题目：无线自组网按需距离向量路由协议代码分析

小组成员：杨韬，叶上维，徐文博

分工：

目录

[1. 基本原理 5](#_Toc534027986)

[1.1 概述 5](#_Toc534027987)

[1.2 特点 5](#_Toc534027988)

[1.3 AODV控制帧 5](#_Toc534027989)

[1.3.1 RREQ路由请求帧 6](#_Toc534027990)

[1.3.2 RREP路由应答帧 7](#_Toc534027991)

[1.3.3 RERR路由错误帧 8](#_Toc534027992)

[1.3.4 RREP\_ACK路由应答确认帧 8](#_Toc534027993)

[1.4 AODV用户态工作流程 8](#_Toc534027994)

[1.4.1 路由发现过程 9](#_Toc534027995)

[1.4.2 路由维护和错误控制 10](#_Toc534027996)

[1.4.3 拥塞控制 10](#_Toc534027997)

[1.4.4 序列号机制 11](#_Toc534027998)

[1.4.5 前驱节点机制 11](#_Toc534027999)

[1.5 用户空间和内核模块的交互 11](#_Toc534028000)

[2. 代码介绍 12](#_Toc534028001)

[2.1 用户态全局变量 13](#_Toc534028002)

[2.1.1 路由表项 13](#_Toc534028003)

[2.1.2 全局链表结构 14](#_Toc534028004)

[2.1.3 全局目的地链表结构 14](#_Toc534028005)

[2.1.4 全局定时器队列 15](#_Toc534028006)

[3. 内核空间函数解读 15](#_Toc534028007)

[3.1 Linux钩子函数简介 15](#_Toc534028008)

[3.2 内核空间对数据包处理流程 16](#_Toc534028009)

[3.3 kaodv-mod.c 17](#_Toc534028010)

[3.3.1 kaodv\_hook-aodv-钩子函数 17](#_Toc534028011)

[3.3.2 kaodv\_update\_route\_timeouts-更新expl\_entry结构和通知用户进程更新用户空间的维护的路由表 20](#_Toc534028012)

[3.3.3 其他函数 20](#_Toc534028013)

[3.4 kaodv-netlink.c 21](#_Toc534028014)

[3.4.1kaodv\_netlink\_build\_msg-创建sk\_buff结构体 21](#_Toc534028015)

[3.4.2 kaodv\_netlink\_receive\_peer-内核收到消息后的处理的方式 22](#_Toc534028016)

[3.4.3其他函数 23](#_Toc534028017)

[3.5 kaodv-expl.c 23](#_Toc534028018)

[3.6 kaodv-ipen.c 24](#_Toc534028019)

[3.6.1 ip\_pkt\_encapsulate-IP数据包封装 24](#_Toc534028020)

[3.6.2 ip\_pkt\_dncapsulate-IP数据包解封装 25](#_Toc534028021)

[3.6.3 其他函数 26](#_Toc534028022)

[3.7 kaodv-queue.c 26](#_Toc534028023)

[3.7.1 kaodv\_queue\_set\_verdict-队列裁决函数 26](#_Toc534028024)

[4. 用户态函数解读 27](#_Toc534028025)

[4.1 main函数 27](#_Toc534028026)

[4.2 main函数文件内其他函数以及变量的定义： 31](#_Toc534028027)

[4.3 AODV\_socket.c 32](#_Toc534028028)

[4.3.1 aodv\_socket\_init函数-套接字初始化函数 32](#_Toc534028029)

[4.3.2 aodv\_socket\_read函数-套接字读取 34](#_Toc534028030)

[4.3.3 aodv\_socket\_process\_packet函数-处理数据包函数 36](#_Toc534028031)

[4.3.4 recvAODVUUPacket函数-接收AODVUUPacket 37](#_Toc534028032)

[4.3.5 aodv\_socket\_send函数-套接字发送函数 38](#_Toc534028033)

[4.3.6 aodv\_socket\_new\_message函数 40](#_Toc534028034)

[4.3.7 aodv\_socket\_queue\_msg函数 41](#_Toc534028035)

[4.3.8 aodv\_socket\_cleanup函数 41](#_Toc534028036)

[4.4 AODV\_rreq.c 41](#_Toc534028037)

[4.4.1 rreq\_process函数-处理rreq消息 41](#_Toc534028038)

[4.4.2 rreq\_route\_discovery函数-路由发现过程 45](#_Toc534028039)

[4.4.3 其他函数 47](#_Toc534028040)

[4.5 AODV\_rrep.c 47](#_Toc534028041)

[4.5.1 rrep\_ack\_process函数 47](#_Toc534028042)

[4.5.2 rrep\_send函数-发送rrep消息 48](#_Toc534028043)

[4.5.3 rrep\_forward函数-转发rrep消息 49](#_Toc534028044)

[4.5.4 rrep\_process函数-处理rrep消息 49](#_Toc534028045)

[4.5.5 其他函数 52](#_Toc534028046)

[4.6 aodv\_rerr.c 53](#_Toc534028047)

[4.6.1 rerr\_create函数-创建 53](#_Toc534028048)

[4.6.2 rerr\_add\_udest函数-添加 53](#_Toc534028049)

[4.6.3 rerr\_process函数-处理 53](#_Toc534028050)

[4.7 aodv\_hello.c 56](#_Toc534028051)

[4.7.1 hello\_jitter()函数-设置jitter值 56](#_Toc534028052)

[4.7.2 hello\_start()函数-启动hello消息 56](#_Toc534028053)

[4.7.3 hello\_stop()函数-停止hello消息 57](#_Toc534028054)

[4.7.4 hello\_send()函数-发送hello消息 57](#_Toc534028055)

[4.7.5 hello\_process()函数-处理hello消息 60](#_Toc534028056)

[4.7.6 hello\_update\_timeout()函数-更新timeout 61](#_Toc534028057)

[4.8 Nl.c 62](#_Toc534028058)

[4.8.1 Nl\_init函数-初始化函数 62](#_Toc534028059)

[4.8.2 Nl\_kaodv\_callback函数-根据aodv套接字中收到的不同命令，执行不同的回调函数 63](#_Toc534028060)

[4.8.3 Nl\_rt\_callback函数-根据路由套接字中收到的不同命令，执行不同的回调函数 67](#_Toc534028061)

[4.8.4 Nl\_send函数-发送数据包给内核模块 68](#_Toc534028062)

[4.8.5 Nl\_kern\_route函数-操作内核路由表，包括增加、修改、删除路由表条目等操作 69](#_Toc534028063)

[4.8.6 Nl\_send\_add\_route\_msg函数-向内核发送一个添加一个路由信息的消息，包括目的地地址、下一跳，生存期，路由状态标志，网络接口等 70](#_Toc534028064)

[4.8.7 其他函数 70](#_Toc534028065)

[4.9 Aodv\_neighbor.c 71](#_Toc534028066)

[**3.10.1更新活跃的邻居节点（更新来自非HELLO AODV控制消息的邻居）（void NS\_CLASS neighbor\_add）** 71](#_Toc534028067)

[3.10.2邻居节点链路中断情况（void NS\_CLASS neighbor\_link\_break） 72](#_Toc534028068)

[3.11 Aodv\_timeout.c 73](#_Toc534028069)

[3.11.1定义定时器到期时调用的超期函数 73](#_Toc534028070)

[3.11.2.定义本地修复超时处理函数 74](#_Toc534028071)

[3.11.3.设置路由过期超时函数 74](#_Toc534028072)

[3.11.4.路由删除函数设置 74](#_Toc534028073)

[3.11.5.HELLO消息超时函数 75](#_Toc534028074)

[3.11.6响应超时函数 75](#_Toc534028075)

# 基本原理

## 概述

AODV协议(Ad hoc on-demand distance vector routing)是应用于无线自组织网络中进行路由选择的路由协议,它能够实现单播和多播路由。该协议是自组织网络中按需生成路由方式的典型协议。用于特定网络中的可移动节点。它能在动态变化的点对点网络中确定一条到目的地的路由，并且具有接入速度快，计算量小，内存占用低，网络负荷轻等特点。它采用目的序列号来确保在任何时候都不会出现回环（在路由控制信息出现异常的时候也是如此），避免了传统的距离向量协议中会出现的很多问题。

在实现方面，AODV分为内核模块和用户用户空间两部分，内核模块。主要负责维护一个expl\_entry结构的数组，其中包括目的地，下一条，超时时间等，类似于路由表。用户空间负责接收来自其他节点的消息，更新用户空间维护的路由表，和通知内核更新路由表。需要注意的是，整个AODV协议一共涉及到三个路由表，分别是用户空间的路由表，结构相对复杂，AODV内核模块维护的路由表，结构较为简单，Linux内核维护的路由表。 所以用户空间需要建立两个和内核联系的套接字，分别对应在内核的两个路由表。在3.2中，我们将详细阐述数据包如何在内核模块处理的。

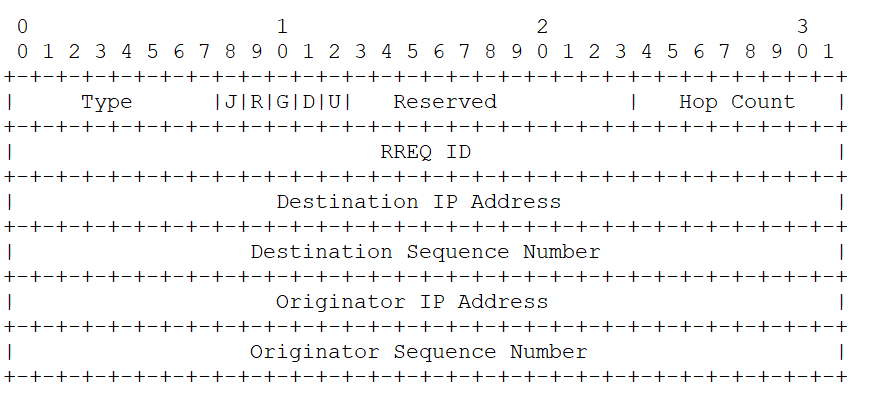
## 特点

1. AODV协议采用的基本路由算法为距离向量算法，但有所改进。
2. AODV协议是按需路由协议。也就是说，只有在主机需要的时候才会激发出路由寻找过程。
3. AODV采用UDP封装，属于应用层协议。每次寻找路由时都要触发应用层协议，增加了实现的复杂度。
4. IEEE 802．15．4规定的帧大小为127字节，MAC头部及尾部校验最多使用了25字节，IPv6头部与UDP头部占用 48字节，只剩下54字节的空余。
5. LR—WPAN中，拓扑结构相对简单，网络的规模相对较小，节点的位置不固定，对它的设计首先要考虑的因素是简单、节能等问题。AODV的路由框架和报文设计并没有考虑这些问题。

## AODV控制帧

AODV控制帧主要包括RREQ路由请求帧、RREP路由应答帧、RERR路由错误帧、RREP\_ACK路由应答确认帧、HELLO活跃路由链路检测帧。其中HELLO帧其实是TTL=1的RREP路由请求帧。

### RREQ路由请求帧



具体每个字段含义如下：

Type 1（这个字段填写帧的类型，1代表RREQ，2:RREP,3:RERR）

J 加入标志; 为多播保留

R 修复标志，为多播保留

G Gratuitous RREP flag; 决定了是否向目标节点地址域指定的节点发送一个免费路由回复消息

D Destination only flag; 决定了是否只允许目标节点回复本条路由请求帧

U Unknown sequence number; 指示目标节点序列号未知.

Reserved 置为0，接受时忽略此字段

Hop Count 从源节点到包处理节点的跳数

RREQ ID 唯一标识一个从源IP节点发出的RREQ请求帧

Destination IP Address

目的地IP地址

Destination Sequence Number

源IP节点在其路由表能找到的最大的目的IP的序列号

Originator IP Address

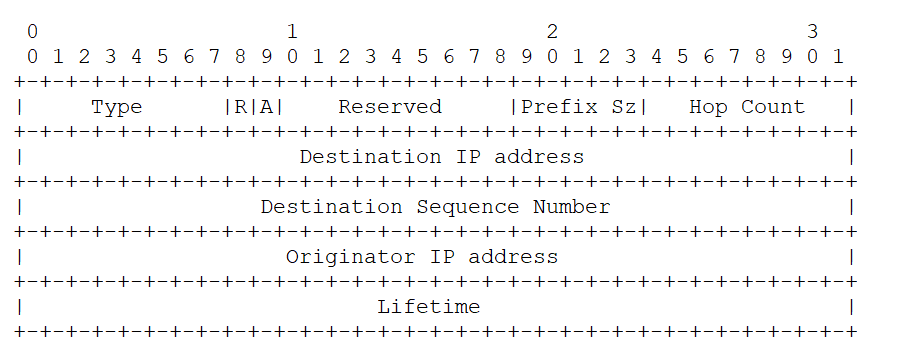
源IP地址，发起路由请求的节点IP地址

Originator Sequence Number

源IP地址的序列号

在源节点发送RREQ路由请求时，它会将种类，和关键字填好，设置一个RREQ ID来唯一标识这个包。从路由表中寻找目的IP最大的序列号填入，自己的序列号填入。当中间节点收到RREQ帧时，通过读取RREQ ID就可以知道之前有没有收到过这次路由请求。然后把HOP Count加1，转发出去。直到目的节点收到这个包。

### RREP路由应答帧



相同的字段就不再重复介绍了，介绍独有的：

R Repair flag; 修复标志，用于广播

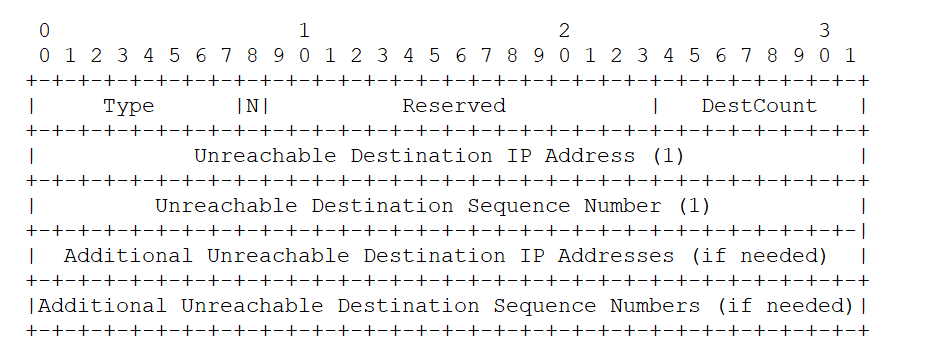
A Acknowledgment required;需要确认位，当发送RREP消息的链路可能不可靠或单向时，置A位，这决定了收到该RREP的节点是否需要回复RREP\_ACK包.

Prefix Size 前缀长度，字段大小为5bit。如果不是0，那么下一跳节点可以作为任何具有相同长度路由前缀的节点被请求时的目的节点.。

Lifetime 路由生命时间，这段时间内，收到这条路由的节点会认为这条路由是有效的

请注意，前缀大小允许子网路由器为由路由前缀定义的子网中的每个主机提供路由，路由前缀由子网路由器的IP地址和前缀大小决定。为了利用这个特性，子网路由器必须保证所有共享指定子网前缀的主机都能访问。详见第7节。当前缀大小不为零时，必须保留与子网路由有关的任何路由信息（和前体数据），而不是该子网上的单个目标IP地址。

### RERR路由错误帧



N No delete flag; 当上一个节点已经对这条连接进行本地修复了则设置这个标志位，这样上游的节点就不用删除这条路由了

DestCount 不可达节点数，至少为1；

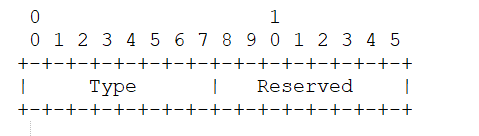
Unreachable Destination IP Address

由于连接断开而不可达的节点

Unreachable Destination Sequence Number

不可达节点的序列号

### RREP\_ACK路由应答确认帧



当节点收到的RREP回复帧中A位置为有效时，节点需要回复RREP\_ACK帧，这通常是为了避免存在单向链路时，路由发现周期无法完成的危险。

## AODV用户态工作流程

aodv协议包括路由发现，路由维护，路由错误控制，拥塞控制4种工作过程。它通过路由发现添加新的路由表项，通过路由维护保证出入口的通畅，路由错误控制来剔除失效的路由项，拥塞控制降低网络负载。

### 路由发现过程

AODV协议是按需平面距离向量路由协议，所以只有当上层有需要发数据且路由表项不存在的时候，才触发aodv的路由发现功能。aodv通过rreq帧和rrep帧实现本功能。

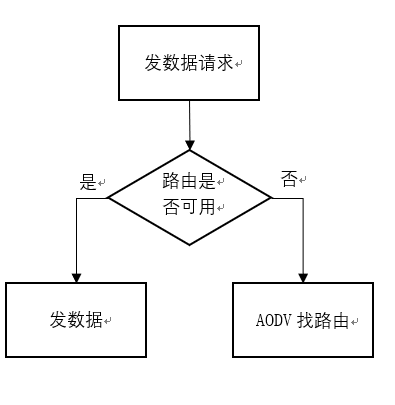


图 1 发现功能触发

首先，作为起始节点向邻居节点发送RREQ帧。邻居节点收到后，也向它的邻居节点转发RREQ帧。最后目标节点也会收到RREQ帧。

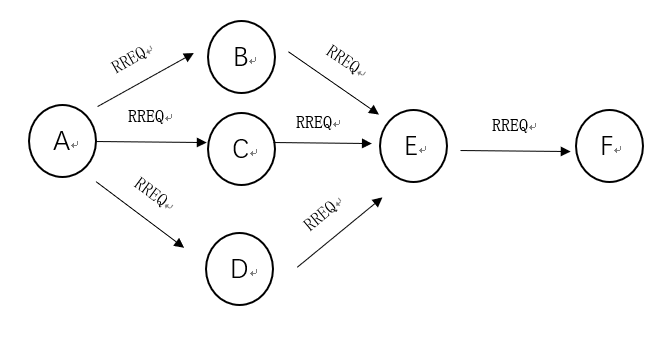


图 2 RREQ帧转发过程

在RREQ帧传播的过程中，各个中间节点在收到帧后更新到源端的路由。对于收到多个源端到一个目的端的RREQ帧的情况，取最早到达的更新到源端的路由表项。收到同一个源端到多个目的端的RREQ帧，取最新的更新到源端的路由表项。

最终目的节点收到RREQ帧后，也更新路由表项，同时查询路由表，向源端回复一个RREP帧。中间节点收到后更新路由表，查询路由表，向源端单播RREP帧。

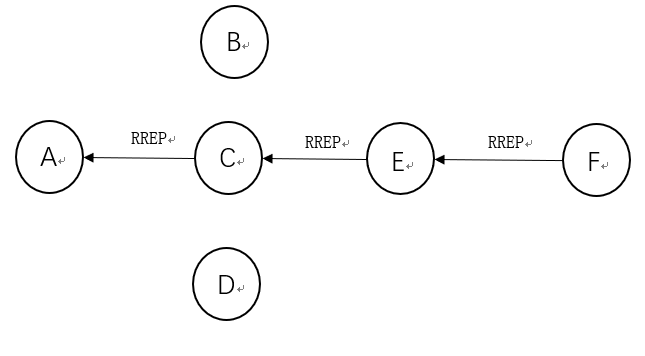


图 3 单播RREP过程

最后源端收到RREP回复帧后，更新路由表项，数据包得以发送。

还有一种情况是，当RREQ帧中相关字段允许的话，中间节点收到RREQ后，查找自己的路由表，如果发现有到达目的地的路由表项，则回复一个RREP帧。

### 路由维护和错误控制

AODV通过发送HELLO帧来实现路由的维护功能，保证了节点各个出口的有效性。

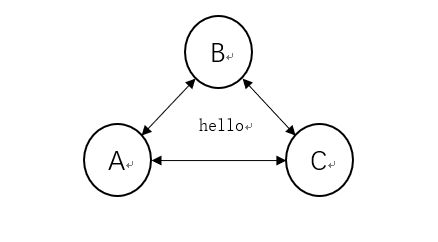


图 4 节点向邻居发hello帧

HELLO帧本质上是TTL为1的RREP帧。当节点收到RREP帧后更新对应的计时器，重

新计时。节点发现自己路由项中某个计时器超时，将该链路设置为无效，同时向相关路由表项中的前期节点发送RERR错误控制帧。

各节点收到RERR后根据帧内容修改路由表，同时把RERR转发。

### 拥塞控制

如果在规定时间内，发送RREQ请求帧的节点没有收到对应的RREP帧，那么节点可以再次发送RREQ请求帧。再次发送RREQ帧时，节点对于RREP帧的等待时间将会翻倍，这使得网络的负担得以减少。在尝试了设定次数后，节点就在路由表中标志该目的地不可达，然后构造消息发送给应用层。

