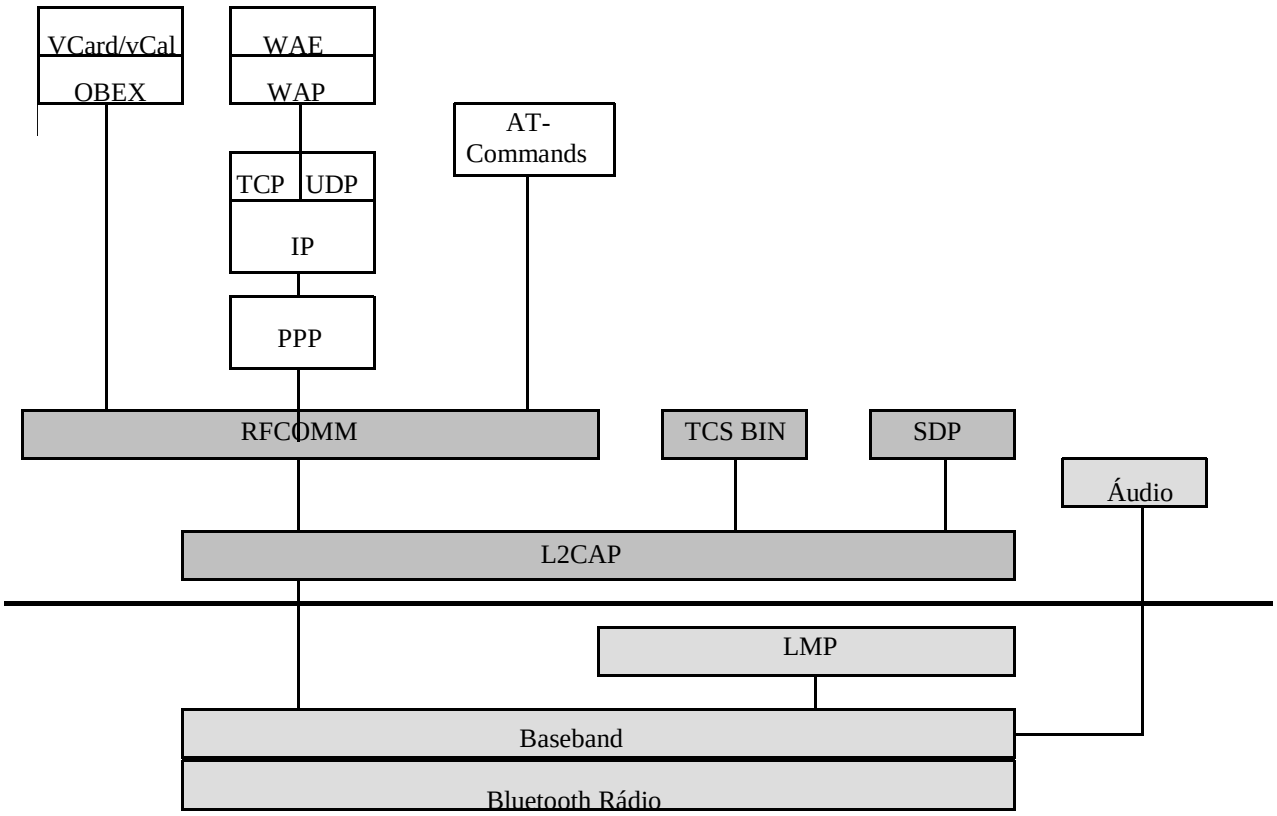


Figura 19 - A pilha de completa de protocolos Bluetooth [7]

3.5.2 OS PROTOCOLOS PRINCIPAIS

Os protocolos principais Bluetooth são utilizados em todos os perfis Bluetooth e fornecem funções de transporte e gerenciamento do link a todas aplicações [7].

3.5.2.1 O Protocolo Baseband

O protocolo Baseband permite a conexão de freqüência de rádio (RF) física (denominada link) entre as duas ou mais unidades Bluetooth que formam uma piconet. Esse protocolo também sincroniza o salto de transmissão de freqüências e os clocks dos dispositivos individuais Bluetooth em uma piconet [7].

Há dois tipos diferentes de links físicos fornecidos pelo protocolo Baseband. Com um link de Conexão Orientada Síncrona (Synchronous Connection-Oriented - SCO), os pacotes podem conter uma combinação de áudio e dados ou apenas um áudio. Com um Link de Conexão Assíncrona (Asynchronous Connection-less - ACL), os pacotes são reservados apenas para dados [7].

O protocolo Baseband também leva em consideração todos os tipos de pacotes (áudio, dados ou a combinação deles) para serem fornecidos com diferentes níveis de correção de erro. A criptografia opcional de dados, também faz parte desse protocolo, para aumentar a segurança [7].

3.5.2.2 Protocolo Link Manager - LMP

Exatamente sobre o protocolo Baseband na pilha está o protocolo de Gerenciamento de Link (LMP). O LMP é responsável pela configuração e controle do link entre dois ou mais dispositivos Bluetooth. Isso inclui diversos aspectos de segurança, como autenticação e criptografia, e o controle e negociação de tamanhos de pacotes da Baseband. O LMP também controla os modos de potência e ciclos de tarefas do rádio Bluetooth, assim como o estado da conexão do dispositivo Bluetooth quando ligada a uma piconet [7].

3.5.2.3 O Protocolo Logical Link Control and Adoption – L2CAP

O protocolo Controle de Vínculo Lógico e Adoção (L2CAP) funciona em paralelo com o LMP para transferir dados de nível mais alto para a camada Baseband e vice-versa. A grande diferença entre o L2CAP e o LMP é que o L2CAP fornece serviços à camada mais alta, o que o LMP não faz [7].

Embora o protocolo Baseband forneça tipos de links SCO e ACL, o L2CAP suporta apenas os links ACL. Os pacotes de dados L2CAP podem ter até 64Kb de comprimento [7].

