UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MANAGEMENT INFORMATION BASE (MIB) DE GERENCIAMENTO DE CONFIANÇA EM REDES AD-HOC

BEATRIZ CAMPOS SANTANA

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
PUBLICAÇÃO: PPGEE.DM – 484/12
BRASÍLIA/DF: ABRIL/2012

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MANAGEMENT INFORMATION BASE (MIB) DE GERENCIAMENTO DE CONFIANÇA EM REDES AD-HOC

BEATRIZ CAMPOS SANTANA

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA.

APROVADA POR:

RAFAEL TIMÓTEO DE SOUSA JÚNIOR, Doutor, ENE/FT/UnB.
(ORIENTADOR)

ROBSON DE OLIVEIRA ALBUQUERQUE, Doutor, ENE/FT/UnB.
(EXAMINADOR INTERNO)

GEORGES DANIEL AMVAME-NZE, Doutor, FGA/UNB.
(EXAMINADOR EXTERNO)

DATA: BRASÍLIA/DF, 17 DE ABRIL DE 2012.

FICHA CATALOGRÁFICA

SANTANA, BEATRIZ CAMPOS

Management Information Base (MIB) de Gerenciamento de Confiança em Redes Ad-Hoc. [Distrito Federal] 2012. xvii, 170p.,210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2012).

Dissertação de Mestrado – Universidade de Brasília.

Faculdade de Tecnologia. Departamento de Engenharia Elétrica

1. Redes móveis *ad hoc* 2. Gerência de redes

3. Gerência da confiança 4. *Management Information Base* - MIB

I. ENE/FT/UnB II. Título

REFERÊNCIA BIBLIOGRÁFICA

SANTANA, B. C. (2012). Management Information Base (MIB) de Gerenciamento de Confiança em Redes Ad-Hoc. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGEE.DM-484/12, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 170p.

CESSÃO DE DIREITOS

Beatriz Campos Santana
Quadra 01 conjunto I casa 313 Setor Norte
Gama - DF. CEP: 72.430-109
biatze.beatriz@gmail.com

AGRADECIMENTOS

Agradeço a Deus por me colocar dentro de algo superior às minhas expectativas, coberto de pessoas significativas e que contribuíram para o meu crescimento. O sofrimento fez parte de mim em alguns momentos, mas o alívio atribuído ao tamanho da minha fé no Senhor fez com que eu continuasse firme e confiante.

Aos meus pais, José e Maria Socorro, pela força, educação, conselho e espelho de orgulho e exemplo. Aos meus irmãos Andréia, Luiz Felipe e Camilla pelo companheirismo e amizade.

Ao meu orientador, chefe e amigo, Rafael Timóteo. O meu medo se transformou em uma admiração irreparável e o seu espírito bondoso me fez crescer. Obrigada por esta oportunidade!

Ao meu amigo Fábio Mendonça, pelo apoio que me foi dado e pela confiança.

Aos professores Robson de Oliveira Albuquerque e Georges Amvame-Nze, obrigada pelas orientações e ajuda durante o desenvolvimento deste trabalho.

Aos amigos do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE, pela amizade e a paciência de me aguentar todos os dias com as minhas trapalhadas e loucuras.

Ao meu amigo Domingos, pela ajuda e atenção.

Não poderia esquecer-me de agradecer ao meu amigo Érico José, que além de me apoiar nesse projeto me apresentou ao Leonardo Cezar que carinhosamente dispôs do seu tempo para me ajudar, com os seus conhecimentos e habilidades. Aos pinguins da Dataprev, que me acolheram com muito carinho e alegria.

Durante o desenvolvimento desta dissertação, fui bolsista do Centro de Apoio ao Desenvolvimento Tecnológico – CDT e do LATITUDE, em projetos de Cooperação Técnica patrocinados pela Secretaria do Patrimônio da União (SPU), Secretaria de Orçamento Federal (SOF) e da Secretaria de Gestão de Pessoal (SEGEP) do Ministério do Planejamento, Orçamento e Gestão. Agradeço ao CDT e ao LATITUDE, bem como ao Ministério pelo apoio recebido.

Dedico este trabalho aos meus pais, Maria Socorro e José.
Em especial, a minha irmã Andréia que ficou ao meu lado em
todos os momentos, me acompanhou em toda a trajetória,
me fortaleceu e se dedicou com muito carinho a mim.
Muito obrigada! Te amo.

RESUMO

MANAGEMNT INFORMATION BASE (MIB) DE GERENCIAMENTO DE CONFIANÇA EM REDES AD-HOC.

Autor: Beatriz Campos Santana

Orientador: Rafael Timóteo de Sousa Júnior

Programa de Pós-graduação em Engenharia Elétrica

Brasília, Abril de 2012.

Derivado do estudo do fenômeno de mesmo nome existente entre os humanos, vem se estabelecendo um conceito de confiança específico para a área computacional. Tendo aplicação diversificada, tal conceito tem sido muito usado para avaliar o comportamento de diversos componentes de redes computacionais e principalmente para classificar nós (componentes de rede, por exemplo, roteadores), de modo a identificar aqueles que possuem intenções maliciosas e perigosas.

Esta dissertação propõe a criação de uma MIB (*Management Information Base*) de gerenciamento da confiança em redes *ad hoc*, para coletar dados sobre o comportamento dos nós de uma rede e, a partir desses dados, aplicar um cálculo de confiança, de modo a tornar possível observar se o comportamento de cada nó está sendo adequado para o bom funcionamento da rede.

Para a realização deste trabalho, foi necessária a pesquisa de métricas de confiança aplicadas em redes *ad hoc* para a implementação da MIB de confiança. Para efeito de validação da proposta, foram usadas as métricas relacionadas ao protocolo OLSR (*Optimized Link State Routing Protocol*), no qual se observa o comportamento do nó escolhido como MPR (*Multipoint-Relays*), em conformidade com o trabalho (De Sousa Jr. & Puttini, 2010).

A especificação da MIB deu-se através da linguagem de definição SMI (*Structure Management Information*). O ambiente de validação foi desenvolvido com a modificação do *deamon* do OLSR (OLSRD), empregando o aplicativo NET-SNMP para validar e acessar a MIB, apresentando a confiança observada em um ambiente controlado.

ABSTRACT

MANAGEMENT INFORMATION BASE (MIB) FOR TRUST MANAGEMENT IN AD HOC NETWORKS

Author: Beatriz Campos Santana

Supervisor: Rafael Timóteo de Sousa Júnior

Programa de Pós-Graduação em Engenharia Elétrica

Brasília, April of 2012.

Resulting from the study of the phenomena with the same name existent among humans, there is an emerging concept of trust applied to the computational area. With a diversified application, this concept has been widely used for evaluating the behavior of several computational network components, especially for node classification (e.g., routers), in order to identify those that present malicious intentions.

This master thesis proposes the creation of a MIB (Management Information Base) for trust management in *ad hoc* networks, allowing the gathering of data about the behavior of the nodes within a network and, according with this data, the estimation of a trust index that is used to verify if each node is acting adequately for the correct network operation.

To accomplish this work, a survey of trust metrics in *ad hoc* networks was performed, giving way to the choice of objects for creating a trust MIB specific to this environment. In order to validate the proposal, metrics related to the OLSR (Optimized Link State Routing) protocol have been used to observe the behavior of the node selected as MPR (Multipoint-Relays) in OLSR, according to the work of (De Sousa Jr. & Puttini, 2010).

The proposed TRUST-MIB was specified according to the rules of the SMI (Structure of Management Information) RFC related to the Internet Simple Network Management Protocol – SNMP. The environment for experimental validation of the proposed TRUST-MIB, and its utilization within a network management process, has been developed by extending the OLSR daemon (OLSRD) with software modules for metrics gathering an MIB operation, and using the network management system NET-SMTP for accessing and validating the MIB, presenting the trust observed in a controlled experimental environment.

SUMÁRIO

LISTA DE TABELAS

Lista de Figuras

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

AgentX	Agent Extensibility
AODV	ad hoc On-Demand Distance Vector
ASN.1	Abstract Notation One
AT	Adress Translation
BER	Basic Encoding Rules
CBC-X	Cipher Block Chaining
CCITT	International Telegraph and Telephone Consultative Committee
CSGR	Cluster Switche Gateway Routing
DSDV	Destination-Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
EGP	Exterior Gateway Protocol
IANA	Internet Assigned Numbers Authority
IAB	Internet Activities Board
ICMP	Internet Control Message Protocol
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
MAC	Media Access Control
MANET	Mobile ad hoc Network
MIB	Management Information Base
MID	Multiple Interface Declaration
MPR	Multipoint Relay
NIST	National Institutes of Standards and Technology
NMS	Network Management Systems
OID	Object Identifier
OLSR	Optimized Link State Routing Protocol
OLSRD	Optimized Link State Routing Protocol Deamon
P2P	Peer-to-Peer
PDU	Protocol Data Unit
REP	Recomendation Exchange Protocol
RREP	Route Replay

RERR	Route Error Message
RFC	Request For Comments
RREQ	Route Request Packet
SGMP	Simple Gateway Management Protocol
SMI	Structure Management Information
SNMP	Simple Network Management Protocol
TC	Topology Control
TCP	Transfer Control Protocol
UDP	User Datagrama Protocol
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

1. INTRODUÇÃO

Mobile ad hoc Networks (MANETs) são redes móveis, cuja característica principal é a ausência de uma infraestrutura. Os nós participantes da rede operam de forma colaborativa e ao mesmo tempo eles podem se movimentar, entrar ou sair da rede, tornando-a dinâmica. Por serem organizadas de maneira espontânea e sem uma entidade centralizadora, as MANETs precisam de protocolos que suportem a diversificação da rede, além de ter propriedades como o baixo consumo de bateria, capacidade de se adaptar a novos integrantes, dentre outros. Nesse contexto, alguns dos protocolos da camada de rede mais conhecidos são: *ad hoc On-Demand Distance Vector* - AODV, *Optimizes Link State Routing Protocol* - OLSR, *Dynamic Source Routing* - DSR (Perkins, 2003; Clausen, 2003; Johnson, 2007).

Segundo (De Sousa Jr. & Puttini, 2010), com as características distintivas das redes *ad hoc* as soluções de segurança tradicionais não são suficientes para resolver os problemas de segurança, necessitando assim de soluções de colaborações com base em confiança. A confiança aplicada às redes *ad hoc* geralmente é utilizada quando os nós participantes de uma rede, que não possuem interações anteriores, desejam estabelecer uma rede com um nível de confiança aceitável (Cho, 2010). Essa ideia é em particular aplicada ao protocolo OLSR, que corresponde a um protocolo de roteamento pró-ativo, utilizando o esquema de *Multipoint Relays* (MPR), que são nós selecionados para fazer a difusão de mensagens de controle na rede.

Em um artigo de síntese sobre o tema de gerenciamento da confiança em Redes *ad hoc*, (Cho, 2010) analisa características relacionadas aos sistemas embasados em confiança e que foram desenvolvidos em MANETs: ataques, métricas de desempenho e métricas de confiança aplicadas aos diversos protocolos e modelos de confiança. Tal artigo apresenta várias métricas de confiança aplicadas às redes *ad hoc*, cuja aplicabilidade é revista nesta dissertação assim como a de outras métricas de confiança relacionadas em outros trabalhos.

O conceito de base de informações de gerenciamento, MIB, constitui um dos pilares do monitoramento e controle de redes TCP/IP usando o protocolo SNMP, o que permite o conhecimento do estado da rede, a administração da rede, a gerência de falhas e problemas, a partir da observação de fatos e comportamentos dos nós participantes de uma rede.

A ideia central desta dissertação é criar uma MIB de gerenciamento da confiança e mostrar que tal MIB contribui efetivamente à gerência de redes *ad hoc* através da observação de comportamento dos nós roteadores. Com tal MIB, será possível a cada nó da rede coletar informações suscetíveis para obter e avaliar a confiança que se pode atribuir aos nós vizinhos responsáveis pelo roteamento. Para tanto, a MIB proposta será implantada no software do *deamon* OLSRD de modo que as métricas de confiança possam ser obtidas durante a operação do protocolo OLSR - RFC 3626 (Clausen, 2003), para simulações ou uso real.

1.1. OBJETIVO GERAL

O objetivo deste trabalho é a criação de uma MIB de gerenciamento da confiança em redes *ad hoc*, utilizando especificamente o protocolo OLSR, com métricas coletadas do trabalho de (De Sousa Jr. & Puttini, 2010), de modo a mostrar em ambiente experimental controlado que a utilização de tal MIB contribui à gerência de redes *ad hoc*, por permitir a um nodo observar o comportamento dos nodos roteadores vizinhos e avaliar a confiança que pode ser atribuída a cada um desses roteadores.

1.2. OBJETIVOS ESPECÍFICOS

Dentro dos objetivos específicos cabem os seguintes itens:

- Realizar uma síntese das métricas da confiança propostas em artigos e livros relacionados ao tema de redes *ad hoc*.
- Criar a MIB de confiança, com as métricas coletadas, usando os padrões de definição e escrita da SMI e ASN.1.
- Criar um agente de gerenciamento, integrado ao *deamon* OLSRD e capaz de coletar as métricas de confiança de uma rede *ad hoc* e preencher a MIB em cada nodo;
- Definir um ambiente experimental controlado, com uma rede *ad hoc* operando pelo *deamon* OLSRD com o agente de gerenciamento atualizando a MIB proposta.
- Coletar de maneira sistemática e repetitiva os dados coletados na MIB e apresentar a análise e os resultados em termos da confiança avaliada pelos nodos acerca de seus vizinhos.

1.3. ORGANIZAÇÃO DO TRABALHO

O trabalho está organizado da seguinte maneira:

- O capítulo 2 apresenta a fundamentação teórica, abordando o Gerenciamento de Redes e a descrição da estrutura de gerência embasada no protocolo SNMP, o que inclui a MIB. Além disso, o capítulo trata do conceito de Redes *ad hoc* e tipos de ataques a essas redes, especialmente os ataques que podem ser contidos pelo emprego de algoritmos baseados na confiança computacional.
- O capítulo 3 trata da definição da confiança, suas derivações e aplicações.
- A proposta de uma MIB de Gerenciamento da Confiança é exposta no capítulo 4, junto com a descrição do experimento e os resultados.
- Por fim, é apresentada no capítulo 5 a conclusão do trabalho, junto com as ideias futuras relacionadas a esta dissertação.

2. FUNDAMENTAÇÃO TÉORICA

Este capítulo tem como objetivo apresentar a fundamentação teórica, abordando os aspectos relevantes e o contexto para o entendimento da ideia principal do projeto, que é a criação de uma MIB de confiança para aplicação em redes *ad hoc*.

Serão abordados os conceitos e fundamentos de Gerenciamento de Rede de cuja necessidade nas redes de computadores surgiu a estruturação da MIB, tema que é o foco desta dissertação. Assim, será abordada a MIB, apresentando seu surgimento, conceituação, principais características, aplicações, bem como regras e modos de construção.

Nesse contexto, apresentam-se os temas da SMI (*Structure of Management Information*) (McCloghrie, 1999) e da ASN.1 (*Abstract Sintax Notation One)* (ISO8824, 1987), bem como uma breve descrição do protocolo de gerência de rede *Simple Network Management Protocol* (SNMP) (Presuhn, 2002) e o padrão para agentes de gerência extensíveis, AgentX *(*Daniele, 2000*)*.

Uma breve apresentação das redes *ad hoc*, e os tipos de ataques a essas redes, também fazem parte deste capítulo como conhecimento prévio para um melhor entendimento da proposta desta dissertação.

2.1. ESTRUTURA DE GERENCIAMENTO DE REDE

A procura por qualidade e desempenho de uma rede de computadores motiva pesquisadores, administradores e gerentes de redes a contribuir com ferramentas, técnicas, *softwares* e protocolos que facilitem o alcance dos objetivos da gerência de redes, uma atividade fundamental para manter as redes em bom funcionamento.

Muitas definições vêm sendo propostas para o Gerenciamento de redes, de modo que alguns elementos comuns a tais definições já se encontram estabelecidos, tais como aqueles reunidos na seguinte proposição:

> "O oferecimento, a integração e a coordenação de elementos de *hardware*, *softwares* e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às

> exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável." (Saydam, 2006)

Em consequência necessidade de articulação entre os diferentes elementos presentes em tais definições, constitui-se o conceito de uma arquitetura de gerenciamento, incluindo a especificação da estrutura e dos papéis de componentes da gerência de redes. Dentre as arquiteturas existentes, destaca-se a arquitetura SNMP justamente por ser aquela para redes TCP/IP, inclusive a Internet.

Na arquitetura SNMP, são propostas em particular definições para as funções de: sistemas de gerência de redes (*Network Management Systems* – NMS), dispositivos gerenciados, objetos gerenciados, base de informações de gerenciamento, agente de gerenciamento e, por fim, protocolo de gerenciamento. Essas funções dependem umas das outras para obter um desempenho satisfatório e a disponibilidade total da rede, além de segurança e preservação das informações (Kurose, 2006).

Para o controle e administração dos recursos e componentes da rede existe a NMS que além de usar uma aplicação em um servidor, trabalha diretamente com o humano para ajudar na configuração, monitoração e resolução de problemas ao seu alcance.

Os dispositivos que integram uma rede, os sistemas, bancos de dados, protocolos entre outros, são classificados como dispositivos gerenciados, pois apresentam características para gerenciamento e ficam sob o controle da entidade gerenciadora.

Os objetos gerenciados representam características operacionais ou administrativas dentro de um dispositivo gerenciado. A MIB é uma base de dados virtual que define os objetos gerenciados.

O agente é um *software* que executa um processo no dispositivo gerenciado para monitorar e controlar características operacionais e administrativas do dispositivo, com ajuda da MIB e, ainda que atue de forma autônoma no dispositivo gerenciado, deve atuar sob o comando e controle da entidade gerenciadora (Kurose, 2006).

O protocolo SNMP trabalha entre a entidade gerenciadora e os dispositivos gerenciados para obter informações necessárias para manter a qualidade da rede e para resolver problemas de maneira rápida e previsível (Saydam, 2006). A Figura 2-1 apresenta o funcionamento básico de um sistema de gerenciamento de rede e os componentes citados.

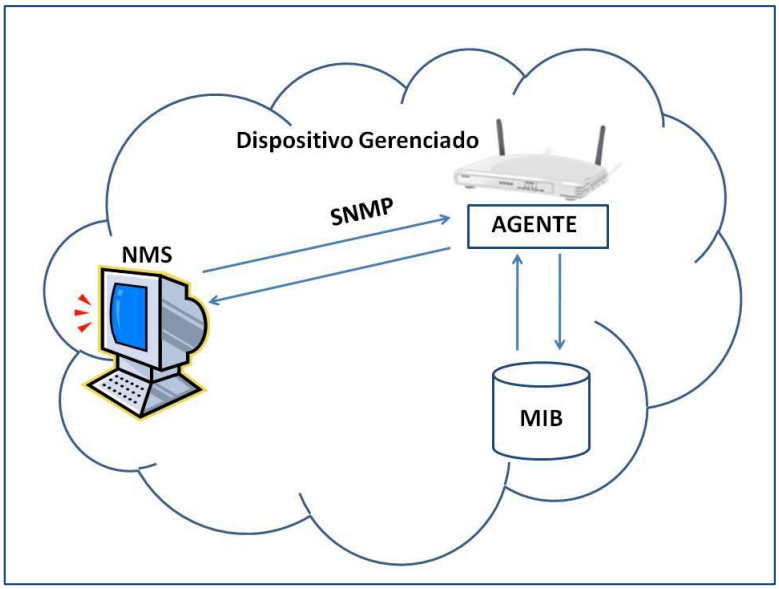


Figura 2-1 Sistema de Gerenciamento de Rede

(Russi, 2005, adaptada)

Segundo (Comer, 1998), a organização do gerenciamento de rede em SNMP se divide em duas partes:

a) A primeira parte define o formato e significado das informações gerenciadas e a segunda refere-se aos dados gerenciados. A MIB é um componente da primeira parte, junto com a SMI e a ASN.1.
b) A segunda parte é composta pelo protocolo SNMP. Os componentes citados serão explicados nos próximos itens deste capítulo.

2.2. MANAGEMENT INFORMATION BASE - MIB

A MIB é um padrão que define os dados e as operações permitidas que os dispositivos gerenciados devem implementar. Além disso, a MIB armazena informações sobre tais dispositivos. O seu surgimento deu-se em duas partes:

- A RFC 1166, também conhecida como MIB I (McCloghrie, 1988), que foi lançada em agosto de 1988, com o objetivo de definir a base de dados de informações de gerenciamento e de controle das redes baseada na arquitetura TCP/IP da Internet.
- A RFC 1213 ou MIB II (McCloghrie, 1991), lançada em março de 1991, veio para evoluir a MIB I, com informações gerais de gerenciamento, além de obter dados como: número de datagramas enviados e recebidos, número de segmentos

recebidos e os recebidos com erros, número de interface, descrição da interface, dentre outros (Silva, 2004).

Além da MIB II, existem mais dois tipos que são as: Experimentais e Privadas.

1. A Experimental é utilizada para projetos em desenvolvimento, testes e experimentos.
2. A Privada é usada para os componentes que possuem informações específicas, por exemplo, os equipamentos desenvolvidos pelos fabricantes, além de não serem definidas no RFC 1213 (Silva, 2004).

A MIB classifica as informações de gerenciamento em grupos funcionais de objetos gerenciados, que possuem características de acordo com o protocolo ou sistema. Esses grupos são codificados no identificador usado para especificar um objeto (Comer, 1998). A Tabela 2-1 apresenta exemplos de alguns dos grupos funcionais.

Tabela 2-1 Grupos Funcionais de Objetos Gerenciados

Grupo	Descrição
SYSTEM	Esse módulo define toda a operação do sistema como tempo de funcionamento, nome do sistema operacional, localização física e serviços;
INTERFACES	Interfaces de redes específicas;
AT	*Address Translation* mantêm a compatibilidade de versões anteriores;
IP	Busca aspectos do protocolo IP, inclusive o roteamento;
ICMP	Contém a entrada ICMP e estatísticas de saída;
TCP	Rastreiam o estado das conexões TCP;
UDP	Rastreia dados estatísticos do UDP datagramas internos e externos;
EGP	Busca dados estatísticos sobre o EGP e mantém uma tabela de vizinhos do EGP.
TRANSMISSION	Reservado para MIBs específicas de mídia

Grupo	Descrição
SNMP	Avalia o tráfego SNMP

Cada grupo possui os objetos gerenciados referentes às suas características. Existem diversos objetos (McCloghrie, 1988 e McCloghrie, 1991) dos grupos citados que não foram relacionados Para verificá-los, podem ser consultados os RFC`s 1066 e 1213 (McCloghrie, 1988; McCloghrie, 1991), além de outros grupos que podem ser encontrados na mesma referência.

2.2.1. Structure Management Information - SMI

A SMI é um método para definir objetos gerenciados e os respectivos comportamentos (Schmidt, 2001). Esses objetos são alocados na MIB e são definidos em módulos. Os módulos são escritos usando o subconjunto adaptado da ASN.1 (McCloghrie, 1999), que será discutido na seção 2.2.2. A SMI utiliza o subconjunto para especificar como os objetos gerenciados são nomeados e os tipos de dados associados (Schmidt, 2001).

A SMI possui duas versões, a SMIv1 e SMIv2. A primeira versão foi descrita em detalhes nas RFCs 1155, 1212, 1215 (Rose, 1990; Rose & McCloghrie, 1991; Rose, 1991), a segunda versão teve algumas modificações em relação a primeira e foi definida na RFC 2578 (McCloghrie, 1999).

A SMI é divida em três partes:

1. Módulo de definições: são usados para descrever módulos de informações. Para a informação ser transmitida de forma concisa. Para manter a semântica é usada a macro da ASN.1, MODULO_IDENTITY.
2. Definições de Objetos: são usados para descrever os objetos gerenciados. A macro utilizada é OBJECT-TYPE.
3. Definições de Notificações: são usadas para descrever as transmissões de informações não solicitadas. A macro utilizada é NOTIFICATION_TYPE. (McCloghrie, 1999)

Além da definição dos módulos, objetos e notificações, o padrão SMI restringe os tipos de variáveis que devem ser usadas na MIB e cria regras para definir os tipos de variáveis. Este

padrão define termos como *Integer*, que são números inteiros de 32 bits; *TimeTicks*, que é o tempo medido em centésimo de segundo, transcorrido a partir de algum evento, *Counter*, Endereço IP, dentre outros (Comer, 1998; Kurose, 2007).

2.2.2. Abstract Syntax Notation One - ASN.1

Elaborada pela *International Organization for Standardization* (ISO) 8824 e 8825 a ASN.1 (ISO8824, 1987) define tipos de dados e especifica valores que os tipos podem assumir. A ASN.1 é de suma importância para a padronização dos dados e a comunicação entre diferentes plataformas. Os tipos recebem um rótulo (*Tag*) e este rótulo pode ter vários tipos e dependendo do contexto em que o rótulo for usado a identificação será decidida. Os rótulos existentes são (Rezende, 2004):

- Universal: Pode ser atribuído a um tipo simples ou a um mecanismo de construção;
- Aplicação: Rótulos atribuídos a tipos por padrões específicos. Em um particular padrão os rótulos da classe de Aplicação somente podem ser atribuídos a um único valor;
- Privada: Rótulos usados em uma empresa específica;
- Especificado-Por-Contexto: Interpretado de acordo com o contexto em que é usado.

A ASN.1 é composta por tipos primitivos, no qual podem ser atribuídos a estruturas complexas, e tipos construídos que são estruturas mais complexas. Os primitivos são: INTEGER, OCTET STRING, BOOLEAN, BITSTRING E NULL. Os tipos construídos são: SEQUENCE, SEQUENCE OF, SET, SET OF, CHOICE. Existem diversos tipos de dados construídos e primitivos, porém os mais citados na literatura são os já apresentados.

Segundo descreve (Kurose, 2006) se não existisse a ASN.1 a transição de dados seria mais difícil. A comunicação feita em um formato reconhecido facilita o armazenamento de dados em um computador. Assim, a ASN.1 é independente de máquina, sistema operacional e linguagem e os seus objetos são usados para a construção da MIB e na adaptação da SMI (Oliveira, 2002).

2.2.3. Definição dos objetos da MIB

Cada tipo de objeto gerenciado tem um nome, sintaxe e um código. O nome é representado como OBJECT-IDENTIFIER, ele é um nome atribuído administrativamente. O tipo ou

sintaxe é formalizado pela ASN.1 especificando como os dados são representados e transmitidos entre gerenciadores e agentes (Schmidt, 2001). A formalização desses objetos influencia principalmente na comunicação contínua com outras plataformas. O código utiliza o método *Basic Encoding Rules* (BER) (Schmidt, 2001) pelo qual um elemento de qualquer tipo definido na ASN.1 deve ser codificado ou decodificado para ser lido.

Nomes são usados para identificar os objetos gerenciados. O OBJECT-IDENTIFIER ou OID é um identificador de objeto que é utilizado para nomear os tipos de objetos gerenciados, por exemplo, cada padrão internacional tem um OID que lhe é atribuído para efeitos de identificação. O OID pode identificar um objeto de rede, padrões de documentos dentre outros.

O OBJECT-IDENTIFIER é uma sequência de números inteiros que atravessa uma árvore hierárquica. A árvore se inicia com uma raiz, nomeada de *root*, conectada a nós. Cada nó pode ter seus próprios filhos e este processo pode continuar em um nível arbitrário ao mais profundo. Esses nós possuem um nome e um número inteiro, os quais são entendidos como um controle administrativo de significado podendo até serem delegados quando se atravessa a árvore. (Rose, 1990)

O nó *root* possui pelo menos três filhos abaixo dele, os quais sejam:

1. ccitt(0): Nó administrado pelo *International Telegraph and Telephone Consultative Committee* (CCITT).
2. iso(1): Um nó administrado pela ISO.
3. joint-iso-ccitt(2): Administrado pela ISO e a CCITT.