为了防止不必要的网络范围的rreq，使用扩展环搜索技术。其工作原理如下：源节点连续搜索更大的区域，直到找到目标节点。这是通过对于每个RREQ重传直到找到路由来完成的，增加 每个RREQ分组中携带的生存时间（TTL）值，从而扩展源中心的“搜索环”。

### 序列号机制

为了保证节点的路由表上的路由表项是最新的，所有节点都只使用收到的包含待更新路由节点最大序列号的包来更新自己的路由表。每个节点都有自己的序列号，每当节点发一次包这个序列号就+1。每个节点记录下收到节点包里最大的序列号，存放到相应的路由表项中。所以当你收到包的序列号大于你路由对应表项里的序列号，你就知道你收到了更新的包，然后更新路由表，不然使用改包更新路由表。

### 前驱节点机制

当链路出现中断时，相关节点需要更新自己的路由。如何确定哪些节点受到了影响呢？这就通过前驱节点得知。当节点直连链路出现中断，它只会向前驱节点发送RERR路由错误帧，收到RERR错误帧的节点更新自己的路由表，同时接着向其他受影响的前驱节点发送RERR错误帧，直到所有受影响的节点都收到RERR错误帧。

每个节点会为路由项维护一个前驱节点列表。当节点收到RREP的时候，会将到RREP包源节点下一跳的节点作为前驱节点添加到本节点到RREP包目的节点的路由项中，同时将到达RREP包目的节点的下一跳节点作为前驱节点加入到本节点到RREP包源节点的路由项中。然后收到RERR路由错误帧时，只向前驱节点转发，就完成了路由信息的更新。

见下图：

RREP

A路由发现E，当C收到回复的RREP时，就把B,D添加为两条路由的前驱节点。

如果收到RERR关于不可达节点A的，那么RERR就会转发给D

C路由表

目的节点 下一跳节点 前驱节点

A B D

E D B

## 用户空间和内核模块的交互

在实现中，用户空间方面AODV后台进程程序是一个无限循环读取事件队列的进程，首先判断是属于哪一种事件(RREQ，RREP，RERR，HELLO，ACK等) ，再开始启动该事件的处理程序，不断重复读取事件队列，直到返回值是NULL 为止。路由算法的功能通过该进程实现，并作为后台守护进程在用户层执行、负责与其它节点进行信息的交互，建立和维护路由表。AODV 路由的发现和维护是通过发送和接收到控制信息分组经过AODV 算法处理后来完成的，该控制信息由UDP socket发送和接收，并由aodv\_socket 模块进行处理。各类控制信息分组的生成、发送、接收、转发、处理是aodv \_hello、aodv \_rerr、aodv \_rrep、aodv\_rreq等模块协作完成的。

在内核模块，AODV使用了Linux内核中Netfilter的挂接功能，Netfilter为每种网络协议定义了一套钩子函数，这些钩子函数在报文流过协议栈的几个关键点被调用。在这几个关键点上，协议栈将把网络报文，钩子函数以及钩子函数标号作为参数调用。AODV协议用到了定义在IP协议上的钩子函数，通过钩子函数来处理报文，具体将在3.2进行阐述

Netlink socket可以在核心层与用户层之间进行双向的数据交互，当路由后台程序将查找到的路由信息通知给内核以修改核心路由表时，用户层使用标准的socket就可以实现Netlink所提供的强大功能，并且在Netlink 的基础上，使用rtnetlink 可以方便地操作Linux 的核心路由表。当内核控制程序需要通知用户层的后台程序进行路由查找时，核心层需要使用专门的内核API 来实现Netlink 数据交互，Netlink socket将核心路由表的使用状态传递给用户层，告知AODV后台进程核心路由表的使用状况，AODV后台进程据此更新路由缓冲表的定时器，同时通过Netlink socket 删除内核路由表中过时的路由条目或增加新的路由表项。具体实现结构图如下：



**图 5 AODV实现结构**

# 代码介绍

该协议实现代码的根目录下共包含17个c文件和17个头文件里；一个记录更改日志的Changelog文件；一个GNU通用公共授权文件GPL；一个用于编译的Makefile文件；一个用于简要介绍AODV和使用方法的README文件；一个lnx文件夹，里面放了AODV协议用于linux 内核实现的代码，共6个c文件和7个头文件；一个patch文件夹，其中有8个补丁文件。

|  |  |
| --- | --- |
| 文件 | 说明 |
| Params.h | 各种参数的定义 |
| routing\_table.h | 路由表定义 |
| routing\_table.c | 路由表操作 |
| defs.h | 宏定义 |
| list.h | 链表结构定义 |
| list.c | 链表操作 |
| timer\_queue.h | 定时器队列定义 |
| timer\_queue.c | 定时器操作 |
| debug.h | 日志操作、转换成string、打印路由表 |
| debug.c |
| Endian.c | 补充某些缺乏〈endian.h〉的系统 |
| Aodv\_hello.h | hello消息的定义 |
| Aodv\_hello.c | hello消息的发送、处理等操作 |
| Aodv\_rerr.h | RERR消息的定义 |
| Aodv\_rerr.c | RERR消息的操作 |
| Aodv\_rrep.h | RREP消息的定义 |
| Aodv\_rrep.c | RREP消息的操作 |
| Aodv\_rreq.h | RREQ消息的定义 |
| Aodv\_rreq.c | RREQ消息的操作 |
| Aodv\_socket.h | AODV套接字定义 |
| Aodv\_socket.c | AODV套接字管理 |
| Aodv\_timeout.h | AODV超时处理 |
| Aodv\_timeout.c |
| Aodv\_neighbor.h | 添加和断开邻居 |
| Aodv\_neighbor.c |
| Kaodv\_mod | 内核主程序，初始化和注销内核 |
| Kaodv\_netlink | 内核层与用户层进行通信 |
| Kaodv\_debug | 显示核心层线程处理流程信息 |
| Kaodv\_ipenc | 对内核路由表中IP地址编码 |
| Kaodv\_queue | 将数据包放入内核队列 |
| Kaodv\_expl | 内核路由表信息到期列表 |

## 用户态全局变量

### 路由表项

AODV是一个路由协议，它的工作是管理路由表。AODV的每一个路由表将包含以下内容：

每个AODV协议的结点都要维护一张路由表，表的各字段如下：

1. 目的节点IP地址
2. 目的节点序列号（Sequence Number）
3. 目的节点序列号是否有效标志位
4. 下一跳节点的IP地址
5. 本节点到达目的节点需要的跳数
6. 前驱节点列表（precursor list）
7. 生存时间（路由失效或应当删除的时间）
8. 网络层接口
9. 其他的状态和路由标志位（e.g有效、无效、可修复、正在修复）

路由表的特征如下：

1. 路由表每项只记录下一跳路由信息，而不是整条路由信息，简化了路由表的建立和维护 。
2. 节点将相邻节点的连接状态保存到活动路由表中。
3. AODV在每一个路由表上使用了目的序列号。 源节点和目的节点都维护各自的序列号 。
4. 当一条链路断裂或失效导致一个节点不可达，路由表将通过对序列号的操作和标注路由表表项错误来使此条路由失效。

### 全局链表结构

全局维护的一个链表结构，从Linux内核列表实现中获得灵感而仿造的简单链接列表，具体实现在list.c文件中。广泛用于各个功能，比如邻居节点列表，计时器列表，前驱节点列表等，方便实例化和操作列表。

|  |  |
| --- | --- |
| 名称 | 功能 |
| typedef struct list\_t | 列表结构体，下面的函数是对列表的操作 |
| static inline int listelm\_detach(list\_t \* prev, list\_t \* next) | 删除某位置上的节点 |
| static inline int listelm\_add(list\_t \* le, list\_t \* prev, list\_t \* next) | 在指定位置添加节点 |
| int list\_add(list\_t \* head, list\_t \* le) | 在头部添加一个节点 |
| int list\_add\_tail(list\_t \* head, list\_t \* le) | 在末尾添加一个节点 |
| int list\_detach(list\_t \* le) | 删除指定节点 |

### 全局目的地链表结构

在路由发现功能中，RREQ发出后不会立即获得回复，而此时可能需要发出另一个节点RREQ请求，所以需要一个链表结构来维护RREQ请求的目的地节点。具体实现在Seek\_list.h和Seek\_list.c文件中。

|  |  |
| --- | --- |
| 名称 | 功能 |
| seek\_list\_t \*NS\_CLASS seek\_list\_insert | 在链表中插入新节点，即增加了一个需要寻找的目的地 |
| int NS\_CLASS seek\_list\_remove | 从列表中删除一个需要寻找的目的地节点 |
| seek\_list\_t \*NS\_CLASS seek\_list\_find(struct in\_addr dest\_addr) | 从列表中找出指定地址的节点 |
| void NS\_CLASS seek\_list\_print() | 打印出每个待寻找目的节点的地址，序列号等信息 |

### 全局定时器队列

AODV很多地方需要使用到定时器，比如说路由表项的维护，邻居活跃情况，还有路由修复等，需要定时器在需要的时候触发超时事件。

|  |  |
| --- | --- |
| 名称 | 功能 |
| int NS\_CLASS timer\_init(struct timer \*t, timeout\_func\_t f, void \*data) | 定时器初始化 |
| void NS\_CLASS timer\_timeout  (struct timeval \*now) | 定时器超时时进行清理工作 |
| NS\_STATIC void NS\_CLASS timer\_add  (struct timer \*t) | 在定时器队列中加一个定时器 |
| int NS\_CLASS timer\_remove(struct timer \*t) | 从定时器队列中移除一个定时器 |
| int NS\_CLASS timer\_timeout\_now  (struct timer \*t) | 手动让一个定时器超时，以触发超时事件 |
| void NS\_CLASS timer\_set\_timeout(struct timer \*t, long msec) | 给指定定时器增加一定的时间 |
| long timer\_left(struct timer \*t) | 计算指定定时器剩余时间 |
| struct timeval \*NS\_CLASS timer\_age\_queue() | 计算定时器队列的生存时间 |
| void NS\_CLASS printTQ(list\_t \* l) | 打印出每个定时器的信息 |

# 内核空间函数解读

## Linux钩子函数简介

在AODV协议的具体实现过程中，Netfilter在处理数据包流程时起到关键性的作用，Netfilter由处于Linux 协议栈中不同点上的五个钩子(hook)关键点组成，用户可以在这些位置注册自己定义的操作函数，经过hook点的数据分组将执行函数操作，帮助用户完成数据分组的过滤和修改等功能。如图所示



数据包网络入口以后，首先对IP进行校验后，经过注册在NF\_ IP\_PIFORWARD的钩子函数处理后，进入内核路由处理模块，接着判断数据包是发送给本机的还是需要转发的，如果是发给本机的，则该数据包经过注册在NF\_IP\_LOCAL\_IN的钩子函数传递给上层协议，若该数据包应该被转发则把它被交给注册在NF\_ IP\_PIFORWARD的钩子函数处理，转发的数据包经过注册在NF\_IP\_LOCAL\_OUT的钩子函数处理后，再发送到网络上。本地产生的数据包经过注册在在NF\_IP\_LOCAL\_OUT钩子函数处理后，进行路由选择处理，然后经注册在NF\_IP\_POST\_ROUTNIG钩子函数处理，最终发送到网络上。每个注册的钩子函数经过处理后都将通过返回值告知Netfilter核心代码，以便对数据包采取相应的动作。返回值的功能如下: NF\_ACCEPT: 继续正常的数据包处理; NF\_DROP: 将数据包丢弃; NF\_STOLEN: 由钩子函数处理了该数据包，不再继续传送; NF \_QUEUE: 将数据包入队，通常交由用户程序理;NF\_REPEAT: 再次调用该钩子函数。

## 内核空间对数据包处理流程

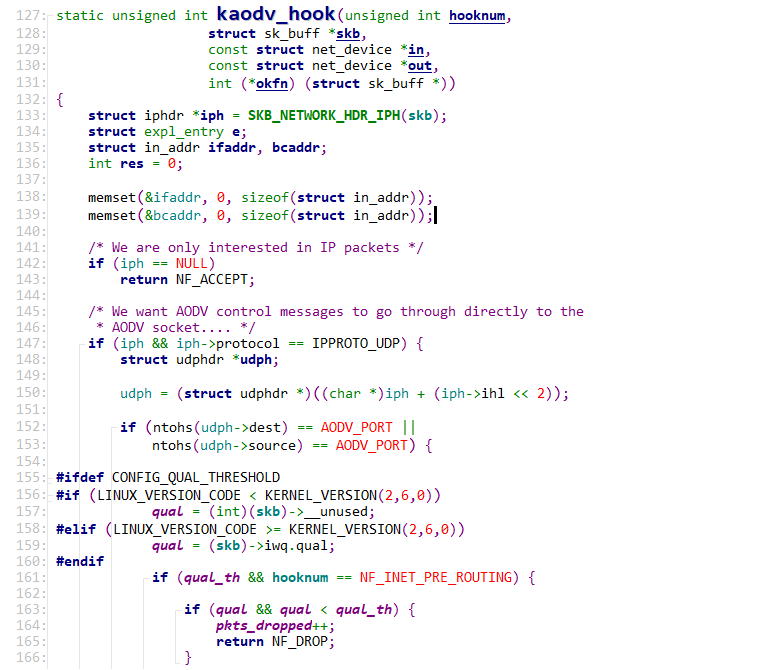
本协议用到了五个关键点中的三个分别为F\_IP\_PRE\_ROUTING(流入数据包在决策路由前执行) 、NF\_IP\_LOCAL\_OUT(本地产生数据包流出路由前执行) 、NF\_IP\_POST\_ROUTING( 在本地数据包或转发数据包在发送之前) 。

在本地直接发送或者转发数据包时，首先判断内核路由表中是否存在与该数据包的目的地址相匹配的路由条目，如果存在，根据该路由条目信息提供的相应网络接口将其发送到对应的下一跳节点地址上，如果不存在与数据包目的地址相匹配的路由条目，向用户层的后台进程发起路由请求，由后台进程发起路由查找过程，并且在路由查找结束和内核路由表更新之前，数据包通过挂接在NF\_IP\_LOCAL\_OUT hook 点的回调函数进行处理，并通过用Linux的原始套接口( Raw Socket) 将数据包送往用户层的数据缓冲区中进行排队。同时，必须用户层维护一个与内核路由表形成映射关系的路由缓冲表。路由缓冲表的所有路由条目都有一个与之相关的定时器，当内核路由表中的路由条目被使用时，与之对应的用户层缓冲路由表的定时器必须被重置，当定时器的时间到期时，该表项就要从路由缓冲表和内核路由表中同时删除。如果查找到与被缓存数据包目的地址匹配的路由，则将这条路由插入到内核路由表中，用原始套接口将缓存的数据分组重新发送出去。如果在规定的时间内未找到相应的路由，则这些缓存的数据报文会被丢弃，并通知源节点出错。

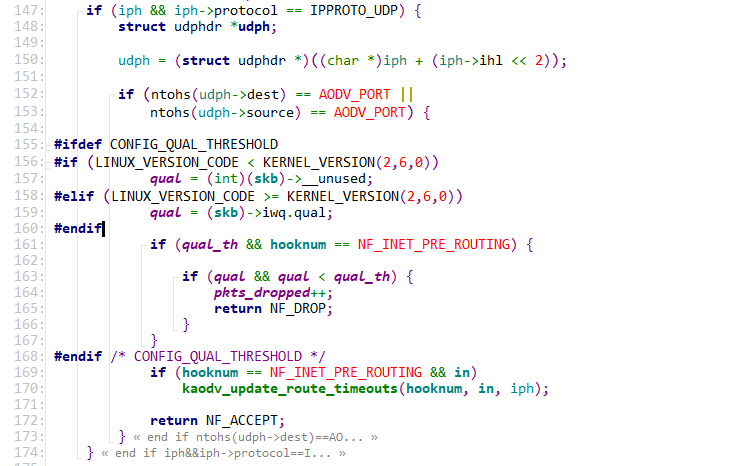
## kaodv-mod.c

本文件是内核模块开始的文件，主要包括了要在三个关键点上挂载的kaodv\_hook函数和更新AODV内核模块维护的路由表的函数

### 3.3.1 kaodv\_hook-aodv-钩子函数

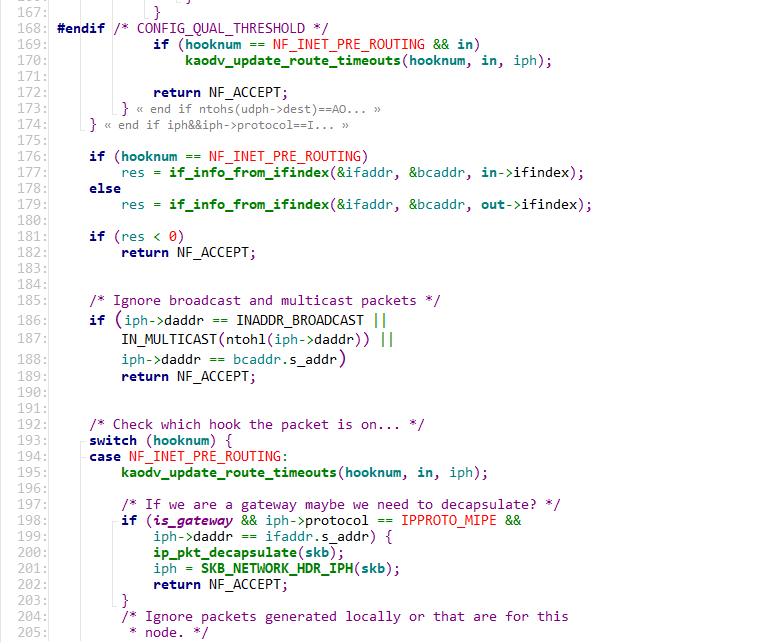


142-143 如果IP为空，则继续正常的数据包处理，即忽略这个数据包，因为协议只对IP数据包感兴趣



147-153 检测是否是AODV socket发来的消息

162-165 如果消息过时了，则丢弃它

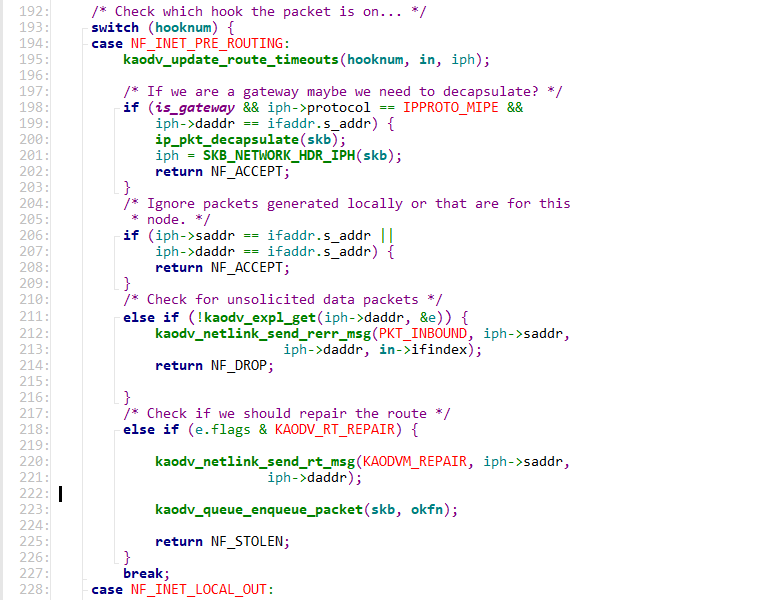


176-177如果流入钩子函数标号代表数据包在决策路由前则查找输入的端口信息，若找到则res=0；否则res=-1

176-177如果流入钩子函数标号代表本地生成数据包或者转发数据包时则查找输出的端口信息，若找到则res=0；否则res=-1

181-182若果没有找到端口信息，则忽略该数据包

186-189如果是广播或者多播信息，则忽略该数据包



193 查找数据包是哪个钩子函数钩来的

194 如果是NF\_INET\_PRE\_ROUTING，即流入数据包在决策路由前钩来的

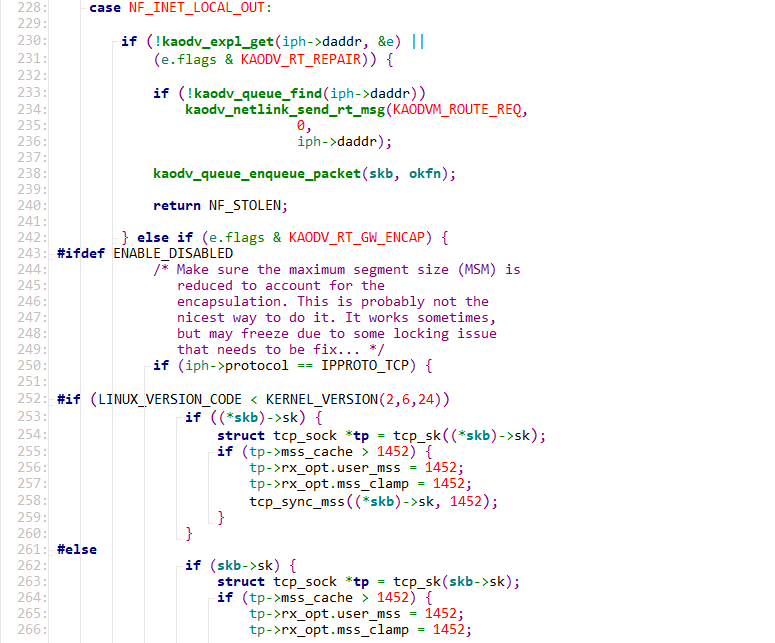
195 更新路由过期时间包括更新expl\_entry结构和通知用户进程更新用户空间的维护的路由表