3.5.2.4 O Protocolo Service Discovery - SDP

Os serviços de Descoberta permitem que dois dispositivos Bluetooth diferentes reconheçam e estabeleçam conexões entre si e forneçam a base de cada perfil individual Bluetooth. O protocolo de Serviço de Descoberta (SDP) permite que cada um dispositivo

consulte o outro sobre informações, serviços e características daqueles serviços. Ele também permite o estabelecimento de uma conexão entre aqueles dois dispositivos [7].

3.5.3 O PROTOCOLO DE SUBSTITUIÇÃO DE CABOS

A especificação Bluetooth inclui apenas um protocolo que trata da emulação sem fio de dados normalmente enviados por links baseados em fios – o RFCOMM [7].

3.5.3.1 O Protocolo RFCOMM

O RFCOMM é um protocolo que emula uma conexão serial RS-232 entre dois dispositivos. Em linguagem simples, esse é o protocolo de substituição de cabo. O RFCOMM leva em consideração a emulação de controle RS-232 e sinais de dados pelo Baseband Bluetooth e também fornece recursos de transporte para serviços de nível superior que do contrário utilizariam uma conexão serial como seu mecanismo de transporte [7].

3.5.4 OS PROTOCOLOS TELEPHONY CONTROL

Os protocolos de Controle de Telefonia permitem que dispositivos Bluetooth manipulem chamadas de voz e dados de dispositivos compatíveis com a tecnologia Bluetooth. Para um dispositivo Bluetooth funcionar como um telefone ou um modem, um dos dois protocolos de Telefonia e Controle deve ser implementado na pilha de protocolos de um perfil [7].

3.5.4.1 O Protocolo Telephony Control Specification - Binary

O protocolo de Especificação de Controle de Telefonia - Binário (TCS-BIN) define a sinalização de controle de chamada necessária para estabelecer chamadas de voz e dados entre dispositivos Bluetooth. Ele também define os procedimentos de gerenciamento de mobilidade utilizados para manipular grupos de dispositivos Bluetooth [7].

3.5.4.2 Os Comandos AT

Todos os telefones e modems são controlados por um conjunto de comandos de áudio e telefonia (AT). Os comandos AT são normalmente utilizados para controlar todas as

funções capazes de serem desempenhadas por um telefone ou modem de dados e são comuns entre vários dispositivos e fabricantes [7].

Os comandos AT da tecnologia Bluetooth são utilizados quando um perfil exige que um dispositivo Bluetooth seja empregado como um telefone ou modem quando se conecta a um sistema de telefonia celular ou fixa [7].

3.5.5 OS PROTOCOLOS ADOTADOS

Além dos protocolos anteriores, vários protocolos estabelecidos em outras indústrias têm sido adotados para a utilização na pilha de protocolos Bluetooth. Isso permite que aplicações mais antigas funcionem com a tecnologia Bluetooth mais nova – e que dispositivos Bluetooth se conectem a redes de comunicações globais [7].

3.5.5.1 O Protocolo PPP

O protocolo Ponto a Ponto (PPP), desenvolvido pela IETF, define como os dados do IP são transmitidos pelos links ponto-a-ponto seriais. Esse protocolo é normalmente empregado em conexões de dial-up da Internet ou ao acessar um roteador de rede por meio de uma linha dedicada [7].

No mundo Bluetooth o PPP é executado no protocolo RFCOMM para estabelecer conexões ponto-a-ponto entre dispositivos Bluetooth. E encontra-se o protocolo PPP sendo utilizado nos perfis LAN Access, Dial-Up Networking e Fax [7].

3.5.5.2 Os Protocolos TCP/IP/UDP

Esses três protocolos: TCP, IP e UDP são protocolos tradicionais que definem a maioria das comunicações baseadas na Internet e relacionadas à rede, como também comunicações entre outros tipos de dispositivos e periféricos de computação. A tecnologia Bluetooth adotou esses protocolos para facilitar a comunicação com qualquer outro dispositivo conectado à Internet [7].

Como pode ser visto, esses três protocolos definem funções similares:

TCP: O protocolo de Controle de Transporte (TCP, Transport Control Protocol) define os procedimentos para os dividir dados em pacotes e, depois, reuni-los na outra extremidade da transmissão.

IP: O protocolo de Internet (IP, Internet Protocol) define como os dados são enviados por roteadores para redes diferentes, atribuindo endereços IP exclusivos a dispositivos diferentes.

UDP: O protocolo Usuário de Datagrama (UDP, User Datagram Protocol) é menos amplamente utilizado do que os protocolos TCP/IP, visto que só transmite mensagens individuais para o IP em uma base de tentativas, sem a entrega garantida [7].

3.5.5.3 O Protocolo OBEX

Dados são trocados essencialmente entre dois dispositivos que utilizam um modelo cliente/servidor. A tecnologia Bluetooth adotou o protocolo de Troca de Objetos ou Dados (OBEX) inicialmente definido pela Associação de Dados Infra-vermelho (IrDA) pra facilitar a troca de objetos de dados entre dispositivos diferentes [7].

O protocolo OBEX não só permite a troca de dados entre dois dispositivos, mas também define um objeto listagem-de-pastas, que pode ser usado para examinar os conteúdos de pastas que residem em um dispositivo remoto [7].

3.5.5.4 O Protocolo Comunicações de Infra-Vermelho Móveis - IrMC

O protocolo Comunicações de Infra-vermelho Móveis (IrMC), também desenvolvido pela IrDA, funciona em combinação com o OBEX para sincronizar a troca de objetos de dados entre dispositivos diferentes [7].

3.5.5.5 O Protocolo de Aplicação sem Fio - WAP

O protocolo de Aplicação sem Fio (WAP) é utilizado para implementar os serviços de Internet em telefones celulares digitais e em outros pequenos dispositivos sem fios. É um protocolo que provê a um telefone móvel a capacidade de navegar pela Web e recuperar correio eletrônico e outras informações baseadas na Internet [7].