O nó detalhado nesta dissertação será o iso(1), pois está relacionado ao seu objetivo que é apresentar um conhecimento de gerência de rede, MIB e SNMP.

Abaixo do nó iso(1) a sub-árvore org(3) é designada para ser usada por outras organizações (inter)nacionais. Os seus nós filhos foram designados para a *National Institutes of Standards and Technology* (NIST) dos Estados Unidos. Um foi transferido para o departamento de defesa dos EUA e foi nomeado como dod(6). O dod(6) não mostra a sua sub-árvore, mas alocou um nó para *Internet Activities Board* (IAB) o qual o nó ficou denominado internet(1). O OBJECT-IDENTIFIER da sub-árvore Internet começa com o prefixo: 1.3.6.1. (Rose, 1990)

O IAB, responsável pela administração do nó Internet, tem a responsabilidade de gerenciar os quatro nós, apresentados na Tabela 2-2. A Figura 2-2 apresenta a árvore de identificadores de objetos.

Tabela 2-2 Nós da Sub-Árvore Internet.

Nome	Descrição
Directory	Usada para o diretório OSI da Internet. Seu OBJECT-IDENTIFIER é directory(1).
Mgmt	A sub-árvore mgmt(2) é usada para definir documentos aprovados pela IAB. Novas versões da MIB obtêm um OID designado pela *Internet Assigned Numbers Authority* (IANA) para identificar os novos objetos definidos no RFC.
Experimental	Usada para identificar objetos feitos para experiências e testes da Internet. A IAB administra esse nó. Seu identificador na árvore é: experimental (3).
Privada	Esse nó é usado para identificar objetos definidos unilateralmente, seu OID é private(4). A IAB administra o nó, que contém um filho denominado *enterprises*(1). Este nó permite que empresas que fabricam dispositivos de rede registrem o seu modelo. Por exemplo, a Cisco, cria o seu dispositivo e define novos objetos gerenciados. Assim ela realiza um registro e recebe um nó abaixo do Enterprise, evitando ambiguidade no mecanismo de identificação. (Sztajnberg, 1996)

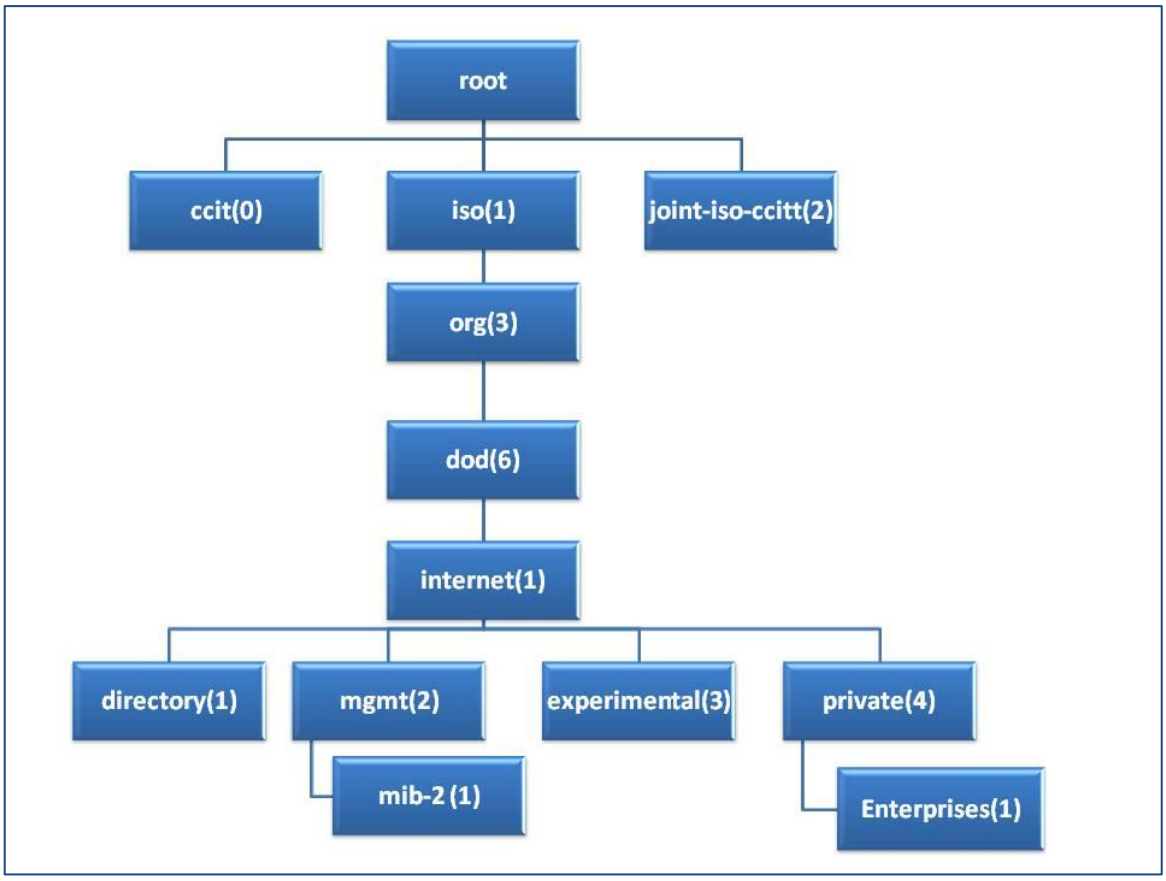


Figura 2-2 Árvore de Identificadores de Objetos

A Sintaxe é usada para definir a estrutura correspondente ao tipo de objeto. A SMIv2 define 13 tipos básicos de objetos. A Tabela 2-3 apresenta as definições dos objetos.

O código é representado quando uma instância de um tipo de objeto é identificada e seu valor deve ser transmitido aplicando as regras da linguagem ASN.1 na sintaxe deste tipo de objeto (Rose, 1990).

Tabela 2-3 Tipos de dados da SMI

Tipo	Descrição
INTEGER	Número inteiro de 32 bits. É usado para modelar os valores de ordem (cardinal) ou inteiros.
Integer32	Número inteiro de 32 bits, com valor entre - 231 e 231 - 1.
Unsigned32	Número inteiro de 32 bits sem sinal na faixa de 0 a 231 - 1.
OctetString	Representa dados binários. É usado para modelar dados de qualquer formato e comprimento múltiplo de 8 bits.

Tipo	Descrição
OBJECT IDENTIFIER	Formato ASN.1 atribuído administrativamente (nome estruturado)
IP Adress	Endereço Internet de 32 bits, na ordem de bytes de rede.
Counter32	Contador de 32 bits que cresce de 0 a 232 - 1 e volta o 0.
Bits	Construção de bytes que representa a enumeração de bits.
Gauge	O mesmo que Unsigned32, usado para contadores.
Gauge32	Número inteiro de 32 bits que não faz contagens até de 232 - 1 nem diminui para menos do que 0.
TimeTicks	Representa um inteiro não negativo que conta o tempo em centenas de segundos desde alguma época. Este tipo de objeto identifica a época correspondente.
Opaque	Cadeia ASN.1 não interpretada, necessária para compatibilidade com versões anteriores
Textual Conventions	Define um contador de 64 bits com um valor inicial de zero, em vez de um valor inicial arbitrário.

2.3. SIMPLE NETWORK MANAGEMENT PROTOCOL - SNMP

O SNMP é um protocolo de gerenciamento de rede capaz de enviar informações dos dispositivos gerenciados para a NMS e até mesmo realizar ações como, alterar o estado dos equipamentos. O protocolo ajuda a manter em alerta as atividades de rede de um setor de monitoramento, possibilitando a tranquilidade em fazer transações, além de tomar a atenção de cada passo dos acontecimentos dentro de uma rede. Isso é de extrema importância, principalmente pelo fato de o gerente da rede ser alertado dos problemas existentes até mesmo no final de semana. O SNMP pode monitorar elementos tais como: sistemas operacionais, modems, impressoras, servidores, estações de trabalho, banco de dados etc.

Este protocolo tem como antecessor, o *Simple Gateway Management Protocol* (SGMP) - RFC 1028 (Davin, 1987), que foi desenvolvido para gerenciar roteadores da Internet (Schmidt, 2001). O SNMP usa o protocolo de transporte *User Datagrama Protocol* (UDP), para o envio de mensagens entre o agente e a entidade de gerenciamento. Este protocolo é

sem conexão, isso quer dizer que o datagrama (Schmidt, 2001) pode se perder e ficará difícil saber se ele foi entregue ou não. Isso o torna não confiável. O próprio SNMP se encarrega de verificar se o datagrama foi entregue e se necessário, o retransmite. A porta 161 do UDP é usada para enviar e receber solicitações. A porta 162 é usada para receber *traps*. Toda essa comunicação de mensagem é feita pelo pacote *Packet Data Unit* (PDU), sendo que elas são encapsuladas no protocolo de transporte.

Para a manipulação das informações e operações do protocolo SNMP, existem as entidades de gerenciamento e os agentes.

2.3.1. Entidade Gerente

A entidade de gerenciamento é uma aplicação que transmite ações de gerenciamento aos agentes e recebe eventos destes (Pinheiro, 2002). Geralmente existe um servidor executando esta entidade, podendo assim lidar com as atividades de gerenciamento, além de poder passar informações para os administradores sobre o estado atual da rede, problemas e estatísticas.

A NMS trabalha consultando e agindo por meio de ações nos agentes. Ele pode, por exemplo, consultar se a conexão com a Internet foi derrubada ou receber um *trap*, que é uma operação realizada pelo agente, e reagir com um aviso querendo saber o que ocorreu (Schmidt, 2001). As informações coletadas são consolidadas de uma maneira mais fácil de interpretar, além de como função de gerente, alertar e tentar solucionar sobre os problemas ocorridos.

2.3.2. Entidade Agente

O agente é um software de gerenciamento executado nos dispositivos gerenciados. Ele pode ser um programa (*deamon*) ou pode ser incorporado no sistema operacional (Kurose, 2006).

O objetivo do agente é coletar as informações dos estados, comportamentos dos dispositivos e armazená-las na MIB. Ele também fornece ao NMS essas informações. Um *trap* é feito somente pelo agente, pois caso ocorra algo de errado em um dispositivo ele informa o problema a entidade de gerenciamento. O código de um agente é composto por contadores, rotinas de teste, temporizadores que autoriza o controle e gerenciamento do

objeto gerenciado (Pinheiro, 2002). Os fornecedores dos dispositivos já programam o agente em seus produtos, facilitando o serviço do administrador e gerente da rede.

A Figura 2-3 apresenta o relacionamento entre o agente e a estação de gerenciamento de rede.

Figura 2-3 Relacionamento entre o Agente e a Estação de Gerenciamento.

2.4. AGENTES EXTENSÍVEIS AGENTX

Dentro da arquitetura MIB e SNMP existem os objetos gerenciados que são padrões para a realização de seus trabalhos. Esses objetos são especificados e definidos nas RFC`s (Case, 1990; Presuhn, 2002; McCloghrie, 1999; Case, 1996; McCloghrie, 1988; McCloghrie, 1991) e geralmente os dispositivos já vêm com as especificações desses padrões. Acontece que acaba existindo novos protocolos, novos dispositivos e a necessidade de novas expansões da MIB que geralmente são específicas de empresas ou experimentais, e tais não se encontram especificadas no padrão existente, necessitando de uma nova criação, para então novo componente poder ser gerenciado, usando a MIB e o SNMP.

Por isso foi criado o padrão *Agent Extensibility* (AgentX) que é definido na RFC 2741 (Daniele, 2000*)*. Ele é uma nova estrutura para agentes SNMP extensíveis (Pacheco, 2007). Essa necessidade dá origem a uma variedade de agentes extensíveis que incluem um Agente Mestre, um conjunto de Subagentes, um protocolo e um conjunto de ferramentas.

O Agente Mestre tem a função de enviar e receber mensagens do protocolo SNMP e gerenciar as MIBs padrões. Além disso, ele aceita pedidos de estabelecimento de sessão do AgentX vinda dos Subagentes; Aceita o registro das MIB por Subagentes; Encaminha a requisição para o software agente responsável pelo objeto que não é implementado na MIB padrão.

O Subagente por sua vez, inicia sessões do protocolo AgentX com o agente Mestre; Registra as MIBs com o agente Mestre; Instancia objetos gerenciados; Vincula OIDs dentro de suas regiões registrando MIBs variáveis; Realiza operações de gestão sobre as variáveis, mas por não implementar o SNMP, as Operações de requisição e reposta são realizadas pelo Subagente via o protocolo AgentX (Pacheco, 2007).

Os agentes Mestres e os Subagentes se comunicam por meio do protocolo AgentX. As operações internas do AgentX são invisíveis para entidades que gerenciam o SNMP. Esta transparência para as entidades gerenciadoras é uma exigência fundamental do AgentX, e é o que diferencia Subagentes AgentX de agentes SNMP. A comunicação usada é orientada a conexão, o protocolo de transporte é o TCP (Lourenço, 2000), além de poder usar outros.

O funcionamento do AgentX ocorre da seguinte maneira: O Subagente solicita a conexão e o registro com o agente Mestre assim que ele inicia, após quando o agente Mestre recebe as mensagens do SNMP relacionados a objetos estendidos (que não são do padrão) ele o redireciona para o Subagente que consulta a MIB estendida e devolve a resposta para o agente Mestre para que ele encaminhe a resposta solicitada. Toda a interação é realizada pelo protocolo AgentX. A Figura 2-4 apresenta a arquitetura SNMP com o AgentX.

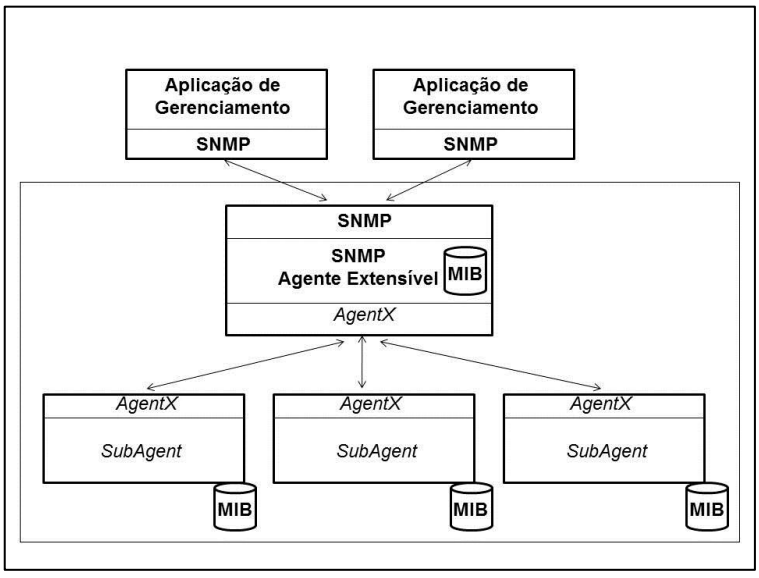


Figura 2-4 Arquitetura SNMP com o AgentX

2.5. CARACTERIZAÇÃO DAS REDES *AD HOC*

As Redes Móveis *ad hoc* – MANET – são redes sem fio onde não existe uma infraestrutura estabelecida (estação base) e então os nós se comunicam diretamente entre si dentro da

área de alcance do sinal de cada um. Nesse contexto, o roteamento acontece de modo cooperativo, sendo que cada nó deve ser capaz de atuar como roteador para os demais. Como a comunicação somente é possível se o nó estiver dentro do raio de alcance do outro nó, o roteamento entre nós distantes na rede é possível somente com a participação de nós intermediários que assumem o papel de roteadores, permitindo o estabelecimento de rotas entre pares de dispositivos com múltiplos saltos (Areal, 2008).

O objetivo das redes móveis *ad hoc* é ampliar a mobilidade em domínios autônomos, móveis e sem fio, onde conjuntos de nós formam a rede de infraestrutura de roteamento de forma *ad hoc* (Corson, 1999). Essas redes se caracterizam por serem autoconfiguráveis, de rápida manutenção, dinâmicas e apresentarem topologias de múltiplos saltos, porém possuem uma largura de banda limitada e alguns recursos de pouca duração.

Por apresentarem tais características, as MANETs possuem diversos cenários aos quais podem ser aplicadas. Como exemplo, pode-se citar:

- Ambientes onde não existe infraestrutura ou onde as infraestruturas foram destruídas: Esses ambientes necessitam de estabelecimento rápido da rede, por exemplo, para operações de resgate, tratamento de acidentes, atentados, incêndios, desabamentos, explosões e outros.
- Ambientes de difícil acesso: ambientes em que existe muita dificuldade de acesso ou eventos impossibilitando a manutenção de uma infraestrutura, por exemplo, furacão, vulcão, mar, dentre outros.
- Ambientes de distância reduzida, onde os nodos podem estabelecer as comunicações diretamente, usando uma tecnologia como Bluetooth (Puttini, 2004).

As redes *ad hoc* apresentam problemas principalmente pelo fato de possuírem enlaces sem fio e permitirem a mobilidade dos dispositivos. Alguns problemas mais conhecidos são os de limitação de banda passante, erro nos enlaces sem fio, localização e roteamento. Tais problemas são gerenciados pelos protocolos específicos de rede ad hoc, especificamente os protocolos de roteamento descritos brevemente a seguir, pelo interesse no contexto da presente dissertação.

2.5.1. Protocolos de Roteamento *ad hoc*

Em redes *ad hoc* o roteamento possui características distintas das redes cabeadas. Ele depende da topologia momentânea, da seleção de roteadores e outras características que são relevantes para a entrega dos dados.

Em 1997 um grupo de trabalho foi formado pela IETF (*Internet Engineering Task Force*) para pesquisar e desenvolver especificações para o roteamento nas redes MANETs, resultando em diversas propostas para a construção de protocolos (Puttini, 2004). Para a criação dos protocolos são levados em conta alguns critérios, tais como, os algoritmos de roteamento e a política de descobrimento de rotas. Para os algoritmos serem projetados devem-se considerar três fatores (Fernandes, 2003):

1. Inexistência de uma entidade central;
2. Capacidade de rápidas mudanças topológicas;
3. Ocorrência de todas as comunicações através de rádio frequência.

Para a política de descobrimento de rotas, podem-se considerar três tipos de classificações quanto aos protocolos: Protocolos pró-ativos, reativos e híbridos.

Os protocolos pró-ativos trabalham com uma tabela de roteamento de cada nó pronta, sendo atualizada em intervalos de tempo periódicos. Essas tabelas facilitam na hora de fazer o encaminhamento do pacote, pois podem ser usadas imediatamente à necessidade de transmissão de pactos. A vantagem é que a rota está sempre pronta para usar quando houver necessidade e a desvantagem é que a atualização da rota gera tráfego permanentemente (consumindo energia dos nodos) e em redes com muita mobilidade acaba trazendo problemas de convergência e roteamento para destinos que deixaram de ser alcançáveis. Exemplos de protocolos pró-ativos são: *Optimized Link State Routing* (OLSR), *Destination-Sequenced Distance Vector Routing* (DSDV), *Wireless Routing Protocol* (WRP) e *Cluster Switche Gateway Routing* (CSGR).

Os protocolos reativos não utilizam tabela de roteamento e sim quando o nó fonte necessita realizar um roteamento a rota é estabelecida. Primeiramente, existe a descoberta da rota, depois que ela é estabelecida, existe a manutenção da rota para ela se manter ativa. A vantagem é a redução de sobrecarga de tráfego, pois não precisa fazer atualização periódica das tabelas, além de economia de energia. A desvantagem é a maior latência na

entrega das mensagens, pois os dados só podem ser entregues depois da construção da rota (Fernandes, 2003). Os protocolos mais conhecido do tipo reativo são: *ad hoc On-Demand Distance Vector Routing* (AODV) e *Dynamic Source Routing* (DSR).

Os protocolos híbridos trabalham de maneira pró-ativa nas informações de roteamento e o descobrimento de rotas de maneira reativa (Puttini, 2004). O ZRP (*Zone Routing Protocol*) é o protocolo híbrido mais conhecido.

2.5.1.1. *Optimized Link State Routing Protocol* -OLSR

O protocolo OLSR é pró-ativo, ou seja, utiliza tabelas para armazenar informações sobre a topologia da rede e o roteamento, tendo funcionamento baseado na otimização do algoritmo *Link State*. Nesse tipo de algoritmo, a estrutura de roteamento é representada por um grafo cujas arestas correspondem à conexão entre os nós e métricas como a largura de banda e o tempo de respostas são usados para definir o cálculo dos custos que são atribuídos em todas as arestas.

OLSR utiliza um procedimento de seleção de nós responsáveis por disseminar mensagens (broadcast), diminuindo assim as mensagens repetidas na rede. Esses nós selecionados são chamados de MPR e são escolhidos pelos vizinhos a um salto (para tanto, o protocolo procede por meio das mensagens *Hello*). Cada nó escolhido como MPR armazena informações sobre o conjunto de nós que o elegeram como roteador.

As mensagens enviadas pelos nós MPRs são recebidas por qualquer nó vizinho, mas se o nó não é um MPR então ele não repassa a mensagem. Já um nó MPR retransmite a mensagem para os seus vizinhos a um salto, diminuindo a quantidade de mensagens repetidas que são enviadas muito raramente (Clausen, 2003).

Existem três mensagens padrão que são enviadas periodicamente e que os nós OLSR reconhecem:

1. *HELLO*: Mensagem responsável pela atualização do conjunto de Links e do conjunto de vizinhos.
2. TC: Mensagem responsável pela declaração de estado de links e declaração de topologia de rede.

3. MID: São mensagens que devem ser enviadas apenas por nós que possuem duas ou mais interfaces de rede. Elas fazem a declaração de múltiplas interfaces, escolhendo uma interface principal para identificar o nó.

2.5.1.2. Ad hoc On-Demand Distance Vector Routing - AODV

O AODV é um protocolo reativo, que oferece para a rede rápida adaptação nas condições do link dinâmico, baixo processamento, baixa utilização da rede e determina rotas *unicast* para destinos dentro da rede *ad hoc*. Esse protocolo utiliza algoritmo de vetor de distância e ele diminui a difusão de mensagens de roteamento. O AODV cria rotas sob demanda, visto que, caso a rota solicitada não esteja ainda na tabela de roteamento, o protocolo efetua o procedimento de descoberta.

Cada nó intermediário possui tabelas com rotas dinâmicas e para manter informações atualizadas o protocolo utiliza o conceito de número sequencial. Neste conceito, cada nó possui um contador de número sequencial crescente, isso faz com que as rotas sejam substituídas pelas mais novas (Fernandes, 2003).

O estabelecimento de rota inicia com o envio de um pacote de solicitação de rota, *Route Request Packet* (RREQ), para os seus vizinhos. Quando os vizinhos recebem o RREQ eles geram uma rota reversa que pode ser usada para o estabelecimento de uma nova rota. O vizinho verifica se já possui a rota reversa, se sim ele utiliza a rota, se não ele incrementa o contador de saltos e envia para o próximo vizinho. O RREQ percorre a rota até achar um nó que possua uma rota válida que o leve ao destino, após isso o pacote *Route Replay* (RREP) é gerado, ele possui informações como o endereço da origem, endereço do destino, número sequencial do destino, contador de saltos e tempo de duração da rota. Após a descoberta da rota o pacote RREP é enviado para o nó de origem. Caso ocorra um erro de transmissão, um pacote sinalizador de erro, *Route Error Message* (RERR), é enviado de volta para o nó de origem informando sobre o erro (Fernandes, 2003).

2.5.2. Ataques em Redes *ad hoc*

Os ataques em MANETs podem ser divididos em ativos e passivos. Os ataques passivos não afetam a operação da rede, sendo caracterizado pela espionagem dos dados sem alterá-los. Já os ataques ativos são mais numerosos, visto que o atacante cria, altera, descarta e/ou torna os dados em trânsito inviáveis (Fernandes, 2006). Os atacantes podem ser internos,

ataques feitos por usuários que têm autorização de acesso à rede, ou externos, ataques feitos ao sistema por usuários não autorizados.

Os ataques em MANETs existem em todas as camadas, mas os ataques da camada de roteamento são os mais graves (Kannhavong, 2007), a exemplo dos seguintes ataques:

- Ataque *Flooding*: O objetivo deste ataque é esgotar os recursos da rede, consumir os recursos de um nó e ainda causar degradação no desempenho da rede. Ele funciona de acordo com a característica de cada protocolo, por exemplo, no caso do AODV ele envia um grande número de RREQs, em um curto período, para um nó que não existe na rede. Como solução para este tipo de ataque, (Yi, 2005) propõe um mecanismo que monitora e calcula a taxa de RREQ de seus vizinhos. Caso a taxa fique acima de um limite definido, o nó registra o ID no vizinho em uma lista negra.
- Ataque *Link Withholding*: Neste ataque, o nó mal intencionado ignora a exigência de anunciar o link de nós específicos ou um grupo de nós, o que pode resultar na perda de link para esses nós. O protocolo OLSR é o mais atingido por este ataque. Como solução para este ataque, (Kannhavong, 2006) propôs uma técnica de detecção baseada na observação de uma mensagem TC e uma mensagem *Hello* gerados pelos nós MPR. Se um nó não ouve uma mensagem TC de seu nó MPR regularmente, mas ouve apenas a mensagem *Hello*, o nó então julga que o nó MPR é suspeito e pode evitar o ataque, selecionando um ou mais nós MPR extra.
- Ataque *BlackHole*: Neste ataque todos os pacotes são atraídos até o nó e são descartados. Dependendo da posição do atacante, este ataque pode ter um efeito totalmente destrutivo na rede, impedindo todo o seu funcionamento. Sua detecção é fácil, pois em muito pouco tempo todo um ramo da rede deixará de funcionar. Outra consequência do buraco negro é que ele acaba atraindo muito tráfego em sua direção e acaba consumindo os recursos dos nós à sua volta (Fernandes, 2006).
- Ataque *Link Spoofing*: Neste ataque um nó mal intencionado anuncia links falsos com os nãos vizinhos para interromper as operações de roteamento. No caso do OLSR, um atacante pode anunciar um link falso com uma meta de vizinhos de dois pulos (Kannhavong, 2007).
- Ataque *Replay*: Neste ataque um nó registra as mensagens de outros nós de controle válidas e reenvia mais tarde. Como a topologia muda frequentemente devido à

mobilidade do nó, isto significa que a topologia da rede atual não pode existir. Com este ataque os outros nós gravam em suas tabelas de roteamento rotas obsoletas. O ataque de repetição pode ser mal utilizado para representar um nó ou simplesmente para atrapalhar o funcionamento do roteamento (Kannhavong, 2007).

- Ataque *Colluding Misrelay*: Neste ataque os atacantes trabalham em conluio para modificar ou descartar pacotes de roteamento para interromper a operação de roteamento em uma MANET (Kannhavong, 2007).
- Inundação de *Hellos*: A inundação de *Hello* só se aplica a protocolos que utilizam a mensagem de *Hello* para identificação dos vizinhos. Para realizar o ataque, o nó malicioso envia *Hellos* com alta potência, informando que o nó possui enlaces muito bons com determinados destinos. Assim, ele atinge um grande número de nós, que por terem ouvido a mensagem, o colocam na sua lista de vizinhos e podem escolhê-lo para encaminhamento de dados (Fernandes, 2006).

Os diversos ataques existentes nas redes *ad hoc* demostram que uma rede precisa constantemente de cuidados e recursos de segurança para manter a integridade, confiabilidade e disponibilidade. O objetivo desta dissertação é apenas mostrar que existem os diversos ataques na camada de rede das MANETs, porém, não será utilizado nenhum tipo destes ataques para qualquer tipo de demonstração ou implementação.