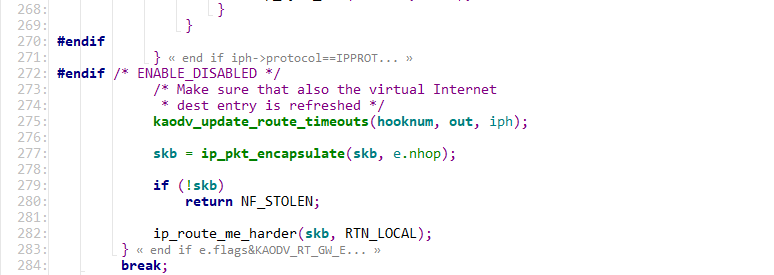
198-203 如果是网关的话，则将数据包解封装

206-209 忽略忽略本地生成的或为此节点生成的数据包

211-216 如果本地路由表中没有数据包的中目标地址的信息，则发送rerr消息，然后丢弃数据包

218-226 如果找到了目标节点的路由，判断是否需要flags是否要修复，如果需要，向用户空间发送修复信息，并将当前数据包放进数据缓存队列中





228 如果是NF\_INET\_LOCAL\_OUT，即本地产生数据包流出路由前钩来到

230-240 如果不存在到目的节点的路由，或者路由需要修复的情况下，首先判断数据缓存队列中有没有关于该目的节点的数据packet,如果有的话，表示已经发送RREQ进行路由请求了，如果没有，则向用户空间通信，发起RREQ路由请求，同时该缓存数据packet进入缓存队列中，不再发送该数据包

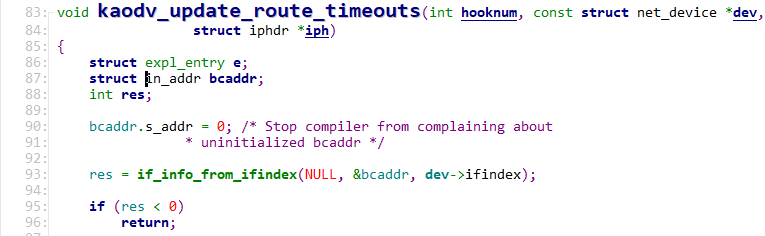
242-269 如果路由条目有KAODV\_RT\_GW\_ENCAP,且上层协议为TCP，设置最大报文段长度为1452B，超过才长度则分片

275-283 更新expl\_entry结构和通知用户进程更新用户空间的维护的路由表，将数据包打包



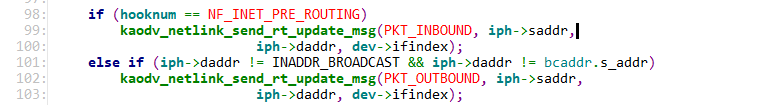
如果是NF\_INET\_POST\_ROUTING，则更新expl\_entry结构和通知用户进程更新用户空间的维护的路由表

### 3.3.2 kaodv\_update\_route\_timeouts-更新expl\_entry结构和通知用户进程更新用户空间的维护的路由表

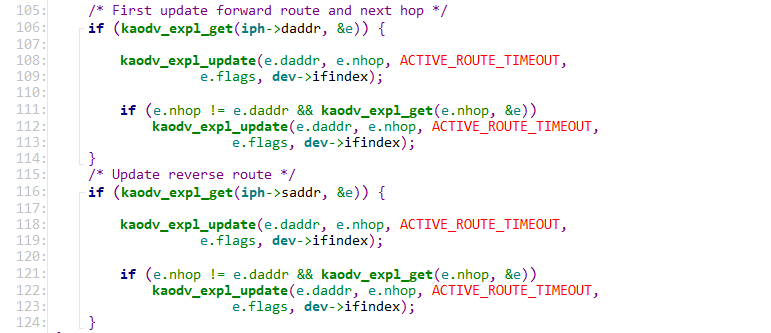


93 根据ifindex查找端口信息

95-96 如果没有找到则退出

98-100 如果数据包是在流入方向被钩到的，则想用户空间发送流入方向路由更新

101-103 如果数据包是在流出方向被钩到的且不是广播数据包，则想用户空间发送流出方向路由更新



105-114 更新expl\_entry结构的前向路由和下一跳

116-124 更新反向路由

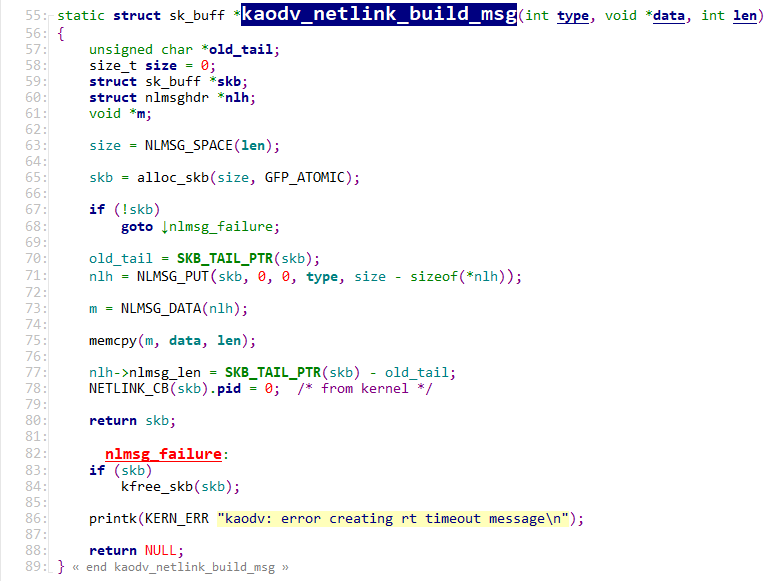
### 3.3.3 其他函数

|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| kaodv\_init | 376-429 | 初始化缓冲队列，初始化设备端口信息等 |
| kaodv\_exit | 457-473 | 退出AODV函数，注销钩子函数，释放缓冲队列，路由表等空间 |

## kaodv-netlink.c

本文件实现了关于AODV协议netlink机制相关的函数

### 3.4.1kaodv\_netlink\_build\_msg-创建sk\_buff结构体



59 skb是一个sk\_buff类型的指针，sk\_buff（socket buffer）结构是linux网络代码中重要的数据结构，它管理和控制接收或发送数据包的信息

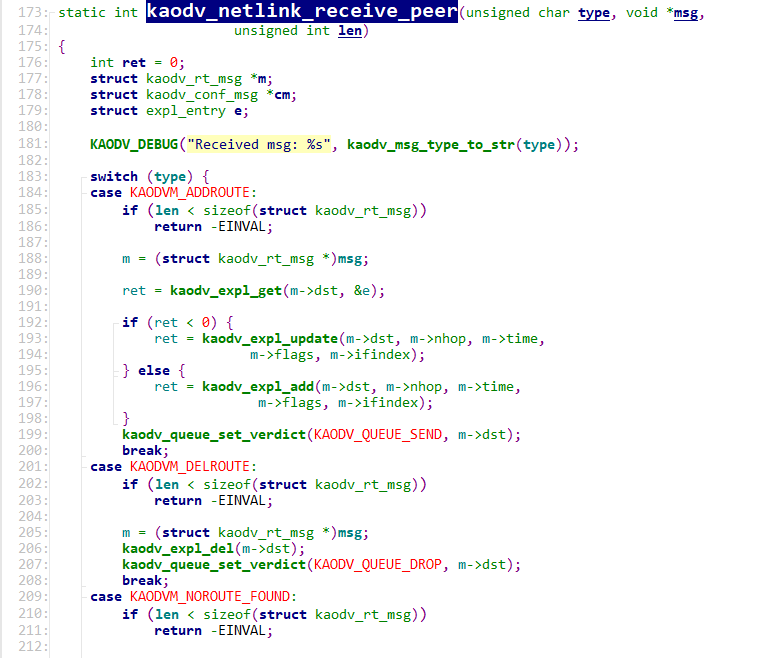
60 nlh是一个nlmsghdr类型的指针

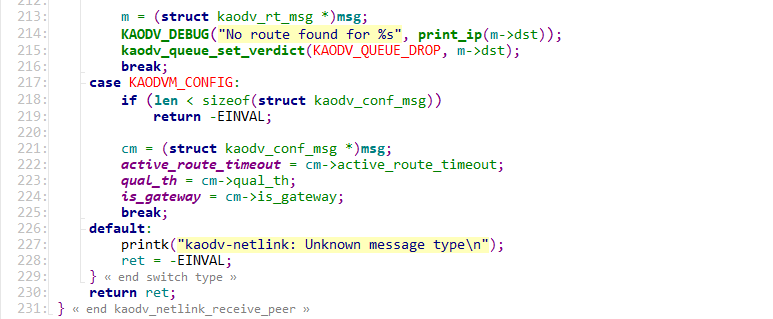
65 alloc\_skb函数分配缓冲区，包括两个缓冲区，一个是数据缓冲区，一个是缓冲区的描述结构sk\_buff

67-68,82-88 如果alloc\_skb失败，则释放skb内存并返回null

70-80 设置skb的各项值，需要注意的是，由于是从内核发出，pid应设置为0

### 3.4.2 kaodv\_netlink\_receive\_peer-内核收到消息后的处理的方式





177 m是一个kaodv\_rt\_msg的指针，携带有路由信息

178 cm是一个kaodv\_conf\_msg的指针，携带有AODV协议设置信息

179 e是一个expl\_entry的指针，这是一个由AODV协议维护的路由信息

184-200 如果消息类型是KAODV\_ADDROUTE，查找AODV协议的路由表是否有关于目的地的路由表项，如果有，则更新路由表项，否则增加路由表项。并交给内核队列裁决模块

201-208如果消息类型是KAODV\_DELROUTE类型，则删除AODV协议维护的路由表中的路由表项，并交给内核队列裁决模块

209-216如果消息类型是KAODV\_NOROUTR\_FOUND类型，输出没有发现前往目的地的路由并交给内核队列裁决模块

217-225如果消息类型是KAODV\_CONFIG类型则将kaodv\_conf\_msg指针指向的参数修改

### 3.4.3其他函数

|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| kaodv\_netlink\_send\_debug\_msg | 91-103 | 输出调试信息 |
| kaodv\_netlink\_send\_rt\_msg | 105-120 | 向应用空间广播路由信息 |
| kaodv\_netlink\_send\_rt\_update\_msg | 126-148 | 向应用空间广播路由更新信息 |
| kaodv\_netlink\_send\_rerr\_msg | 150-171 | 向应用空间广播端口路由信息 |
| kaodv\_netlink\_rcv\_nl\_event | 233-248 | 如果是内核消息，则刷新expl\_entry和缓冲队列 |
| kaodv\_netlink\_rcv\_skb | 256-319 | 处理sk\_buff，调用kaodv\_netlink\_receive\_peer处理消息 |
| kaodv\_netlink\_init | 343-362 | Netlink初始化，注册事件通知链 |
| kaodv\_netlink\_fini | 364-371 | 注销事件通知链 |

## kaodv-expl.c

本文件负责维护expl\_entry结构体，即内核中的路由表，该结构体包括过期时间，标准，目的地IP，跳数，端口编号信息

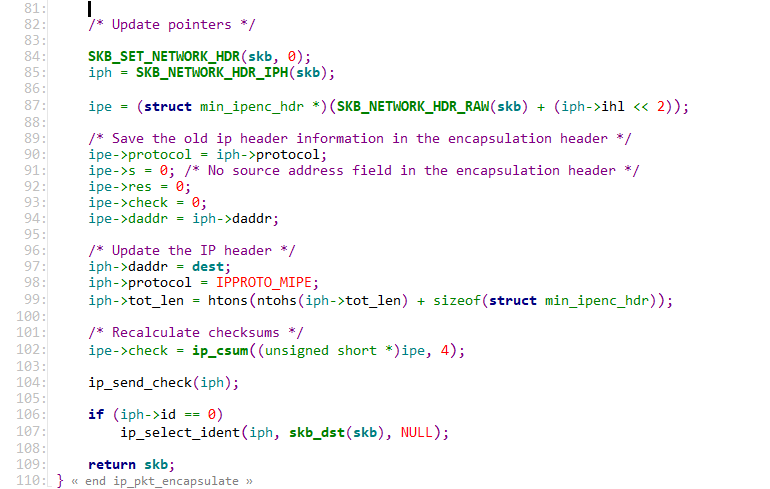
|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| kaodv\_expl\_timeout | 74-98 | 获取当前时间，将已经失效的路由表项删除，注意对路由表的操作是加写锁的 |
| \_\_kaodv\_expl\_flush | 101-111 | 删除路由表 |
| \_\_kaodv\_expl\_add，kaodv\_expl\_add | 113-135，220-261 | 按过期时间顺序增加路由表项 |
| \_\_kaodv\_expl\_find | 137-148 | 根据IP地址查找特定的路由表项 |
| \_\_kaodv\_expl\_del | 150-174 | 根据路由表项删除特定路由表项 |
| kaodv\_expl\_del | 176-199 | 根据IP地址删除特定的路由表项 |
| kaodv\_expl\_get | 201-218 | 查找特定路由表项，若查到返回1，否则返回0 |
| kaodv\_expl\_print | 271-320 | 打印expl\_entry结构体 |
| kaodv\_expl\_proc\_info | 325-357 | 返回剩下的分片长度 |
| kaodv\_expl\_update | 259-392 | 更新expl\_entry结构体，更新时加写锁 |
| kaodv\_expl\_init | 408-420 | 初始化expl\_entry结构体 |
| kaodv\_expl\_fini | 422-430 | 删除expl\_entry结构体 |

## kaodv-ipen.c

本文件负责在两个不直接相连的AODV网络传递信息时，在边缘网关将IP数据包封装，使其能在普通网络中传递，类似于IPv6的数据包的隧道技术。

### ip\_pkt\_encapsulate-IP数据包封装





54-63 在首部申请新的空间，若果申请失败打印失败信息并退出

65-71 第67行将nskb这个数据缓冲区控制结构和数据缓冲区关联起来。

第71行修改指向数据区末尾的指针，并向下扩大ipenc头部大小

73-77 将IP头部和数据都后移

79 释放原来的sk\_buff

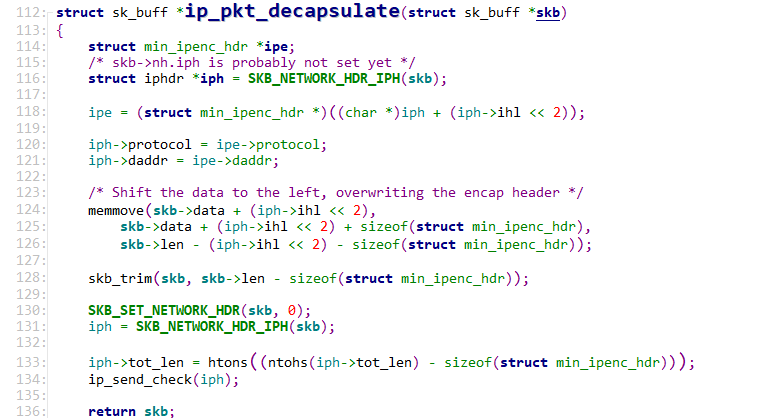
84-87 设置首部指针

90-94 将原来的IP首部信息保存到封装的首部

97-99 更新IP头部，将协议类型改为自己定义的IPPROTO\_MIPE,重新计算包大小

102 重新计算首部校验和

### ip\_pkt\_dncapsulate-IP数据包解封装



124-126由于封装时讲原来的首部和数据右移，只需要将其左移覆盖封装的首部即可

133-134 重新计算数据包长度并检验

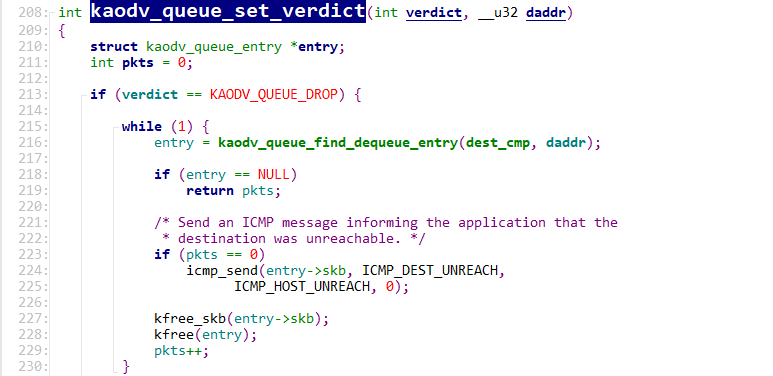
### 其他函数

|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| ip\_pkt\_encapsulate | 31-43 | 计算IP首部校验和 |

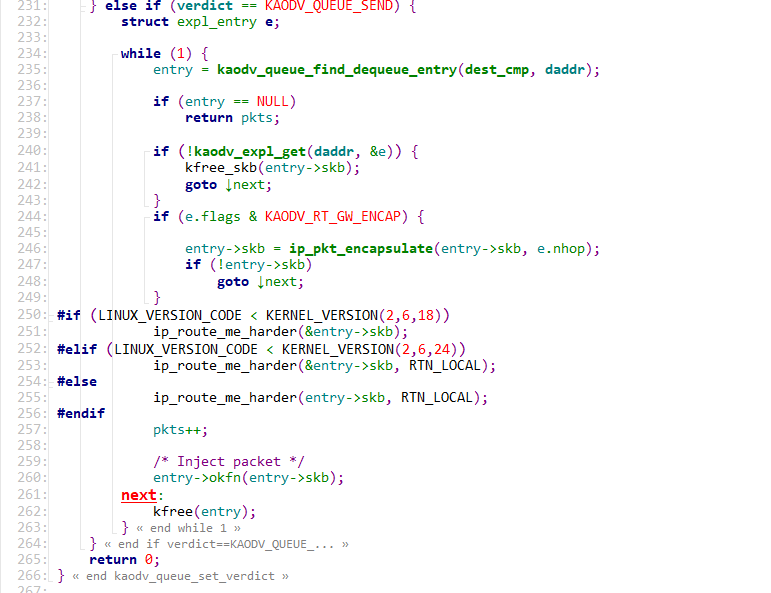
## kaodv-queue.c

本文件负责建立数据包缓存队列，注意对于该队列的写操作都是加写锁。同时该文件还接受来自AODV内核模块的消息处理队列里的数据包即kaodv\_queue\_set\_verdict实现的功能。