3.5.5.6 O Protocolo de Ambiente de Aplicação sem Fios - WAE

O protocolo de Ambiente de Aplicação sem Fios (WAE) fornece uma variedade de aplicações de softwares para utilização em telefones e PDAs compatíveis com o WAP. As aplicações podem ser baseadas em clientes (denominadas WAE de Agentes de Usuário) ou em servidores (denominadas Geradores Contente) [7].

3.6 PACOTES

Cada pacote usa um formato fixo começando com 72 bits de código de acesso derivados da identidade do dispositivo mestre, que é o único para o canal [9].

Na Figura 20 cada pacote troca no canal esse código de acesso. Cada receptor na piconet compara o código de um pacote que armazenou o código de acesso; se eles não coincidirem, o resto do pacote é ignorado. Alem disso, o código de acesso é de importância para a sincronização. Então, um cabeçalho do pacote (packet header) segue e finalmente 0 – 2.745 bit payload é enviado [9].

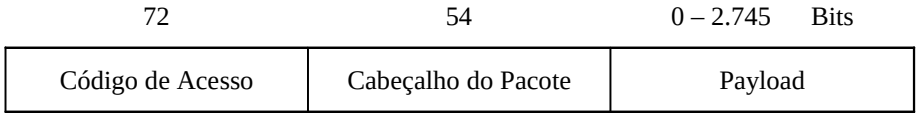


Figura 20 - Formato de um cabeçalho de pacote Bluetooth [9]

O cabeçalho do pacote começa com três bits MAC address, por isso, uma piconet pode conter no máximo um mestre e sete escravos. 4 bits definem o tipo de pacote, logo dezesseis tipos de links podem ser definidos. Existe um bit de confirmação (acknowledgement - ACK) e não confirmação (negative acknowledgement - NACK). Se a confirmação de pacotes é requerida, o Bluetooth envia essa confirmação num slot seguido do dado (TDD). Assim, é suficiente usar uma simples alternativa de bit protocol com uma única seqüência de bits numéricos (SEQN) e confirmação numérica (ARQN). Alem disso, 18 bits de informação do cabeçalho requerem 54 bits no pacote. Bluetooth define quatro pacotes de controle:

- ID ou identificação de pacotes: Consiste no código de acesso; usado para sinalização.
- Null packet (Pacote Nulo): Tem um código de acesso e um cabeçalho de pacote; usado se o link de controle de informação carregado pelo cabeçalho de pacote tivesse sido transmitido.
- Poll packet: Similar ao Null; usado pelo mestre para forçar os escravos retornarem a responder.
- FHS packet: Um FH-sincronização de pacote; usados para mudar o tempo real do clock e a identidade de informação entre as unidades; contém todas as informações para pegar duas unidades sincronizadas [9].

3.7 SEGURANÇA

Sinais de rádio podem ser facilmente interceptados, por isso é importante que os dispositivos Bluetooth disponíveis sejam seguros para prevenir mensagens de origem não autorizada, acesso a dados importantes ou que suas conversas sejam ouvidas sem autorização. Os seguintes níveis de segurança fazem com que a tecnologia Bluetooth alcance esse objetivos básicos. **A autenticação**, a qual evita o recebimento de mensagens de origem duvidosa e acessos não desejados a dados, é função importante. **A criptografia**, a qual evita escutas não autorizadas, mantém a privacidade do canal. O fato do alcance de transmissão dos dispositivos Bluetooth estar limitado a 10 m ajuda na prevenção de escutas. Há três modos de segurança que cobre a funcionalidade e aplicação do dispositivo [9].

3.7.1 SEM SEGURANÇA

Este modo é usado com dispositivos que não tenham aplicações críticas. Isto passa as funções do nível de segurança, sendo os dados sem importância vital facilmente acessados. A troca automática de cartões de negócio eletrônico, é um típico exemplo de transferência de dados sem segurança [9].

3.7.2 SEGURANÇA NO NÍVEL DE SERVIÇO

Este modo permite procedimento de acesso versátil, especialmente para acionar aplicações com diferentes níveis de segurança em paralelo [9]. É estabelecida após a conexão [7].

3.7.3 SEGURANÇA NO NÍVEL DE LINK

Neste modo, o nível de segurança é o mesmo para todas as aplicações, para cada conexão que é iniciada. Embora menos flexível, este modo é adequado para manter o nível comum de segurança, e é mais fácil de implementar que o modo anterior [9]. É estabelecida antes da conexão [7].

4 INTEGRAÇÃO BLUETOOTH E TCP/IP

A integração entre o Bluetooth e TCP/IP é promovida através de perfis diferentes: o primeiro que é atualmente mais utilizado promove-se através do protocolo PPP e o RFCOMM que serve como uma ponte entre a especificação Bluetooth e o TCP/IP. Para o primeiro perfil será utilizado no modelo BlueWINTM - rede sem fio do Bluetooth em recinto fechado que foi produzido pela Companhia de Tecnologia Initium; o segundo ainda não está totalmente definido sendo alvo de muitos estudos principalmente pelo Grupo Bluetooth SIG (Ericsson, Nokia, Toshiba, IBM, Intel, 3Com, Lucent Technologies, Microsoft e Motorola), ele acontece através do protocolo L2CAP diretamente com o TCP/IP. O propósito é fazer um estudo de caso do dois perfis, mostrando como se dá a integração através de protocolos. A implementação dessas integrações ficará como projeto futuro, devido a necessidade de se utilizar tecnologia de ponta a qual não se dispõem, da demanda de um tempo muito extenso e também um alto custo

Ambos os perfis definem especificações detalhadas para dispositivos Bluetooth habilitados terem acesso a uma rede local e a Internet. O segundo perfil LAN Access foi desenvolvido para implementar o modelo de uso LAN de Acesso. Também é utilizado para a implementação baseada em rede local do modelo Internet Bridge – Pontes para Internet.

Nesse perfil, diversos terminais de dados utilizam um ponto de acesso de rede local como uma conexão sem fio a uma rede local. Uma vez conectados, os terminais de dados operam como se eles estivessem conectados à rede local por meio da rede dial-up tradicional e podem acessar todos os serviços fornecidos pela rede .