Ao invés disso, propõe-se um processo de monitoração dos vizinhos, e especificamente dos vizinhos que se constituem como roteadores, de modo a coletar métricas que indiquem a normalidade ou anomalias no comportamento desses vizinhos no que se refere ao repasse das mensagens de roteamento. Desse modo, com base nas métricas, coletadas e armazenadas em uma MIB de gerenciamento, torna-se possível calcular uma expectativa quanto ao comportamento futuro de um vizinho com base na observação do comportamento passado desse vizinho. Conforme definido anteriormente, tal processo constitui a noção de confiança no vizinho empregada na presente dissertação.

A confiança nessa situação específica é útil para contrabalançar ataques por detecção de anomalias de comportamento (Adnane et al, 2008), mas também se constitui genericamente um elemento de gerência de rede, conforme descrito adiante na presente dissertação.

3. CONFIANÇA COMPUTACIONAL

A confiança possui visões múltiplas no que se relaciona ao seu uso e no que aplicar para caracterizá-la. Segundo (Carbone, 2003) a confiança é uma necessidade fundamental no comportamento humano, que, por milênios, contribui para a colaboração entre pessoas e organizações. Portanto, a junção de confiança com algumas áreas é motivo de estudo e principalmente à colaboração do seu conceito e uso na área computacional.

A confiança está presente no dia a dia em diversos aspectos e diversas aplicações (Marsh, 1994; Gambetta, 1988). Encontra-se a confiança no mundo social, entre os humanos e seus comportamentos no sentido de ajudar uns aos outros, esperando que no futuro possam receber a mesma ajuda prestada (Marsh, 1994).

Inspirada nessa noção social, mas com as devidas restrições, define-se a possibilidade de uso da confiança no mundo computacional na forma de uma expectativa calculada por um processo computacional acerca do comportamento esperado de outro processo com base na observação do comportamento passado deste último. Tal conceito aplica-se em rede ad hoc, onde um nó confia em outro nó, para que no trajeto, o envio dos dados possa chegar ao seu destino com perfeição, não ocorrendo nenhum tipo de ataque ou falsidade em relação às ações de repasse dos pacotes até o destino.

3.1. CONFIANÇA APLICADA A AMBIENTES COMPUTACIONAIS

Segundo (Josang, 1996) a confiança é uma de uma entidade apaixonada (humanos) é uma crença de que o outro irá se comportar sem intenção maliciosa. Já a confiança em uma entidade racional (sistema) é um meio de ação que permite resistir à manipulação maliciosa.

Essa definição se aplica na área computacional, onde um nó a partir do conhecimento de interações ou informações sobre outro nó pode confiar que as suas futuras interações ocorrerão sem má-fé. Assim, há na área computacional aspectos onde um nó, com base nas experiências anteriores ou por meio de sua percepção, gera a sua própria confiança, definida como confiança direta. Mas há também a confiança indireta que é baseada em recomendações e relacionamentos de outros nós confiáveis. A confiança também é dependente do tempo, ela cresce e decai ao longo de um período de tempo (Pirzada, 2004).

O compartilhamento de atividades computacionais entre entidades desconhecidas aumenta o interesse no uso da confiança, visto que dividir tarefas e acreditar que outro desconhecido possa realizar vai depender muito da sua boa intenção. Entidades mal-intencionadas e que não cooperam podem destruir a rede, diminuindo o seu desempenho, aumentando o consumo de recursos ou até mesmo espalhando vírus. A cooperação entre os nós de uma rede aumenta a capacidade da rede que acaba trabalhando com mais confiabilidade, segurança e integridade.

Assim, as aplicações de redes como *ad hoc*, Redes P2P, *Grid Computing*, dentre outras, têm motivado o estudo da confiança (Meka, 2006; Dinh, 2009; Papalilo, 2008). Nessas redes há várias operações que podem ser associadas uma avaliação da confiança, tais como o envio e o encaminhamento de pacotes, resposta a mensagens de roteamento, etc. A decisão de confiar em uma entidade para realizar essas operações pode ser condicionada a uma avaliação, de acordo com uma análise prévia dos nós da rede, para acreditar que o pacote possa chegar ao destino sem passar por um nó traidor ou falso que vá atrapalhar todo o processo de entrega dos dados.

Por resolver problemas comuns nessas redes, as aplicações de confiança computacional têm sido bastante usadas, exigindo a criação de modelos de confiança para os vários tipos de redes e camadas, envolvendo variadas métricas, processos de cálculo, armazenamento e tomada de decisão, aspectos estes tratados a seguir.

3.2. ASPECTOS QUE INFLUENCIAM NA CONFIANÇA

Resultados provenientes de domínios do conhecimento como Sociologia, Economia, Psicologia, Administração, dentre outros, apresentam conceitos e propriedades de confiança (Cho, 2010). Por meio dessas definições de confiança de vários campos é possível construir uma relação de métricas e processos da confiança com as seguintes características gerais:

a) A confiança deve ser estabelecida com base em riscos potenciais,
b) A confiança deve ser dependente do contexto,
c) A confiança deve ser baseada em interesse próprio de cada parte (por exemplo, o egoísmo),
d) A confiança é aprendida (ou seja, um processo cognitivo) e
e) A confiança pode representar a confiabilidade do sistema (Cho, 2010).

Além dos resultados das interações diretas com a outra entidade, existem outros fatores que influenciam na confiança, tais como, as informações de terceiros sobre essa entidade e a apresentação de uma entidade para outra (Albuquerque, 2008). Assim, o outro aspecto importante, que influencia no grau de confiança, é a recomendação, ou seja, as informações repassadas a respeito de outra entidade. Nesse caso, deve-se averiguar não somente a reputação do indicado, mas também do indicando, e a partir da análise de todo o contexto, verificar se o agente é capaz de cooperar e auxiliar na solução do problema ou situação e por fim, determinar se a relação de confiança a ser mantida ou não. Algumas dessas características são conceituadas nos próximos tópicos.

3.2.1. Contexto

Na representação de confiança, a entidade A, para criar um relacionamento simples de confiança, comunica-se com outra entidade, a entidade B, a fim de solucionar uma tarefa ou um problema específico. Nesta situação, a entidade A verifica se B pode ou não auxiliá-lo na solução do referido problema, ocasionando em função do resultado obtido, aumento ou diminuição da confiança de A em B.

Concomitantemente, a entidade A poderá comunicar-se com outros nós, sejam eles: C e D devendo manter informações da confiança percebida especificamente para cada um deles, o que configura a relação de confiança de um para um (1:1) e condicionada ao contexto que inclui a tipo de operação, as métricas utilizadas, os métodos de cálculo, etc. (Albuquerque, 2008).

3.2.2. Informações Terceiras

Uma nova entidade poderá ser inserida na rede de relacionamentos, desde que, sejam adquiridas informações a respeito da sua reputação, para tanto, será verificado se algum integrante da rede conhece tal terceiro. De posse das respostas, o cálculo de confiança poderá ser realizado e a partir daí, tomada uma decisão de relacionamento ou não, sendo válida também, na perspectiva da nova entidade (Albuquerque, 2008).

3.2.3. Apresentação de uma Entidade

No que tange a relacionamento com valores de confiança sugere-se que seja feita uma apresentação entre as entidades. Caso já mantenham relacionamento, dispensa-se a busca

de informações por uma das entidades, tendo em vista que já possuem um grau de confiança. Caso contrário, para solucionar um determinado problema a entidade que está buscando informações terceiras terá as seguintes opções: relacionar-se ou não, relacionar-se em um contexto ou buscar mais informações terceiras da nova entidade (Albuquerque, 2008).

3.2.4. Confiança, Confiabilidade e Risco

Confiança e confiabilidade são termos que na literatura, parecem ser usados sem uma clara distinção. A diferença entre a confiança e a confiabilidade é esclarecida por (Josang, 2004) usando definições de (Gambetta, 1988), para quem o nível de confiança varia de uma desconfiança total (0) a uma total confiança (1). Com isso, a confiabilidade é a medida da probabilidade real de que o comportamento será conforme o esperado.

A estimativa do risco está intimamente ligada com a construção de relações de confiança entre as entidades participantes. Segundo (Josang, 2004), há dois tipos interessantes de confiança em função da consideração ao risco: 1) a confiança percebida por um agente, independentemente das situações que tal agente pode enfrentar ao reconhecer o possível risco, 2) a confiança de tomada de decisão medida pelo grau em que uma determinada parte está disposta a depender de algo ou de outra parta, em uma dada situação e com um sentimento de relativa segurança, embora as consequências negativas sejam possíveis. Como por exemplo, não se pode confiar em uma corda velha para descer do 3º andar de um prédio durante um exercício de fogo, enquanto se confia na mesma corda em caso de um incêndio real (ou seja, a confiança de decisão). A relação entre confiança e risco tem sido investigada e trabalhos como (Josang, 2004) e (Solhaug, 2007) defendem que o risco pode ser caracterizado por diferentes valores:

- O valor do risco é baixo para todos os valores de confiança quando a causa está perto de zero. Da mesma forma, se a causa é muito alta, o risco é considerado elevado, independentemente do valor de confiança estimado. Risco é geralmente baixo quando o valor da confiança é alto. No entanto, o valor de risco deve ser determinado com base no valor da causa (por exemplo, a probabilidade de risco).
- O alto risco existe mesmo para o caso de o valor de confiança ser igual a 1. Igualmente importantes são os aspectos (ou probabilidade) de oportunidade e perspectiva (ou a consequência positiva de uma oportunidade) (Josang, 2004;

Solhaug, 2007). Por exemplo, pode-se considerar que comprar borracha é fazer um negócio arriscado, mas também dá a oportunidade de vender produtos refinados, com lucro líquido. O comprador da borracha deve estimar seu nível de risco aceitável em termos de perspectivas calculadas. Alguns pesquisadores comentam que a confiança e a incerteza estão intimamente ligadas – a confiança é um mecanismo para lidar com a incerteza. O nível de incerteza na informação usada como prova de confiança também influencia consideravelmente a precisão de confiança de avaliação (Walker, 2003).

3.3. GERENCIAMENTO DA CONFIANÇA EM REDES *AD HOC*

Em redes *ad hoc* os nós trabalham em colaboração, para realizar o cálculo das rotas, o envio dos dados, dentre outras operações. Para realizar os trabalhos colaborativos, a rede precisa escolher bem os nós vizinhos para que a comunicação entre a origem e o destino ocorra sem problemas, pois a troca de informações em uma rede comprometida pode levar à ineficiência e instabilidade de toda a rede *ad hoc* (Velloso, 2006).

Para contrabalançar tais problemas, entre outras técnicas, vem se estabelecendo o Gerenciamento da Confiança. O trabalho de (Blaze, 1996) introduziu esse termo e o delimitou como um componente separado dos serviços de segurança das redes, esclarecendo que o gerenciamento da confiança fornece uma abordagem unificada para especificar e interpretar as políticas de segurança, credenciais e relacionamentos.

O gerenciamento da confiança é muito usado também como sinônimo de gestão da reputação. No entanto, há uma ligeira diferença entre a confiança e reputação. Segundo (Cho, 2010), a reputação é passiva, enquanto a confiança é ativa, isso porque a primeira faz o levantamento de informações passadas junto aos nós de uma rede que estabeleceram conexão com o nó que se deseja interagir, enquanto na segunda, existe a interação direta entre nós independente de se levar em consideração o histórico percebido por outros.

Já em (De Sousa et al, 2010) a confiança existente de forma implícita em OLSR é descrita através de uma linguagem específica que permite a implementação de raciocínios artificiais aplicáveis à detecção de anomalias do protocolo.

3.3.1. Classificações para Gerenciamento da Confiança em MANETs

O gerenciamento da confiança é um caso especial de gestão de risco, com uma ênfase particular sobre a incerteza e a tomada de decisão em matéria de cooperação com entidades desconhecidas (Solhaug, 2007). No entanto, a aplicação de gerenciamento de confiança ultrapassa a questão de autenticação e se estende para vários aspectos de comunicações e de redes, incluindo roteamento seguro para isolar os nós maliciosos ou egoístas, detecção de intrusão, gerenciamento de chaves, controle de acesso e mecanismos de tomada de decisão. O gerenciamento da confiança inclui a coleta de provas de confiança apropriadas, geração de valores para expressar o nível de confiança, distribuição de confiança, descoberta de confiança, avaliação da prova de confiança, atualização da confiança e revogação de confiança (Theodorakopoulos, 2006; Solhaug, 2007).

Cabe também notar duas abordagens diferentes sobre gerenciamento da confiança:

a) (Yunfang, 2007) sugere um gerenciamento de confiança baseado em políticas, ou seja, fundamentado em sistemas de segurança forte e objetivos, tais como regras lógicas e as propriedades verificáveis codificadas em credenciais assinadas para controle de acesso de usuários aos recursos. O gerenciamento da confiança baseado em política geralmente toma uma decisão binária segundo a qual o solicitante é confiável ou não, e, consequentemente, o pedido de acesso é permitido ou não. Devido à natureza probabilística de avaliação da confiança, o gerenciamento da confiança baseado em políticas tem menos flexibilidade. Além disso, a disponibilidade de (ou acesso a) autoridades de certificação confiável (CA) nem sempre pode ser garantida, particularmente para sistemas distribuídos, tais como MANETs.
b) Por outro lado, o gerenciamento da confiança baseado em reputação utiliza mecanismos numéricos e computacionais para avaliar a confiança. Normalmente, em tal sistema, a confiança é calculada mediante a coleta, agregação e disseminação de reputação entre as entidades. De acordo com (Li, 2007), essa forma de gerenciamento da confiança pode ser classificada como o gerenciamento da confiança baseado em evidências e gerenciamento da confiança baseado em monitoramento. O gerenciamento baseado em evidências considera tudo o que prova as relações de confiança entre nós: estes podem incluir a chave pública, endereço, identidade ou qualquer evidência de que qualquer nó pode gerar para si

ou para outros nós por meio de um processo de desafio e resposta. O gerenciamento baseado em monitoramento considera as taxas de gerenciamento do nível de confiança de cada nó participante com base em informações diretas (por exemplo, observando o comportamento benigno ou malicioso de nós vizinhos, como o descarte de pacote, e inundações de pacotes levando ao consumo excessivo de recursos na rede, ou ataques de negação de serviço), bem como informação indireta (por exemplo, as classificações de reputação como recomendações encaminhadas de outros nós).

3.3.2. Métricas para Gerenciamento de Confiança em MANETs

Segundo (Cho, 2010) muitos sistemas de gerenciamento da confiança têm sido propostos, mas nenhum trabalho aborda claramente o que deve ser medido a fim de avaliar a confiança da rede. Medidas de confiança podem ser dependentes da aplicação e serão diferentes com base nos objetivos dos projetos propostos.

A Figura 3-1, baseada em 31 trabalhos analisados por (Cho, 2010), apresenta as propriedades de confiança utilizadas em gerenciamento de confiança. São mostradas várias métricas de desempenho que têm sido usadas para avaliar a confiança em MANETs. Pode-se observar que a maioria dos trabalhos usa mais de uma métrica e incluem: *overhead, throughput, goodput,* pacotes descartados e *delay*.

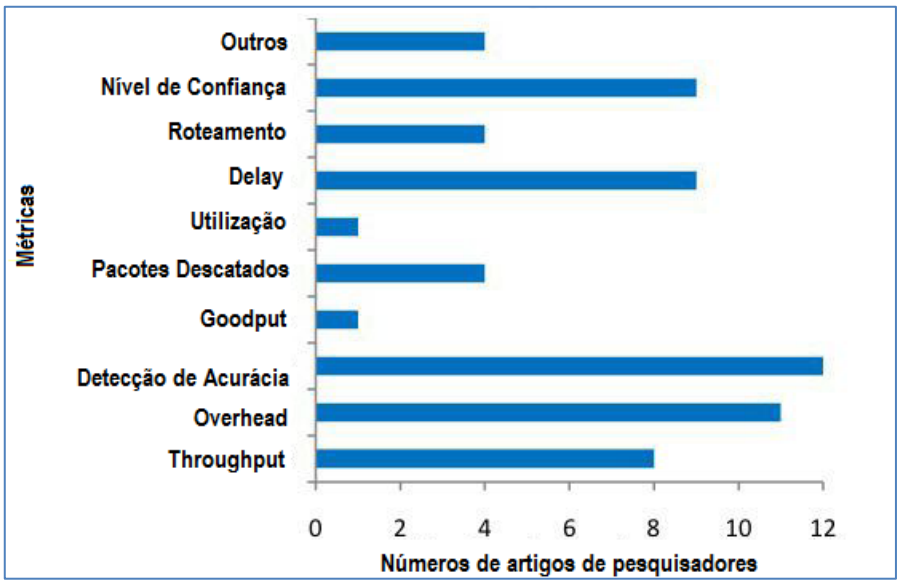


Figura 3-1 Propriedades de Confiança em Gerenciamento de Confiança em MANETs

(Cho, 2010, adaptada)

Entre tais métricas, a de Roteamento refere-se ao número de rotas selecionadas especialmente quando o objetivo é determinar a rota segura. Já as métricas de Nível de Confiança incluem o valor de confiança, credibilidade, valores de opiniões sobre os outros nós, e nível de confiança por sessão. O grupo de Outros indica métricas que consideram a tolerância do sistema com base no limiar de reputação incorreta, disponibilidade, tempo de convergência para alcançar o estado estacionário em confiabilidade de todos os nós participantes, e porcentagem de nós maliciosos (Cho, 2010).

3.3.3. Aplicações de Confiança em MANETs

No que se refere a modelos de confiança para redes *ad hoc*, muitos trabalhos utilizam métricas para obter dados dos nós e medir o grau de confiança de cada um, de modo a assim avaliar se vale a pena confiar em determinado nó para o repasse dos pacotes.

Diversos autores apresentam trabalhos de confiança para as redes *ad hoc*. Por exemplo, (Rajaram, 2010) propõe um protocolo baseado em confiança na camada *Media Access Control* (MAC) das redes *ad hoc*, provendo serviços de confidencialidade e autenticação dos pacotes em ambas as camadas de enlace e roteamento usando o modo de autenticação *Cipher Block Chaining* (CBC-X) e criptografia simétrica na camada de enlace. Foi projetado um sistema de confiança baseado em encaminhamento de pacotes para detectar e isolar os nós maliciosos usando as informações da camada de roteamento. São usados valores de confiança e um contador de confiança para cada nó. Existe um limiar que é medido com os valores do contador, se o valor do contador cair abaixo desse limiar o nó é marcado como mal-intencionado, ao contrário, se o limiar for maior o nó é marcado como confiável. O algoritmo de criptografia, CBC-X, foi usado para satisfazer a necessidade de overhead de comunicação. Esse algoritmo oferece suporte a criptografia e autenticação de pacotes em uma única operação. As camadas superiores da pilha de protocolos são fornecidas com os serviços de segurança. O mecanismo de chave simétrica CBC-X foi concebido para empregar o sistema de segurança na camada de enlace. A Criptografia e operações de autenticação foram incluídas em uma única etapa, pois reduz a sobrecarga computacional para metade, em vez de calculá-los individualmente.

Já (Velloso, 2006) tem como objetivo prover aos nós de uma rede *ad hoc* um mecanismo para construir relações de confiança com seus vizinhos. O modelo apresentado permite a construção de uma ligação de confiança entre os nós da rede a partir de troca de

recomendações e do monitoramento do comportamento dos vizinhos. O modelo de confiança é dividido em duas camadas. A camada de confiança é responsável por calcular o grau da confiança para cada vizinho, utilizando para tanto informações enviadas pelos vizinhos dos vizinhos e também informações obtidas da outra camada que é denominada de aprendizado. Este grau de confiança pode ser usado como métrica por protocolos e aplicações. A outra camada é a de aprendizado cuja responsabilidade é julgar o comportamento dos nós vizinhos a partir das informações coletadas. Esse julgamento é passado para a camada de confiança. Cada nó computa e armazena um grau de confiança para cada vizinho direto. Esse valor é continuamente atualizado e os nós são responsáveis pelos seus próprios processos de avaliação do grau de confiança. O grau de confiança é um valor contínuo que pode variar no intervalo [0,1]. Os nós utilizam o protocolo de troca de recomendações *Recomendation Exchange Protocol* (REP) para considerar as recomendações de outros vizinhos.

O modelo apresentado por (Pirzada, 2004), faz uma adaptação do modelo de confiança de Marsh (Marsh, 1994) que é configurado para uso em redes *ad hoc* puras. A fim de reduzir o número de variáveis no modelo, mesclam-se a utilidade e a importância de uma situação em uma única variável chamada peso, que aumenta ou diminui com o tempo. O modelo faz o uso de agentes de confiança que residem em nós da rede. Cada agente opera de forma independente e mantém a sua perspectiva individual da hierarquia de confiança. Um agente reúne dados de eventos em todos os estados, filtra, atribui pesos a cada evento e calcula os níveis de confiança diferentes, com base neles. Cada agente de confiança basicamente executa três funções: derivação de confiança, quantificação e computação. O modelo de confiança apresentado cria e mantém os níveis de confiança com base em esforço e mecanismo de retorno. Os percursos selecionados usando o modelo pode não ser criptograficamente seguros, mas os procedimentos estabelecem níveis relativos de confiança para eles. O modelo é aplicável tanto a redes *ad hoc* puras, como gerenciadas, proporcionando medidas de confiança em relação à confiabilidade das rotas calculadas utilizando os mecanismos de confiança direta, ao invés de recomendações de terceiros.

O trabalho de (De Sousa Jr & Puttini, 2010), além de apresentar características das redes *ad hoc*, examina os modos de utilização de confiança, o conceito de confiança, as características e funções de confiança neste contexto. Não é objetivo desta dissertação detalhar o trabalho dos autores e sim apresentar as métricas usadas para delinear confiança.

(De Sousa Jr & Puttini, 2010) afirmam que como as redes *ad hoc* não possuem um nó central e nem uma infraestrutura, para que ocorra a entrega de pacotes confiável em uma rota, um nó deve confiar nos nós intermediários para transmitir os seus pacotes ao longo das rotas multi-hop. Então, o trabalho de colaboração é essencial para atingir um grau de confiança representativo na hora do roteamento de pacotes. A avaliação da confiança, em relação à ação de encaminhar pacotes, trabalha com integração forte ao comportamento da entidade que implementa o protocolo. No caso do OLSR, após enviar um pacote, o nó continuar a escutar o enlace para verificar se o nó escolhido como MPR teve sucesso ou falha ao encaminhar o pacote dado. Para visualizar a verificação local da relação de confiança entre vizinhos, os autores apresentam o exemplo do encaminhamento de mensagens *topology* control – TC que são utilizadas para atualizar as tabelas de roteamento. Em OLSR, se o nó X escolheu o nó Y como um MPR, e X envia uma mensagem TC, logo X espera ouvir o encaminhamento da mensagem TC por Y. Se X não ouvir a mensagem, então X deve considerar que Y falhou no encaminhamento. Então, é proposto o uso de duas métricas para X avaliar a confiança que pode depositar em Y:

- TCX: Número de mensagens TC enviadas por X.
- TCXfw-Y: Número de mensagens TC enviadas por X e encaminhadas por Y.

A Figura 3-2 apresenta casos de evolução de uma possível relação de confiança de X para Y. Na figura, o gráfico "a", mostra o comportamento ideal caso o nó Y trabalhe de forma correta e sem falhas na transmissão, encaminhando as mensagens enviadas por X. No caso do gráfico "c", é apresentado um comportamento indesejável, mas a confiança específica para o serviço de roteamento não é capaz de caracterizá-lo como mau comportamento. Já no caso do gráfico "d", ocorre um mau comportamento, que indica a ocorrência de um ataque.

Com base na relação de confiança apresentada, está dissertação apresenta no próximo capítulo a implementação de uma MIB de confiança, permitindo monitorar e aramzenar métricas que possam ser utilizadas tanto no contexto local de um nó, quanto genericamente na gerência de uma rede *ad hoc*. A validação dessa MIB será feita usando as métricas que verificam a confiança relacionada ao encaminhamento de mensagens TC, realizado pelo nó MPR do protocolo OLSR.

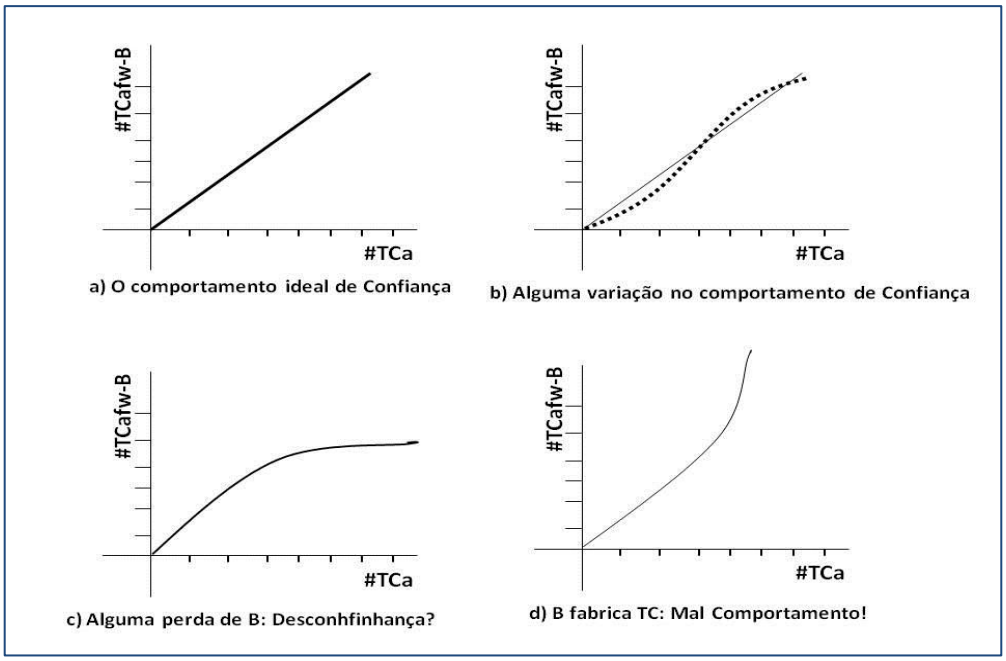


Figura 3-2 Visualização das métricas de confiança relacionado ao encaminhamento de mensagens OLSR.

(De Sousa Jr & Puttini, 2010, adaptada)

4. PROPOSTA DA MIB DE CONFIANÇA PARA REDES *AD HOC*

Este capítulo aborda a proposta de uma MIB de confiança computacional, apresentando as métricas de confiança escolhidas, o próprio processo de criação e implementação da MIB e por fim os resultados da validação dessa MIB com um agente de gerência integrado ao *deamon* OLSRd que constitui uma entidade operacional do protocolo OLSR.

O objetivo desta proposta é a criação de uma MIB de gerenciamento da confiança em redes *ad hoc*. Foram retomadas métricas do trabalho de (De Sousa Jr. & Puttini, 2010), para serem os objetos gerenciados. Essas métricas se referem com efeito à operação do protocolo OLSR, no qual se apresenta de interesse a quantidade de mensagens TC (*Topology Control*) enviadas e ouvidas na rede.

A construção de uma MIB para o protocolo OLSR foi proposta por (Pacheco, 2007), que desenvolveu uma OLSR MIB para o monitoramento do protocolo permitindo a manipulação dos respectivos parâmetros da configuração padrão e das variáveis operacionais. Assim, a OLSR-MIB é um documento contendo a base de informações modelada para o OLSR, cuja sua compilação especifica todos os parâmetros necessários para monitorar, controlar e proteger o protocolo (Pacheco, 2007). Entretanto, tal proposta não contempla os aspectos específicos da confiança.

Então, a presente dissertação não estende o trabalho de (Pacheco, 2007), mas apenas especifica a proposta de uma MIB para a confiança, cuja implementação é desenvolvida no protocolo OLSR, o que permite obter informações para a análise de confiança em um ambiente *ad hoc,* validando a proposta em um ambiente operacional controlado.