### kaodv\_queue\_set\_verdict-队列裁决函数



213-230 如果是需要丢弃的，查找队列，找到所有目的地为该IP地址的数据包做出队操作，并且发送ICMP消息告知目的地不可达



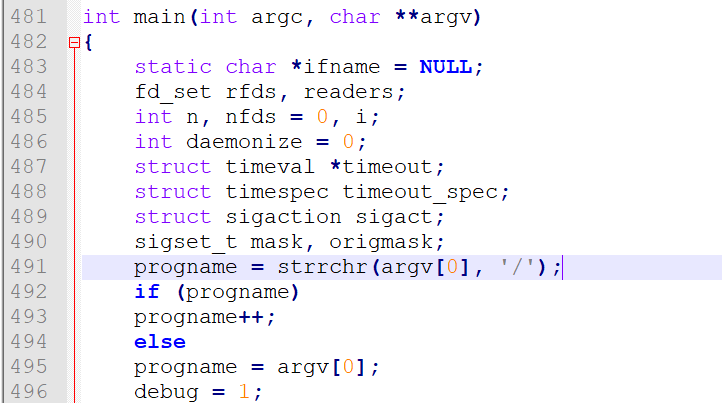
234-263 如果是需要发送的，找到所有目的地为该IP地址的数据包，如果是网关，则讲数据包封装后交给kofn指向的函数处理，如果不是网关，直接交给okfn指向的函数处理

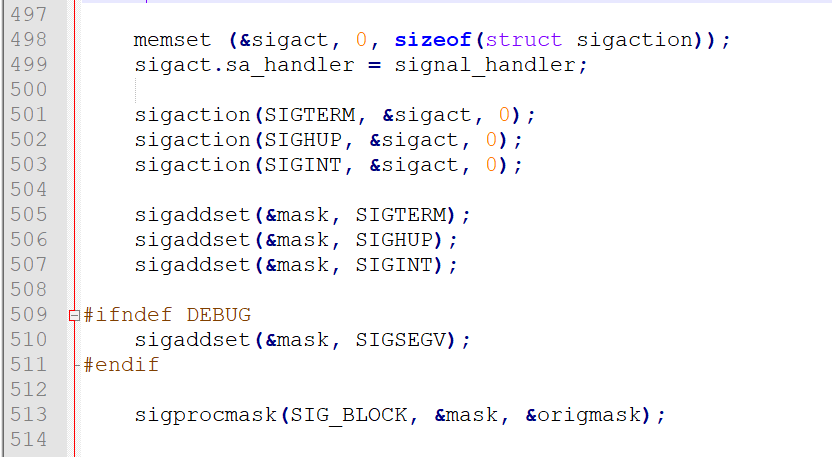
|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| kaodv\_queue\_enqueue\_packet | 151-187 | 元素入队，其中队列元素的属性其中okfn是该数据包经过所有钩子函数后需要执行的函数指针 |
| kaodv\_queue\_find\_dequeue\_entry | 133-141 | 删除队列元素 |
| kaodv\_queue\_flush | 143-148 | 清空队列 |
| kaodv\_queue\_find | 194-206 | 查找队列中是否对应IP的元素 |
| init\_or\_cleanup | 303-351 | 初始化队列或者删除队列，如果是0则清空并删除队列 |

# 用户态函数解读

## main函数

main函数主要功能是对于各个变量的初始化，包括应用到的套接字，全局链表，路由表，信号等。读取命令行参数以对相关变量进行设置，使得协议执行不同的动作。最终通过pselect轮询函数来实现节点的各个功能。





481-496 声明各变量，包括文件描述符集，计时器，信号量，读取文件名等

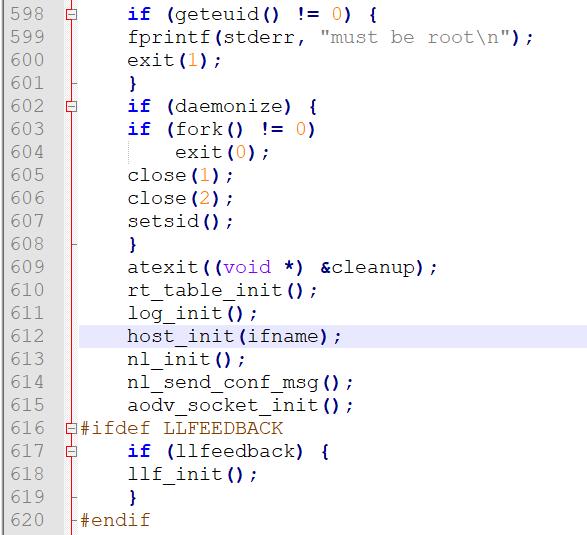
497-514 先是通过memset函数来清空结构体的内存，然后对信号结构体进行相关设置，最后将信号结构体阻塞住，将来在pselect函数中处理它。

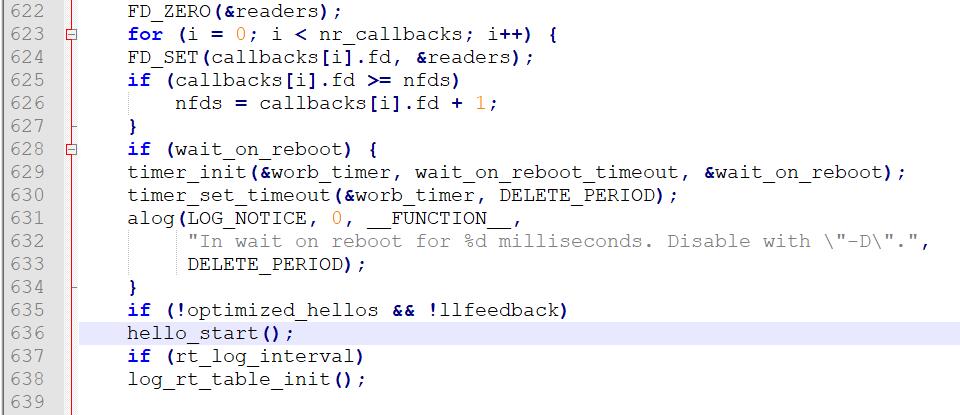




515-596 这是一个永真循环，它读取用户输入的命令行参数，然后根据输入的命令执行AODV不同的工作分支。具体操作，如下表所示：

|  |  |  |
| --- | --- | --- |
| 命令行参数 | 全称 | 说明 |
| -d | daemon | 开启守护进程模式，离开控制台窗口 |
| -f | llfeedback | 开启链路层反馈 |
| -g | force-gratuitous | 在每个传输的消息上设置gratuitous标志 |
| -i | interface | 后接端口，表示绑定到某端口；如没有，则自动分配 |
| -j | hello-jitter | 启用hello-jitter服务，默认也是启用的 |
| -l | log | 显示日志 |
| -n | n-hello | 将某节点设置成活跃邻居所需要接收到HELLO帧数 |
| -o | opt-hellos | 设置只在转发消息时才发送hello数据包 |
| -q | quality-threshold | 设置消息质量的最小阙值 |
| -r | log-rt-table | 每个一段时间记录一次路由表 |
| -u | unidir-hack | 开启检测服务 |
| -w | gateway-mode | 开启网管支持 |
| -x | no-expanding-ring | 禁用RREQ的拓展环搜索法 |
| -L | local-repair | 开启本地修复 |
| -D | no-worb | 禁用开启延迟的等待 |
| -R | ratelimit | 开启RREP和RREQ的速率限制 |
| -V | version | 输出版本信息 |
| -: | exit | 退出 |





598-601  检查AODV是否在root权限下运行，否则退出

602-608  检查变量daemonize，若不等于0，检测当前是否是父进程，是父进程则退出，不是父进程，就把输入，输出，错误流都关闭了，并且使当前进程成为新的会话组长和新的进程组长，并与原来的登录会话和进程组脱离。

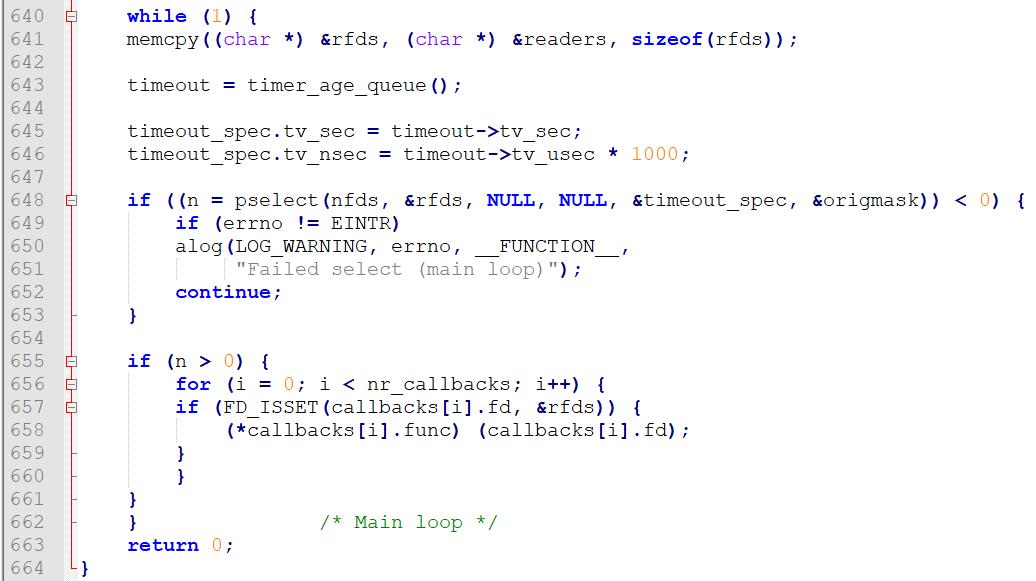
609-619  调用各初始化函数，初始化路由表，日志，各种套接字。

622-627 把需要监听的套接字描述符加入到文件描述符集中去，为以后pselect使用作准备

628-634 如果wait\_on\_reboot不为零，设置重启定时器，超出一定时间进行重启

635-637 启动HELLO帧，准备发第一个

637-369 初始化日志路由表



641-641 复制文件描述符集

643-646 设置定时器

648-653 pselect轮询函数，当文件描述符集中出现描述符对应套接字可读的时候，函数返回可读的个数n。

655-661 如果套接字可读数大于0，则通过FD\_ISSET遍历文件描述符集，判断具体是哪个可读，然后执行对应的回调函数。回调函数通过attach\_callback\_func函数来指定。

## main函数文件内其他函数以及变量的定义：

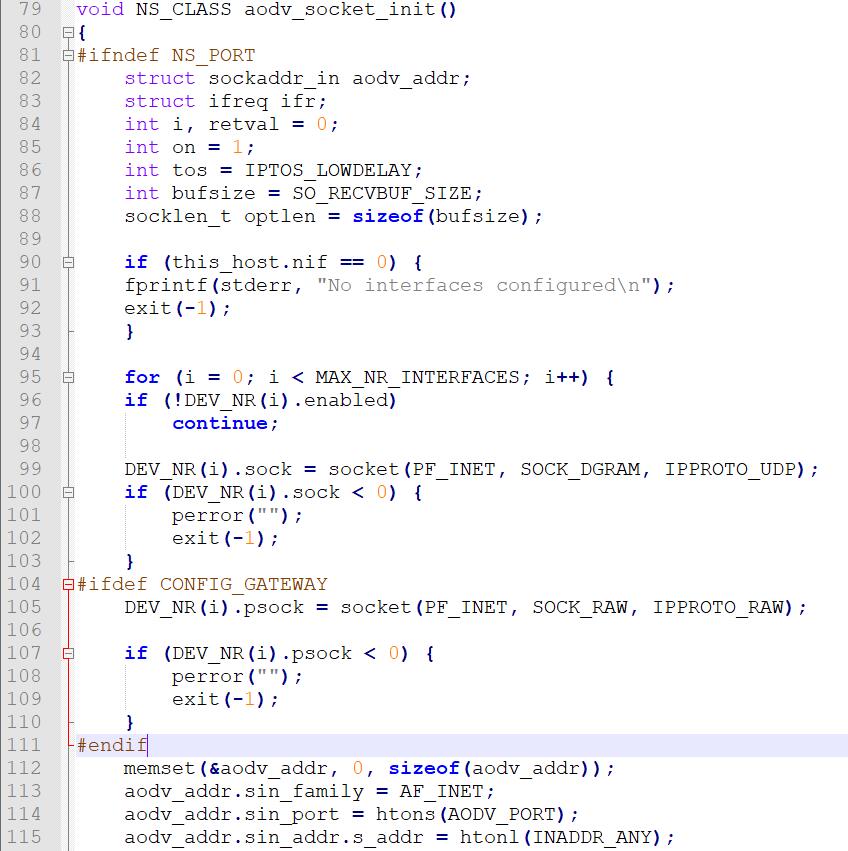
在这里以表格的形式简单说明main.c中剩下的函数功能和变量

|  |  |
| --- | --- |
| 名称 | 说明 |
| voidusage(intstatus) | 打印命令行参数和说明 |
| voidcleanup() | 里面调用了各个部件的cleanup函数，实现了清空套接字、路由表等信息的功能 |
| struct callback | Callback结构体，成员变量包含一个int型的文件描述符和一个回调函数型的函数 |
| int attach\_callback\_func(int fd, callback\_func\_t func) | 增加一个callback元素 ，设置它的套接字描述符和对应的函数 |
| int find\_default\_gw(void) | 寻找节点默认网关 |
| struct sockaddr\_in \*get\_if\_info(char \*ifname, int type) | 根据套接字接口名字和其类型获取详细信息 |
| void host\_init(char \*ifname) | 初始化某个端口 |
| void load\_modules(char \*ifname) | 装载内核模块 |
| void remove\_modules(void) | 删除某个模块 |
| int set\_kernel\_options() | 设置内核选项 |
| void signal\_handler(int type) | 信号处理函数，根据不同类型的信号作不同的操作 |

## AODV\_socket.c

### aodv\_socket\_init函数-套接字初始化函数

该函数主要实现了对应aodv套接字的初始化。可以清晰的看到，该套接字是用UDP协议进行传输的。可以看到函数末尾调用了attach\_callback\_func函数，将自己的套接字描述符和aodv处理函数作为参数传了进去。说明这个套接字是用来接收aodv控制帧的，当套接字可读的时候，调用了aodv\_socket\_read函数来处理接收到的包。

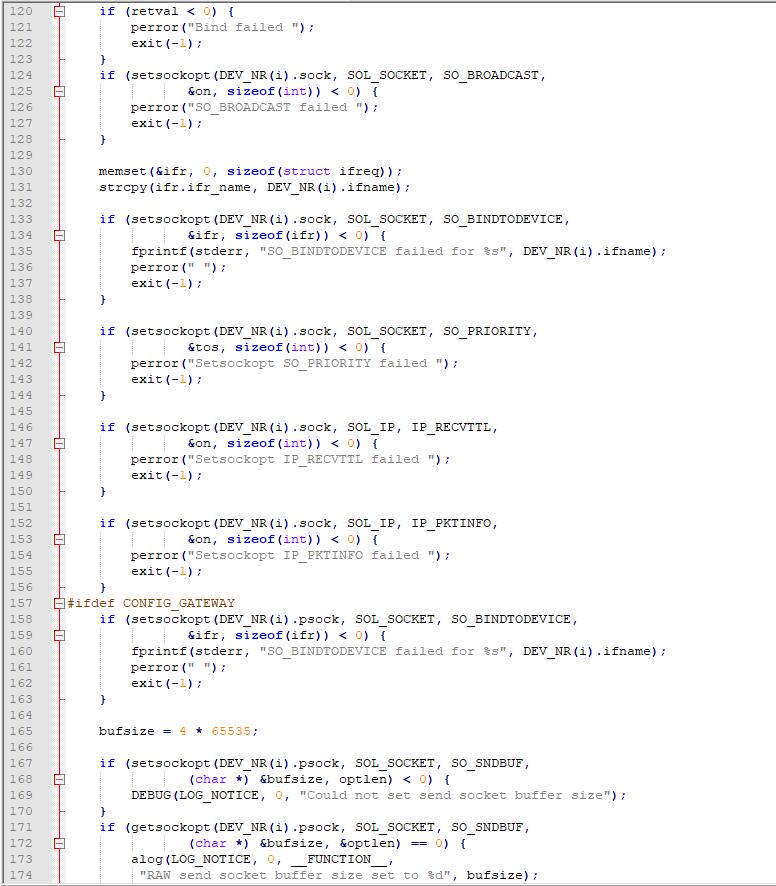


79-88 声明UDP套接字所需要的变量

90-93 如果没有可用接口的话之间退出

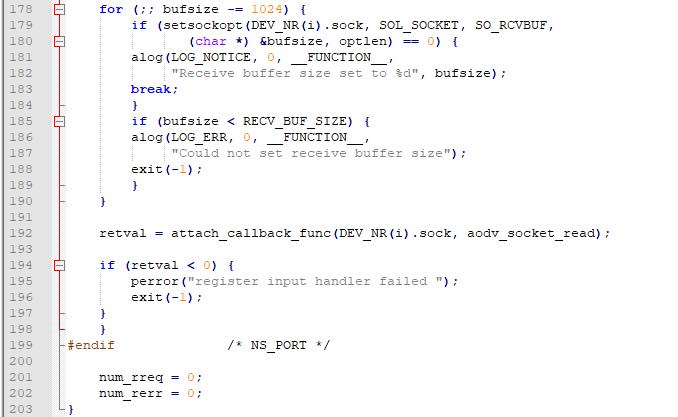
95-97 这个循环将在规定值范围内，为所有可用的接口创建套接字连接。

99-115 创建并检测生成的UDP套接字和与内核沟通的原始套接字，设置aodv地址参数





120-176 设置套接字选项，如果其中一个设定失败则显示错误，并返回



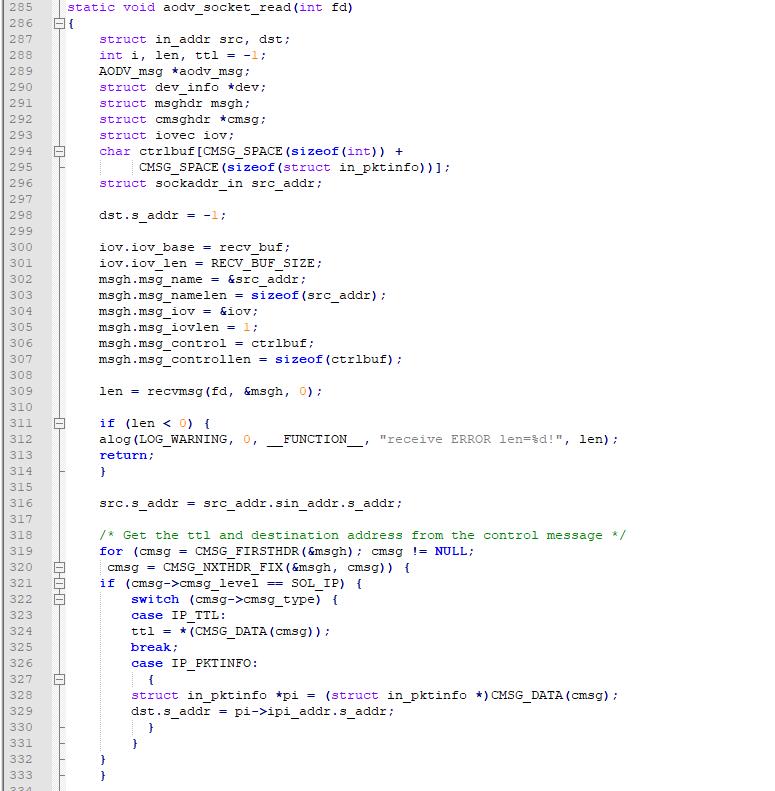
178-190 设置收控制帧的缓冲区大小，失败则显示消息并返回

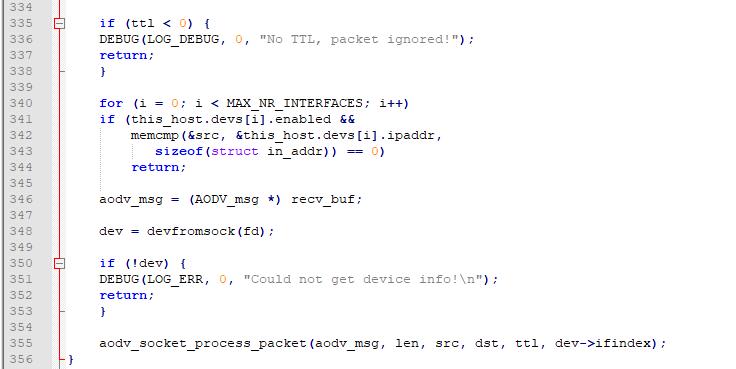
192-192 把创建好的套接字挂载到主函数的callback结构体当中

117-123 绑定套接字和AODV端口号

### aodv\_socket\_read函数-套接字读取

该函数被设定为callback结构体中某成员的回调函数，当aodv套接字可读时将会调用这个函数对收到的包进行处理。这个函数对接收到的aodv控制帧包进行过滤操作，丢弃长度小于0的和本地生成的数据包。因为发送和接受用同一个套接字进行传输，当我们需要发送帧时，把信息写入缓冲区中，套接字同样可读，会调用这个函数，所以需要判断。