4.1 BLUEWINTM - REDE SEM FIO DO BLUETOOTH – LAN ACCESS

Agora o serviço de alcance pode ser estendido, criando uma célula em rede em um recinto fechado sem fios, o BlueWINTM fará a rede mais acessível e permitirá assim que usuários de Bluetooth possam levar vantagens na *Web-based* utilizando seus recursos. Este modelo utiliza os protocolos PPP e RFCOMM como ponte para a integração Bluetooth e TCP/IP, esta ponte através de outros modelos é a mais utilizada pelos dispositivos Bluetooth para acesso à Internet [10].

4.1.1 HANDOVER DE BLUETOOTH EM BLUEWINTM

O perfil LAN Access define o acesso de rede que usa o PPP em cima de RFCOMM que é o Protocolo de Emulação Serial de Cabo do Bluetooth, após a utilização do PPP, este se comunica com o IP e o RFCOMM comunica-se com o L2CAP, a Figura 21 mostra como é a disposição desses protocolos. A propósito o BlueWINTM funciona de acordo com o perfil que utiliza o PPP e o RFCOMM como ponte de integração [10].

A comunicação entre os protocolos se dá de forma que cada um pega os segmentos de dados armazena em seu buffer e depois transmiti a camada seguinte com seu cabeçalho específico, a direção do tráfego dos dados pode ser dos protocolos de nível superior para os de nível inferior ou vice-versa. Esta comunicação entre estes protocolos será melhor definida no segundo perfil de integração que será visto no item 4.2.

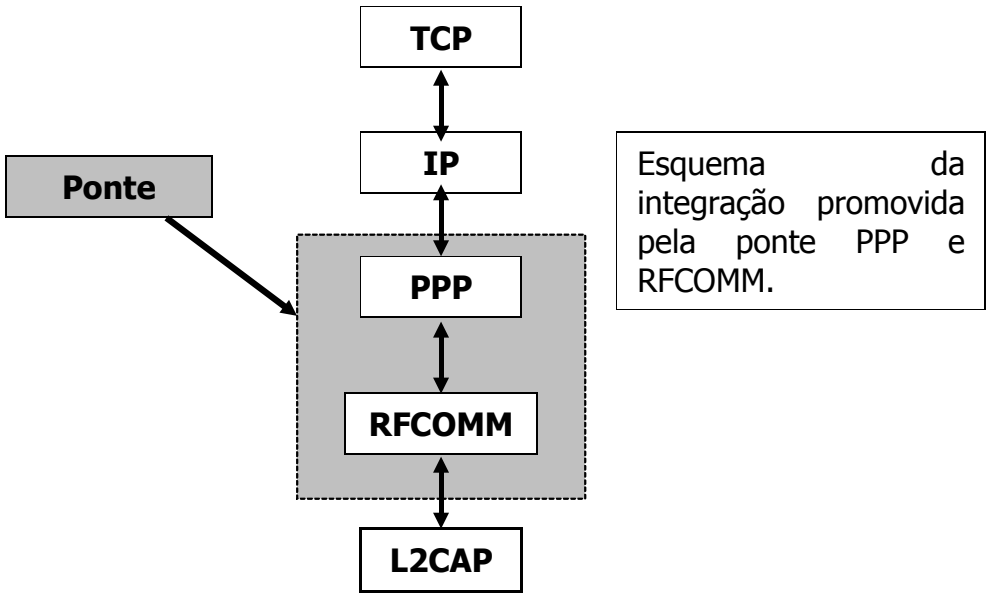


Figura 21 - Pilha de protocolos do Perfil LAN Access [10]

4.1.2 ESTRUTURA DE BLUEWINTM

BlueWINTM habilita dispositivos móveis equipados com um módulo de Bluetooth para conectar o IP-based de rede. Está composto de três elementos funcionais: agente de handover, pontos de acesso, e dispositivos móveis, como descrito na Figura 22. Os papéis e comportamento dos elementos são projetados para adequar-se basicamente ao perfil da LAN de acesso e ao cenário de ponto de acesso de rede do perfil de PAN, e é estendido para apoiar handover. O agente de handover se comporta como um portal entre a rede local e a Internet. Também representa o papel de Agente Estrangeiro definido em IP móvel, administra informação sobre os pontos de acesso e atualmente conecta e dirige pacotes para dispositivos móveis [10].

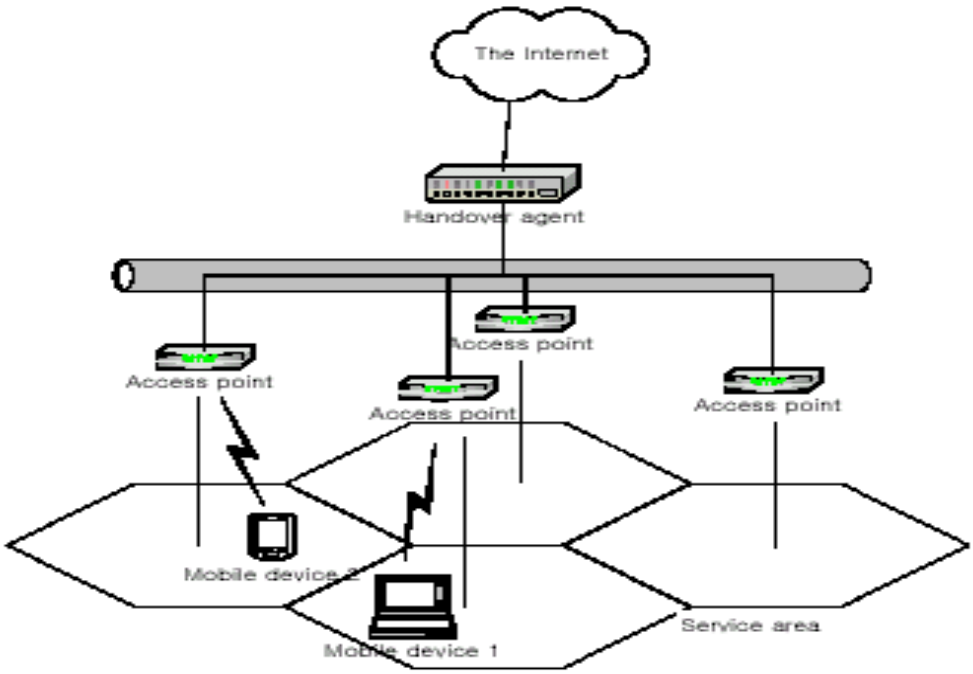


Figura 22 - BlueWINTM [10]

Quando um dispositivo móvel faz uso do perfil de acesso LAN, usa PPP de tunelamento. Servidores de PPP executam programas no agente de handover em lugar dos pontos de acesso. O ponto de acesso simplesmente transfere pacotes PPP entre os dispositivos móveis e o agente de handover [10].