4.1. MÉTRICAS

As métricas foram escolhidas com o propósito de por meio delas avaliar a confiança usando uma MIB. Baseado no trabalho de (De Sousa Jr & Puttini, 2010), as métricas são apresentadas na Tabela 4-1. De acordo com as métricas apresentadas na Tabela 4-1, podem-se apresentar as seguintes características:

- Toda vez que uma mensagem TC é enviada, um contador (TCx) sofre um incremento unitário na contagem. O endereço IP do nó que enviou a mensagem é a variável Endereço TCx.

- Quando o nó MPR (nó avaliado) recebe a mensagem TC, ele encaminha essa mensagem. Com isso, o nó que originou a mensagem irá escutar a mensagem encaminhada. Então, um contador de mensagens TC encaminhadas (TCxfw-Y) é incrementado e realiza o registro de cada mensagem. O endereço IP do nó que repassou a mensagem fica na variável Endereço TCxfw-Y.
- Observa-se que os dois contadores TCx e TCxfw-Y devem crescer de forma monotônica.
- É necessário implementar o conjunto de métricas na forma de tabela, contendo entradas correspondentes a cada nó vizinho que deva fazer repasse de mensagens TC.

Tabela 4-1 Métricas de Confiança

Métricas	Descrição
TCx	Quantidade de mensagens enviadas pelo nó de origem.
TCxfw-Y	Quantidade de mensagens repassadas e que serão refletidas (e ouvidas) para o nó de origem.
Endereço TCx	Endereço IP do nó que enviou as mensagens TC.
Endereço TCxfw-Y	Endereço do nó que repassou as mensagens TC.

As métricas apresentadas na Tabela 4.1 são usadas para implementar a MIB, além de serem acrescidas dos endereços, cujo objetivo é identificar os nós que originaram e encaminharam as mensagens. Os nomes das métricas, apresentados neste item para manter a mesma terminologia de (De Sousa Jr & Puttini, 2010), serão mudados na criação formal da MIB.

4.2. CÁLCULO DE CONFIANÇA

O cálculo de confiança proposto como outra contribuição deste trabalho baseia-se na função de densidade de probabilidade Beta que pode ser usada para representar distribuições de probabilidades de eventos binários. Isso fornece uma base matemática sólida para combinar *feedback* e expressão de estimativas de probabilidade. As análises de probabilidade apresentadas nesta proposta foram obtidas de (Josang, 2002). A utilização da

MIB para obter informações relacionadas à confiança tem o interesse de fornecer uma base formal para o uso de um método matemático que permita uma melhor percepção dos resultados.

O cálculo que propomos para validar a utilização da MIB parte então do princípio que as probabilidades de eventos binários podem ser representadas como distribuição beta. A família beta de funções de densidade de probabilidade é uma família contínua de funções indexadas por dois parâmetros α e β. A distribuição beta $f(p|\alpha,\beta)$ pode ser expressada usando a função Gamma (Γ) como:

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-p)^{\beta-1} \text{ , onde } 0 \leq p \leq 1, \alpha > 0, \beta > 1 \quad (1)$$

com a restrição de que a variável de probabilidade $p \neq 0$ se $\alpha < 1$ e $p \neq 1$ se $\beta < 1$. O valor esperado da distribuição de probabilidade beta é dado por:

$$E(p) = \alpha/(\alpha+\beta) \quad (2)$$

Considerando um processo com duas possíveis respostas $\{\boldsymbol{x}, \overline{\boldsymbol{x}}\}$, seja r o número de respostas observadas x e seja s o número de respostas observadas $\overline{\boldsymbol{x}}$**.** Então a função de densidade de probabilidade de respostas observadas no futuro x, pode ser expressa como uma função de observações do passado definido por:

$$\alpha = r + 1 \; e \; \beta = s + 1 \text{ , onde } r, s \geq \quad (3)$$

Como um exemplo, um processo com duas possíveis respostas $\{\boldsymbol{x}, \overline{\boldsymbol{x}}\}$ que produzem respostas x sete vezes e respostas $\bar{x}$ somente uma vez, terá uma função beta expressa como $f(p|8,2)$ que está representado na Figura 4-1.

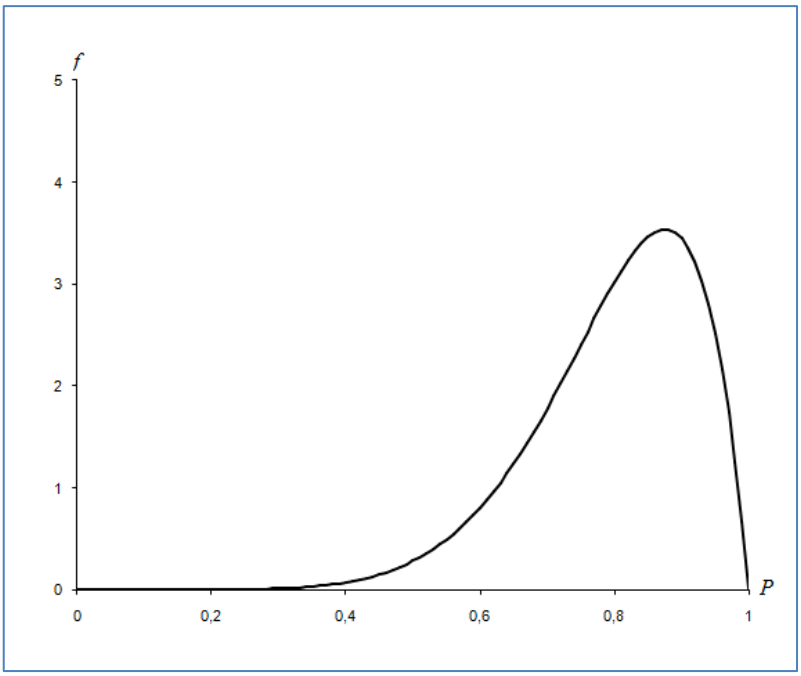


Figura 4-1 Função beta do evento x depois de 7 observações de x e 1 observação de $\bar{x}$

(Josang, 2002, adaptado)

A curva da Figura 4-1 expressa a probabilidade de que o processo produzirá respostas x durante observações futuras. O valor da esperança é dado por $E(p) = 0{,}8$. Isso pode ser interpretado como dizendo que a frequência relativa de resultados x no futuro é bastante incerta e que o valor mais provável é 0,8.

A variável p é uma variável de probabilidade, de modo que para um dado p a densidade de probabilidade $f(p|\alpha,\beta)$ representa a probabilidade de segunda ordem. A variável de primeira ordem p representa a probabilidade de um evento, considerando que a densidade $f(p|\alpha,\beta)$ representa a probabilidade de que a variável de primeira ordem ter um valor específico. Uma vez que a variável de primeira ordem p é contínua, a probabilidade de segunda ordem $f(p|\alpha,\beta)$ para qualquer valor dado de p, é extremamente pequena e, portanto, sem sentido. É apenas significativo computar $\int_{p1}^{p2} f(p|\alpha,\beta)$ para um dado intervalo $[p1,p2]$, ou simplesmente para calcular o valor esperado de p.

4.3. ESTRUTURA DA MIB DE CONFIANÇA

O gerenciamento de confiança neste trabalho objetiva monitorar por meio de uma MIB as informações referentes às interações dos nós roteadores de redes *ad hoc*, como os MPRs do protocolo OLSR. Para isso, foi construída uma MIB seguindo as definições da SMI e

ASN.1 que se encontram apresentadas no capítulo 1.

Com o objetivo de avaliar a confiança por meio de elementos padrão do gerenciamento de redes, este tópico detalha a criação e implementação da MIB de confiança nomeada como TRUST-MIB.

A primeira etapa do trabalho consiste em escrever as métricas escolhidas como objetos gerenciados, conforme Tabelas 4.2 e 4.3, que foram definidas dentro dos padrões das RFCs do SNMP (McCloghrie, 1988 & McCloghrie, 1991).

A segunda etapa consiste na implementação da TRUST-MIB em ambiente operacional de um protocolo *ad hoc* (OLSR) e do protocolo de gerência de rede SNMP, o que envolve a operacionalização do sistema de gerência NET-SNMP, a modificação do *deamon* OSLRD e o *Plugin* OLSRD.

4.3.1. Objetos da TRUST-MIB

A Figura 4-2 apresenta os objetos da TRUST-MIB, mostrando como os objetos da MIB estão hierarquizados. As descrições dos objetos são apresentadas nas Tabelas 4-2 e 4-3 respectivamente. As redações formais dos objetos da MIB encontram-se no Apêndice A.

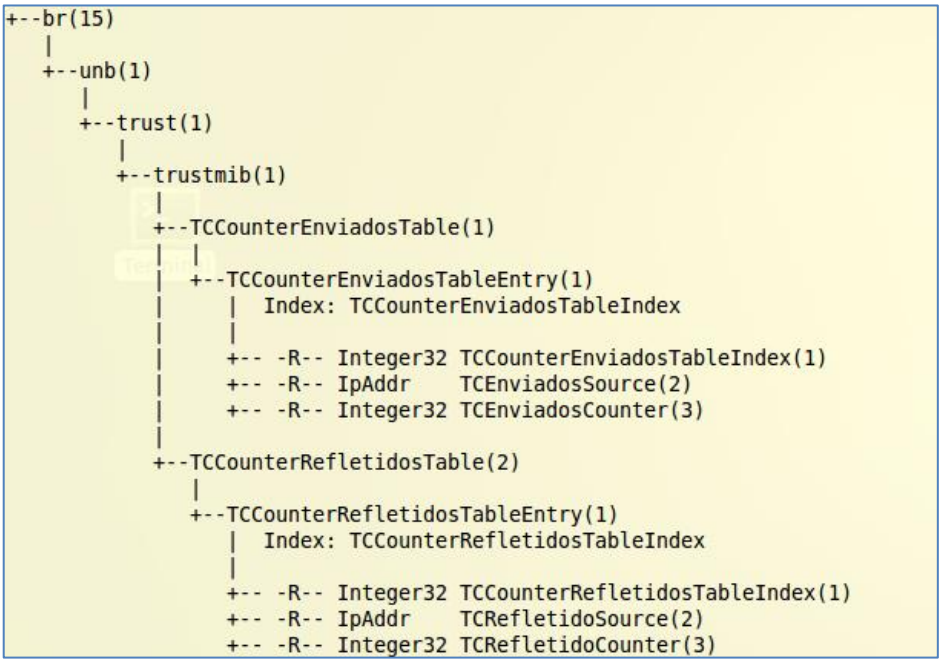


Figura 4-2 Árvore da TRUST-MIB

Tabela 4-2 Tabela Mensagens Enviadas - TCx

Tabela TCCounterEnviadosTable	Tabela que contém os objetos referentes às mensagens TC enviadas. Seus objetos, tipos e níveis de acesso são:			
	Objetos	**Descrição**	**Tipo**	**Acesso**
	TCCounterEnviadosTableIndex	Inteiro que indexa a tabela.	Inteiro	Leitura
	TCCounterEnviados	Contador de mensagens TC encaminhadas pela origem.	Counter32	Leitura
	TCEnvidosSource	Endereço IP da interface do nó que originou a mensagem TC.	Endereço IP	Leitura

Tabela 4-3 Tabela Mensagens Refletidas - TCxfw-Y

Tabela TCCounterRefletidosTable	Tabela que contém os objetos referentes às mensagens refletidas. Seus objetos, tipos e níveis de acesso são:			
	Objetos	**Descrição**	**Tipo**	**Acesso**
	TCCounterRefletidosTableIndex	Inteiro que indexa a tabela.	Inteiro	Leitura
	TCRefletidosCounter	Contador de mensagens encaminhadas pelo nó MPR.	Counter32	Leitura
	TCRefletidosSource	Endereço IP do nó que refletiu a mensagem TC.	Endereço IP	Leitura

4.4. IMPLEMENTAÇÃO DA TRUST-MIB

Após apresentar a proposta desta dissertação, as métricas utilizadas para a criação da MIB e a especificação da TRUST-MIB, objetiva-se agora descrever toda a implementação da MIB e o seu funcionamento.

Para a criação da TRUST-MIB, foi necessário utilizar as ferramentas para o desenvolvimento e validação dos resultados.

O NET-SNMP e o OLSRD foram as ferramentas fundamentais para a implementação da MIB. As definições dessas ferramentas são apresentadas nos itens a seguir e nos itens subsequentes todo o funcionamento da implementação da TRUST-MIB.

4.4.1. NET-SNMP

O NET-SNMP é um pacote de aplicativos para implementar o protocolo SNMP e pode ser utilizado nos sistemas operacionais Unix ou Microsoft Windows (NET-SNMP).O seu objetivo é o monitoramento e configuração de dispositivos e serviços de rede. Os programas de aplicação são:

- Aplicações de linha de comando, podendo usar comandos como *snmpget, snmpgetnext, snmpwalk, snmptable, snmpset*, dentre outros.
- Um MIB Browser gráfico, usando TK/Perl.
- Aplicação *deamon* para receber notificações SNMP.
- Um agente extensível para responder a consultas SNMP para gerenciamento de informações (snmpd). Isso inclui suporte módulos de informações MIB, e pode ser estendido com módulos carregados dinamicamente, scripts e comandos externos, e o protocolo AgentX.
- Uma biblioteca para o desenvolvimento de novas aplicações SNMP, com as APIsde C e Perl.

4.4.2. OLSRD

O OLSR *Deamon* é uma implementação em linguagem C do protocolo OLSR, usando como padrão as definições do RFC 3626 (Clausen, 2003). Desenvolvido pelo *Unik Graduate Center* da Universidade de Oslo – Noruega, ele tem como objetivo realizar o roteamento *ad hoc* para qualquer equipamento de rede, além de poder ser usado para simulação. O OLSRD pode ser executado em qualquer dispositivo que tenha suporte para o modo *ad hoc*, além de possuir suporte a *Ethernet* (Tonessen, 2004).

Tal implementação é compatível com a funcionalidade núcleo e funcionalidade auxiliar descritas no RFC 3626 (Clausen, 2003). Existe também a implementação do *Link Quality*, que não está no padrão do RFC, mas em função dos testes realizados no presente trabalho foi possível verificar a necessidade de usar tal funcionalidade.

O OLSRD é executado tanto nos sistemas operacionais Linux, Windows, Symbian, IOS e Android, dentre outros. Essa implementação é registrada e possui uma comunidade que trabalha com o suporte as versões do projeto. Para a utilização da implementação do protocolo foi necessário instalar a versão 0.5.3 do OLSRD.

A implementação do OLSRD é representada na Figura 4-3, onde são apresentadas as entidades de funcionamento do protocolo, as quais são:

- Parser de Sockets: A Figura 4-3 mostra que o tráfego OLSR é tratado no Parser de Sockets, cuja responsabilidade é escutar os dados de um determinado conjunto de sockets.
- Parser de Pacotes: Ao iniciar, o Parser de Sockets registra todo o tráfego de controle de sockets. Estes sockets são registrados com a função Parser de Pacotes a serem chamados sempre que há dados disponíveis.
- Repositório de Informação: Protocolos baseados em tabelas dirigidas são atualizados dinamicamente e removidas com base em mudanças na topologia da rede. Todas as informações são mantidas em tabelas e estes devem ser firmados de forma inteligente. Com isso, o OLSRD implementou o repositório de informação com listas encadeadas indexadas por *hashes* (Tonessen, 2004).
- Agendador: O Agendador no OLSRD executa as tarefas registradas em intervalos determinados (Tonessen, 2004).O intervalo 0,1 segundo é considerado padrão e este intervalo pode ser definido no arquivo de configuração do OLSRD, *olsrd.config* e o parâmetro a ser configurado é o *PoolRate*. Funções como *void olsr_register_scheduler_event()* e *int olsr_register_timeout_function()* são usadas para realizar tarefas em intervalos regulares (Tonessen, 2004).

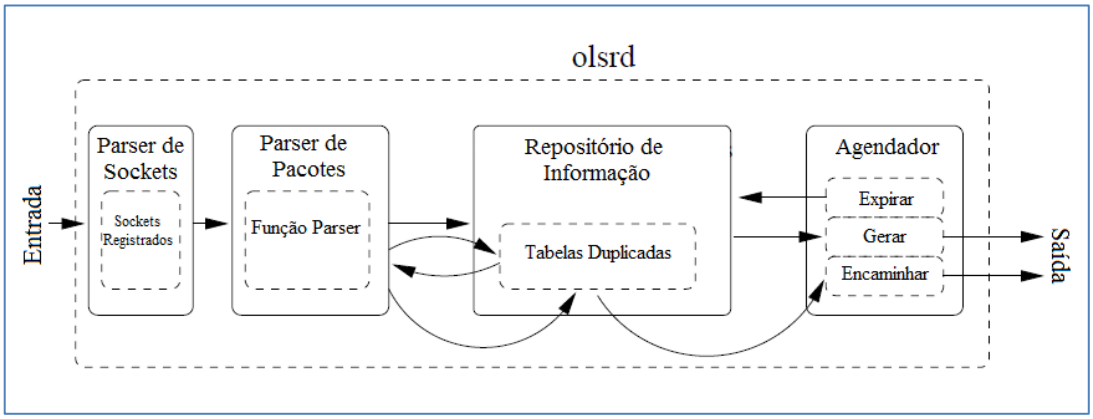


Figura 4-3 Visão geral do OLSRD (Tonessen, 2004, adaptada)

O uso do OLSRD neste trabalho é importante, pois é necessário o seu funcionamento para alcançar o objetivo proposto de demonstrar a utilidade de uma MIB de confiança em redes *ad hoc*.

Por ter sido baseada na RFC 3626 (Clausen, 2003), a codificação do protocolo não possuía a contagem específica das mensagens TC enviadas e refletidas. Desse modo, foi necessário desenvolver modificações nos arquivos *lq_packet.c* e *parser.c* dos fontes do pacote OLSRD para ocorrem as devidas contagens.

a) *Plugin* OLSRD

A implementação do protocolo tem a possibilidade de estender o código usando bibliotecas dinamicamente carregáveis, ou seja, *plugins* que ajudam as comunidades no desenvolvimento do protocolo sem qualquer modificação no código. Os *plugins* são bibliotecas dinamicamente carregáveis (DLL), de modo que resultam para o desenvolvedor na capacidade de adicionar extensões ou alterar o funcionamento normal na implementação do protocolo. Isso facilita o teste de novas extensões, além de não precisar modificar o código básico (Tonessen, 2004).

Os *plugins* geram e processam pacotes de tipo particular e qualquer outra funcionalidade personalizada. Uma DLL é um código executável que contém funções e dados, podendo ser usado simultaneamente por vários processos e permitindo a um aplicativo poder carregar e executar funções de uma DLL. *Plugins* fornecem novas funções para um aplicativo existente, sem alterar a aplicação original.

4.4.3. Funcionamento da TRUST-MIB

A Figura 4-4 mostra a estrutura de comunicação que ocorre na implementação da TRUST-MIB. Esta, ao se comunicar com o agente mestre, se torna um subagente e se integra ao OLSRD utilizando a implementação deste como repositório. O AgentX faz a comunicação com o agente mestre e o OLSRD com o *plugin* nomeado como trust_mib_agentx.

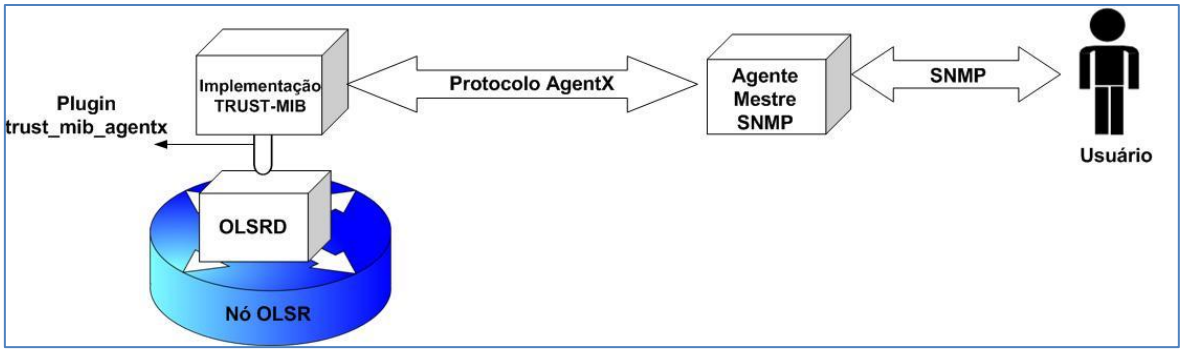


Figura 4-4 Estrutura de funcionamento da TRUST-MIB

A implementação da TRUST-MIB foi criada na forma de um *plugin* OLSRD com bibliotecas AgentX implantadas, facilitando a junção do suporte ao protocolo AgentX quanto a interface *plugin*. Vale notar que o NET-SNMP possui bibliotecas gratuitas do AgentX, que foram usadas para testar e validar esta implementação.

O programa seguiu as especificações determinadas pela interface *plugin* em (Tonessen, 2004), de modo a se apresentar em uma DLL.

4.4.3.1. Interfaceamento com o OLSRD e com o Agente Mestre

O interfaceamento da TRUST-MIB e o agente mestre SNMP visa tornar real o repositório de informação e a comunicação do protocolo AgentX com o agente mestre. A modificação da implementação do protocolo OLSRD visa coletar o número de mensagens TC enviadas e mensagens TC refletidas. Contudo, as informações quando geradas pela implementação são armazenadas nos repositórios de informação do OLSRD. Para ter acesso às informações é preciso que as variáveis e tabelas do OLSRD sejam mapeadas para os objetos da TRUST-MIB, sendo necessária a busca direta aos endereços de memória de tais informações dentro do OLSRD.

Todas essas tarefas são registradas e realizadas pelo Agendador do OLSRD. As funções temporizadas do Agendador dão à TRUST-MIB a possibilidade de administrar eventos e transições do programa.

a) Interfaceamento com o OLSRD

O *plugin* trust_mib_agentx realiza o interfaceamento da implementação OLSRD. Ele necessita apenas das funcionalidades de acesso ao repositório de informação e o registro de funções junto ao Agendador.

Para o acesso ao repositório de informação, ao ser iniciado o OLSRD verifica no seu arquivo de configuração, *olsrd.config*, a chamada do *plugin* trust_mib_agentx identificado pelo parâmetro LoadPlugin. Após,as funções *olsrd_plugin_register_param()* e *olsrd_plugin_init()* são chamadas e a elas são fornecidas o acesso aos parâmetros especificados para a chamada do *plugin* e aos repositórios de informações do OLSRD.

Para o registro das funções com o Agendador, as funções *olsr_register_scheduler_event()* e *olsr_register_timeout_function()*, disponibilizadas pela interface *plugin*, são utilizadas. A

função *olsrd_snmpd()* registrada pela *olsr_register_scheduler_event()* tem como objetivo implementar o *deamon* de atualização das variáveis e tabelas dinâmicas, pois elas mudam constantemente e precisam de atualizações junto aos objetos da MIB. O intervalo de chamada da função e, consequentemente, de atualização dos objetos da MIB, é determinado pelo parâmetro arbitrário passado pela diretiva LoadPlugin do carregamento deste *software*. A função *olsr_register_timeout_function()* registra o *agentx()*, no qual trata as transações AgentX com o agente mestre SNMP registrado. A Figura 4-5 mostra o fluxo de execução da implementação TRUST-MIB.

b) Interfaceamento com o Agente Mestre

O interfaceamento com o Agente Mestre realiza o registro da TRUST-MIB como um subagente e o tratamento das transações SNMP via protocolo AgentX. O registro do subagente é inicializado dentro da função *olsrd_plugin_init*, no qual é chamada no início da execução do *plugin*.

Para o tratamento das transações SNMP que são recebidas vindas do agente mestre SNMP, a função *agent_check_and_process()* oferecida pelo NET-SNMP (NET-SNMP) é utilizada. Ela é chamada dentro da função *agentx()* registrada junto ao Agendador.

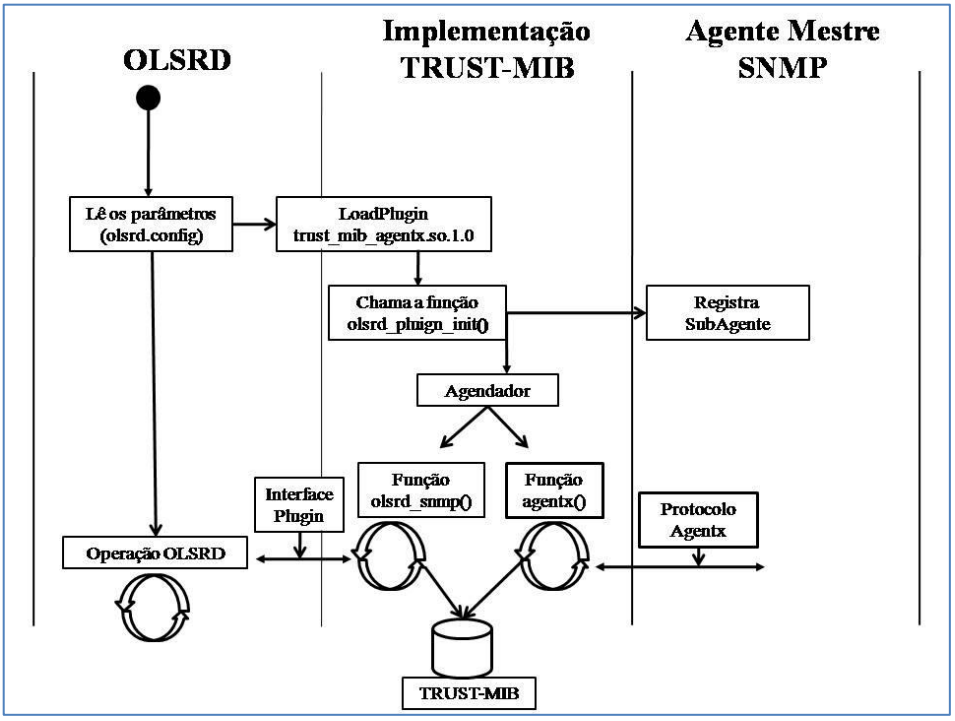


Figura 4-5 Fluxo de Execução da TRUST-MIB

4.5. VALIDAÇÃO EXPERIMENTAL DA TRUST-MIB

A ideia central do processo de validação é verificar não apenas o modelo de observação de métricas, armazenamento na MIB, monitoração via protocolo de gerência de rede, mas também de validar como a confiança no ambiente da rede *ad hoc* pode ser avaliada a partir das interações ao longo do tempo entre os nós, constituindo-se uma grandeza representativa do funcionamento da rede.

Vale notar que os valores relativos à confiança são o resultado final de todo o processo de coleta dos dados operacionais e preenchimento da MIB, seguido da monitoração da MIB via protocolo de gerência de rede e cálculo da confiança para apresentação ao usuário, conforme indica a Figura 4-4. Então, os valores resultantes desse cálculo serão utilizados como validadores do conjunto de elementos da proposta desta dissertação.

Os resultados dos experimentos são apresentados em dois tópicos, sendo o primeiro destinado a descrever o comportamento esperado para a confiança, por meio de um processo analítico das métricas utilizadas na base do processo. Tais métricas são apresentadas na forma de tabelas e gráficos acerca das expectativas para resultados no futuro, expressas como uma função de observações do passado. Ou seja, com base no cálculo de confiança proposto no item 4.2, são feitos os raciocínios que levam à previsão dos valores da confiança futura.

Já o segundo tópico a seguir apresenta os resultados obtidos a partir de medições realizadas no ambiente real de rede *ad hoc* em situação controlada, conforme descrito abaixo.

4.5.1. Resultados esperados para a confiança

São levados em consideração três tipos de comportamentos do roteador das mensagens TC em redes *ad hoc*, conforme Tabela 4-4. As mensagens enviadas pelo nó que deseja atualizar as informações de roteamento serão representadas como TC, enquanto as correspondentes mensagens que o roteador encaminha, e que na rede *ad hoc são* refletidas para o nó de origem, são representadas como TCr.