287-307 声明各消息变量，以待使用

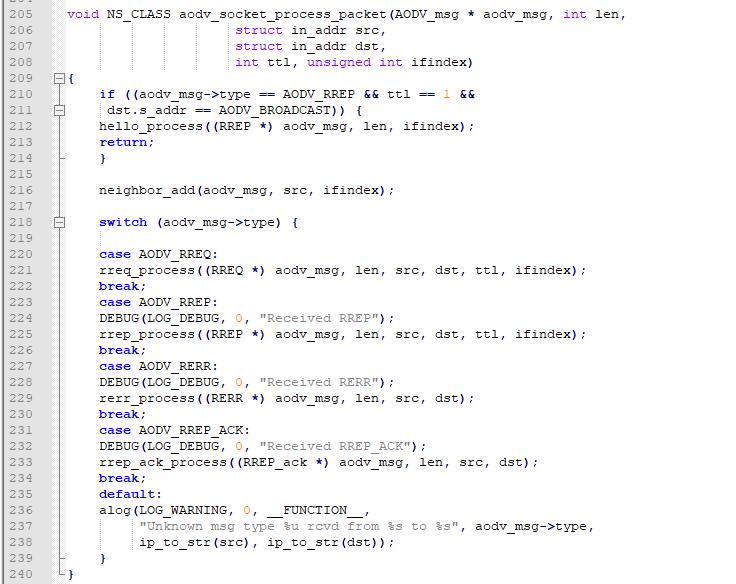
309-314 收取套接字接收到的信息，如果长度小于0，则丢弃

319-344 获取控制帧的ttl和目的地址，判断如果ttl<0或者是本节点生成的数据包则忽略掉。

346-355 提取相应消息，把包传给aodv\_socket\_process\_packet函数进行进一步处理

### aodv\_socket\_process\_packet函数-处理数据包函数

控制帧在经过aodv\_socket\_read函数初步筛选过后递交给本函数进行进一步处理，本函数主要实现的是一个分发处理功能。收到包后判断其类型，递交给对应的处理函数进行工作。

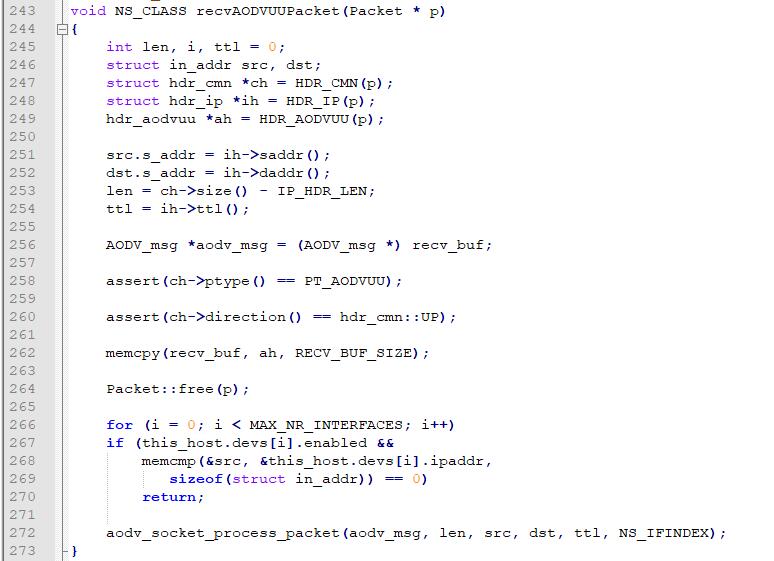


210-214 如果包是一个HELLO帧，则把该包传给hello\_process函数进行处理

226-226 根据aodv消息，src和ifindex参数添加邻居节点

218-239 提取包类型，将包递交给对应的函数进行处理

### recvAODVUUPacket函数-接收AODVUUPacket

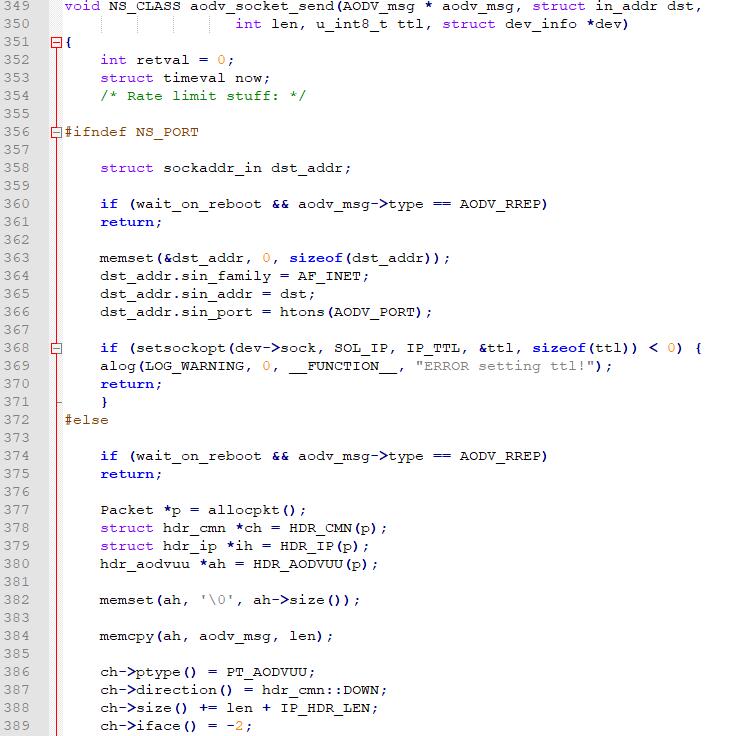


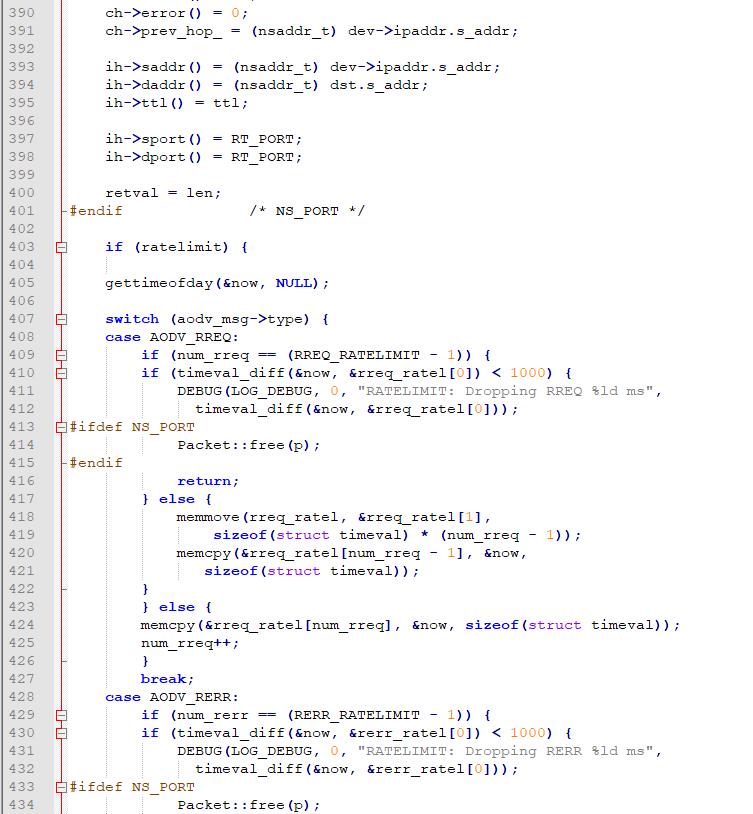
245-264 给收到的数据包先分配缓存空间，然后释放掉

266-270 检查包是否是本节点任意一个活跃接口发出的，如果是，则直接返回

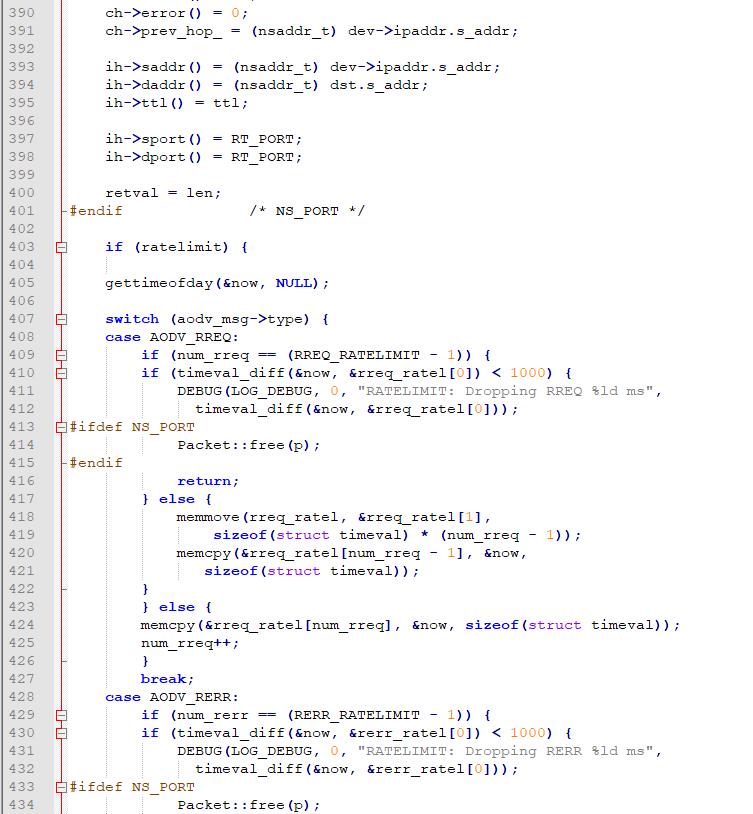
272-272 把包递交给下一函数进行处理

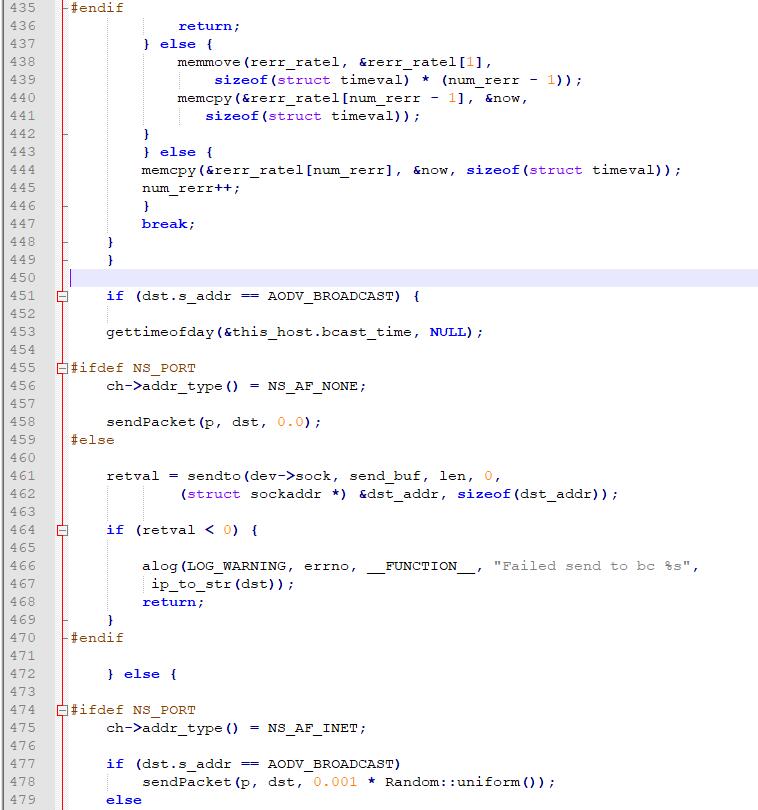
### aodv\_socket\_send函数-套接字发送函数



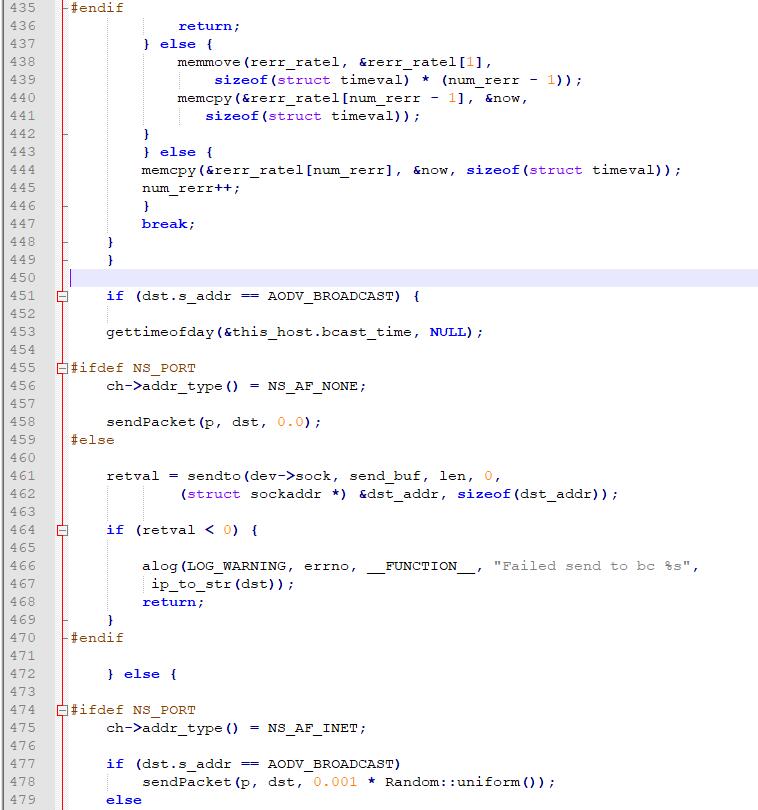


352-401 如果没有定义NS\_PORT设置头部消息和TTL，否则检查是否是RREP，不是则为包申请空间，将相关信息填入。





403-449 如果存在发送速率限制，检测包的最低传输速率是否比其类型对应的限定值小，如果小，则丢弃。如果符合则自身对应类型序列+1。





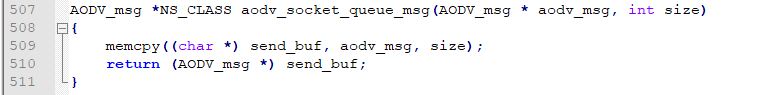
450-497 如果要发送的包是要广播的，那么更新最后广播该数据的时间，能够避免HELLO消息重复广播。

### aodv\_socket\_new\_message函数



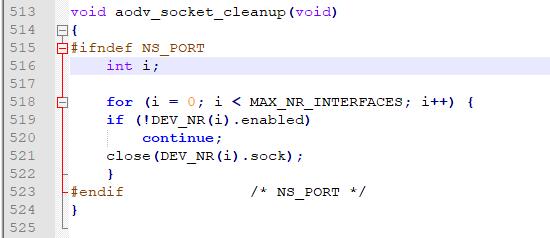
500-504 为新消息分配空间，并返回该消息的指针

### aodv\_socket\_queue\_msg函数



507-511 一个AODV消息存储在发送队列中

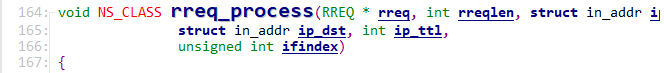
### aodv\_socket\_cleanup函数

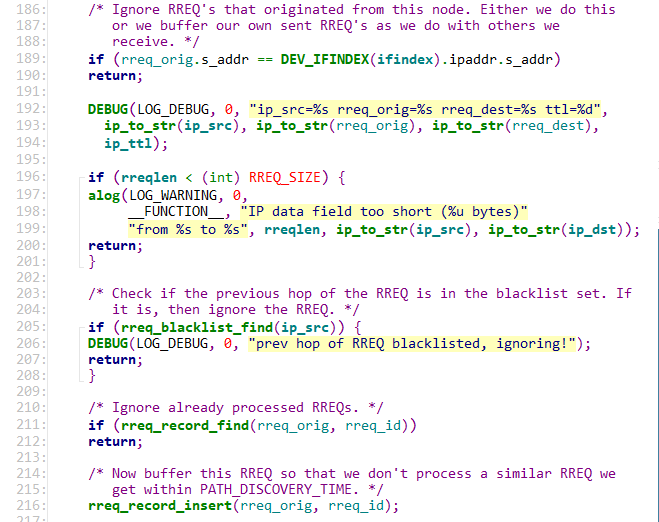


513-525 关闭每个开放接口的套接字连接

## AODV\_rreq.c

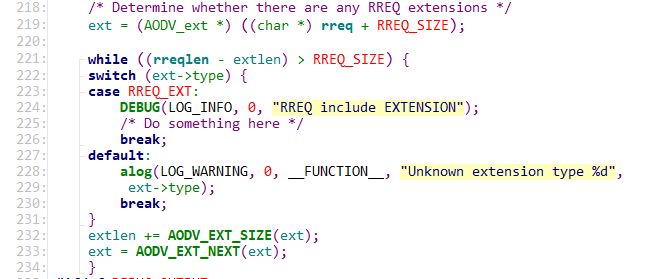
### rreq\_process函数-处理rreq消息



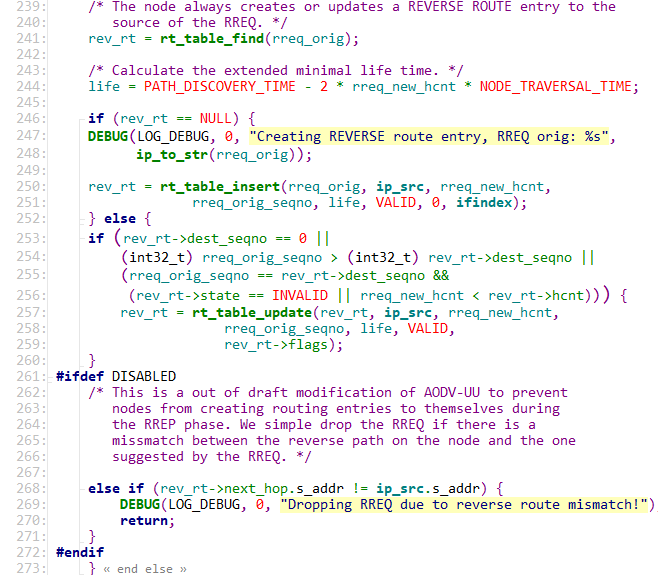


186-212 检查rreq消息，如果来自节点自身或已被加入黑名单或已有记录，则忽略该消息

216 将该消息加入record中，防止在路由发现时间内处理相同的消息



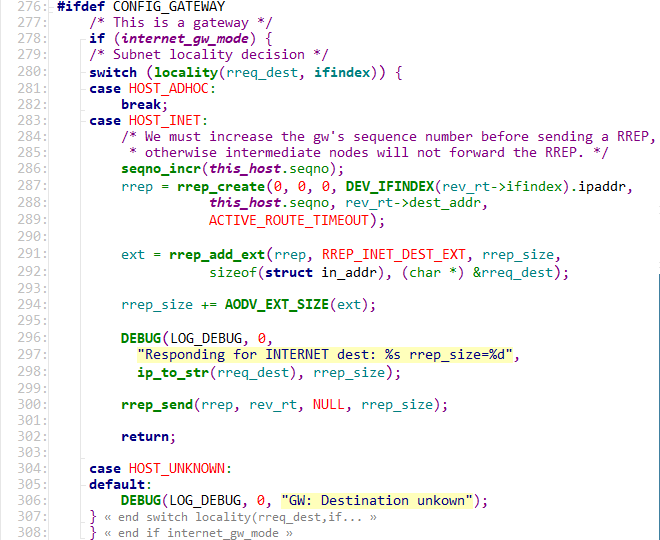
218-237 检查是否还存在RREQ拓展消息



241-273 更新反向路由，具体方法为：

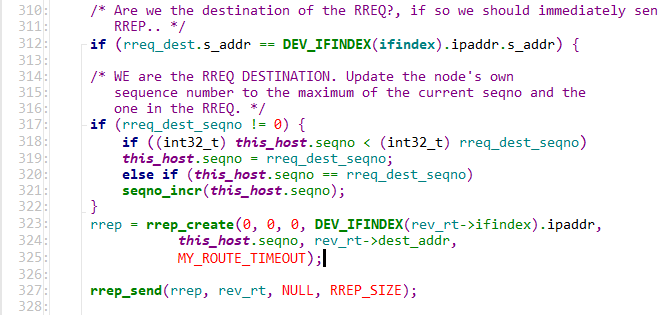
1. 如果路由表没有该rreq的源地址，则插入一条关于该源地址的路由表项；
2. 如果路由表有关于源地址的路由表项，满足下面三个条件之一则更新路由表项
3. 路由表的目的地址序列号为0；
4. Rreq的目的地址的序列号是否大于路由表项的序列号；
5. 序列号相等但是rreq跳数较少或者该路由表项因超时等失效了