Quando um dispositivo móvel usa o perfil de PAN, o agente de handover mantém uma tabela marcando pares de dispositivos contendo endereços IP e os pontos de acesso atualmente conectados a eles. A mesa é atualizada depois de um handover ser bem sucedido [10].

Pontos de acesso e o agente de handover são conectados por uma rede sem fio como a Ethernet. São instalados em posições predeterminadas para prover cobertura contínua ao longo de uma área de serviço. Dispositvos móveis e dispositivos portáteis são Bluetooth-habilitados com a pilha de protocolos TCP/IP. Esses dispositivos têm acesso à rede conectando-se a um ponto de acesso, a informação sobre as localizações relativas dos pontos de acesso no sistema de rede de comunicação é necessária para o método de handover.Esta informação de localização para pontos de acesso é armazenada em um banco de dados no

agente de handover e enviada aos pontos de acesso sempre que um novo ponto é conectado pela primeira vez ao agente de handover [10].

4.2 INTEGRAÇÃO BLUETOOTH (L2CAP) E TCP/IP

Um dos perfis de integração entre Bluetooth e TCP/IP é promovido através de protocolos dessas tecnologias como: TCP e o IP no caso do TCP/IP e L2CAP no Bluetooth. No caso descrito nos itens seguintes será utilizado apenas o Link Assíncrono Sem-Conexão (Asynchronous Connection-less – ACL), devido que o L2CAP suporta somente este tipo de pacote que é reservado somente a dados. A utilização desse perfil de integração vai colaborar para que uma transmissão seja mais rápida, por não precisar passar pela ponte (PPP e RFCOMM), além da implementação deste modelo de integração ser mais fácil.

4.2.1 MODELO PROPOSTO

Um modelo de transmissão contém Bluetooth e TCP/IP. A rede modelada foi uma piconet em Bluetooth com dois nodos. Os dois nodos podem ser por exemplo um laptop e um servidor, como na Figura 23 [11].

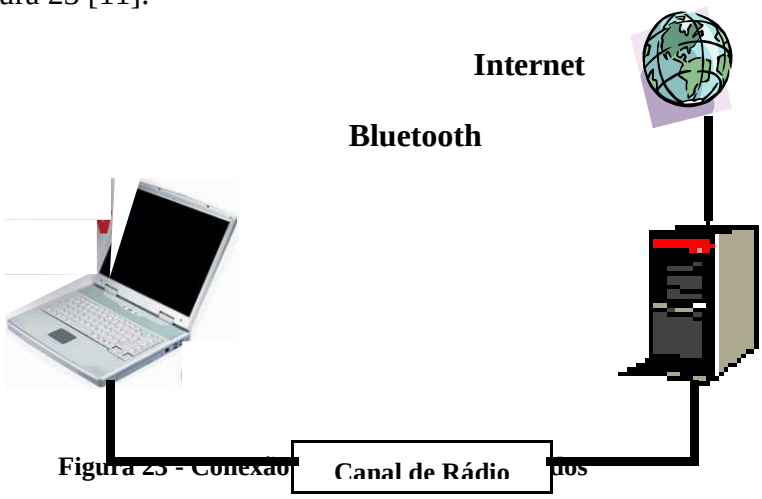


Figura 23 - Conexão [illegible]dos

Neste modelo a integração entre o Bluetooth e a pilha de protocolos TCP/IP será direta sem a necessidade de se utilizar a ponte com os protocolos PPP e RFCOMM. Na Figura 24 será mostrado como fica a disposição dos protocolos sem esta ponte.

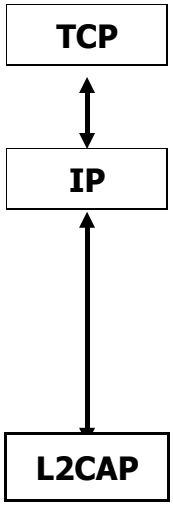


Figura 24 - Integração direta TCP/IP e Bluetooth (L2CAP) [11]

4.2.1.1 Processo de Chegada

O processo de chegada determina como a camada de aplicação entrega os dados à camada TCP. Os processo de chegada podem definir a combinação TCP/IP e Bluetooth, sendo que o processamento de um canal Bluetooth tem seus segmentos enviados pelo mecanismo de janela TCP. São utilizados dois processos de chegada diferentes:

1) Utiliza-se meios de processamento máximo para o sistema, sendo que a camada TCP sempre tem que ter dados para enviar. A taxa de chegada de dados de aplicação sempre é alta, tendo que se ordenar as filas a serem preenchidas na camada TCP;

2) Neste segundo caso o processo é modelado por um Processo Interrompido de Bernoulli (IBP), i.e. para um período geometricamente distribuído (estado ativo) as chegadas acontecem de acordo com um processo de Bernoulli. Teste período é seguido por outro período (estado inativo) durante qual nenhuma chegada acontece. Estando no estado ativo, ele ficará ativo com probabilidade 1 – p ou irá para o estado inativo com probabilidade p. Se o processo estiver no estado inativo ficará com probabilidade 1 – q ou irá para o estado ativo com probabilidade q. Quando em estado ativo, uma abertura contém um pacote com probabilidade igual

a 1. Após algum tempo são alinhadas aberturas para os geradores de tráfico como as aberturas de tempo para uma piconet modelada [11].