Tabela 4-4 Tipos de comportamentos esperados da relação entre mensagens TCr e TC

Tipo de comportamento	Descrição
Ideal: TCr = TC	Ao longo do tempo, a quantidade de mensagens TCr refletidas pelo roteador *ad hoc* permanece igual à quantidade de mensagens TC enviadas pelo nó.
Real Normal: TCr <≅ TC	A quantidade de mensagens TCr refletidas é aproximadamente igual, mas menor, que a quantidade de mensagens TC enviadas
Real Ruim: TCr<< TC	A quantidade de mensagens TCr refletidas é muito inferior à quantidade de mensagens TC enviadas.

No mundo ideal e perfeito (sem perda), as mensagens enviadas são sempre refletidas, resultando em uma total confiança do nó em seu roteador:

$$TCr = TC$$

Entretanto, em uma rede real funcional, é natural que haja alguma perda nas transmissões ou no tratamento da mensagem TC pelo vizinho. Assim, espera-se que a quantidade de refletidas (TCr) seja sempre menor, mas aproximadamente igual, à quantidade de enviadas (TC) em determinados intervalos de tempo:

$$TCr \leq TC$$

Por oummmmmm,uyuyu787w’]]’/.tro lado, se o comportamento do vizinho ou o meio de transmissão estão causando perdas no repasse das mensagens TC, então o número de mensagens refletidas se torna ao longo do tempo muito menor que o das enviadas:

$$TCr \ll TC$$

Tal situação pode decorrer de mau comportamento do vizinho roteador, mas também de problemas operacionais e de desempenho nesse roteador. Não é possível somente com o modelo proposto distinguir as duas situações, mas de todo modo do ponto de vista do nó solicitante a rota pode ser considerada como não confiável.

As três situações acima podem ser verificadas no ambiente experimental definido nesta dissertação e são o referencial para os experimentos realizados. Entretanto, vale a pena observar que existe uma situação possível em que o roteador vizinho se comporta como

gerador de um conhecido ataque em que o roteador cria falsas mensagens TC para burlar o roteamento normal na rede (o roteador envia mensagens TCr em nome de um vizinho inexistente). Nessa situação, a quantidade de mensagens TCr observadas é maior que o de mensagens TC realmente enviadas pelo nó:

$$TCr > TC$$

Esta última situação não é objeto da experimentação pois requer a implementação do atque no código do OLSRD, o que está fora do escopo desta dissertação.

Para as situações passíveis de previsão analítica, as tabelas e gráficos descritos a seguir apresentam o comportamento previsto para os resultados dos experimentos com a confiança no contexto da utilização da MIB proposta na presente dissertação.

As Tabelas 4-5, 4-6 e 4-7 apresentam os valores correspondentes aos tipos de comportamentos especificados na Tabela 4-4 para a relação entre as mensagens TCr e TC. Tais tabelas apresentam o cálculo de confiança abordado no item 4-2 e os gráficos de acordo com o resultado de cada valor apresentado por TCr e TC. Em tais tabelas, adotam-se as seguintes convenções:

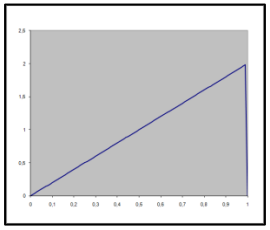
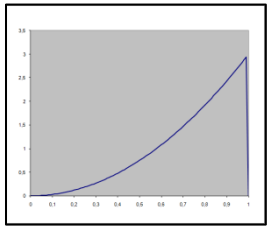
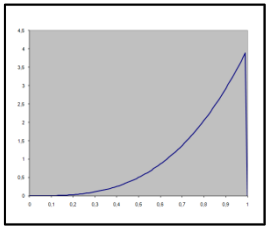
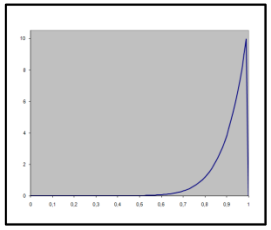
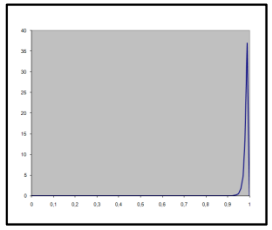
- As linhas cujos primeiros campos são TC e TCr mostram respectivamente as quantidades de mensagens enviadas e refletidas.
- As linhas encabeçadas por x representam a quantidade de mensagens refletidas. Já as linhas encabeçadas por $\bar{x}$ o resultado da subtração de TC - TCr. Trata-se da conversão das observações físicas na rede em resultados positivos (x) e negativos ($\bar{x}$) considerados na definição da distribuição Beta que é utilizada nos cálculos da confiança.
- As próximas duas linhas da tabela mostram os valores de alfa e beta da distribuição Beta e, por fim, é calculado o valor da esperança com os valores de alfa e beta encontrados.
- Os gráficos pequenos apresentam a função de densidade da distribuição Beta e ilustram a evolução dos valores da esperança.

A Tabela 4-5 corresponde ao ambiente ideal, ou seja, a esperança indica que no futuro as interações serão perfeitas. Assim, o gráfico à Figura 4-6 mostra a evolução crescente dos valores de confiança com tendência de chegar o mais próximo de 1, que é a confiança total.

Já a Tabela 4-6 mostra um ambiente mais realista, no qual a confiança varia no tempo dentro de limites aceitáveis para a realização das interações futuras, observado que as interações passadas deram certo em sua maioria e as perdas se deveram a problemas operacionais aceitávies. O número de mensagens refletidas (ou seja, encaminhadas pelo vizinho) é pouco menor ou igual ao número das mensagens TC enviadas em cada intervalo. Assim, o gráfico da Figura 4-7 mostra a oscilação da curva de valores da confiança em torno de uma linha horizontal.

Por fim, a Tabela 4-7 apresenta os valores quando a quantidade de mensagens TCr é bem inferior à das mensagens enviadas. Sendo assim, a confiança apresenta valores relativamente baixos e com tendência de queda no que se refere às expectativas quanto às interações futuras, o que é mostrado no gráfico da Figura 4-8.

Tabela 4-5 Tipo de comportamento: TCr = TC

	T1	**T2**	**T3**	**T10**	**T100**
TCr (refletidos)	1	2	3	10	100
TC (enviados)	1	2	3	10	100
x = refletidos = TCr	1	2	3	10	100
$\bar{x}$ = não refletidos = TC- TCr	0	0	0	0	0
α = x + 1	2	3	4	11	101
β = $\bar{x}$ + 1	1	1	1	1	1
E (x) = α/α+β	0,67	0,75	0,80	0,92	0,99
Gráficos - Distribuição Beta ***O eixoY representa a Função de Densidade de Probabilidade.** ****O eixoX representa a Probabilidade**					

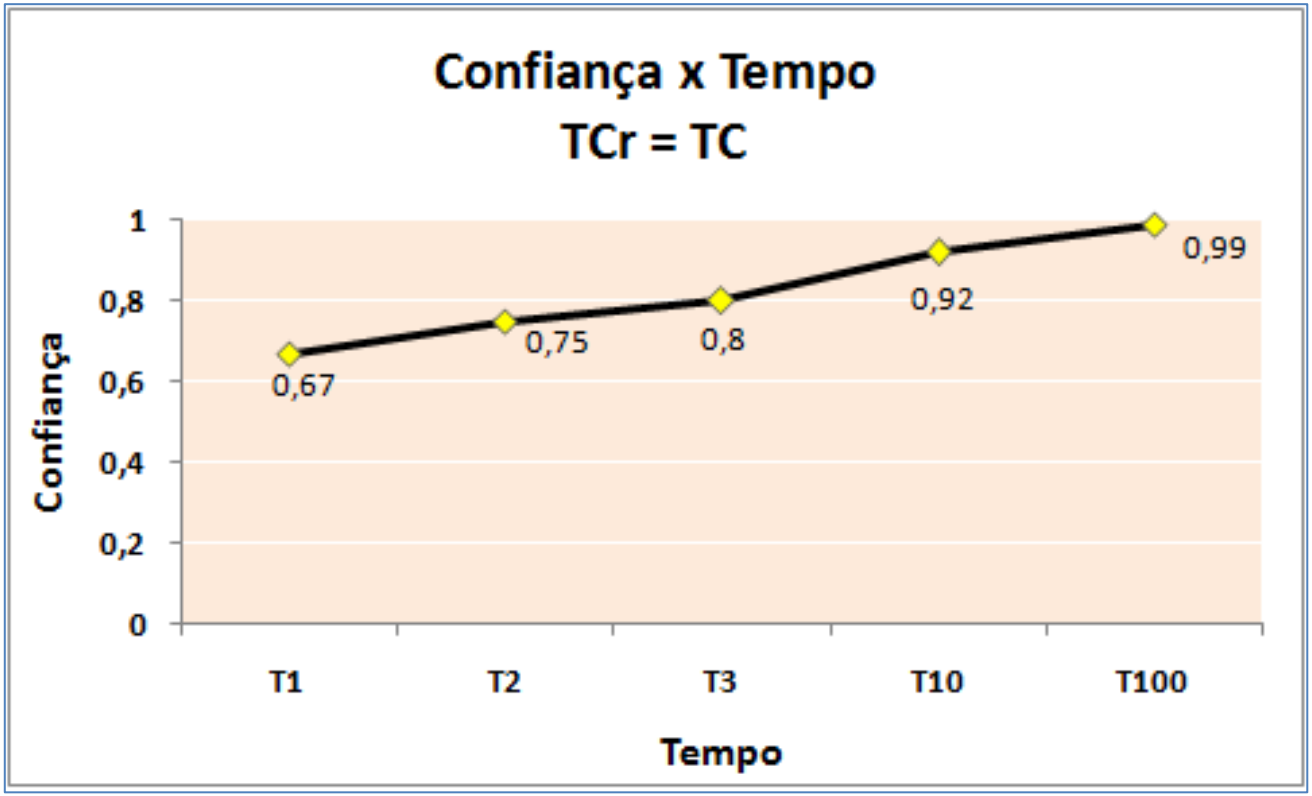
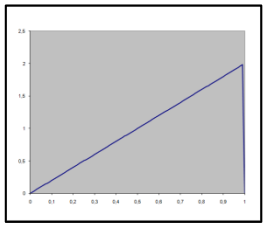
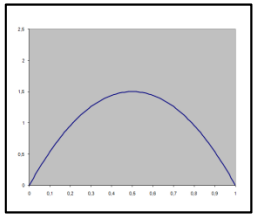
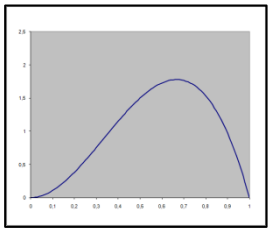
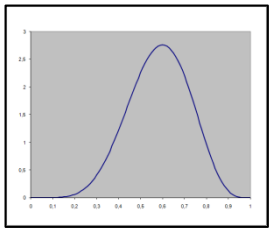
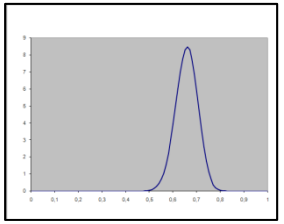


Figura 4-6 Confiança x Tempo quando TCr = TC

Tabela 4-6 Tipo de comportamento: TCr≅ TC

	T1	T2	T3	T10	T100
TCr (refletidos)	1	1	2	6	66
TC (enviados)	1	2	3	10	100
x = refletidos = TCr	1	1	2	6	66
$\bar{x}$ = não refletidos = TC- TCr	0	1	1	4	34
α = x + 1	2	2	3	7	67
β = $\bar{x}$ + 1	1	2	2	5	35
E (x) = α/α+β	0,67	0,50	0,60	0,58	0,66
Gráficos - Distribuição Beta ***O eixo Y representa a Função de Densidade de Probabilidade.** ****O eixo X representa a Probabilidade**					

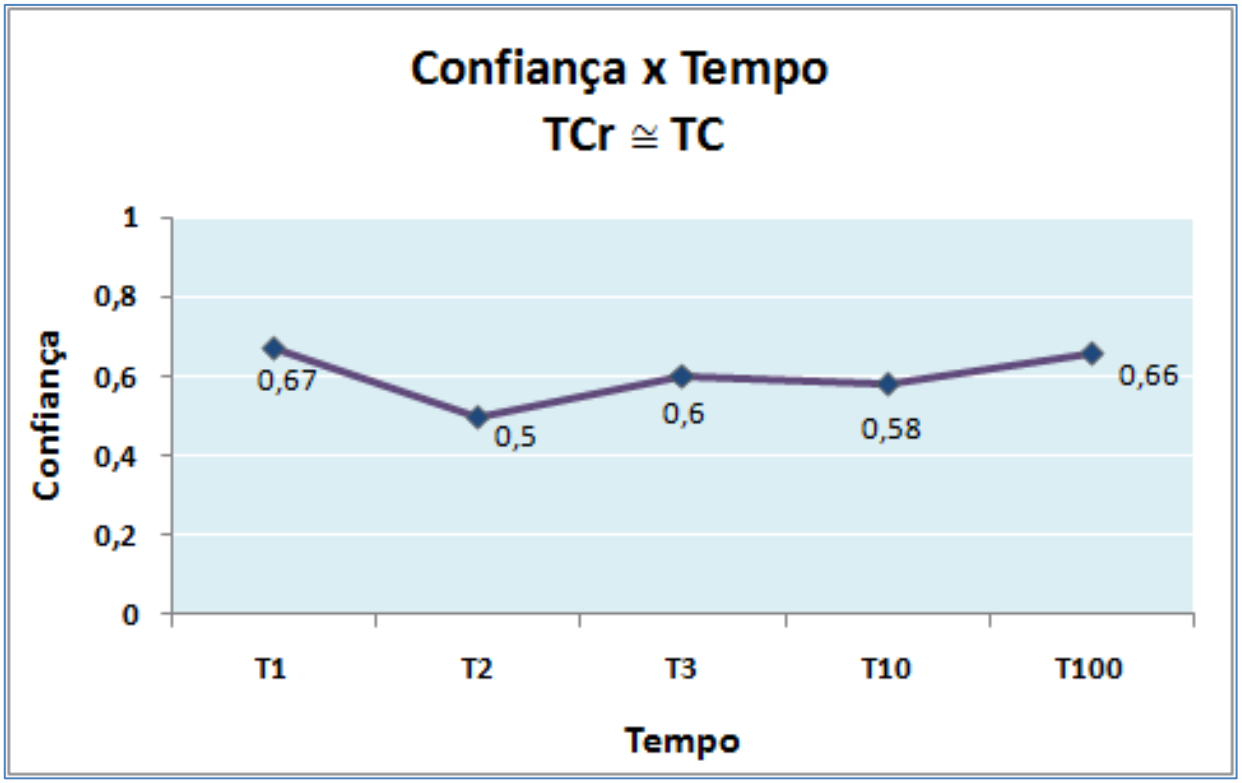
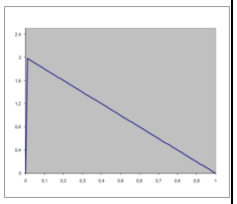
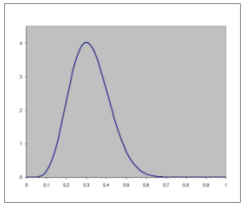
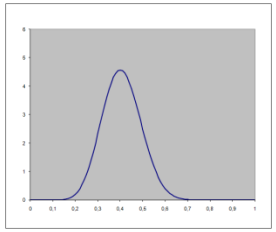
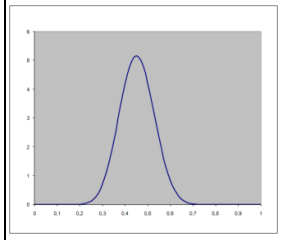
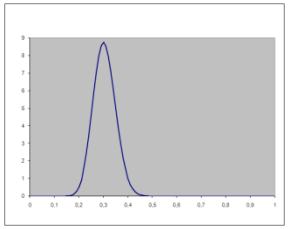


Figura 4-7 Confiança x Tempo quando TCr≅ TC

Tabela 4-7 Tipo de comportamento: TCr<< TC

	T1	**T20**	**T30**	**T40**	**T100**
TCr (refletidos)	0	6	12	18	30
TC (enviados)	1	20	30	40	100
x = refletidos = TCr	0	6	12	18	30
$\bar{x}$ = não refletidos = TC- TCr	1	14	18	22	70
α = x + 1	1	7	13	19	31
β = $\bar{x}$ + 1	2	15	19	23	71
E (x) = α/α+β	0,33	0,32	0,41	0,45	0,30
Gráficos - Distribuição Beta ***O eixo Y representa a Função de Densidade de Probabilidade.** ****O eixo X representa a Probabilidade**					

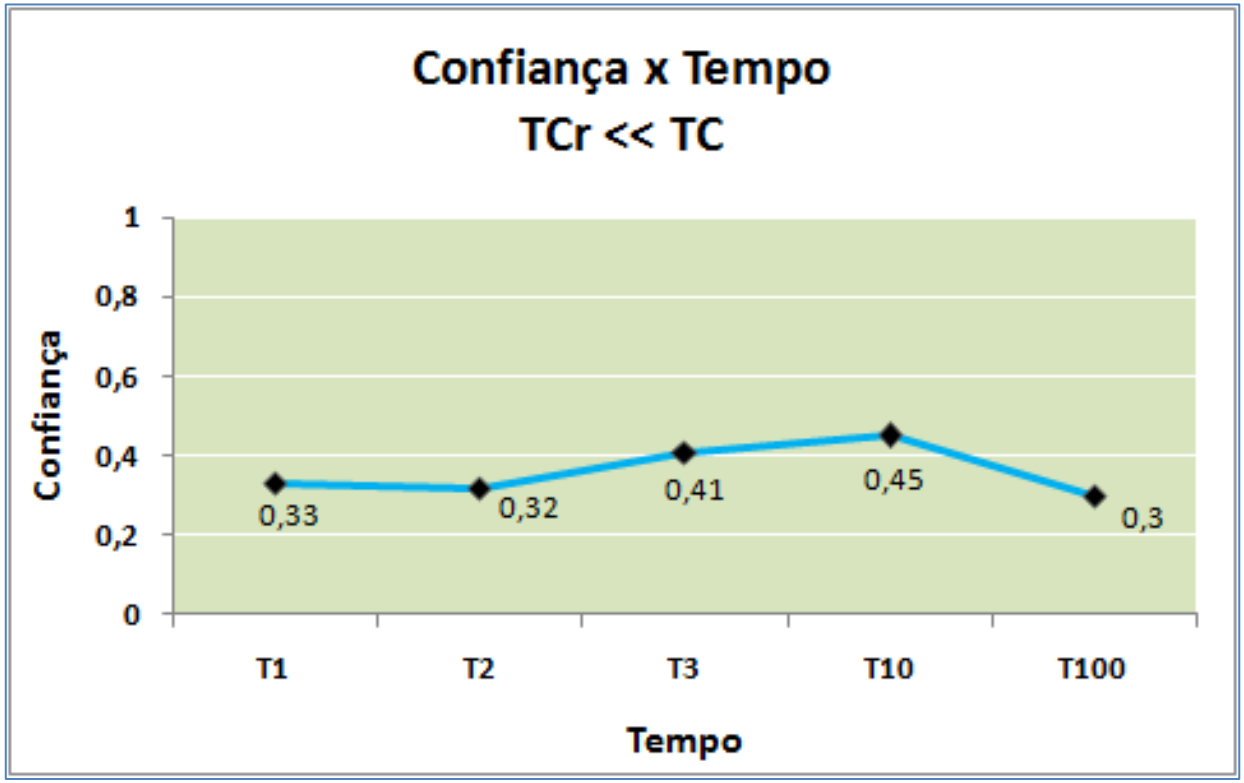


Figura 4-8 Confiança x Tempo quando TCr<<TC

4.5.2. Ambiente experimental controlado

A Figura 4-9 apresenta a estrutura usada para realizar os experimentos e validar a TRUST-MIB. Foram usadas três carcaças desativadas de aparelhos de micro-ondas, quatro notebooks com função de roteador, sendo que, diferente da estrutura de gerenciamento padrão, todos os roteadores possuem o seu próprio gerenciamento de confiança. Em cada notebook foi instalado o NET-SNMP, o *deamon* OLSRD e a implementação da TRUST-MIB, sob controle do sistema operacional Ubuntu-br, versão 10.10. O arquivo de configuração do *deamon*, *olsrd.conf*, foi composto de acordo com as necessidades do projeto e pode ser verificado no Apêndice B.

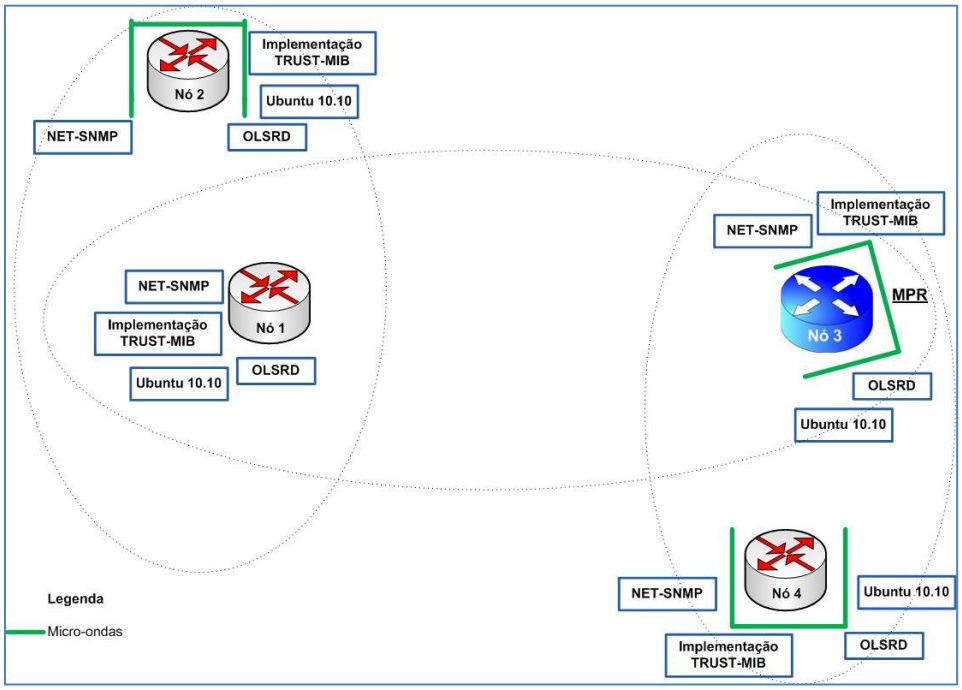


Figura 4-9 Ambiente Experimental de Validação da TRUST-MIB

Os notebooks foram nomeados de 1 a 4, sendo tal valor colocado no campo identificador de estação (*host*) do endereço IP configurado para em cada um. Além disso, receberam a configuração para redes *ad hoc*. Os parâmetros de configuração podem ser verificados na Tabela 4.8.

Tabela 4-8 Parâmetros de configuração

Parâmetro	Configuração
Aparelho de Micro-ondas	03
Quantidade de nós	04
Endereços	192.0.0.1 a 192.0.0.4
Máscara de rede	255.0.0.0
Tempo de simulação	300 segundos

Neste experimento, o uso de carcaças desativadas de fornos de micro-ondas tem como objetivo utilizar a gaiola de Faraday da carcaça desses aparelhos de modo a constituir um ambiente controlado para realizar medições sistemáticas e repetitivas, tanto com o protocolo operando sem interferências, quanto interferindo no funcionamento do protocolo de modo a provocar falhas de transmissão que afetem o envio e o retorno de mensagens de roteamento.

O objetivo é diminuir de forma controlada a potência do dos nós, além de poder direcionar o sinal e simular o funcionamento da rede sob condições variadas, de acordo com o ângulo de abertura da porta do micro-ondas, ângulo este que é mensurável e pode ser controlado em experimentos repetitivos.

Como o objetivo da proposta é avaliar o nó escolhido como MPR, foi necessário criar uma rede com mais de três nós, pois com dois a interação é direta, sem a necessidade de um nó MPR, enquanto que a partir de três nós já é possível obter o trabalho do nó MPR (Clausen, 2003).

O tempo para acumular dados de teste foi escolhido após repetitivas observações dos testes preliminares e determinação experimental de valores para obter informações necessárias para avaliar a rede de forma apresentável e compreensível para seres humanos.

Com a estrutura toda pronta e os parâmetros configurados, o próximo passo para a obtenção de resultados deste experimento foi colocar o OLSRD para rodar em todas as máquinas. Quando o OLSRD é iniciado o *plugin* faz a coleta das métricas e a atualização dos valores na TRUST-MIB, tornando então possível utilizar comandos SNMP para a obtenção de informações da MIB.

Com as informações passadas pela MIB, aplica-se a equação de cálculo de confiança e apresenta-se a expectativa referente às próximas interações. Como a MIB é atualizada

permanentemente pelo *plugin* agente do OLSRD, sucessivos cálculos da confiança são produzidos, o que permite registrar a evolução da confiança durante a operação do protocolo.

4.5.3. Medições e Análise dos Resultados

Reitera- se que os experimentos realizados têm o objetivo de validar a conformidade da TRUST-MIB e a sua operacionalidade, por intermédio da apresentação dos resultados obtidos para a confiança, a partir do conjunto de processos em torno da TRUST-MIB, desde a coleta de dados operacionais da rede até os cálculos da confiança.

Os resultados apresentados nesta seção são baseados no ambiente especificado no item precedente. O ambiente foi todo configurado com objetos reais, especificamente utilizando carcaças desativadas de fornos de micro-ondas como objetos portadores dos notebooks, conforme fotos mostradas à Figura 4.10.

Figura 4-10 Equipamentos usados no ambiente experimental

O controle do nível de sinal pela abertura das portas dos microondas em ângulos pré-definidos (0 , 15 , 30 , 60 e 90) permitiu criar condições diferenciadas de perdas nos enlaces da rede *ad hoc*. Tais perdas, por sua vez, provocaram variações nas perdas de pacotes TC na camada de rede operada pelo *deamon* OLSRD que foi produzido com o *plugin* da TRUST-MIB e colocado em operação nos notebooks.

Assim, o agente implantado no citado *plugin* pode preencher a TRUST-MIB em cada notebook e os valores acumulados nas MIB puderam ser coletados em intervalos regulares por intermédio do protocolo de gerência de rede. Para facilitar a compreensão dos valores por humanos, os intervalos regulares foram fixados em 2 minutos, o que permite também capturar os detalhes da operação do protocolo OLSR que regularmente envia mensagens de atualização da vizinhança e do roteamento.

O foco principal do experimento foi avaliar o Nó 03 que foi o escolhido como o nó MPR. O nó 04 ficou fora da carcaça de um micro-ondas, pois serviu como sistema de gerência limitando-se a coletar via protocolo SNMP os dados da MIB que permitiram avaliar o comportamento do MPR.

Para avaliar o MPR, foram definidos cinco ângulos do posicionamento da porta do micro-ondas do Nó 03, desde a posição da porta fechada (0), passando pelos ângulos de quinze (15), trinta (30), sessenta (60) e por fim noventa graus (90). Tais ângulos foram escolhidos de forma empírica, a partir de observações experimentais de que o nível de interferências no sinal é muito sensível a pequenos movimentos da porta quando esta se encontra perto da posição fechada (0°, 15° e 30°), enquanto tais interferências são menos sensíveis a mudanças de posição da porta quando esta se encontra mais aberta (60° e 90°). Vale notar que, definidas tais posições, as exaustivas repetições dos experimentos mostram valores homogêneos quando se compara um ciclo de medições com os demais.