268-271检查是否在RREP阶段建立了自环

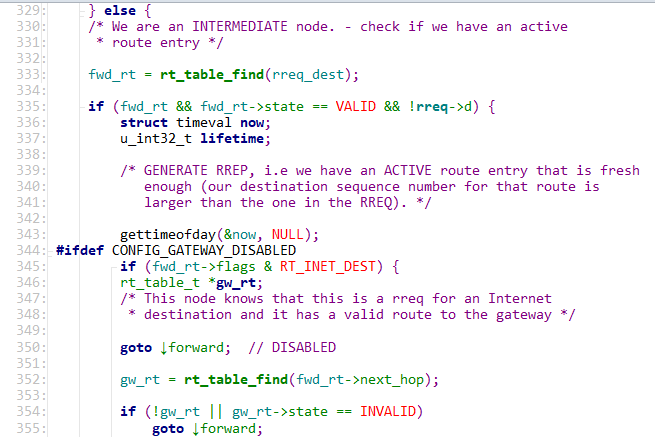


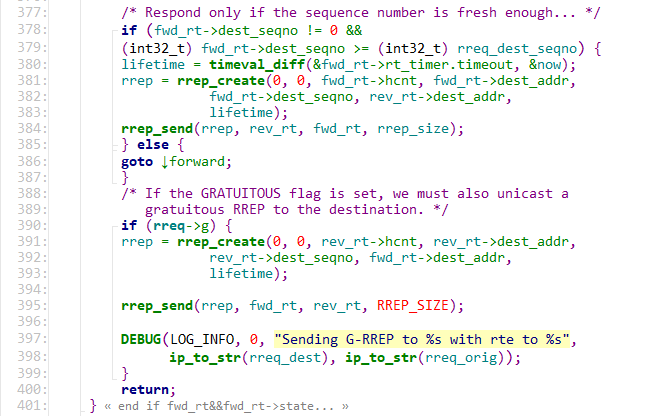
281-306 如果网关的模式，如果为HOST\_INET，则序列号自增，并创建和发送rrep消息

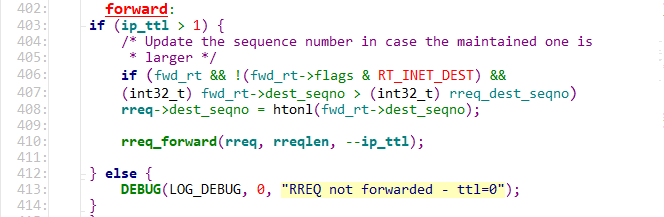
防止中间节点不转发rrep消息？



310-327 如果本节点为rreq的目标节点，更新自己的序列为rreq序列号如果自己的序列号与rreq序列目的地序列号相同，则更新自己序列号维rreq目的地序列号+1，然后回复rrep消息

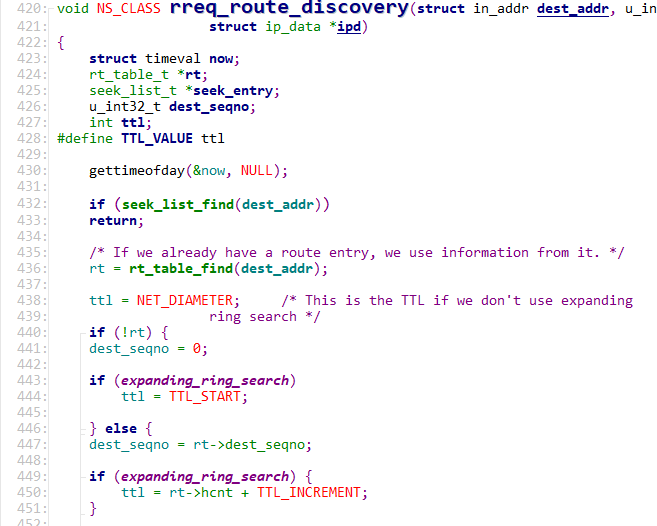


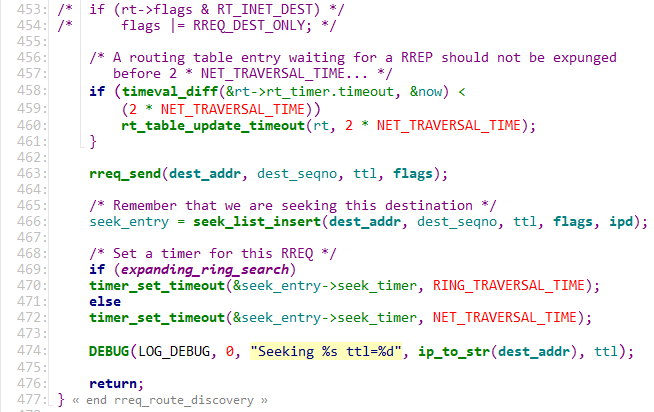




329-343,377-401，402-414如果本节点不是目标节点则查找路由表中有无该路由表项如果有有效的路由表项，当路由表的序列号比rreq目的地序列号大或者rreq的g为1的时候回复rrep否则转发ttl>1的rreq消息

### rreq\_route\_discovery函数-路由发现过程





432 如果源节点路由表中存在到目的节点的路由，则不调用AODV协议

434-463 如果没有，源节点广播rreq消息并记录在seek\_list里面

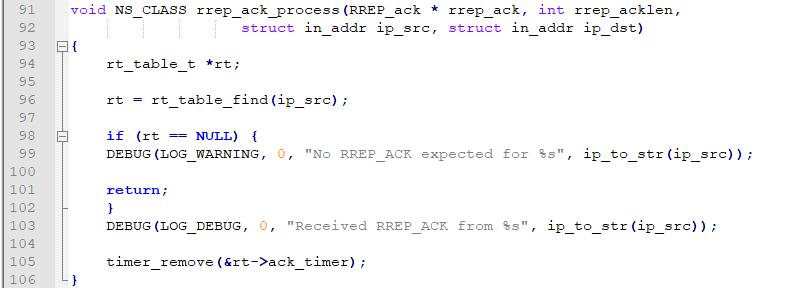
### 其他函数

|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| void NS\_CLASS rreq\_send | 116-136 | 向所有端口转发rreq消息 |
| void NS\_CLASS rreq\_forward | 138-162 | 跳数加1，并向所有端口转发rreq消息 |
| RREQ \*NS\_CLASS rreq\_create | 61-96 | 创建rreq消息，设置jrgd四个参数值。当一个节点要产生RREQ洪泛之前，必须要增大序列号， |
| AODV\_ext \*rreq\_add\_ext | 98-114 | 增加rreq拓展消息 |
| void NS\_CLASS rreq\_local\_repair | 480-540 | 作用与路由发现函数类似 |
| NS\_STATIC struct rreq\_record \*NS\_CLASS rreq  \_record\_insert | 542-572 | 记录rreq消息 |
| NS\_STATIC struct rreq\_record \*NS\_CLASS rreq\_record\_find | 574-587 | 查找rreq消息是否在记录中 |
| void NS\_CLASS rreq\_record\_timeout | 589-595 | 销毁记录 |
| struct blacklist \*NS\_CLASS rreq\_blacklist\_insert | 597-621 | 将某目的地址加入黑名单 |
| struct blacklist \*NS\_CLASS rreq\_blacklist\_find | 623-634 | 查找目的地址是否在黑名单中 |
| void NS\_CLASS rreq\_blacklist\_timeout | 636-643 | 销毁黑名单 |

## AODV\_rrep.c

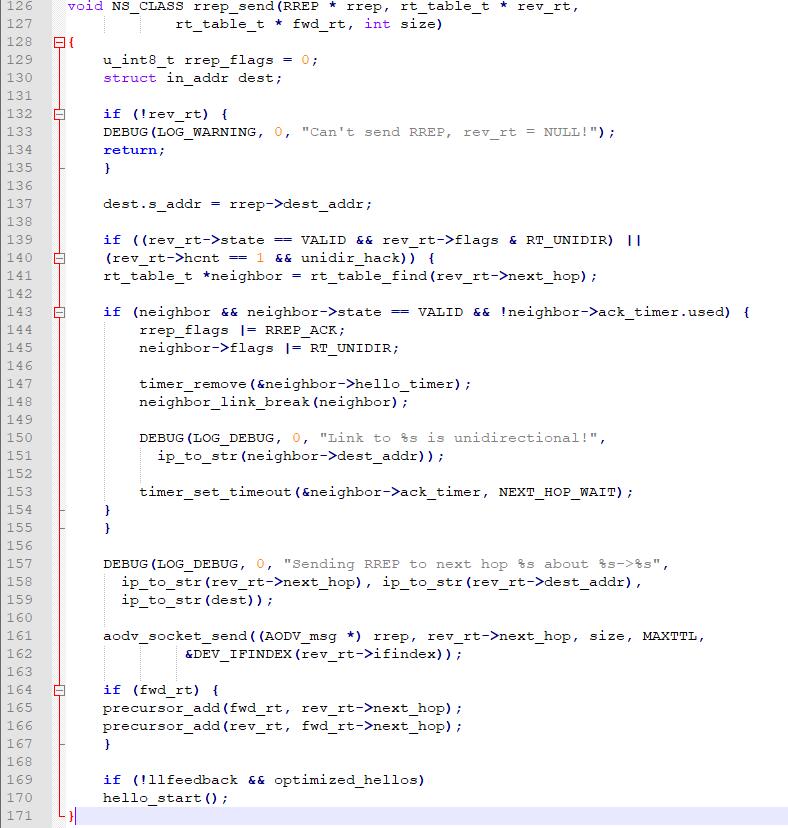
路由节点进行路由发现的时候，RREP路由控制帧会从目的节点或中间节点单播回原节点，这时候中间节点和源节点都会收到RREP帧，所以需要有RREP帧的处理函数。同时中间节点需要发送RREP帧，所以还要有生成和发送RREP帧的函数。

### rrep\_ack\_process函数



91-106 判断路由表中是否有该包的源IP相关路由项，如果没有就说明该消息非法，如果有则在控制台显示相关信息，移除ack计时器。

### rrep\_send函数-发送rrep消息



132-135 如果当前节点路由表为空，那么不能发送RREP消息

139-141 检查是否应该发送RREP\_ACK消息

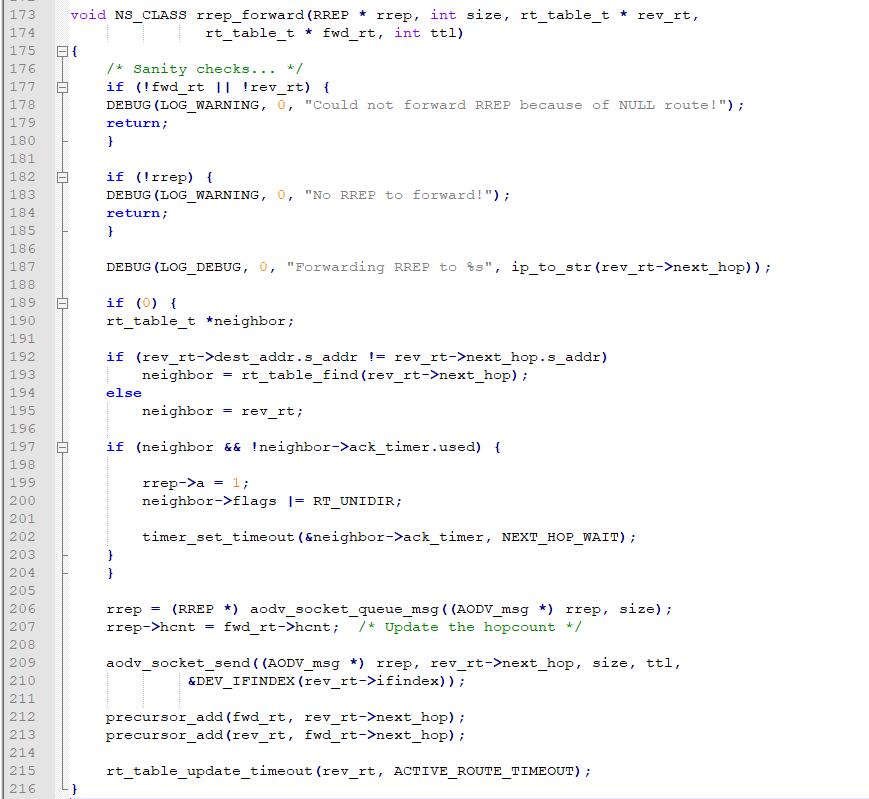
143-155 如果邻居存在并且邻居的状态是有效的，计时器还没使用，那么就将包的flag设置为RREP\_ACK，邻居标记为非单向，移除邻居的hello计时器，设置ack计时器。

157-159  更新路由表项

161-161 交由aodv\_socket\_send函数去发送消息

164-167 更新fwd\_rt和rev\_rt的前驱节点

### rrep\_forward函数-转发rrep消息



176-180 当路由表项fwd\_rt或rev\_rt不存在时，无法进行转发，因此返回；

182-185当rrep是空时，返回

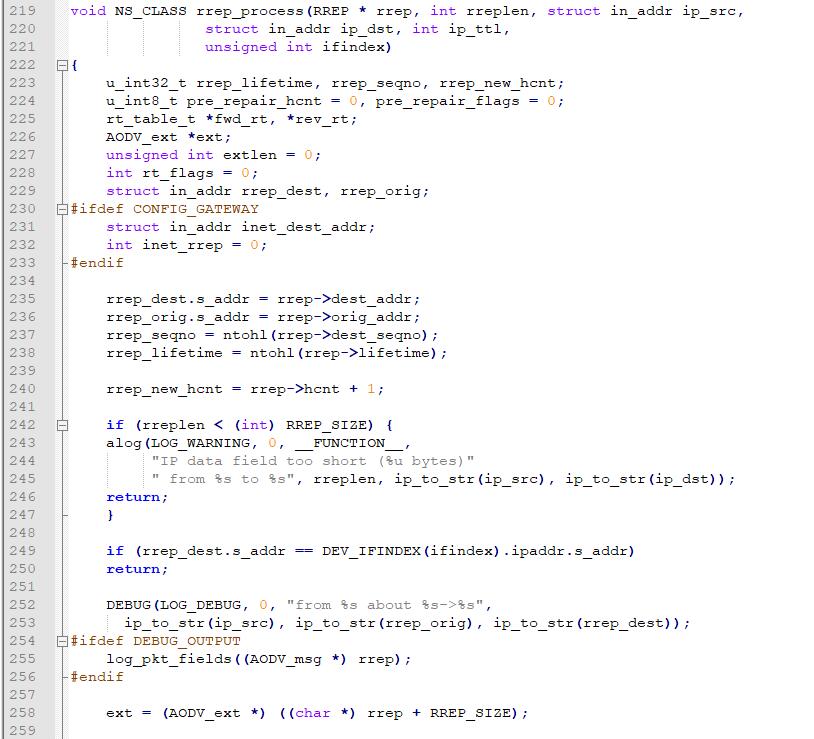
192-195 如果RREP消息的源IP地址不是相邻节点，那么我们必须找到通向源节点的下一跳IP地址。

197-204 如果我们收到邻居的RREQ控制帧，那么我们可能面临单项连接，需要将该链路设置为非单向，然后设置定时器，请求RREP\_ACK。

206-216 ，将RREP加入消息队列，交由下一函数发送，更新前驱列表，更新路由表项的有效时间

### rrep\_process函数-处理rrep消息

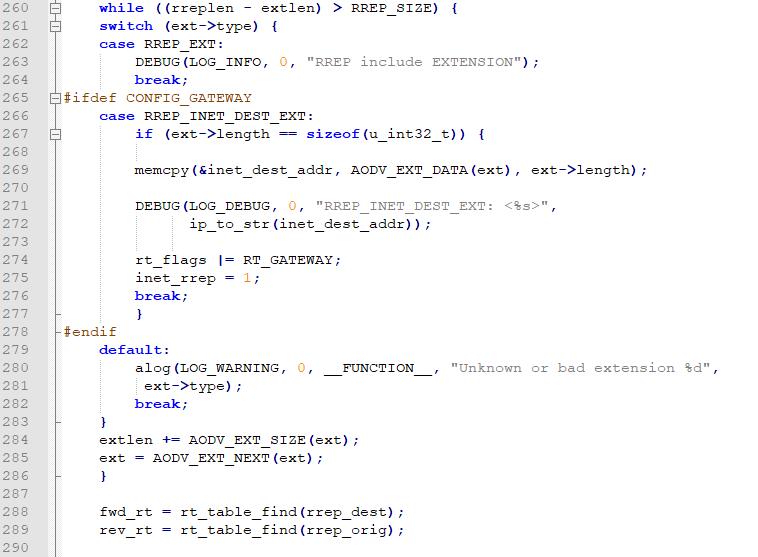
当套接字接收到RREP回复帧的时候，经过初步的过滤操作，最终会递交给这个函数进行处理。一个节点接受到RREP回复帧的时候需要判断是否是自己发出的RREQ回复的，如果不是则查询路由表项，将RREP重新单播回去。



223-240 声明变量，提取RREP回复帧中的各种消息，方便后续使用

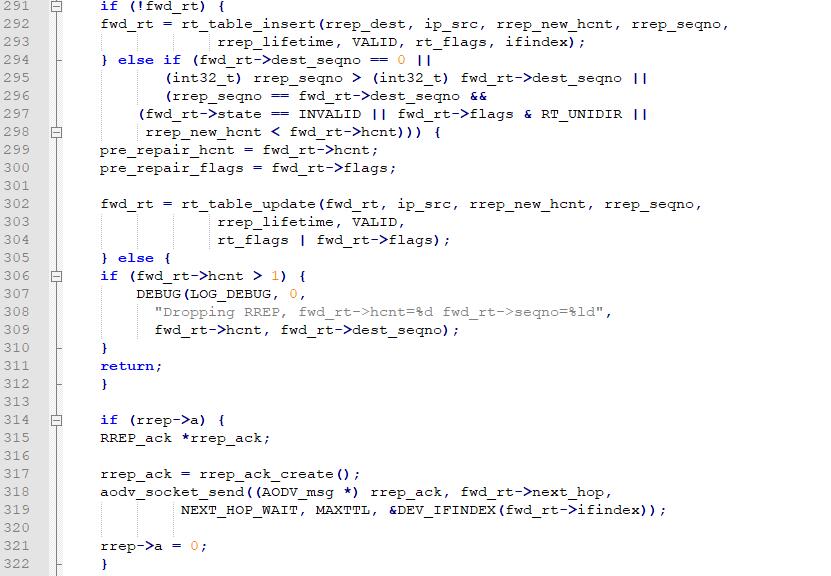
242-247 如果RREP包的长度小于限定值，显示错误信息，返回

249-250 如果是自己发出的包，直接忽略



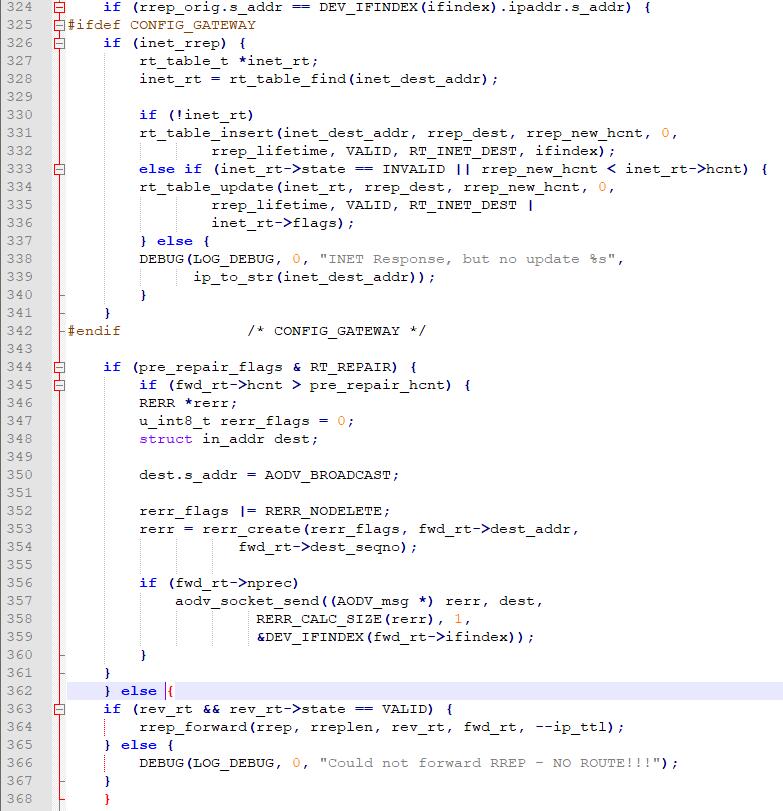
260-286 如果包的长度减去扩展长度仍大于RREP包的设定大小则进入该循环。该循环对RREP扩展和目的节点的拓展进行处理