O Bluetooth possui um vínculo assimétrico de máximo 721 Kbps em uma direção, enquanto permite 57.6 Kbps na direção de retorno, ou um vínculo simétrico de 432.6 Kbps duplex. Para se achar um processamento máximo (goodput) em cima de um canal Bluetooth interrompido, gera-se segmentos de dados de forma que um segmento para ser enviado, deve sempre utilizar o mecanismo de janela TCP permitido [11].

4.2.1.2 Procedimentos de transmissão

A camada de aplicação de através de um transmissor gera segmentos de dados de acordo com algum processo de chegada. Os segmentos são diretamente transmitido à camada TCP. Esses segmentos são colocados no buffer do TCP remetente onde serão atrasados (Dtcp). Esta demora modela o processo que se precisa, formando um cabeçalho de TCP. Conforme Figura 25 [11].

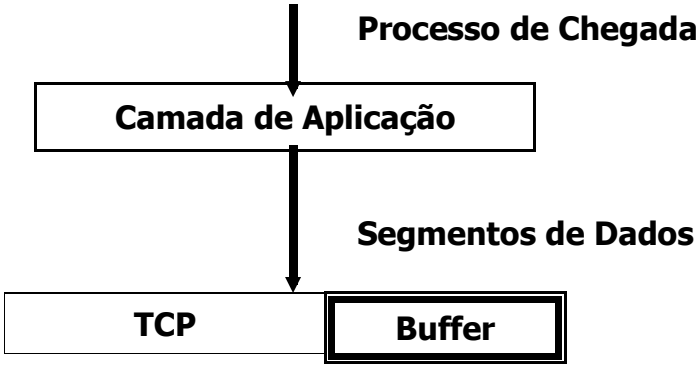
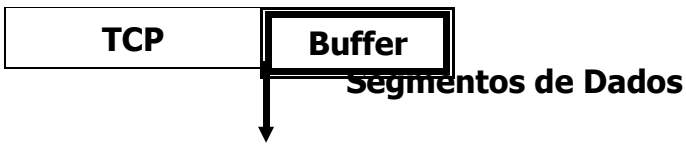


Figura 25 - Transmissão de dados entre Camada de Aplicação e TCP [11]

Quando o cabeçalho é formado o TCP removerá os segmentos do buffer e os enviará à camada IP. Na camada IP, os segmentos são colocados no buffer do IP remetente. Em intervalos de duração regulares o IP (Dip) remove um segmento do buffer e envia-o ao L2CAP, conforme mostrado na Figura 26 [11].



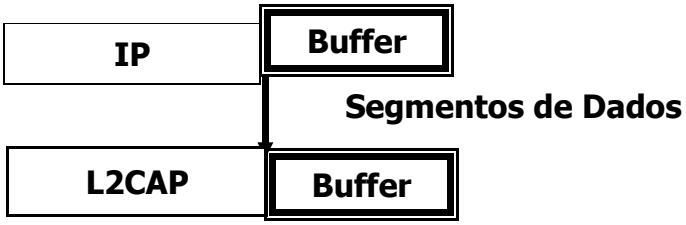


Figura 26 - Transmissão de dados entre TCP, IP e L2CAP [11]

Os segmentos são postos no buffer do L2CAP do remetente. O L2CAP remove os segmentos em intervalos regulares de alguns milisegundos (Dl2cap); divide o segmento em pacotes de Bluetooth e os envia ao buffer do Bluetooth Baseband remetente. O Baseband será o responsável pela transmissão dos pacotes, pois permite a conexão de freqüência de rádio através do canal de rádio, entre as duas unidades Bluetooth (laptop e o servidor). Podem ser perdidos pacotes de Baseband transmitidos devido a pedaços com erros. Quando a camada Baseband do receptor recebe um pacote correto este também é atrasado alguns milisegundos (Dbase) e enviado ao buffer do L2CAP do receptor onde será atrasado outros milisegundos (Dl2cap). Esse esquema é demonstrado na Figura 27 [11].

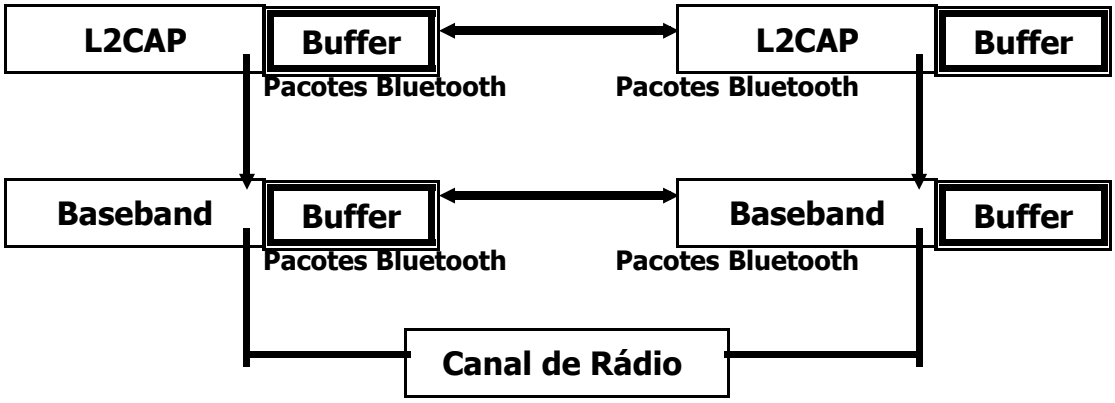


Figura 27 - Transmissão de dados do L2CAP para Baseband e Vice-versa [11]

Por sua vez na Figura 28 o L2CAP junta (transforma) os pacotes de Bluetooth em TCP/IP, segmenta e envia-os para o buffer do IP do receptor. Em intervalos regulares, a camada de IP remove um segmento do buffer e envia-o à camada de TCP do receptor onde é colocado em seu buffer [11].