A Figura 4-11 mostra uma tela de *log* do *deamon* OLSRD em funcionamento. Nela se pode observar campos com os nomes *Links, Neighbors, Two-Hop Neighbors, Topology*, que são campos padrão da implementação do protocolo OLSR, cujas definições se encontram em (Clausen, 2003). Já os campos Mensagens Enviadas e Mensagens Refletidas, foram implementados como proposta desta dissertação. As Figuras dos Apêndices C, D, E e F mostram as telas de log correspondentes aos experimentos realizados. Vale notar que no canto direito no alto das telas é apresentada a TRUST-MIB em funcionamento. No caso de

telas onde não houve mensagens enviadas e refletidas, a MIB mostra apenas uma mensagem do sistema de gerência.

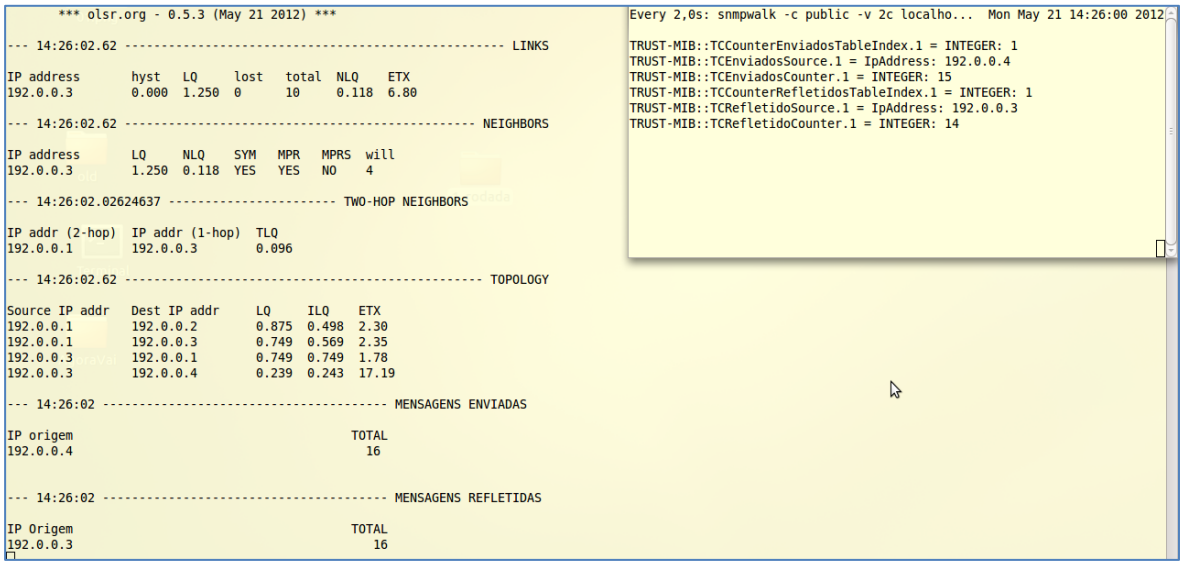


Figura 4-11 Exemplo de tela de log da operação do deamon OLSRD

Foram feitos exaustivos testes repetitivos que mostraram uma grande homogeneidade de resultados. Por essa razão, são reunidos aqui apenas quatro testes, sendo que cada teste consistiu de dois ciclos em que se posicionou a porta da carcaça do Nó 03 de 0° a 15°, daí a 30°, daí a 60° e então até 90° e depois nos mesmos ângulos na ordem inversa, de 90° até 0°, mantendo a porta em cada posição por um período de 2 minutos. As tabelas 4-9, 4-10, 4-11 e 4-12 apresentam os resultados dos testes. Em tais tabelas, a primeira coluna contém o índice das amostras de amostras, a segunda o ângulo de abertura da porta (ou seja, o nível de interferência sobre o sinal) durante o período de medição, a terceira e a quarta colunas mostram a quantidade de mensagens TC enviadas e refletidas respectivamente. As colunas **Δ**TC e **Δ**TCR apresentam a subtração dos valores de TC e TCR do período atual com o período anterior (por exemplo, na Tabela 4-9 o valor **Δ**TC do período 60 é 24, pois o valor de 60 é 64 e de 30 é 40, 64-40=24), visto que a MIB armazena os valores TC e TCR na forma de contadores monotonicamente crescentes, ou seja, contadores cumulativos da grandeza.

Os gráficos 4-12, 4-13, 4-14 e 4-15 mostram as curvas de quantidade de mensagens TC enviadas (TC) e mensagens TC refletidas (TCr) de cada teste. É possível observar a variação das duas grandezas de acordo com cada ângulo de posicionamento da porta do microondas, ou seja, sempre que a porta é fechada a quantidade de mensagens refletidas

cai, pois o nó 03 diminui o seu alcance, perdendo eventualmente o conhecimento dos vizinhos e deixando de rotear mensagens. Vale notar que nos casos extremos em que a porta é fechada, provocando perda de enlace entre os vizinhos, não apenas o MPR para de rotear as mensagens TC, mas também o Nó de origem, ao perceber (com algum retardo) a perda do enlace, para de enviar as próprias mensagens TC, situação que em termos de medições se reflete na redução do número de mensagens TC enviadas no intervalo considerado, mas sem zerar a quantidade em questão. Tal efeito retroativo sobre o envio das mensagens do nó de origem seria evitado caso tivesse sido implementado um defeito operacional no próprio software OLSRD do MPR, ao invés de uma interferência sobre as transmissões do OLSR com o fechamento da porta do forno de micro-ondas. Entretanto, modificar o OLSRD nesse sentido estava fora do escopo da presente dissertação , ficando para possíveis trabalhos futuros, mas sem invalidar os testes com a TRUST-MIB aqui proposta.

A Tabela 4-13 apresenta a média das quantidades de mensagens enviadas e refletidas dos quatro testes. O gráfico correspondente à quantidades médias pode ser observado na Figura 4-16. Como esperado, tal gráfico atenua flutuações eventuais ocorrentes em cada ciclo dos quatro testes. É interessante notar acerca de tais flutuações nas medições:

- As flutuações se devem em parte a atrasos de processamento na atualização da MIB e na natural ausência de sincronismo entre os diferentes nodos especificamente no que se refere ao processamento do protocolo OLSR. Tal constatação foi feita de forma experimental observando ao mesmo tempo o log do OLSRD em determinado instante e o valor escrito efetivamente na MIB naquele instante. Por razão de projeto do agente de gerência, a atualização da MIB é forçosamente atrasada com relação ao fenômeno real e, além disso, a coleta dos dados da MIB por um sistema de gerência utilizando o protocolo SNMP também faz com que a informação apresentada na estação de gerência seja atrasada com relação à atualização da MIB. Tais atrasos são característicos da gerência de redes segundo a arquitetura SNMP;
- Por outro lado, é provável que haja flutuações nas medições decorrentes de serem feitos movimentos da porta do microondas de forma manual. Não foi feito estudo experimental desse aspecto da medição. De todo modo, a ocorrência de tal imprecisão não compromete a validação da TRUST-MIB, mas pelo contrário, mostra que o processo como um todo está funcional.

Para finalizar a validação da TRUST-MIB, cabe analisar o cálculo da confiança, que segundo a definição adotada no escopo desta monografia se expressa pela esperança de que no futuro o MPR terá um comportamento que pode ser previsto a partir das frequências de repasses positivos ($\boldsymbol{x = TCR}$) e de repasses negativos ($\boldsymbol{\overline{x} = TC - TCR)}$ feitos no passado, (em conformidade com a distribuição Beta). Os valores obtidos a partir dos experimentos realizados encontram-se na Tabela 4-14, com cálculos realizados conforme especificado no item 4-3 e com dados da Tabela 4-13, de médias dos valores dos testes.

Vale notar que o comportamento da variável confiança encontra-se em conformidade com o comportamento previsto por método analítico na seção 4.5.1, em particular considerando que a curva de evolução da confiança, da Figura 4-17, traz os seguintes resultados:

- Mostra corretamente a tendência de uma confiança relativamente alta quando a quantidade de TCR é menor, mas tem valor próximo à da quantidade de TC, o que constitui uma situação de funcionamento normal da rede ad hoc com alguma perda de pacotes que não impede o roteamento;
- Ocorre tendência de queda abrupta que resulta subsequentemente em um valor relativamente baixo da confiança quando TCR << TC, ou seja, quando o MPR se torna incapaz de rotear corretamente;
- Ocorre redenção do MPR, ou seja, os valores da confiança apresentam tendência crescente que resulta subsequentemente em um valor relativamente alto para a grandeza, a partir do momento em que o MPR retoma o repasse correto das mensagens TC.

Conclui-se assim, pela abordagem experimental, pela validação da TRUST-MIB, no contexto do processo completo que vai da coleta dos dados operacionais do OLSRD e preenchimento da MIB, seguido da monitoração da MIB via protocolo de gerência de rede e cálculo da confiança para apresentação ao usuário, conforme indica a Figura 4-4. Reitera-se que os valores relativos à confiança são o resultado final de todo o processo e as características observadas em tais valores constituem elementos validadores da proposta desta dissertação.

Tabela 4-9 Medições com a TRUST-MIB e OLSRD - Teste 01

	Período	TC	TCr	ΔTC	ΔTCr
1	0°	0	0	0	0
2	15°	15	15	15	15
3	30°	40	37	25	22
4	60°	64	60	24	23
5	90°	87	80	23	20
6	60°	108	102	21	22
7	30°	130	126	22	24
8	15°	153	140	23	14
9	0	170	140	17	0
10	15°	193	158	23	18
11	30°	218	178	25	20
12	60°	241	200	23	22
13	90°	265	221	24	21
14	60°	289	241	24	20
15	30°	311	261	22	20
16	15°	335	280	24	19
17	0°	339	281	4	1

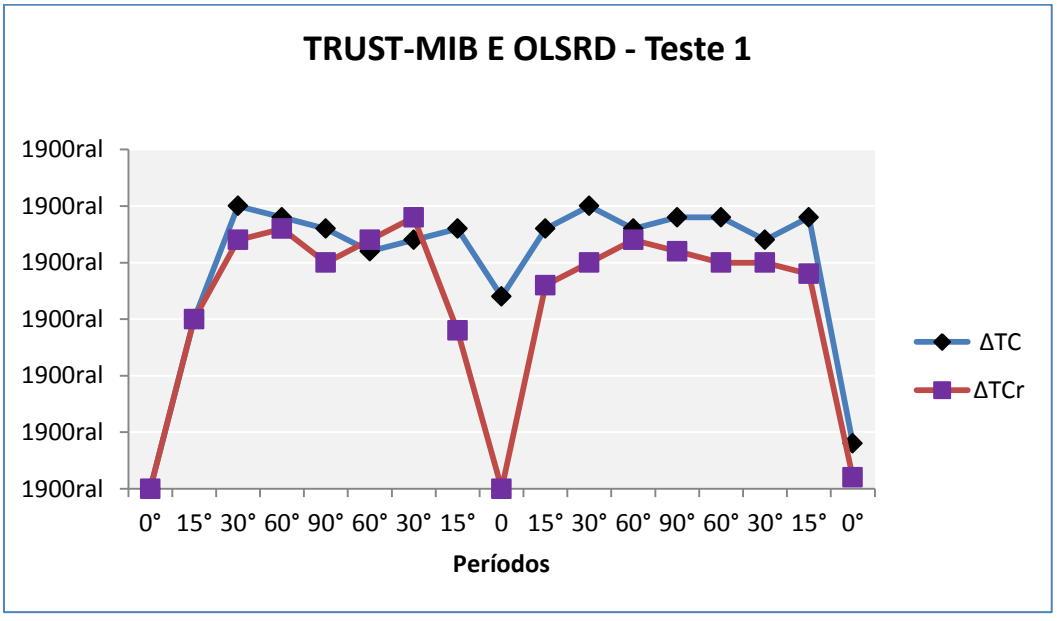


Figura 4-12 Medições com a TRUST-MIB e o OLSRD - Teste 01

Tabela 4-10 Medições com a TRUST-MIB e OLSRD - Teste 02

	Período	TC	TCr	Δ TC	ΔTCr
1	0°	0	0	0	0
2	15°	21	16	21	16
3	30°	44	38	23	22
4	60°	70	56	26	18
5	90°	94	76	24	20
6	60°	115	92	21	16
7	30°	138	107	23	15
8	15°	160	123	22	16
9	0	168	124	8	1
10	15°	202	149	34	25
11	30°	223	168	21	19
12	60°	248	188	25	20
13	90°	269	205	21	17
14	60°	293	226	24	21
15	30°	317	246	24	20
16	15°	341	264	24	18
17	0°	346	264	5	0

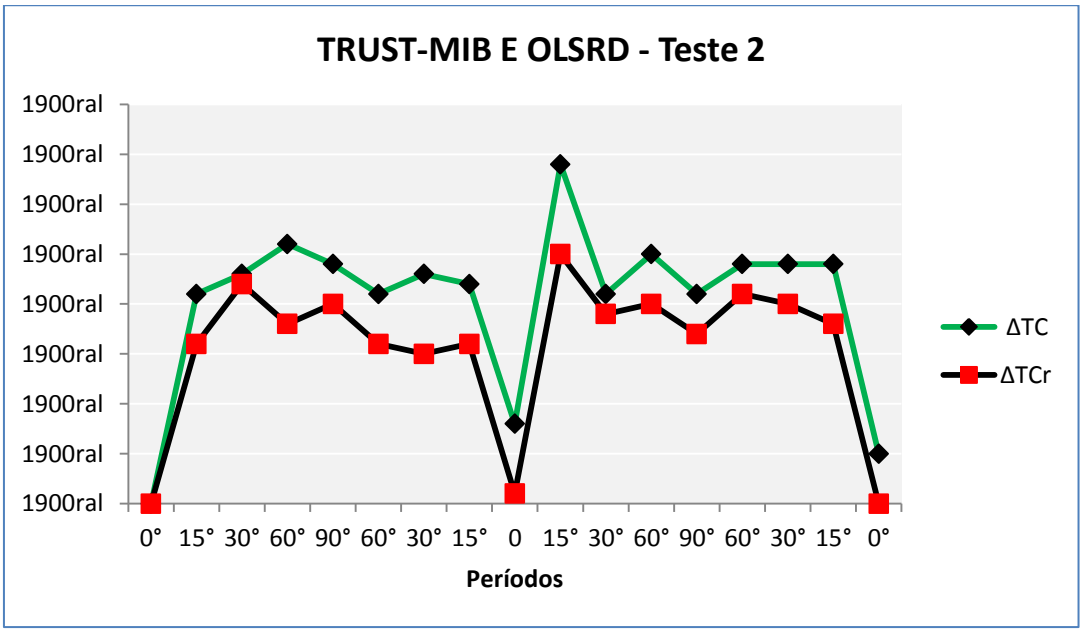


Figura 4-13 Medições com a TRUST-MIB e o OLSRD - Teste 02

Tabela 4-11 Medições com a TRUST-MIB e OLSRD - Teste 03

	Período	TC	TCr	Δ TC	ΔTCr
1	0°	0	0	0	0
2	15°	21	18	21	18
3	30°	45	35	24	17
4	60°	69	54	24	19
5	90°	92	75	23	21
6	60°	110	92	18	17
7	30°	132	109	22	17
8	15°	155	124	23	15
9	0	164	125	9	1
10	15°	186	141	22	16
11	30°	211	163	25	22
12	60°	235	185	24	22
13	90°	259	206	24	21
14	60°	284	227	25	21
15	30°	307	248	23	21
16	15°	330	266	23	18
17	0°	339	268	9	2

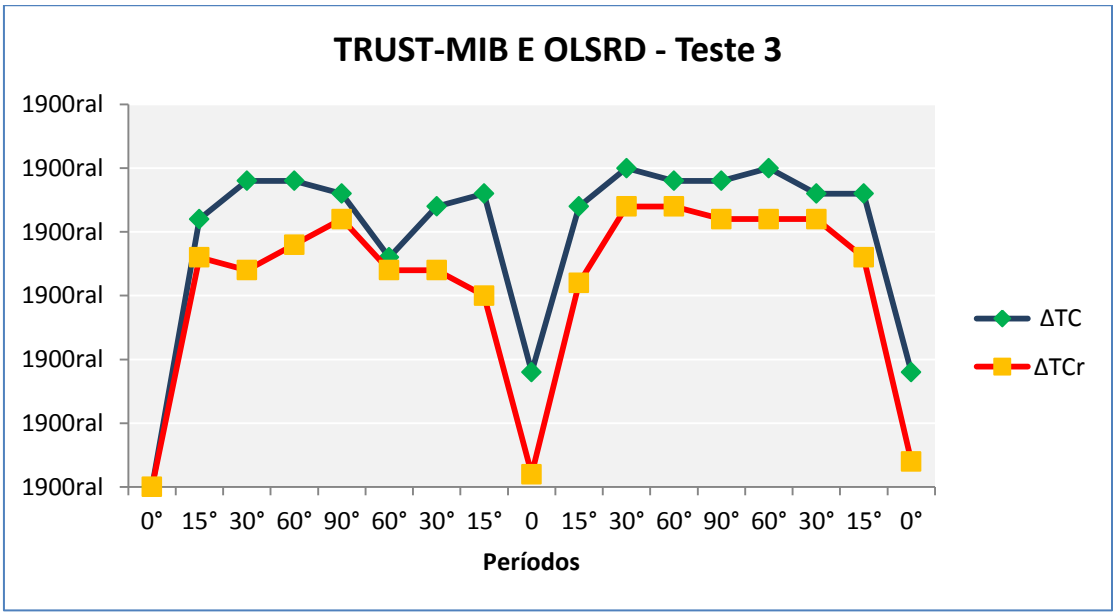


Figura 4-14 Medições com a TRUST-MIB e o OLSRD - Teste 03

Tabela 4-12 Medições com a TRUST-MIB e OLSRD - Teste 04

	Período	TC	TCr	Δ TC	ΔTCr
1	0°	0	0	0	0
2	15°	16	13	16	13
3	30°	42	34	26	21
4	60°	66	54	24	20
5	90°	88	75	22	21
6	60°	109	93	21	18
7	30°	133	114	24	21
8	15°	156	131	23	17
9	0	161	132	5	1
10	15°	183	149	22	17
11	30°	204	170	21	21
12	60°	223	189	19	19
13	90°	246	203	23	14
14	60°	270	225	24	22
15	30°	294	242	24	17
16	15°	316	260	22	18
17	0°	320	260	4	0

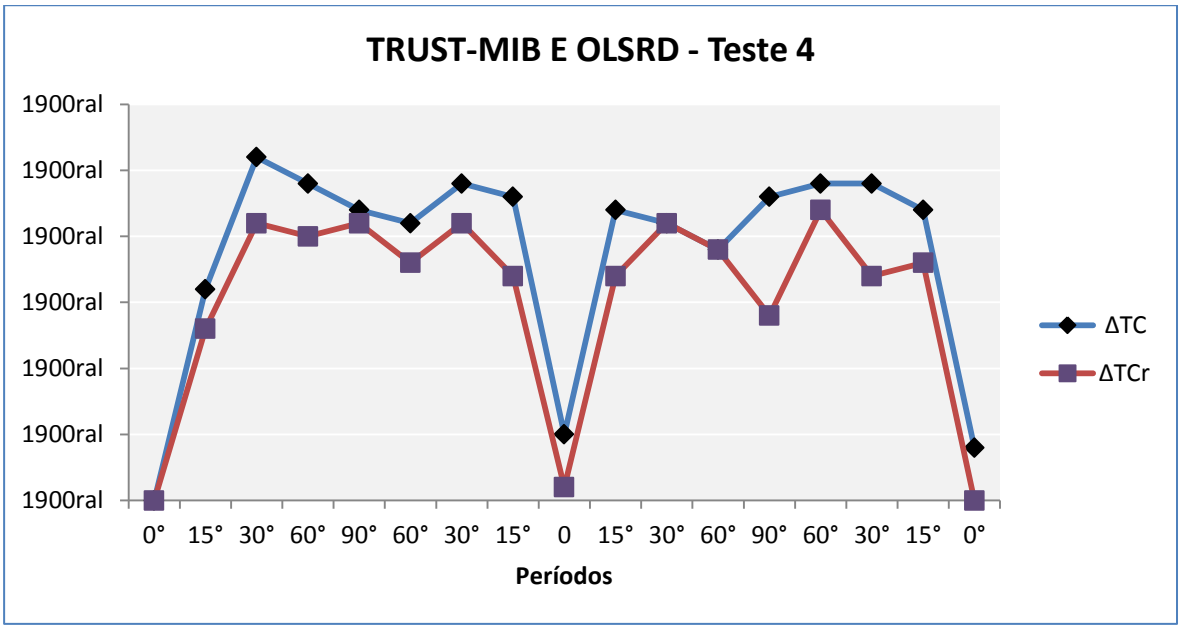


Figura 4-15 Medições com a da TRUST-MIB e o OLSRD - Teste 04

Tabela 4-13 Média das Medições com a TRUST-MIB e OLSRD

	Período	**ΔTC**	**ΔTCr**	**ΔTC**	**ΔTCr**	**ΔTC**	**ΔTCr**	**ΔTC**	**ΔTCr**	**Média ΔTC**	**Média ΔTCr**
1	0°	0	0	0	0	0	0	0	0	0	0
2	15°	15	15	21	16	21	18	16	13	18	16
3	30°	25	22	23	22	24	17	26	21	25	21
4	60°	24	23	26	18	24	19	24	20	25	20
5	90°	23	20	24	20	23	21	22	21	23	21
6	60°	21	22	21	16	18	17	21	18	20	18
7	30°	22	24	23	15	22	17	24	21	23	19
8	15°	23	14	22	16	23	15	23	17	23	16
9	0	17	0	8	1	9	1	5	1	10	1
10	15°	23	18	34	25	22	16	22	17	25	19
11	30°	25	20	21	19	25	22	21	21	23	21
12	60°	23	22	25	20	24	22	19	19	23	21
13	90°	24	21	21	17	24	21	23	14	23	18
14	60°	24	20	24	21	25	21	24	22	24	21
15	30°	22	20	24	20	23	21	24	17	23	20
16	15°	24	19	24	18	23	18	22	18	23	18
17	0°	4	1	5	0	9	2	4	0	6	1

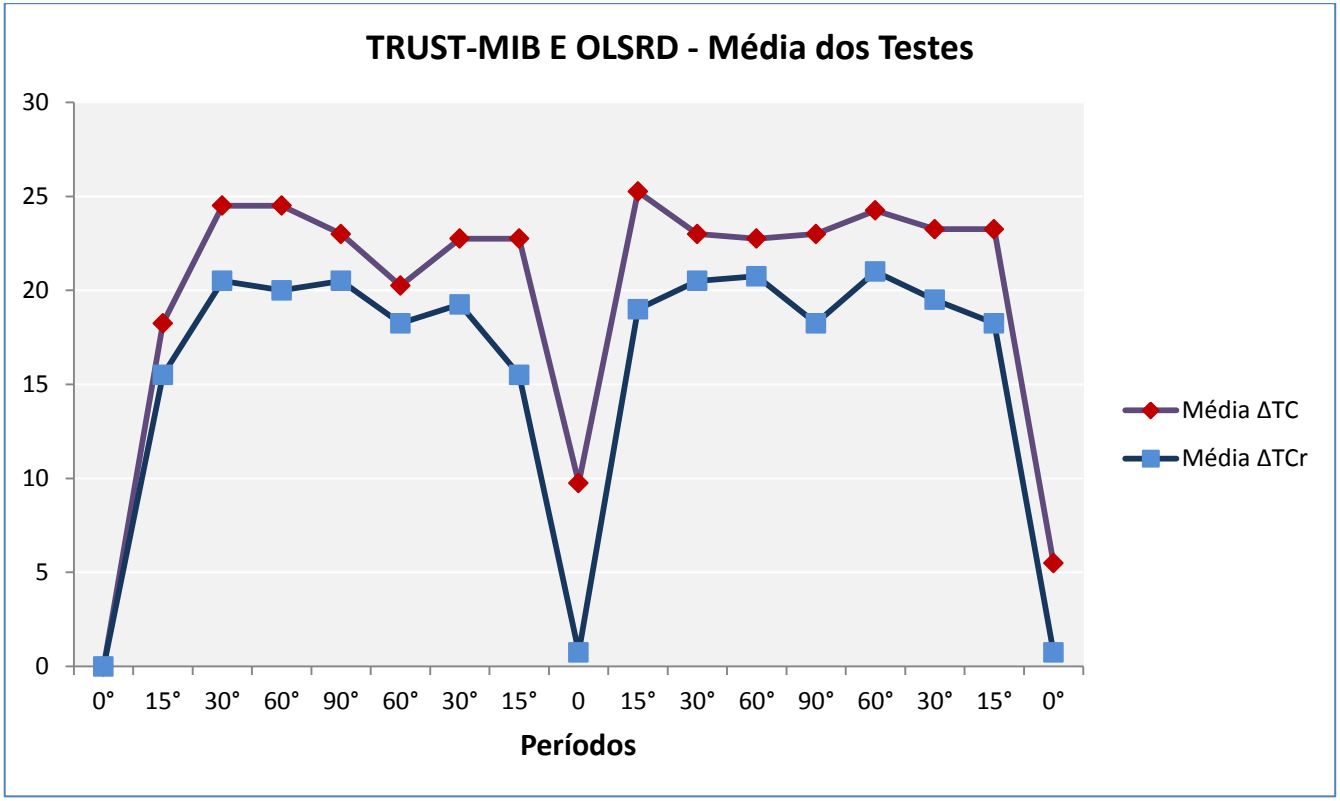


Figura 4-16 Média das Medições com a TRUST-MIB e o OLSRD

Tabela 4-14 Cálculo da Confiança (Esperança) a partir das Medições com a TRUST-MIB e OLSRD

	Período	**Média ΔTC**	**Média ΔTCr**	**x**	$\bar{x}$	**Alfa**	**Beta**	**Alfa+Beta**	**Esperança**
1	0°	0	0	0	0	1	1	2	0,50
2	15°	18	16	16	3	17	4	20	0,81
3	30°	25	21	21	4	22	5	27	0,81
4	60°	25	20	20	5	21	6	27	0,79
5	90°	23	21	21	3	22	4	25	0,86
6	60°	20	18	18	2	19	3	22	0,87
7	30°	23	19	19	4	20	5	25	0,82
8	15°	23	16	16	7	17	8	25	0,67
9	0	10	1	1	9	2	10	12	0,15
10	15°	25	19	19	6	20	7	27	0,73
11	30°	23	21	21	3	22	4	25	0,86
12	60°	23	21	21	2	22	3	25	0,88
13	90°	23	18	18	5	19	6	25	0,77
14	60°	24	21	21	3	22	4	26	0,84
15	30°	23	20	20	4	21	5	25	0,81
16	15°	23	18	18	5	19	6	25	0,76
17	0°	6	1	1	5	2	6	8	0,23

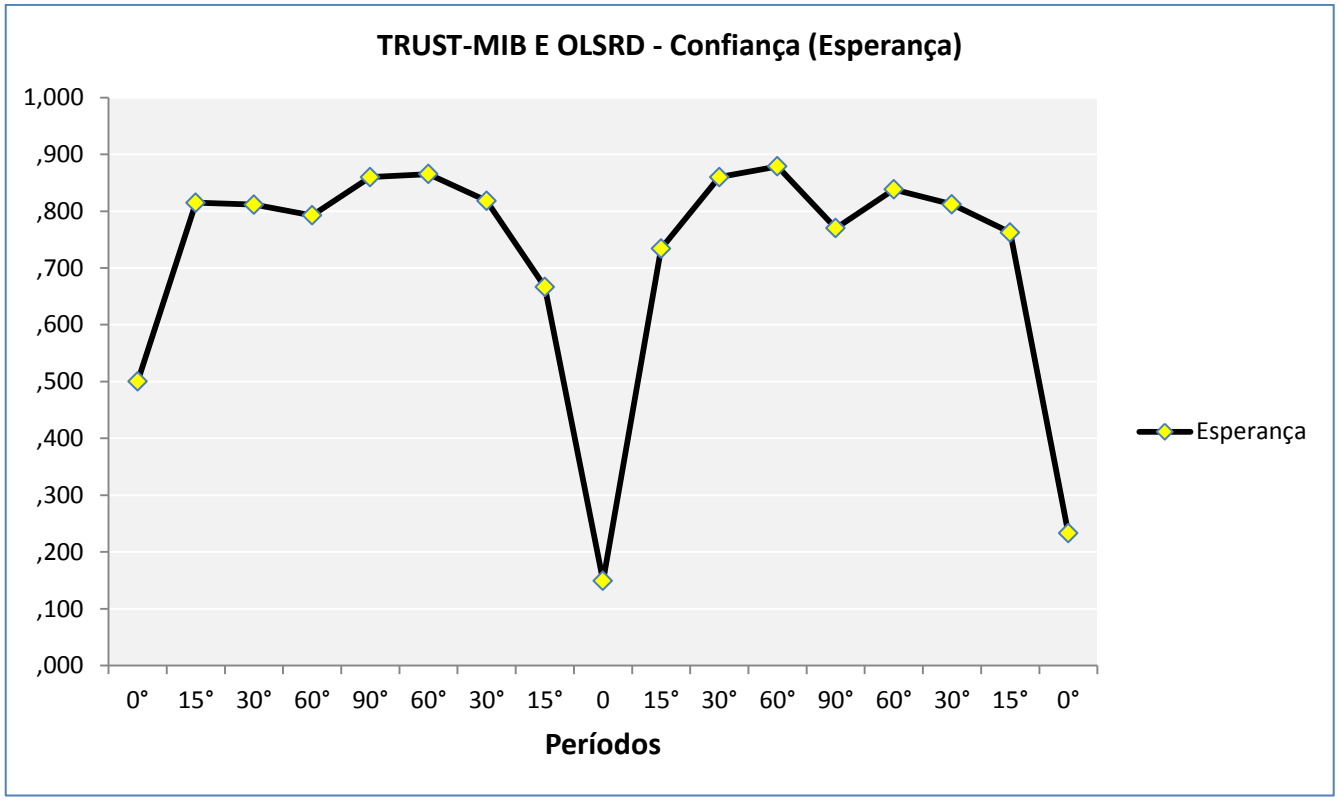


Figura 4-17 Evolução da Confiança (Esperança) calculada a partir das Medições com a TRUST-MIB e OLSRD

5. CONCLUSÃO

A principal motivação para a realização deste trabalho foi a possibilidade de monitorar uma rede *ad hoc* e capturar dados operacionais para armazenar em uma MIB contendo objetos que possam ser correlacionados a uma definição de confiança particular ao comportamento que se pode esperar dos roteadores nessas redes.