288-290 获取有关RREP目的节点和源节点的路由表项以待后续使用



291-312 如果没有关于目的节点的表项，那么就在路由表新加入该表项，如果有而且序列号大于路由表项记录的序列号，那么更新路由表，否则忽略

314-322 检测是否需要发送RREP\_ACK，需要则发送



324-368 如果源地址就是本节点，那么如果定义了默认网关，就进行对应的更新和插入操作。如果断开的节点处于被修复状态，一个NODELETERERR应该被发送到源节点，源节点重新发起路由发现过程。如果源地址不是本节点，判断是否需要转发RREP包，需要转发则转发。

369-370 根据条件，决定是否开启HELLO帧。

### 其他函数

一些实现上与RREQ帧重复的和不是那么重要的函数以表格的形式展示，就不进行深入解读了

|  |  |
| --- | --- |
| 名称 | 功能说明 |
| RREP \*NS\_CLASS rrep\_create | 该函数通过传入的参数设置RREP包的prefix，hop count，目的IP和对应序列号，源IP和对应序列号等信息，返回一个新创建好的RREP包 |
| RREP\_ack \*NS\_CLASS rrep\_ack\_create() | 创建RREP\_ACK控制帧 |
| AODV\_ext \*NS\_CLASS rrep\_add\_ext(RREP \* rrep, int type, unsigned int offset, int len, char \*data) | 为RREP包添加扩展，并返回拓展后的包 |
| int rrep\_add\_hello\_ext(RREP \* rrep, int offset, u\_int32\_t interval) | 在RREP中包括Hello Interval扩展并返回新的偏移量 |

## aodv\_rerr.c

### rerr\_create函数-创建

该函数有三个形参，包括：flag，dest\_addr，dest\_sepno。C:\Users\755261024\AppData\Roaming\Tencent\Users\755261024\QQ\WinTemp\RichOle\7I29ID5EG]G5OH`J7576IJE.png

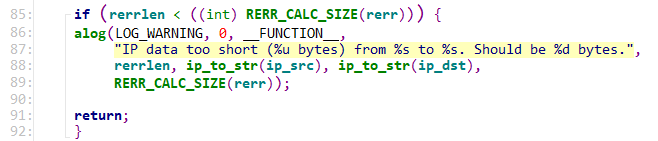
flag有0和1两个值，置1时，表示路由已经执行了错误链路的修复，前驱节点不用再删除路由；dest\_addr和dest\_seqno分别表示不可达地址的IP和序列号。

### rerr\_add\_udest函数-添加

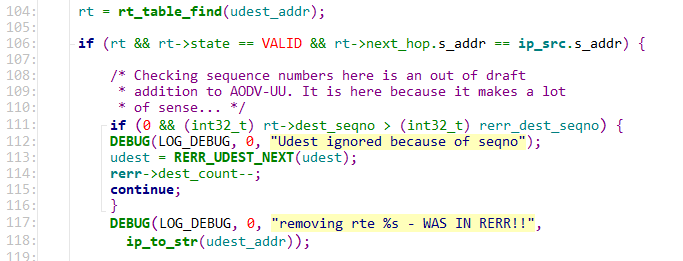
当一个节点收到一条rerr消息后，会在本节点路由表中查找是否包含不可达节点的前驱，若包含，通过调用rerr\_add\_udst函数，添加一条不可达节点到rerr消息中。

### rerr\_process函数-处理

节点收到一条rerr消息后，调用该函数。程序的流程如图所示：



85-92首先判断数据包的有效性，若收到的rerr消息，小于RERR\_CALC\_SIZE（rerr）时，说明该rerr在传输的过程中出现错误，丢弃数据包；



104-116 判断数据包有效后，节点在本地路由表中查找不可达节点。找到不可达节点后，若该节点所在路由表项依然有效。在111行，比较不可达节点的目的序列号和路由表中最新节点的序列号，如果后者大于前者，则说明接收到的rerr消息已经过期，直接丢弃。否则，117行，删除改有效路由表项。 

124-126 调用rt\_table\_invalidate函数，将包含不可达节点的表项设置为无效。

135-170 判断不可达节点是否包含前驱节点。若new\_rerr仍为NULL，生成一条新的rerr消息，将不可达节点IP加到不可达列表中。若包含一个前驱节点，将该前驱节点地址设置为rerr消息单播地址。若包含多个前驱节点，，将所有节点添加到本节点新生成的rerr消息中。

176-177 删除所有不可达节点的前驱节点



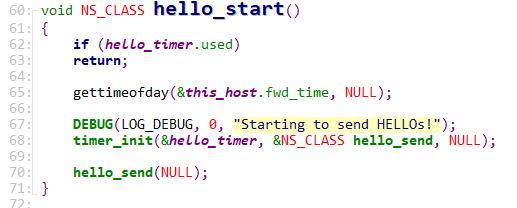
190-209 发送新生成的rerr消息。若只有一个目标节点，则单播该消息。否则，将rerr消息逐个发送到受影响的节点中。因为本段代码将ttl=1，所以仅发送给本节点的邻居节点。

## aodv\_hello.c

### hello\_jitter()函数-设置jitter值

该函数返回一个long型数值，用于表示在不同发送条件下，可以允许的hello消息发送时间的抖动值。

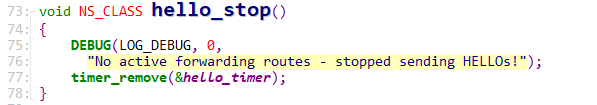
### hello\_start()函数-启动hello消息



62-63 若定时器处于开启状态，直接返回

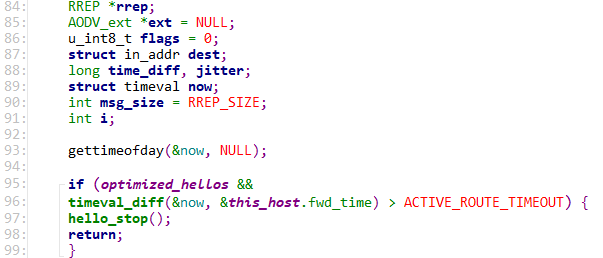
65-70 开启hello消息计时器，首先获取系统当前时间，设定DEBUG参数，表示开启发送hello消息的操作。68行，启动hello消息定时器，70行，将hello消息发送出去。

### hello\_stop()函数-停止hello消息



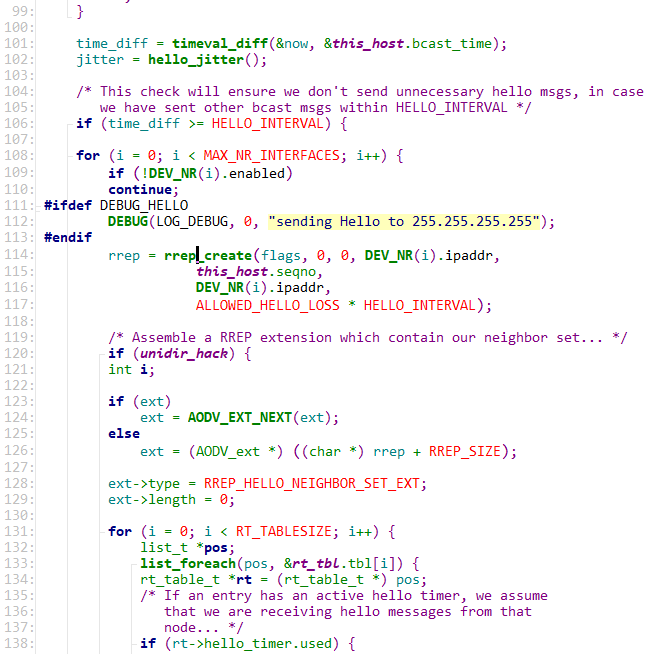
75-77： 调用DEBUG函数，输出无有效转发路由提示，然后将hello消息的计时器从计时器队列中移除。则hello消息关闭成功，程序可以重新启动hello消息的发送。

### hello\_send()函数-发送hello消息



84-89 hello消息属于rrep消息类型。所以发送函数想要发送一个hello消息，首先要构造一条rrep消息。这些参数的功能分别是：dest，属于in\_addr结构体，用于存放目的地址; now，属于timeval结构体，用于存放系统当前时间；msg\_size，整型数据，用于存放刚刚生成的rrep数据包的大小。time\_diff 和 jitter是用于计时的参数。

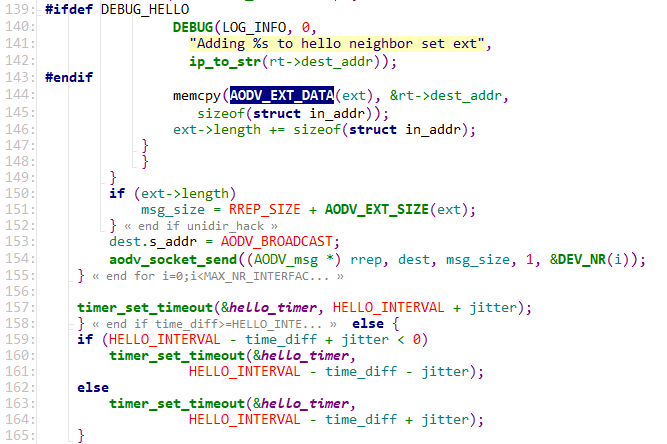
91-97：获取系统当前时间，存放于now中。计算当前时间与上次发送hello数据包的时间差，若大于路由超时时间，则说明节点和邻居节点的链接处于断开状态，调用hello\_stop函数，关闭hello消息，函数返回。



99-104：计算当前系统时间与节点上一次广播hello消息的时间，记为time\_diff。若time\_diff大于HELLO\_INTERVAL,说明未发送不必要的hello消息，否则，说明发送了不必要的消息。

104-110 查看每一个设备是否处于就绪状态，如果设备就绪且DEBUG\_HELLO已经定义，则广播hello消息并输出消息提示。

111-136 宏DEBUG\_HELLO未定义，通过调用rrep\_creat函数组装一个rrep数据包，将所有的邻居节点加到这个数据包中。



137-147：在此判断DEBUG\_HELLO, 如果已经定义，则将rt节点的所有dest\_addr添加到rrep数据包的邻居组中，否则，将dest\_addr中长度为in\_addr的结构体长度的字节，通过调用memcpy函数，添加到AODV\_EXT\_DATA中，同时更新ext的长度。

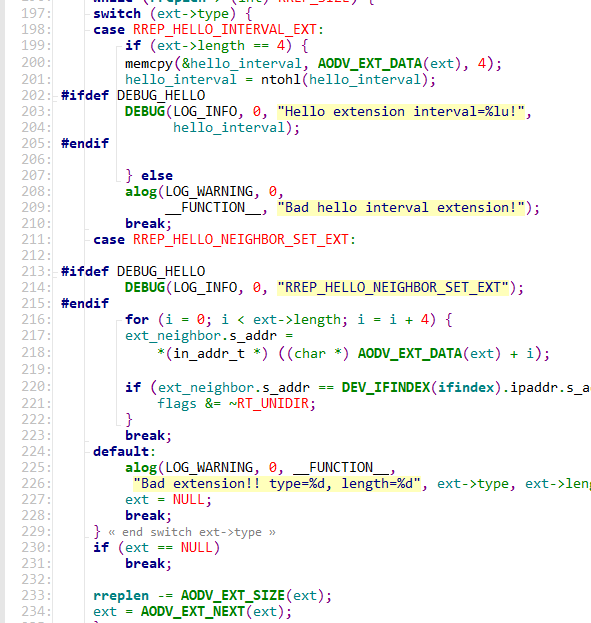
148-157：初始化数据包的大小，将组装好的rrep消息，广播给所有的邻居节点。调用time\_set\_timeout函数，设定计时器时间为HELLO\_INTERVAL + jitter；

157-162：如果两个hello消息的时间差小于设定的标准时间差，差值小于抖动值jitter，设定hello消息计时器的值为HELLO\_INTERVAL - time\_diff – jitter，否则，设为HELLO\_INTERVAL - time\_diff + jitter；

### hello\_process()函数-处理hello消息



172-191 接收hello消息，并在自己的路由表象中查找hello消息中包含的dest\_addr条目。找到对应条目后，将flag的值设为1。



197-234：如果接收到的hello消息长度有效，根据ext->type构成switch语句，从接收到的两次相邻的hello消息，计算时间间隔。同时记录rrep消息的长度。

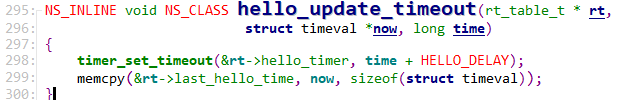
240-246：要成功接收到来自邻居节点的三条连续hello消息才有效。收到三条hello消息，则对应的receive\_n\_hellos置1，则state置为VALID，否则，state为INVALID。

248： 计算hello消息的超时时长timeout。

250-264：如果本节点的路由表项内，没有找到和hello消息中dest\_addr相关的路由表项，则在路由表中调用rt\_table\_insert()函数添加一个新的路由表项，通过包含hello消息的rrep数据包，初始化新的路由表项。

265-282 在路由表中找到对应的表项后，则通过执行hello\_update程序，增加该表项的生命周期。同时，若这条路由表项包含hello消息中的目的序列号，则表项中hello\_cnt+1，否则，通过调用rt\_table\_update()函数，将hello消息中的目的序列号添加到路由表项中。

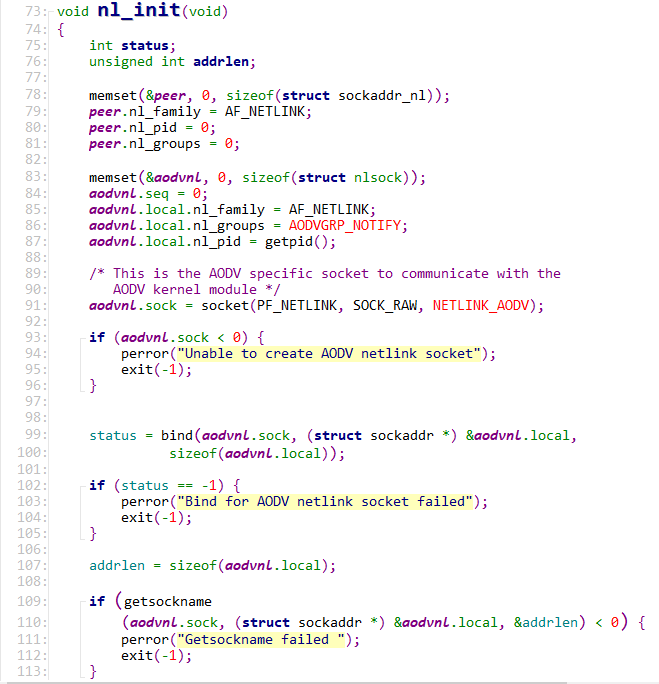
### hello\_update\_timeout()函数-更新timeout



295-300： 由于存在处理消息的时间，所以在假设hello消息超时之前，应该允许占用额外的时间，即将timeout增加一段处理消息的时间。

## Nl.c

### Nl\_init函数-初始化函数





以上为nl\_init函数第一部分主要是建立AODV套接字，此套接字负责与AODV内核模块通信。

75-87：将aodvnl，peer分别进行初始化

91：创建一个原始套接口，这是AODV特定的用于与AODV内核模块通信的套接口，socket函数第一参数为PF\_NETLINK，表明套接字遵循协议族NETLINK。第二参数SOCK\_RAW，表明采用原始套接字。第三参数NETLINK\_AODV，表明采用的协议为AODV特有的netlink协议。具体的AODV的netlink部分在/lnx/kaodv-netlink中，这部分将在3.11中具体阐述

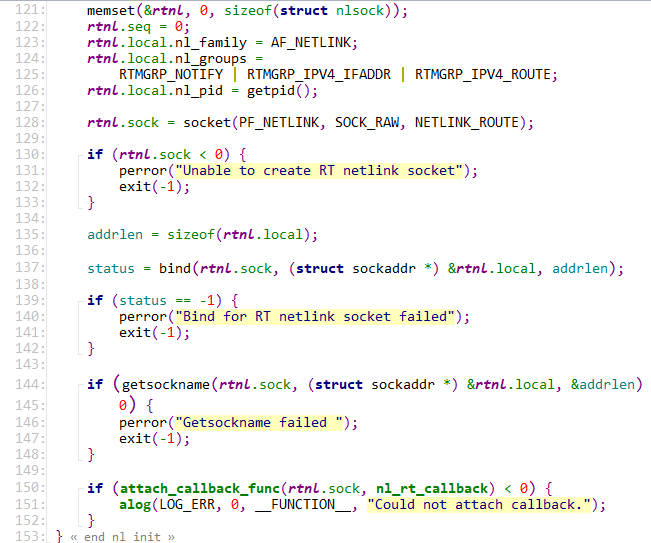
93-96：如果创建套接字失败，则输出Unable to create AODV netlink socket，并返回-1

99-100：调用bind函数，为aodvnl创建的套接字关联一个相应地址并赋给state

102-105：如果bind函数出错则输出Bind for AODV netlink socket failed，并返回-1

109-113：获取aodvnl.sock套接字的本地地址保存在aodv.local中，名字缓冲区长度保存在addrlen中，如果返回失败则返回-1退出

115-117 nl\_kaodv\_callback函数和aodv套接字放入到callback结构体里面



以上为nl\_init函数的第二部分，主要是创建的rtnl套接字

122-126：对rtnl进行初始化并赋值

128：将rtnl.sock创建为一个原始套接口，这个套接口通用路由套接口，是用于添加和的删除内核路由表项

130-133：如果这个套接口创建失败，则输出nable to create RT netlink socket并返回-1退出

137：调用bind函数，为rtnl创建的套接字关联一个相应地址并赋给state

139-142：如果赋予协议地址出错，则输出Bind for RT netlink socket failed并返回-1退出

144-148：如果获取rtnl.sock的本地地址失败，则输出Getsockname failed 并返回-1退出

150-153：l\_kaodv\_callback函数和aodv套接字放入到callback结构体里面,如果失败，则输出Could not attach callback.