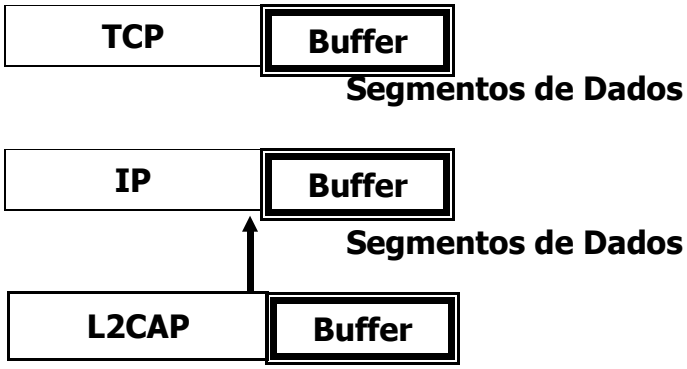


Figura 28 - Transmissão de dados entre L2CAP, IP e TCP [11]

Quando o TCP envia um ACK (reconhecedores) para um segmento, o segmento é removido do buffer e é enviado à camada de aplicação, mostrado na Figura 29. Os ACKs são apoiados em segmentos de TCP que entram na direção oposta. De acordo com TCP, os ACKs são enviados separadamente só se estes estão atrasados, ou se dois ou mais segmentos de TCP estão esperando para serem reconhecidos. É aconselhável usar um tempo maior para a transmissão de dados de um pacote não codificado por exigirem um processamento ideal maior [11].

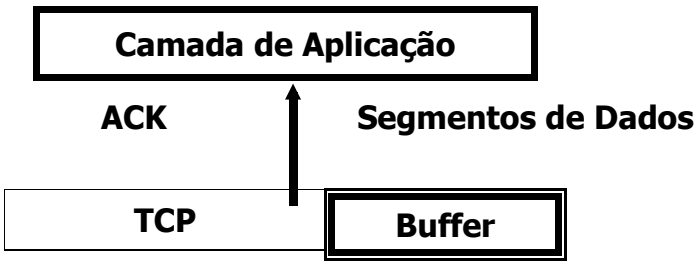
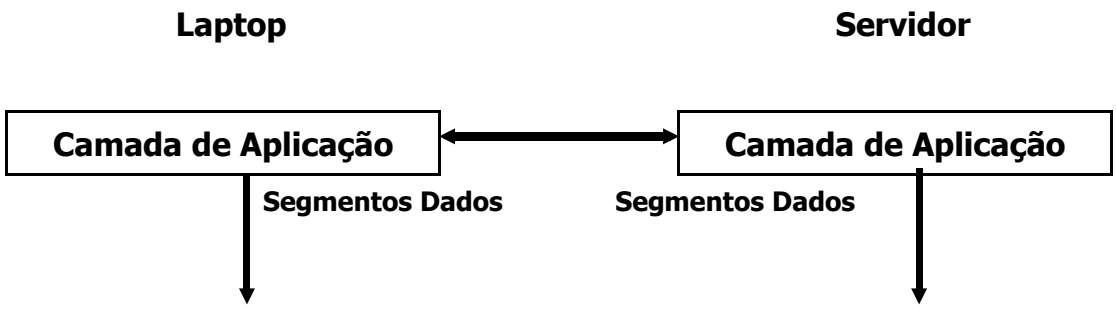


Figura 29 - Transmissão de dados entre TCP e a Camada de Aplicação [11]

Demonstrado passo a passo com se dá a comunicação entre as camadas e o que acontece com os dados durante o tráfego será mostrado um esquema completo dessa comunicação observando a direção da transmissão: do laptop para o servidor e do servidor para o laptop, conforme o mostrado na Figura 30 [11].