O uso dessa definição da confiança, bem como o seu cálculo em termos da esperança probabilística de bom ou mau comportamento dos roteadores, parecem de interesse para ambientes de rede *ad hoc* que constitui um critério a mais da seleção de rota, permitindo evitar nós defeituosos ou mesmo maliciosos, contribuindo assim para a obtenção de melhor desempenho nas entregas dos pacotes e na operação da rede.

Considerando tais interesses, foi desenvolvido o trabalho de mestrado de modo a verificar se a proposta de uma MIB de confiança (TRUST-MIB) e sua operacionalização poderiam efetivamente trazer os benefícios esperados.

Foi então realizado um estudo de trabalhos acerca de parâmetros operacionais que podem ser monitorados em uma rede *ad hoc* e que poderiam caracterizar um comportamento confiável dos roteadores. Tal estudo resultou em uma primeira contribuição desta dissertação na forma de uma síntese das métricas da confiança propostas em artigos e livros relacionados ao tema de redes *ad hoc*. Para as métricas escolhidas, propôs-se utilizar o cálculo de esperança da distribuição Beta como representativo da confiança no comportamento do roteador *ad hoc*.

O estudo desses parâmetros ou métricas permitiu desenvolver a segunda contribuição deste trabalho, com a criação da MIB de confiança, com as métricas coletadas, usando os padrões de definição e escrita da SMI e ASN.1, em conformidade com a arquitetura de gerência SNMP.

Para validar tal MIB foram produzidos resultados analíticos acerca do comportamento esperado das métricas selecionadas para a MIB e foi desenvolvido um ambiente experimental de validação para o processo completo de coleta das métricas, atualização da MIB, monitoração da MIB via SNMP e cálculo da confiança no sistema de gerência.

Para tanto, três outras contribuições desta dissertação consistiram de:

- Desenvolvimento de um agente de gerenciamento, integrado ao *deamon* OLSRD do protocolo de rede *ad hoc* OLSR e capaz de coletar as métricas de confiança de uma rede experimental controlada, preenchendo a MIB em cada nodo;
- Definição de um ambiente experimental controlado, com uma rede *ad hoc* operando pelo *deamon* OLSRD, este integrado com o agente de gerenciamento capaz de atualizar a MIB proposta. Operacionalização dos nodos em carcaças de fornos de micro-ondas desativados que foram utilizados como gaiolas de Faraday para variação controlada das interferências de modo a permitir a validação da pertinência da operação e dos valores da MIB como representativos do comportamento dos roteadores *ad hoc*;
- Coleta de maneira sistemática e repetitiva dos dados da MIB e apresentação da análise e dos resultados em termos da confiança avaliada pelos nodos acerca de seus vizinhos roteadores, tanto na forma de tabelas quanto de curvas de evolução da confiança.

Tais desenvolvimentos, bem como a abordagem experimental, levaram à validação da TRUST-MIB, no contexto do processo completo que vai da coleta dos dados operacionais do OLSRD e preenchimento da MIB, seguido da monitoração da MIB via protocolo de gerência de rede e cálculo da confiança para apresentação ao usuário.

Desse modo, espera-se que esta dissertação contribua para uma solidificação do gerenciamento de redes *ad hoc*, com utilização da noção de confiança proposta e sua implementação por intermédio da TRUST-MIB.

5.1. TRABALHOS FUTUROS

Como proposta de trabalhos futuros, podem ser consideradas as seguintes evoluções:

- Expandir os objetos da MIB com mais características que identifiquem o comportamento do nó. Por exemplo, o número de sequência da mensagem.
- Simulação ou implementação de possíveis ataques, como por exemplo o ataque em que o roteador gera mensagens TC em nome de um vizinho, sem que este tenha efetivamente enviado tais mensagens.

- Implementação de falhas no próprio software OLSRD de modo a permitir medições em função dessas falhas e não apenas pela criação de uma interferência sobre as transmissões do OLSR com o fechamento da porta do forno de micro-ondas.
- Análise da complexidade do armazenamento e visualização das métricas de confiança quando da existência de múltiplos roteadores disponíveis para um determinado nó.

REFERÊNCIAS BIBLIOGRÁFICAS

Adnane, A., de Sousa, R. T., Jr., Bidan, C. and Mé, L. (2007). Analysis of the implicit trust within the OLSR protocol,.in IFIP international Federation for Information Processing, Volume 238, Trust Management, eds. Etalle, S., Marsh, S., (Boston: Springer), pp. 75–90.

Adnane, A., De Sousa Jr., R. T., Bidan, C., & Mé, L. (2008). Autonomic Trust Reasoning Enables Misbehavior Detection in OLSR. In Proceedings of the 23rd Annual ACM Symposium on Applied Computing (ACM SAC 2008): Trust, Recommendations, Evidence and other Collaboration Know-how (TRECK track), Fortaleza, Ceará, Brazil: ACM.

Albuquerque, R. de O. (2008). Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos. Tese de Doutorado. Departamento de Engenharia Elétrica - Universidade de Brasília.

Areal, J. L. (2008). Proposta de um Modelo de Confiança para o Protocolo OLSR. Dissertação de Mestrado. Departamento de Engenharia Elétrica - Universidade de Brasília.

Areal, J. L., Puttini, R. S., & De Sousa Jr., R. T. (2008). A New Trust-Based Extension to the HELLO Message Improves the Choice of Routes in OLSR Networks. *In Proceedings of the 7th International Information and Telecommunication Technologies Symposium I2TS'2008*. Foz do Iguaçu, Brazil.

Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized Trust Management. *Proc. IEEE Symposium on Security and Privacy* (pp. 164 - 173).

Carbone, M., Nielsen, M., & Sassone, V. (2003). A formal model for trust in dynamic networks. *First International Conference on Software Engineering and Formal Methods SEFM`03*. Society Press, pp. 54-63.

Case, J., Fedor, M., Schoffstall, M., & Davin, J. (1990). IETF RFC 1157. A Simple Network Management Protocol (SNMP).

Case, J., McCloghrie, K., Rose, M., & Waldbusser, S. (1996). IETF RFC 1902. Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2).

Cho, J. H.; *et al*. (2010). A Survey on Trust Management for Mobile *ad hoc* Networks. *IEEE Communications Surveys & Tutorials* (pp. 1-22). Vol. 12.

Clausen, T., Jacquet, P. (2003). IETF RFC 3626. Optimized Link State Routing Protocol (OLSR).

Comer, D. E. (1998). Interligação em Rede com TCP/IP. Princípios, protocolos e arquitetura. Tradução da 3º edição. Vol. I. Editora Campus.

Corson, S., & Macker, J. (1999). IETF RFC 2501. Mobile *ad hoc* Networking (MANET): Routing protocol performance issues and evaluation consideration.

Davin, J., Case, J., Fedor, M., & Schoffstall, M. (1987). IETF RFC 1028. A Simple Gateway Monitoring Protocol.

Daniele, M., et al. (2000). IETF RFC 2741. Agent Extensibility (AgentX) Protocol Version

De Sousa, R. T.; Adnane, A. H.; Bidan, C.; Me, L.; (2009). On the Vulnerabilities and Protections of the OLSR ad hoc Routing Protocol from the point of view of Trust. *Latin America Transactions, IEEE (Revista IEEE America Latina). V*ol.7, no.5, pp.594-602.

De Sousa Jr, R. T., & Puttini, R. S. (2010). Trust Management in *ad hoc* Networks. *Trust Modeling and Management in Digital Enviroments: From Social Concept to System Development* (pp 224-249).Nokia Research Center. Finlândia.

Dinh, T. T. A., et al. (2009). A trusted infrastructure for P2P-bases marketplaces. *Peer-to-Peer Computing, P2P `09. IEEE Ninth International Conference*. Seatle.

e-Física. Ensino de Física On-Line. Endereço: <http://efisica.if.usp.br/eletricidade/basico/campo/blindagens_eletrostaticas-gaiola_faraday_/>. Acesso em: 12/05/2012

Fernandes, B. V. (2003). Protocolos de Roteamento em Redes *ad hoc*. Dissertação de Mestrado Profissional. Universidade Estadual de Campinas.

Fernandes, N. C., Moreira, M. D. D., Velloso, P. B., Costa, L. H. M. K., & Duarte, O. C. M. B. (2006). Ataques e Mecanismos de Segurança em Redes *ad hoc*. *Minicurso do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSeg* (pp. 49-102). Santos, Brasil.

Gambetta, D. (1988). Can We Trust Trust? *Trust: Making and Breaking Cooperative Relations* (pp. 213-237). Department of Sociology - University of Oxford. Cap. 13.

Gourdon, X., & Sebah, P. (2002). Introduction to the Gamma Function. Endereço: <http://numbers.computation.free.fr/Constants/Miscellaneous/gammaFunction.html>. Acesso em: 12/09/2011.

ISO8824. (1987). Information processing systems Open Systems Interconnection, Specification of Abstract Syntax Notation One (ASN.1). *International Organization for Standardization*. Endereço: <http://www.iso.org>. Acesso em: 13/05/2011.

Johnson, D., Hu, Y., Maltz, D. (2007). IETF RFC 4728. The Dynamic Source Routing Protocol (DSR) for Mobile *ad hoc* Networks for IPv4.

Josang, A. (1996). The right type of trust for distributed systems. *Proceedings of the workshop on New Security Paradigms NSPW* (pp 119-131). ACM - Nova York.

Josang, A., & Ismail, R. (2002). The Beta Reputation System. *In Proceedings of the 15th Bled Electronic Commerce Conference*.

Josang, A., & LoPresti, S. (2004). Analyzing the Relationship between Riskand Trust. *Proc. 2nd Int'l Conf. Trust Management LNCS*(pp. 135-145).Springer.

Kannhavong, B., *et al*. (2006). Analysis of the Node Isolation Attack against OLSR-Based Mobile *ad hoc* Network.*7th Intenational Symposium, Computers Networks* (pp. 30-35).

Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A. (2007). A survey of routing attacks in mobile *ad hoc* networks. *Wireless Communications, IEEE* (pp.85-91). Vol.14.

Kurose, J. F; & Ross, K. W. (2006). Redes de Computadores e a Internet: Uma abordagem top-down. Pearson Addison Wesley.3 ed. - São Paulo.

Li, H., & Singhal, M. (2007). Trust Management in Distributed Systems. *Computers*(pp. 45-53). Vol. 40.

Lourenço, E., et al. (2000). AgentX: Uma Ferramenta para Extensão Dinâmica de Agentes SNMP. University of Coimbra, Polo II, Portugal.

Marsh, S., (1994). Formalising Trust as a Computational Concept. Tese de PHD, Department of Mathematics and Computer Science, University of Sterling.

McCloghrie, K., & Perkins, D., Schoenwaelder, J. (1999). IETF RFC 2578. Structure of Management Information Base Version 2.

McCloghrie, K., & Rose, M. (1991). IETF RFC 1213. Management Information Base for network management of TCP/IP-based Internets: MIB II.

McCloghrie, K., & Rose, M. (1988). IETF RFC 1066. Management Information Base for Network Management of TCP/IP-based Internets.

Meka, D. K, Vidrenda, M., & Upadhyaya, S. (2006). Trust Based Routing Decisions in Mobile Ad-hoc Networks. *In Proceedings of the Workshop on Secure Knowledge Management SKM.*

NET-SNMP. Endereço: <http://www.net-snmp.org/docs/README.agentx.html>. Acesso em: 27/05/2011.

Oliveira, D. T. (2002). Gerência de Redes de Computadores: Uma abordagem com o uso do SNMP. Centro Universitário do Triângulo - Unit. Uberlândia - MG.

Pacheco, V. M. (2007). Proposta e Implementação de uma MIB para o Protocolo OLSR. Dissertação de Mestrado. Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

Papalilo, E., Freisleben, B. (2008). Managing Behaviour Trust in Grid Computing Environments. *Journal of Information Assurance and Security 1* (pp. 27 a 37).

Perkins, C., Belding-Royer, E. & Das, S. (2003). IETF RFC 3561. *ad hoc* On-Demand Distance Vector (AODV).

Pinheiro, J. I. D., et al. (2009). Estatística Básica - A Arte de Trabalhar com Dados. Ed. Elsevier - Rio de Janeiro.

Pinheiro, J. M. dos S. (2002). Gerenciamento de Redes de Computadores - Versão 2.0. Endereço: <http://www.projetoderedes.com.br/index.php>. Acesso em: 14/04/2011.

Pirzada, A. A., & McDonald, C. (2004). Establishing Trust In Pure Ad-hoc Networks. *27th Australasian Computer Science Conference*. The University of Otago, Nova Zelândia. Vol. 26.

Presuhn, R. et al. (2002). IETF RFC 3416. Version 2 of the Protocol Operation for the Simple Network Management Protocol (SNMP).

Puttini, R. S. (2004). Um Modelo de Segurança para Redes Móveis ad hoc. Tese de Doutorado. Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

Rajaram, A. & Palaniswami, D. S. (2010). The Trust-Base MAC-Layer Security Protocol for Mobile *ad hoc* Networks. *IJCSE - International Journal on Computer Science and Engineering* (pp. 400-408). Vol. 02.

Rezende, P. A. D. (2004). O Uso de ASN. 1 para Especificação Formal de Protocolos. Endereço: <http://www.cic.unb.br/~pedro/c003/asn1_ufrgs.pdf>. Acesso em: 25/09/2010.

Rose, M., & McCloghrie, K. (1990). IETF RFC 1155. Structure and Identification of Management Information for TCP/IP-based Internets.

Rose, M., & McCloghrie, K. (1991). IETF RFC 1212. Concise MIB Definitions.

Rose, M., (1991). IETF RFC 1215. A Convention for Defining Traps for use with the SNMP.

Russi, J. M. (2005). Protótipo de um Agente SNMP para MIB MPLS-LSR e MIB MPLS-FTN. Dissertação de Mestrado. Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 178 p.

Saydam, T., & Magedanz, T.; (2006). From Networks and Network Management into Service and Service Management. *Journal of Networks and System Management* (pp. 345-348). Vol. 4.

Silva, R. S., (2004). Simple Network Management Protocol. Universidade Federal do Rio de Janeiro. Departamento de Engenharia Eletrônica.

Schmidt, K. J., & Mauro, D. R. (2001). SNMP Essencial. Editora Campus.

Solhaug, B., Elgesem, D., & Stolen, K. (2007). Why Trust is not proportional to Risk? *Proc. 2nd Int'l Conf. on Availability, Reliability, and Security* (pp. 11-18). Vienna, Austria.

Sztajnberg, A. (1996). Conceitos Básicos sobre os Protocolos SNMP e CMIP. Programa de Engenharia Elétrica - Universidade Federal do Rio de Janeiro.

Theodorakopoulos, G., & Baras, J. S. (2006). On Trust Models and Trust Evaluation Metrics for *ad hoc* Networks. *IEEE J. Sel. Areas Commun* (pp. 318-328). Vol. 24.

Tonessen, A. et al. (2004). OLSRD, an *ad hoc* Wireless Mesh Routing Deamon. Endereço: <http://www.olsr.org/?q=download>. Acesso em: 10/09/2011.

Velloso, P. B, *et al*. (2006). Análise de um modelo de confiança para redes móveis *ad hoc*. *24º Simpósio Brasileiro de Redes de Computadores*.

Walker, W. E., *et al*. (2003). Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-based Decision Support. *Integrated Assessment* (pp. 05-17). Vol. 4.

Yi, P., *et al*. (2005). A New Routing Attack in Mobile *ad hoc* Networks. *International. Journal of Information Technology* (pp. 83-94). Vol. 11.

Yunfang, F. (2007). Adaptive Trust Management in MANETs. *Proc. 2007 Int'l Conf. on Computational Intelligence and Security* (pp. 804-808). Harbin, China.

APÊNDICES

A - TRUST-MIB.txt

```
TRUST-MIB DEFINITIONS ::= BEGIN

IMPORTS
     MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
     IpAddress, Integer32, Gauge32, Counter 32, experimental,
     TimeTicks, snmpModules          FROM SNMPv2-SMI;


TRUST-MIB MODULE-IDENTITY
     LAST-UPDATED "201107122116Z"
     ORGANIZATION "UnB"
     CONTACT-INFO "beatriz.santana@redes.unb.br, desousa@unb.br"
     DESCRIPTION "A MIB module for the construction of confidence
applied to MIB - Beatriz Campos Santana,
     Rafael de Sousa." ::= {experimental 15 }

     br OBJECT IDENTIFIER ::= { experimental 15 }
     unb OBJECT IDENTIFIER ::= { br 1 }
     trust OBJECT IDENTIFIER ::= { unb 1 }


-- the trust group

trustmib OBJECT IDENTIFIER ::= { trust 1 }

     TCCounterEnviadosTable OBJECT-TYPE
     SYNTAX SEQUENCE OF TCCounterEnviadosTableEntry
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION "Tabela com as informacoes sobre o comportamento
do no TC enviado. As informacoessao o endereco IP do No e a
quantidade de mensagens enviadas."
     ::= { trustmib 1}

          TCCounterEnviadosTableEntry OBJECT-TYPE
          SYNTAX TCCounterEnviadosTableEntry
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION "Uma linha conceitual da
TCCounterEnviados."
          INDEX { TCCounterEnviadosTableIndex }
          ::= { TCCounterEnviadosTable 1}

          TCCounterEnviadosTableEntry ::= SEQUENCE   {
          TCCounterEnviadosTableIndex               Integer32,
          TCEnviadosSource                IpAddress,
          TCEnviadosCounter                     Integer32
          }

               TCCounterEnviadosTableIndex OBJECT-TYPE
               SYNTAX Integer32
               MAX-ACCESS read-only
               STATUS current
```

```
                DESCRIPTION "The integer index of the
TCCounterEnviadosTable."
                ::= { TCCounterEnviadosTableEntry 1 }

                TCEnviadosSource OBJECT-TYPE
                SYNTAX IpAddress
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION "Endereco IP do no que originou a
mensagem TC"
                ::= { TCCounterEnviadosTableEntry 2 }

                TCEnviadosCounter OBJECT-TYPE
                SYNTAX Integer32
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION "Contador de mensagens TC enviadas."
                ::= { TCCounterEnviadosTableEntry 3 }


     TCCounterRefletidosTable OBJECT-TYPE
     SYNTAX SEQUENCE OF TCCounterRefletidosTableEntry
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION "Tabela com informacoes sobre o comportamento do
no TC refletido. As informacoessao o endereco IP do No e a
quantidade de mensagens refletidas."
     ::= { trustmib 2}

          TCCounterRefletidosTableEntry OBJECT-TYPE
          SYNTAX TCCounterRefletidosTableEntry
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION "Uma linha conceitual do
trustCounterTable."
          INDEX { TCCounterRefletidosTableIndex }
          ::= { TCCounterRefletidosTable 1}

          TCCounterRefletidosTableEntry ::= SEQUENCE {
          TCCounterRefletidosTableIndex              Integer32,
          TCRefletidoSource                    IpAddress,
          TCRefletidoCounter                   Integer32
          }

                TCCounterRefletidosTableIndex OBJECT-TYPE
                SYNTAX Integer32
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION "The integer index of the
TCCounterRefletidosTable."
                ::= { TCCounterRefletidosTableEntry 1 }

                TCRefletidoSource OBJECT-TYPE
                SYNTAX IpAddress
                MAX-ACCESS read-only
                STATUS current
```

```
                DESCRIPTION "Endereco IP do no que enviou a
mensagem TC refletida"
                ::= { TCCounterRefletidosTableEntry 2 }

                TCRefletidoCounter OBJECT-TYPE
                SYNTAX Integer32
                MAX-ACCESS read-only
                STATUS current
                DESCRIPTION "Contador de mensagens TC refletidas."
                ::= { TCCounterRefletidosTableEntry 3 }


END
```

B - OLSRD.CONF

```
#
# olsr.org OLSR daemon config file
#
# Lines starting with a # are discarded
#
# This file was shipped with olsrd 0.X.X
#

# Debug level(0-9)
# If set to 0 the daemon runs in the background

DebugLevel 1

# IP version to use (4 or 6)

IpVersion  4

# Clear the screen each time the internal state changes

ClearScreen     yes

# HNA IPv4 routes
# syntax: netaddrnetmask
# Example Internet gateway:
# 0.0.0.0 0.0.0.0

Hna4
{
#   Internet gateway:
   0.0.0.0      0.0.0.0
#   more entries can be added:
#   192.168.1.0  255.255.255.0
}

# HNA IPv6 routes
# syntax: netaddr prefix
# Example Internet gateway:
Hna6
{
#   Internet gateway:
#   ::               0
#   more entries can be added:
#   fec0:2200:106:: 48
}


# Shouldolsrd keep on running even if there are
# no interfaces available? This is a good idea
# for a PCMCIA/USB hotswap environment.
# "yes" OR "no"

AllowNoInt yes

# TOS(type of service) value for
# the IP header of control traffic.
```

```
# If not set it will default to 16

TosValue   16

# The fixed willingness to use(0-7)
# If not set willingness will be calculated
# dynamically based on battery/power status
# if such information is available

Willingness     4

# Allow processes like the GUI front-end
# to connect to the daemon.

IpcConnect
{
     # Determines how many simultaneously
     # IPC connections that will be allowed
     # Setting this to 0 disables IPC

MaxConnections  0

     # By default only 127.0.0.1 is allowed
     # to connect. Here allowed hosts can
     # be added

     Host            127.0.0.1
     # Host          10.0.0.5

     # You can also specify entire net-ranges
     # that are allowed to connect. Multiple
     # entries are allowed

     #Net             192.168.1.0 255.255.255.0
}

# Whether to use hysteresis or not
# Hysteresis adds more robustness to the
# link sensing but delays neighbor registration.
# Used by default. 'yes' or 'no'

UseHysteresis   no

# Hysteresis parameters
# Do not alter these unless you know
# what you are doing!
# Set to auto by default. Allowed
# values are floating point values
# in the interval 0,1
# THR_LOW must always be lower than
# THR_HIGH.

HystScaling     0.50
HystThrHigh     0.80
HystThrLow 0.30
```

```
# Link quality level
# 0 = do not use link quality
# 1 = use link quality for MPR selection
# 2 = use link quality for MPR selection and routing
# Defaults to 0

LinkQualityLevel2

# Link quality window size
# Defaults to 10

LinkQualityWinSize   10

# Polling rate in seconds(float).
# Default value 0.05 sec

Pollrate   0.05

# Interval to poll network interfaces for configuration
# changes. Defaults to 2.5 seconds

NicChgsPollInt  3.0

# TC redundancy
# Specifies how much neighbor info should
# be sent in TC messages
# Possible values are:
# 0 - only send MPR selectors
# 1 - send MPR selectors and MPRs
# 2 - send all neighbors
#
# defaults to 0

TcRedundancy    1


#
# MPR coverage
# Specifies how many MPRs a node should
# try select to reach every 2 hop neighbor
#
# Can be set to any integer >0
#
# defaults to 1

#MprCoverage    1


# Olsrd plugins to load
# This must be the absolute path to the file
# or the loader will use the following scheme:
# - Try the paths in the LD_LIBRARY_PATH
#   environment variable.
# - The list of libraries cached in /etc/ld.so.cache
# - /lib, followed by /usr/lib
```