### Nl\_kaodv\_callback函数-根据aodv套接字中收到的不同命令，执行不同的回调函数



164-171：addrlen：socklen\_t类型

nlm：nlmsghdr类型的指针, nlmsghdr具体如下

nlmerr：nlmsgerr类型的指针该结构体携带有错误消息

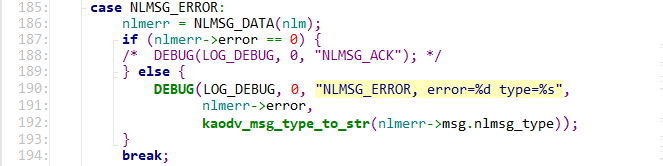
dest\_addr，src\_addr：in\_addr类型的指针，分别表示目的IP地址和源IP地址

m：kaodv\_rt\_msg\_t类型的指针，在kaodv-netlink.h中定义，携带aodv路由消息

rt, fwd\_rt, rev\_rt：rt\_table\_t类型的指针，代表路由表项

179-180：如果读取失败，便返回空

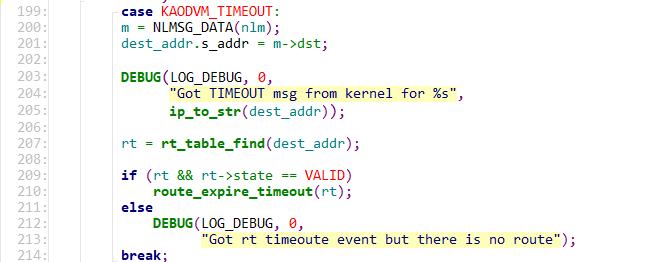
184：根据内核套接字nlm接受到的不同命令类型选择不同的处理方式



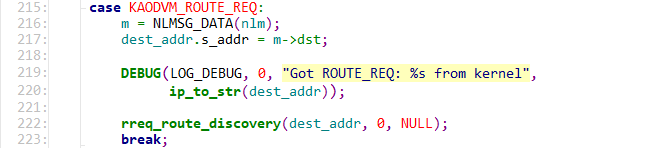
185-197：如果nlm的类型为NLMSG\_ERROR，且nlmerr->error值不为0，则输出错误信息，包括错误号和错误类型



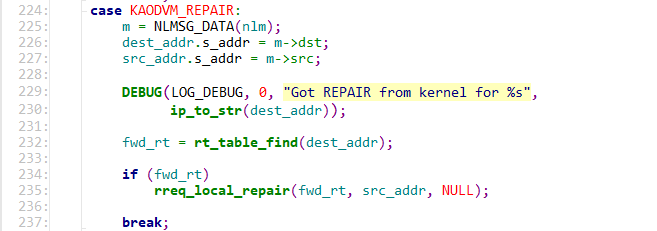
196-198如果消息类型为KAODVM\_DEBUG则输出输出附带的调试信息



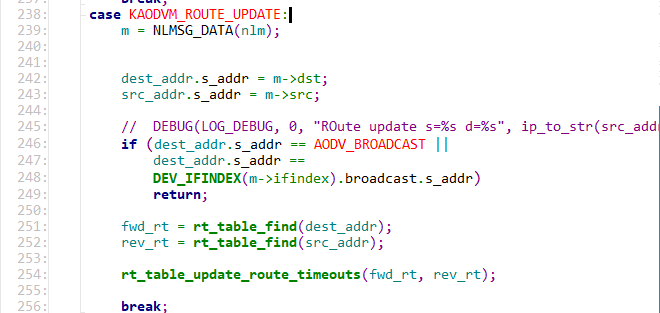
199-214如果消息类型为KAODVM\_TIMEOUT,如果路由表中目的地的路由表项有效，则将它设置为超时无效状态



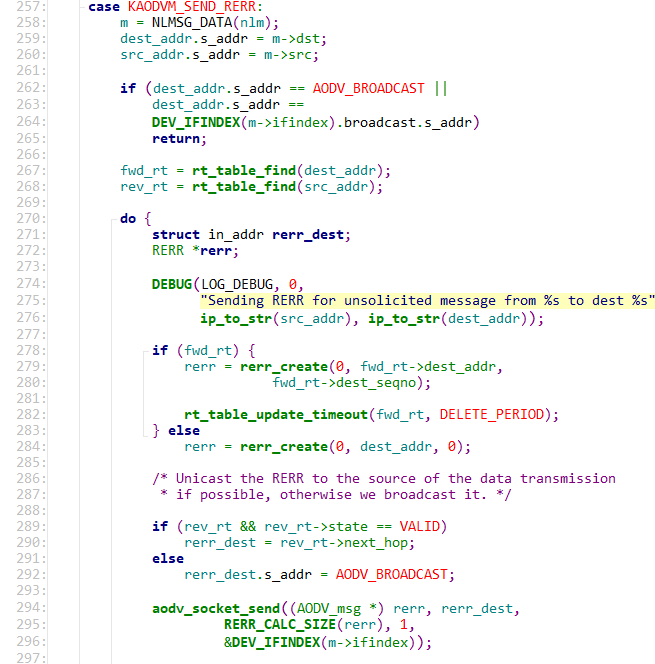
215-223如果消息类型为KAODVM \_ROUTE\_REQ类型，开始路由发现过程

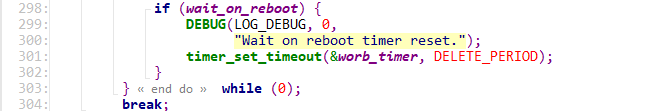


224-237 如果类型为 KAODVM \_REPAIR且目的地址在路由表中，开始本地修复过程



238-256：如果类型为 KAODVM\_ROUTE\_UPDATE，如果要广播目的地址，那么便返回，否则刷新路由表中路由表项的过期时间





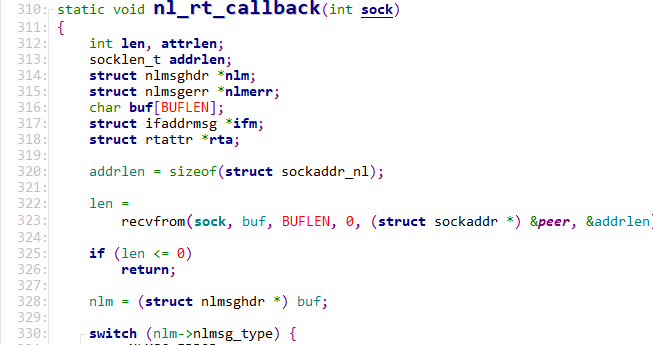
257：如果类型为KAODVM\_SEND\_RERR

262-268：如果目的地址是广播地址，那么便返回空，否则便找到目的地址和源地址

270-287：进入循环，如果路由表有关于目标地址的路由表项，则创建一个rerr 的消息类型，并且更新该路由表项的过期时间，否则便创建一个将序列号置为0的rerr类型的消息

289-303：如果源地址路由表项类型的状态是VALID，那么便将这个rev\_rt的目的地址指向下一跳，否则便广播目的地址，也就是说如果可能我们将单播RERR从源地址的数据传输，否则我们将广播它

### Nl\_rt\_callback函数-根据路由套接字中收到的不同命令，执行不同的回调函数



312-318：addrlen：socklen\_t类型，用于表示地址长度

nlm：nlmsghdr类型的指针

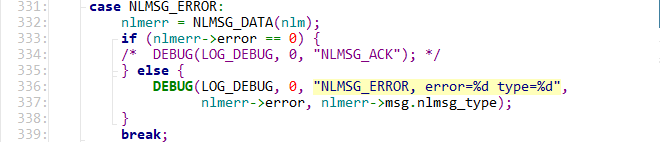
nlmerr：nlmsgerr类型的指针

ifm：ifaddrmsg类型的指针，该类型的消息携带添加,删除或者接收一个和接口相关的IP地址的信息

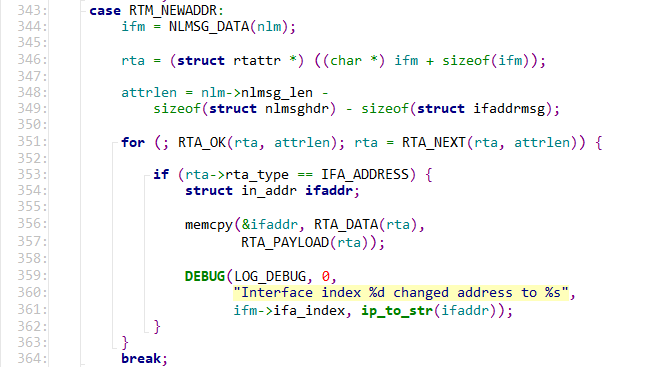
rta：rtattr类型的指针，创建或者删除一个特定的网络接口，或者从一个特定的网络接口上获得信息会使用到该类型

322-326：如果recvfrom调用失败，则返回空

330：根据nlm->nlmsg\_type即路由套接字收到的不同命令选择分支语句

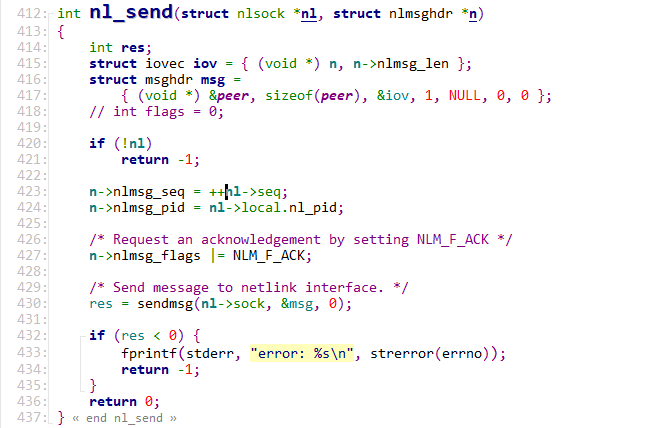


331-339：如果值为NLMSG\_ERROR且nlmerr->error的值不为0，则输出错误编号和类型



343-364如果值为RTM\_NEWADDR，则首先为ifm、rta、attrlen赋初值。在rta队列中寻找谁的rta\_type的值为IFA\_ADDRESS，则将RTA\_PAYLOAD(rta)长度的RTA\_DATA(rta)复制到&ifaddr，即将对应端口的IP地址改为消息指定的IP地址。

### Nl\_send函数-发送数据包给内核模块



415-420：如果nl指针不为空，那么便对指针n进行赋值，否则便返回-1

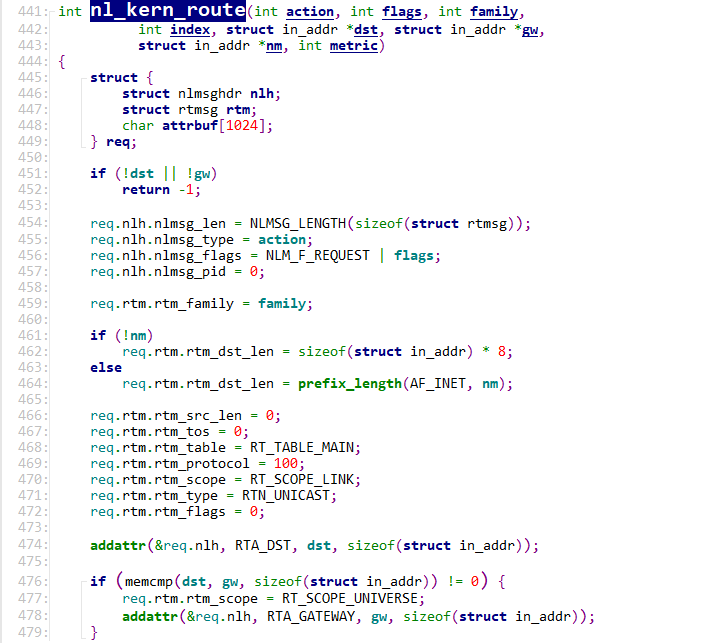
423-424序列号加1，设置目标的pid

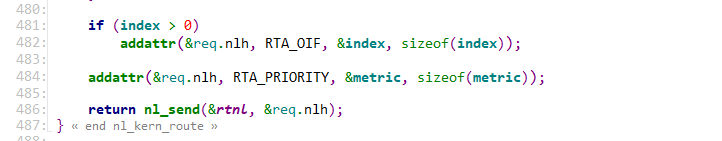
427：通过设置NLM\_F\_ACK来请求确认

430：发送消息到netlink接口，res为负，表明函数调用失败

432-435：如果函数sendmsg（）调用失败，便打印出error，退出函数，返回-1

### Nl\_kern\_route函数-操作内核路由表，包括增加、修改、删除路由表条目等操作





445-449：定义结构体req，包括一个nlmsghdr结构体,一个rtmsg结构体和一个char数组

451-452：如果没有目标IP地址或没有网关IP地址，则退出函数，返回-1

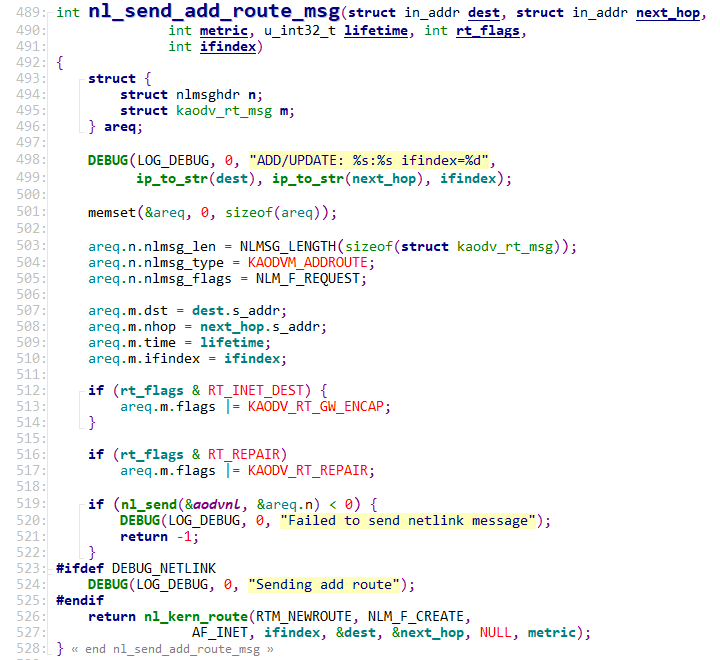
454-459：对req的成员变量进行赋值

461-462：如果nm的值为0，则req.rtm.rtm\_dst\_len便重新赋值，并再添加一个RTA\_GATEWAY类型的路由表项

481-483：如果index的值大于0便添加一个类型为RTA\_OIF的attribute

484：添加一个类型为RTA\_PRIORITY的attributer

### Nl\_send\_add\_route\_msg函数-向内核发送一个添加一个路由信息的消息，包括目的地地址、下一跳，生存期，路由状态标志，网络接口等



492-496：定义areq的结构体,包括一个nlmsghdr结构体和一个kaodv\_rt\_msg结构体（在kaodv-netlink.h中定义）

501：清空areq结构体

503-510：为areq的结构体进行赋值

512-513：如果rt\_flags右起第四位为1，则对areq.m.flags右起第一位置为1

516-517：如果rt\_flags右起第二位为1，则对areq.m.flags右起第二位置为1

519-521：如果nl发送失败，则打印消息后退出函数返回-1

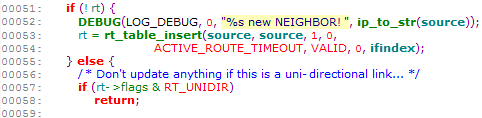
### 其他函数

|  |  |  |
| --- | --- | --- |
| 函数名 | 行数 | 说明 |
| void nl\_cleanup | 155-159 | 关闭两个套接字 |
| int prefix\_length | 372-391 | 计算前缀长度 |
| int nl\_send\_no\_route\_found\_msg | 530-549 | 向内核发特定目标地址没有找到路由消息 |
| nt nl\_send\_del\_route\_msg | 551-581 | 向内核发删除特定路由的消息 |
| int nl\_send\_conf\_msg | 583-604 | 向内核发送设置参数 |

* 1. Aodv\_neighbor.c

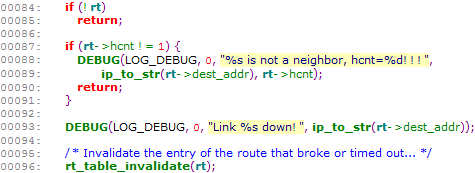
**3.10.1更新活跃的邻居节点（更新来自非HELLO AODV控制消息的邻居）（void NS\_CLASS neighbor\_add）**

 代码如下：

 043-045 行代码定义了变量类型，now的作用是记录当前时间； rt作用是用作路由表（初始值设置为NULL）；seqno作用是序列号（初始值设置为0）。

051-055行代码判断路由表上是否存在sourse指向的目的节点。若不存在，利用rt\_table\_insert()函数传入参数、添加路由信息。

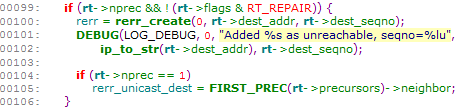
 056-059 行代码判断如果为单向链路直接返回，不用更新路由信息。

 067-068 行代码表示如果路由信息是存在且活跃的，则需要用ALLOWED\_HELLO\_LOSS \* HELLO\_INTERVAL来添加对应路由的活跃周期。

### 3.10.2邻居节点链路中断情况（void NS\_CLASS neighbor\_link\_break）

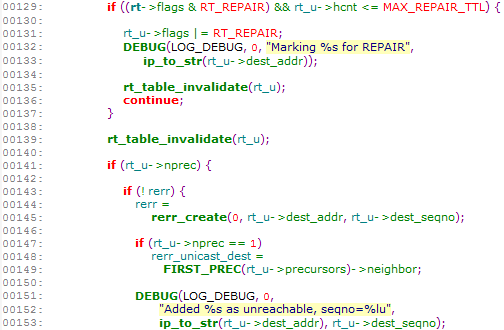
084-086 行代码判断路由表是否为空若为空则直接返回。

087-092 行代码判断若rt->hcnt跳数不为1时，则不是直接邻居节点。将目的地址和跳数传入函数并返回。

 096 行代码若判断函数为跳数为1的直接邻居节点，输出链路断开信息并将目的地址传入。同时将对应的路由表置为无效化。

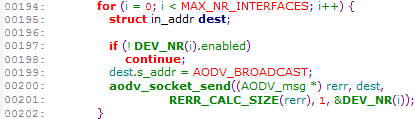
099-106行代码，除去路由被回复的情况，创建一个路由错误信息rerr。调用rerr\_create()函数来传入目的地址和序列号。

109-110 行代码用来清除了路由前驱列表。

129-152 行代码用来检测路由表的下一跳条目中知否存在不可达的目标。如果条目是不可达的，应包含在RERR中。

131-137 行代码，将损失的链接标记为要修复。

139-153 行代码将损失的链接标记为要修复的情况下，在对其他所有不可达条目应执行相同的操作。

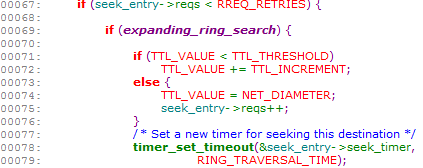
194-202 行代码表示只在不可达路由结点的先驱结点的接口上传输RERR。

## 3.11 Aodv\_timeout.c

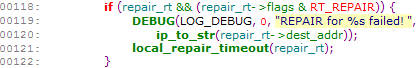
### 3.11.1定义定时器到期时调用的超期函数

059-061 行代码检查完整性。

063-065 行代码记录当前时间并写在日志中。

067-079 行代码当不满足超时的条件时，设置一个新的计时器来寻找目的地址。

088-090 行代码AODV应该使用二进制指数来退避RREP等待时间。

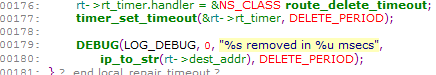


118-122 行代码保证了当路径被修复后，节点返回超时信号。

### 3.11.2.定义本地修复超时处理函数

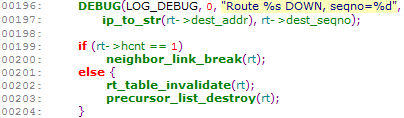


137-140 行代码默认了目的地，并清除RERAIR标志。



176-181 行代码表当修复超时，清除可能在排队中的数据包，并记录到日志中。

### 3.11.3.设置路由过期超时函数



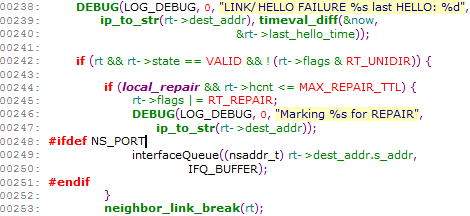
196-204 行代码当路由消息长时间没有收到对应的HELLO()函数消息时，设置这条路由超时，将其断开，并从路由表里删除。

### 3.11.4.路由删除函数设置



214-217行代码进行路由表完整性检测。从路由表中删除路由信息，并记录在日志中。

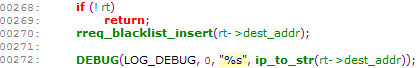
### 3.11.5.HELLO消息超时函数



238-253 行代码表示当我们停止接收来自邻居节点的HELLO()信息时，这个函数就会被调用。Hello消息超时函数与路由超时功能基本一致。当我们在修理路线时，将其标记（标志位设置为REPAIR）进行维修.

缓冲区内容来自接口队列的数据包。

### 3.11.6响应超时函数



268-272 行代码，当RREP传输失败时（即缺少RREP\_ACK）时，添加到黑名单设置中。