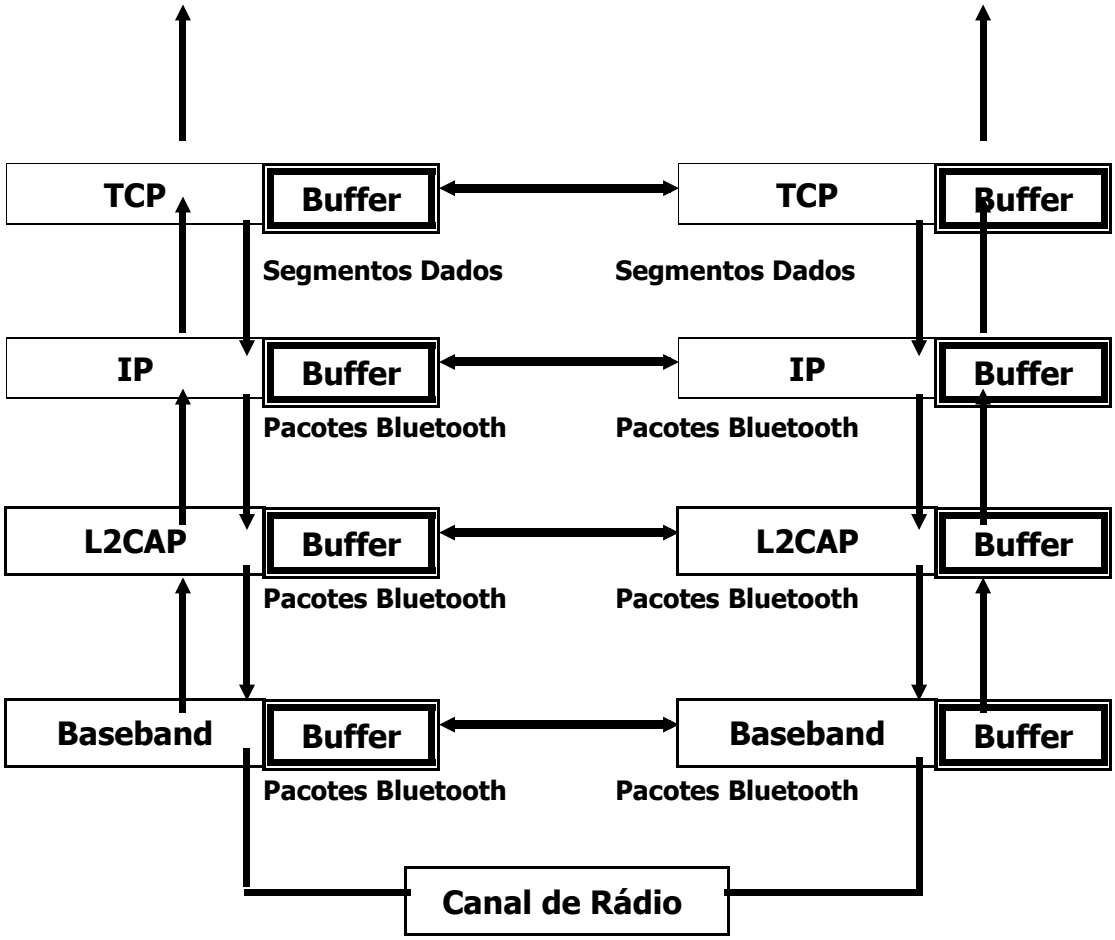


Figura 30 - Esquema Geral da Integração Direta [11]

4.2.1.3 Formatos de Pacote de Dados

Um pacote que chega às camadas do Bluetooth consiste em três partes, Figura 31: Um cabeçalho de TCP, um cabeçalho de IP e payload [11].

	Cabeçalho TCP	Cabeçalho IP	Payload
12	20	20	1429

Figura 31 - Pacote nas camadas Bluetooth [11]

L2CAP coloca 4 bytes como identificação de canal e duração de pacote. Decidiu-se usar um tamanho de pacote com cerca de 1500 bytes (i.e tamanho de pacote - Ethernet) para evitar possíveis problemas com o número de pacotes Bluetooth a serem ajustados [11].

O cabeçalho do TCP é de 32 bytes em vez do normal 20 bytes, os 12 bytes extras são necessários para os cálculos do tempo de ida e volta (RTT) do pacote. O cabeçalho do IP é de 20 bytes. Com um payload de 1429 bytes, onde o pacote total tem tamanho de 1485 bytes, como visto na Figura 32, e o pacote ajusta-se em 55 pacotes de Bluetooth [11].

	Cabeçalho TCP	Cabeçalho IP	Payload	L2CAP
12	20	20	1429	4

1485 bytes

Figura 32 - Pacote total [11]

Normalmente, os reconhecedores (ACKs) são pegam carona em segmentos de TCP que entram na direção oposta. Quando um ACK separado é enviado, vai consistir em um cabeçalho com 56 bytes. Um ACK separado é dividido em 3 pacotes DH1 [11].

4.2.1.4 Modelo de Parâmetros

O modelo de parâmetros é mostrado na Tabela 4. O Tamanho de Segmentos de Dados (DSS) vem descrito no payload com 1429 bytes. Foram fixados parâmetros que possuem valores realistas para este sistema [11].

Tabela 4 - Modelo de Parâmetros [11]

Parâmetros	Valor
Tamanho de Segmentos de Dados (DSS)	1429 bytes
Janela do Receptor de Máximo (Max rwnd)	12 segmentos, i.e 17.148 Kbytes
Tamanho total do buffer nas camadas do Bluetooth	15 Kbytes
Demora de segmento na camada de TCP (DTCP)	1 µs

Demora de segmento na camada de IP (DIP)	1 µs
Demora de segmento na camada L2CAP (DL2CAP)	1 ms
Demora de segmento na camada Baseband (DBase)	1 ms

5 CONCLUSÃO

Com o advento de novas tecnologias de rede como o Bluetooth faz-se necessário sua utilização em serviços que necessitem principalmente da Internet, surgindo a partir disto a necessidade de se integrar esta tecnologia com o conjunto de protocolos TCP/IP que foram projetados especialmente para serem protocolos utilizados na Internet.

Os dois perfis de integração estudados suprem a necessidade do Bluetooth de fazer o acesso à Internet, sendo que o primeiro perfil mesmo sendo uma ponte através do protocolo PPP e o RFCOMM satisfaz as necessidades de acesso. O segundo perfil mesmo não estando completamente pronto mostra-se mais prático e fácil de se implementar, sendo ele também o perfil de integração que tem o menor tempo de transmissão de dados (ida e volta) de um dispositivo ao outro.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] COMER, Douglas E. – **Interligação em Rede com TCP/IP – Volume I Princípios, Protocolos e Arquitetura** / Douglas E. Comer: Tradução da Terceira Edição. Rio de Janeiro: Editora Campus, 1998

[2] **Internet e Arquitetura TCP/IP – Volume I,** http://www.gta.ufrj.br/7Evidal/ip/indice.html - acessado em 10/09/2003

[3] TANENBAUM, Andrew S.,1944 – **Redes de Computadores** / Andrew S. Tanenbaum: Tradução da Terceira Edição do original. Rio de Janeiro: Editora Campus, 1997.

[4] **Protocolos de Rede TCP/IP -** www.fe.up/~mricardo/cm/ - acessado em 10/09/2003

[5] **Protocolos de Rede (Internet) -** www.oit.umass.edu/helpscript/display.cgi/doc_id=834 - acessado em 13/09/2003

[6] **Pilha de Protocolos TCP/IP** – www.geocities.com/philipappleyaduk/tcp.html - acessado em 17/08/2003

[7] MILLER, Michael – **Descobrindo Bluetooth** / Michael Miller: Lançado em outubro de 2001: Editora Campus.

[8] **The Bluetooth SIG**, www.bluetooth.com - acessado em 10/04/2003

[9] **Bluetooth** - www.gta.ufrj.br/publicações - acessado em 05/06/2003

[10] **JOHANSSON**, Niklas, **KIHL**, Maria e **KÖRNER**, Ulf. **TCP/IP over the Bluetooth Wireless Ad-hoc Network** - Department of Communication Systems, Lund University, Sweden niklasj.Maria.ulfk@telecom.th - acessado em 29/10/2003

[11] **Hyun**-Sang Jang Ph.D. VP/CTO Initium Co. Ltd. hsjang@initium.co - acessado em 05/11/2003