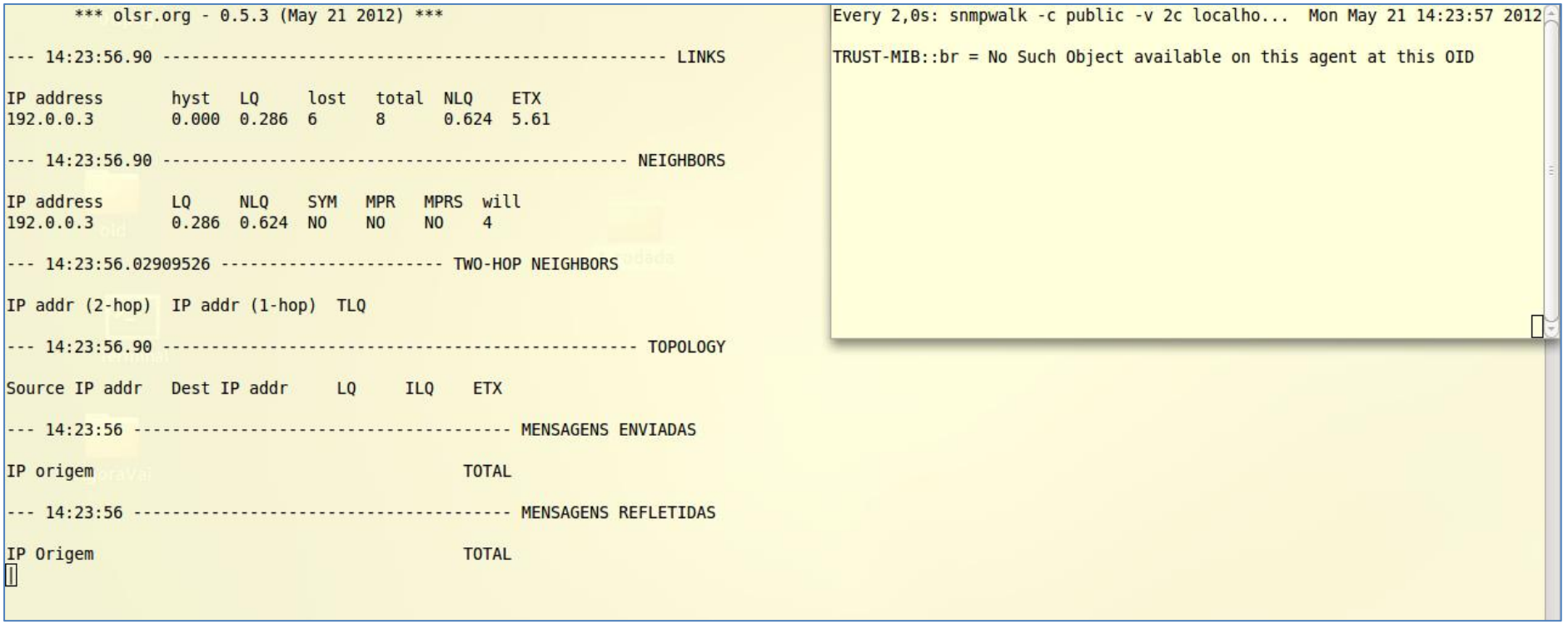
```
# Example plugin entry with parameters:

#LoadPlugin "olsrd_dyn_gw.so.0.3"
#{
    # Here parameters are set to be sent to the
    # plugin. Theese are on the form "key" "value".
    # Parameters ofcause, differs from plugin to plugin.
    # Consult the documentation of your plugin for details.

    # Example: dyn_gwparams

    # how often to check for Internet connectivity
    # defaults to 5 secs
  # PlParam     "Interval"   "40"

    # if one or more IPv4 addresses are given, do a ping on these
in
    # descending order to validate that there is not only an entry
in
# routing table, but also a real internet connection. If any of
    # these addresses could be pinged successfully, the test was
    # succesful, i.e. if the ping on the 1st address was
successful,the
    # 2nd won't be pinged
   #PlParam     "Ping"       "141.1.1.1"
   #PlParam     "Ping"       "194.25.2.129"
#}



# Interfaces and their rules
# Omitted options will be set to the
# default values. Multiple interfaces
# can be specified in the same block
# and multiple blocks can be set.

# !!CHANGE THE INTERFACE LABEL(s) TO MATCH YOUR INTERFACE(s)!!
# (eg. wlan0 or eth1):

Interface "wlan0"
{
    # Olsrdcanautodetect changes in NIC
    # configurations(IP address changes etc.).
    # This is Enabled by default and the interval
    # to poll for changes on is defined by
# NicChgsPollInt.
    # This polling can be disabled pr. NIC by setting
# AutoDetectChanges to no.

    # AutoDetectChanges           yes

    # IPv4 broadcast address to use. The
    # oneusefull example would be 255.255.255.255
    # If not defined the broadcastaddress
    # every card is configured with is used
```

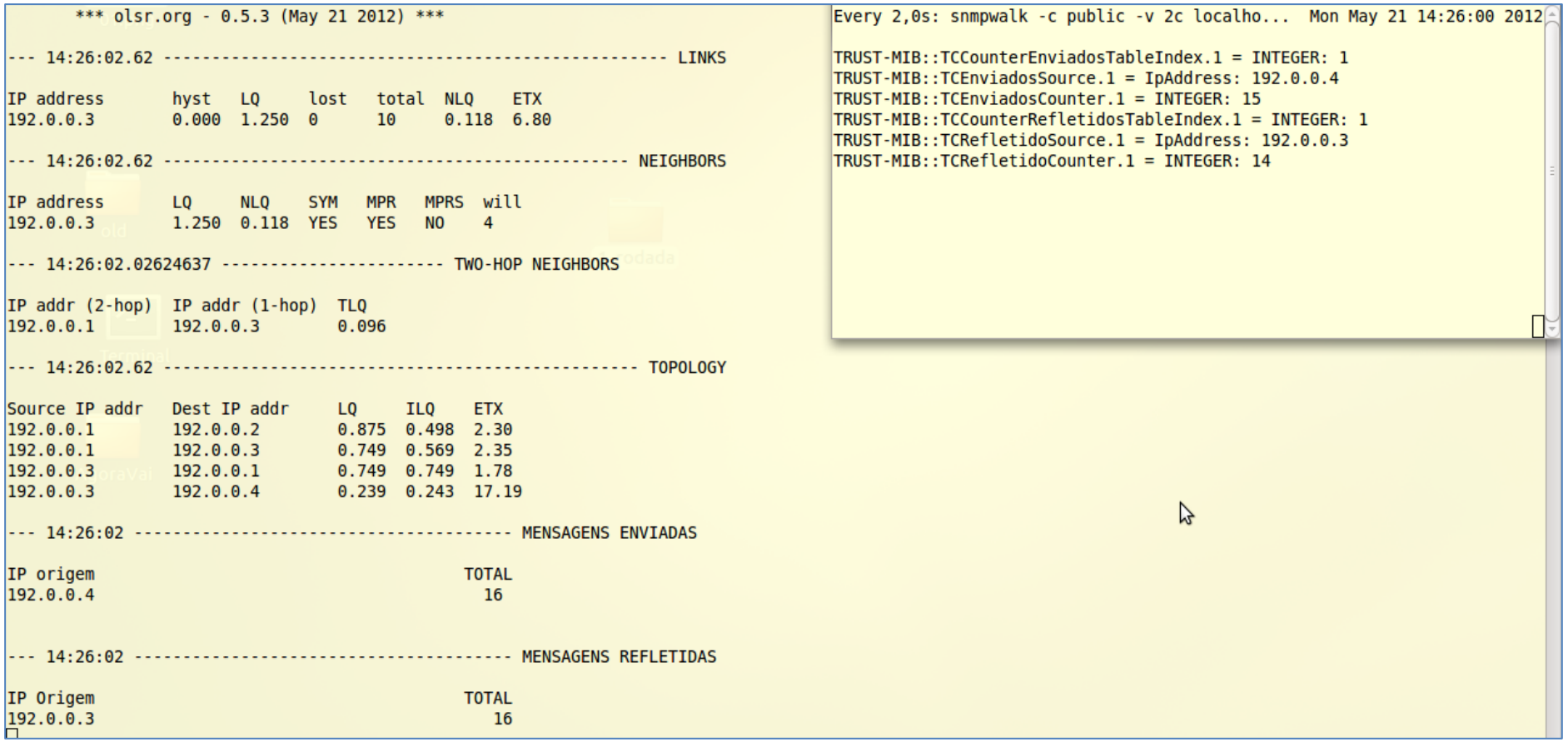
```
     Ip4Broadcast          255.255.255.255

    # IPv6 address scope to use.
    # Must be 'site-local' or 'global'

    # Ip6AddrType          site-local

    # IPv6 multicast address to use when
    # using site-local addresses.
    # If not defined, ff05::15 is used

    # Ip6MulticastSite          ff05::11

    # IPv6 multicast address to use when
    # using global addresses
    # If not defined, ff0e::1 is used

    # Ip6MulticastGlobal   ff0e::1


# Emission intervals.
    # If not defined, RFC proposed values will
    # be used in most cases.

    # Hello interval in seconds(float)
HelloInterval    2.0

    # HELLO validity time
HelloValidityTime    6.0

    # TC interval in seconds(float)
TcInterval        5.0

    # TC validity time
TcValidityTime  15.0

    # MID interval in seconds(float)
MidInterval     5.0

    # MID validity time
MidValidityTime 15.0

    # HNA interval in seconds(float)
HnaInterval     5.0

    # HNA validity time
HnaValidityTime 15.0


    # When multiple links exist between hosts
    # the weight of interface is used to determine
    # the link to use. Normally the weight is
    # automatically calculated by olsrd based
    # on the characteristics of the interface,
    # but here you can specify a fixed value.
```

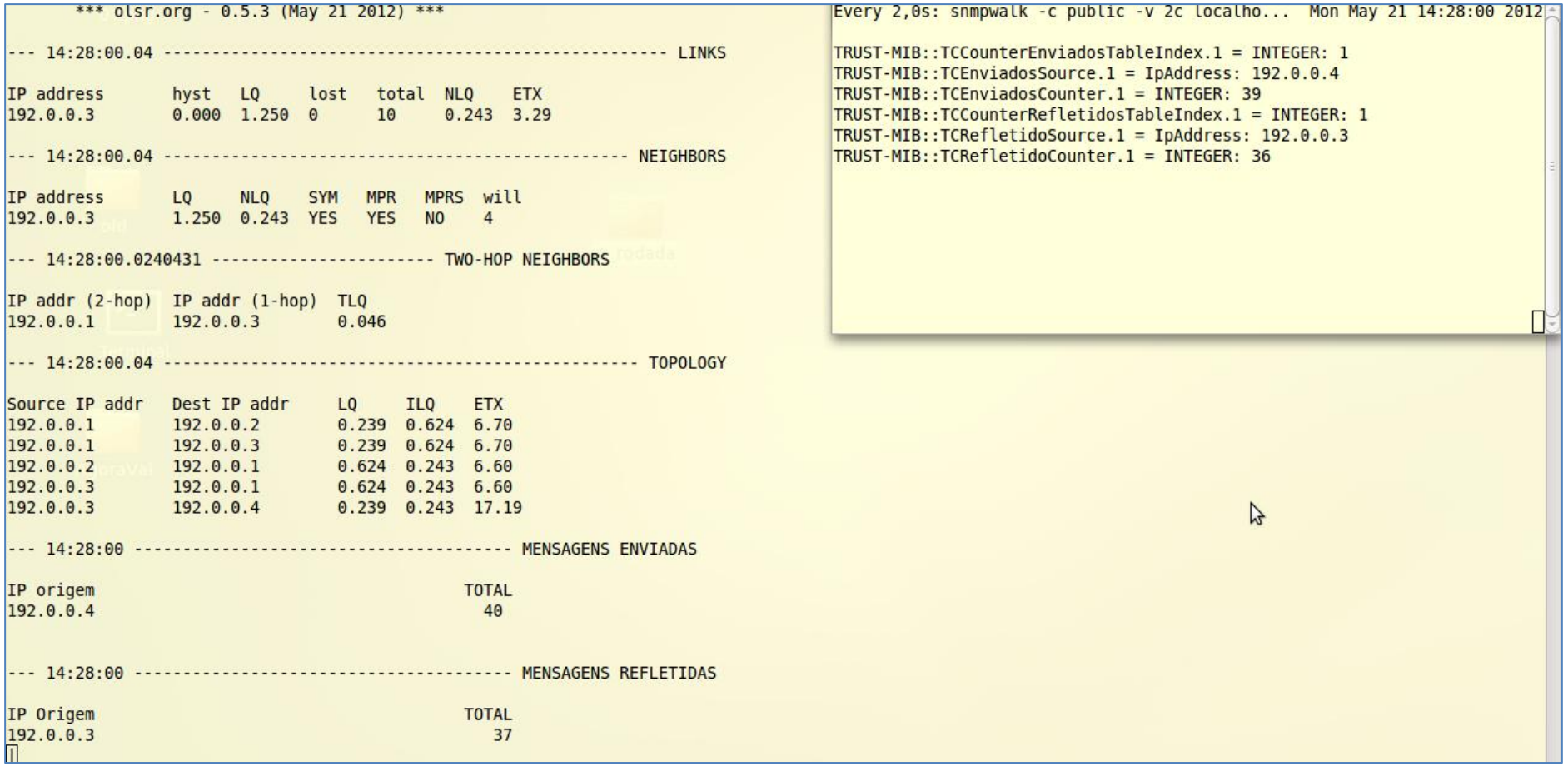
```
    # Olsrd will choose links with the lowest value.
    # Note:
    # Interface weight is used only when LinkQualityLevel is set
to 0.
    # For any other value of LinkQualityLevel, the interface ETX
    # value is used instead.
    # Weight 0


    # If a certain route should be preferred
    # or ignored by the mesh, the Link Quality
    # value of a node can be multiplied with a factor
    # entered here. In the example the route
    # using 192.168.0.1 would rather be ignored.
    # A multiplier of 0.5 will result in a small
    # (bad) LinkQuality value and a high (bad)
# ETX value.
    # Note:
    # Link quality multiplier is used only when
    # LinkQualityLevel is > 0.

    # LinkQualityMult 192.168.0.1 0.5

    # This multiplier applies to all other nodes
    # LinkQualityMult default 0.8

}

LoadPlugin "trust_mib_agentx.so.1.0"
{
PlParam "poll" "10.0",
}
```

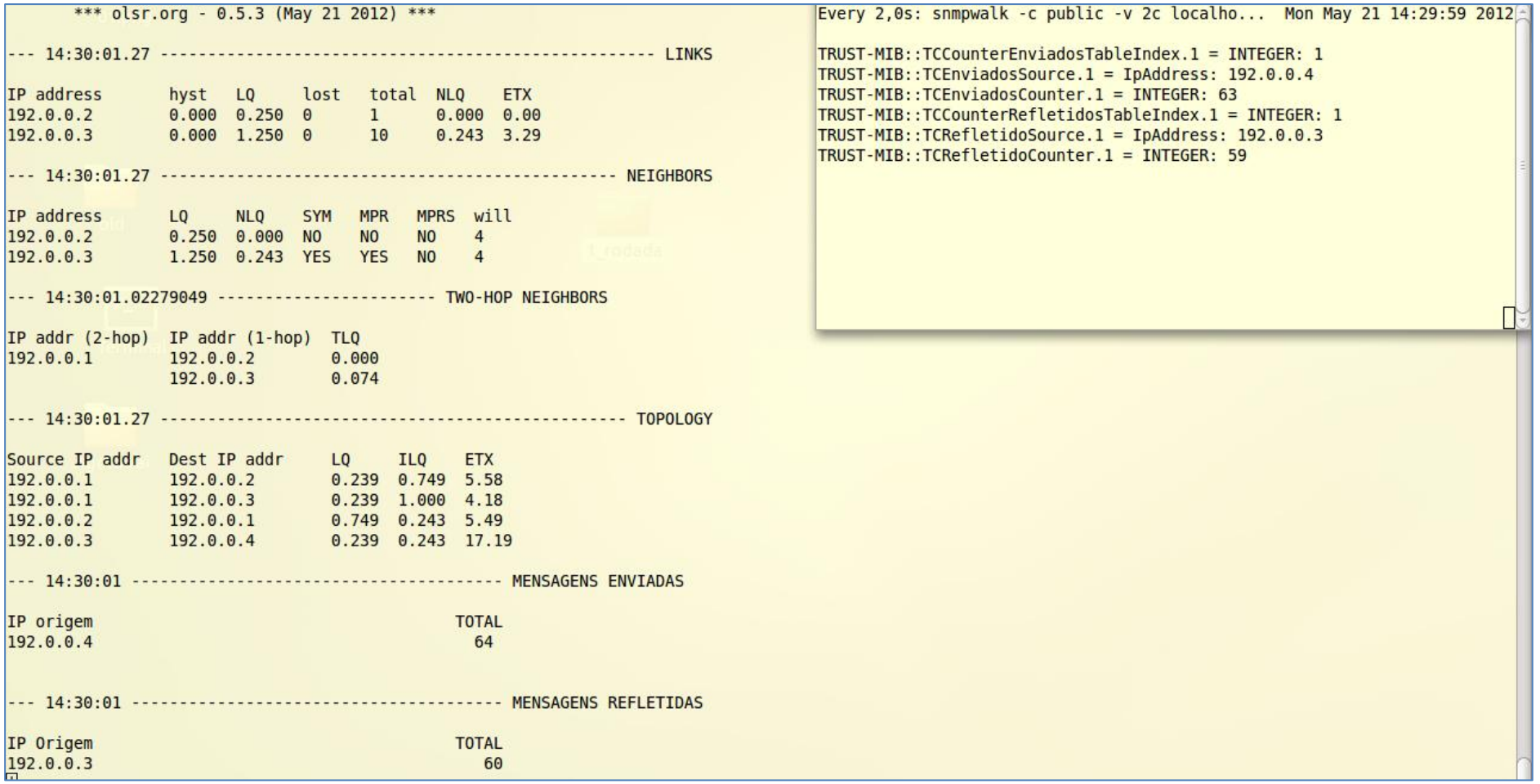
C - SIMULAÇÃO DA TRUST-MIB E OLSRD - Teste 01

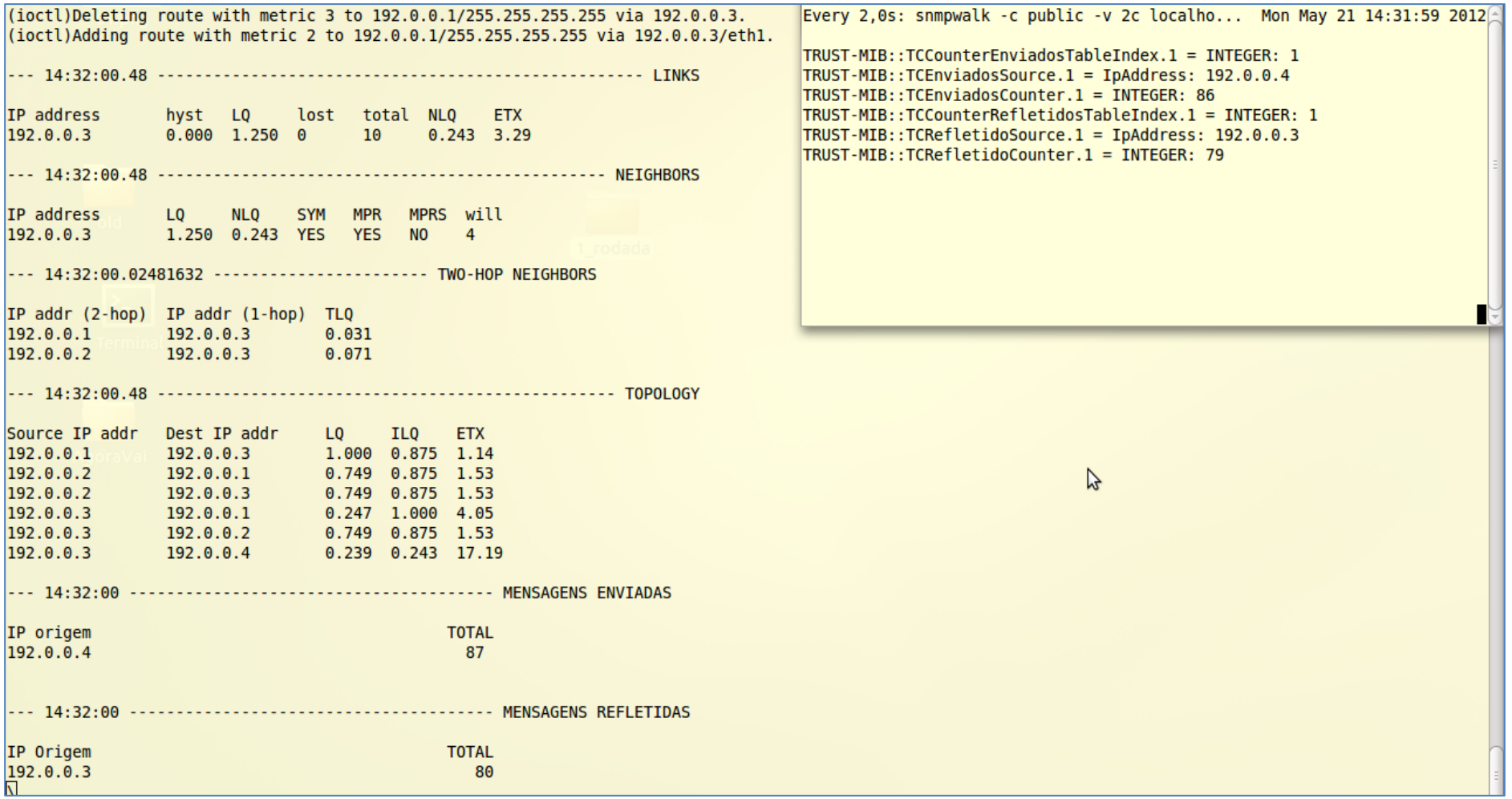
Telas do teste 01 da simulação realizada com o protocolo OLSRD e a TRUST-MIB.

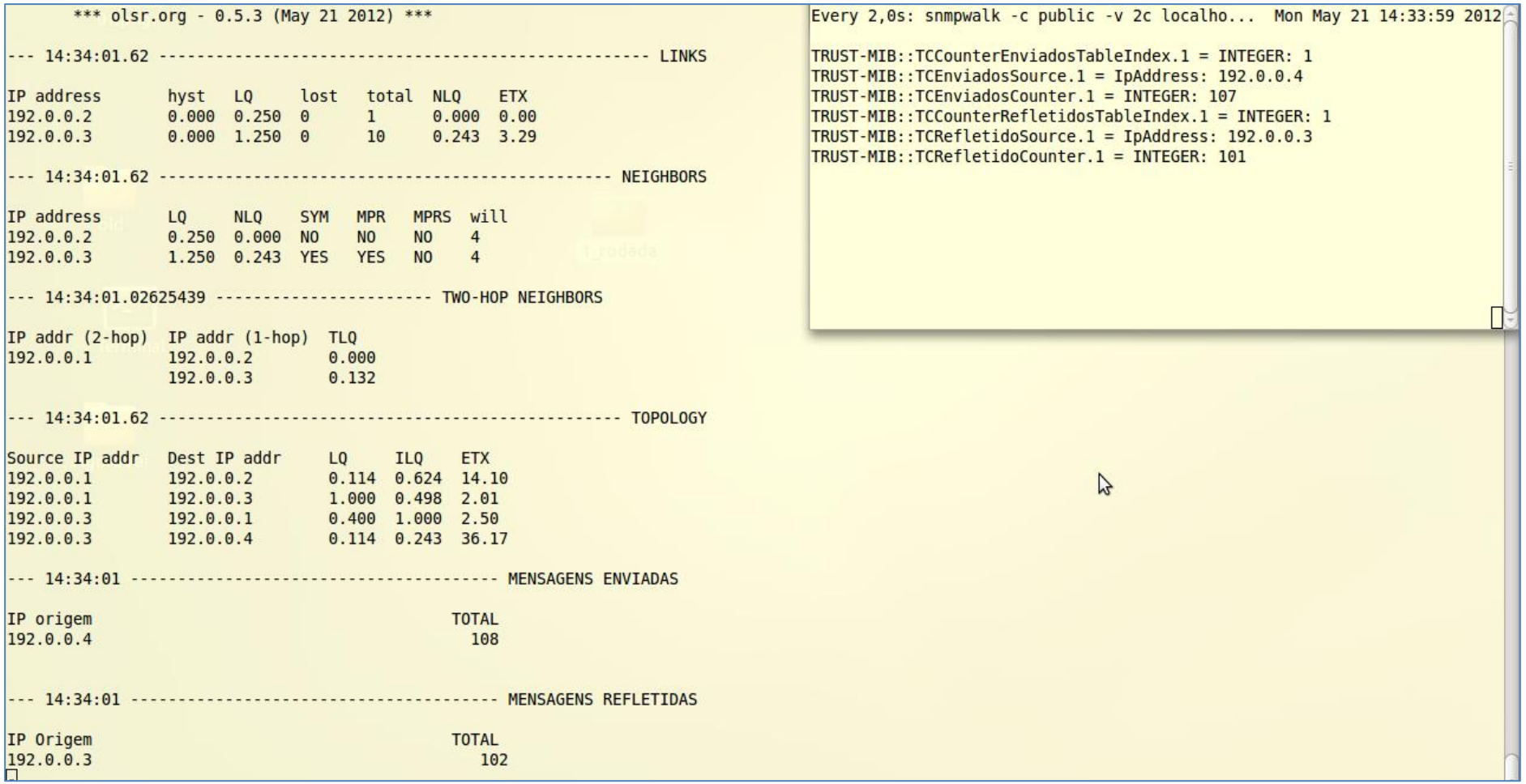


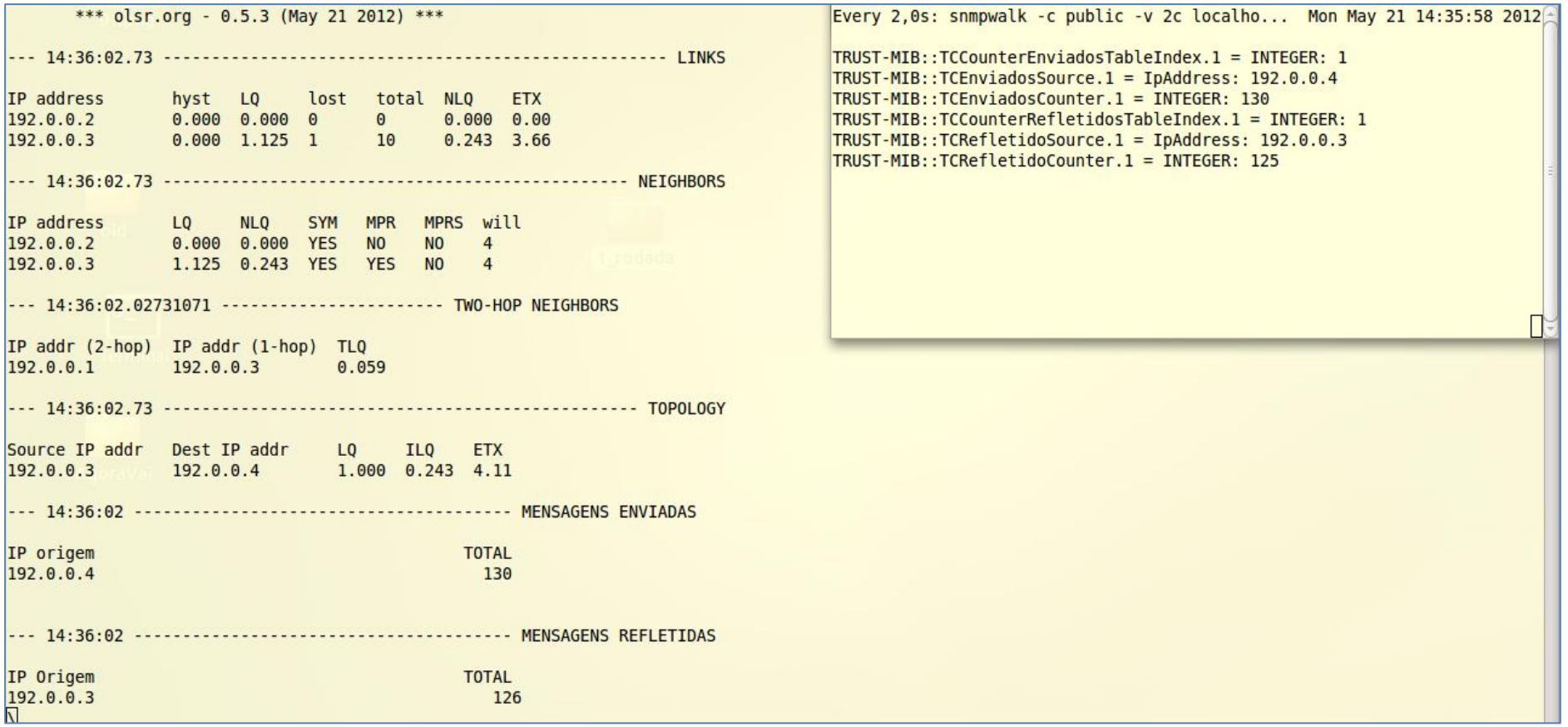

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:26:02.62 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.118 6.80
--- 14:26:02.62 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.118 YES YES NO 4
--- 14:26:02.02624637 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.096
--- 14:26:02.62 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.875 0.498 2.30
192.0.0.1 192.0.0.3 0.749 0.569 2.35
192.0.0.3 192.0.0.1 0.749 0.749 1.78
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:26:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 16
--- 14:26:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 16
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:26:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 15
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 14

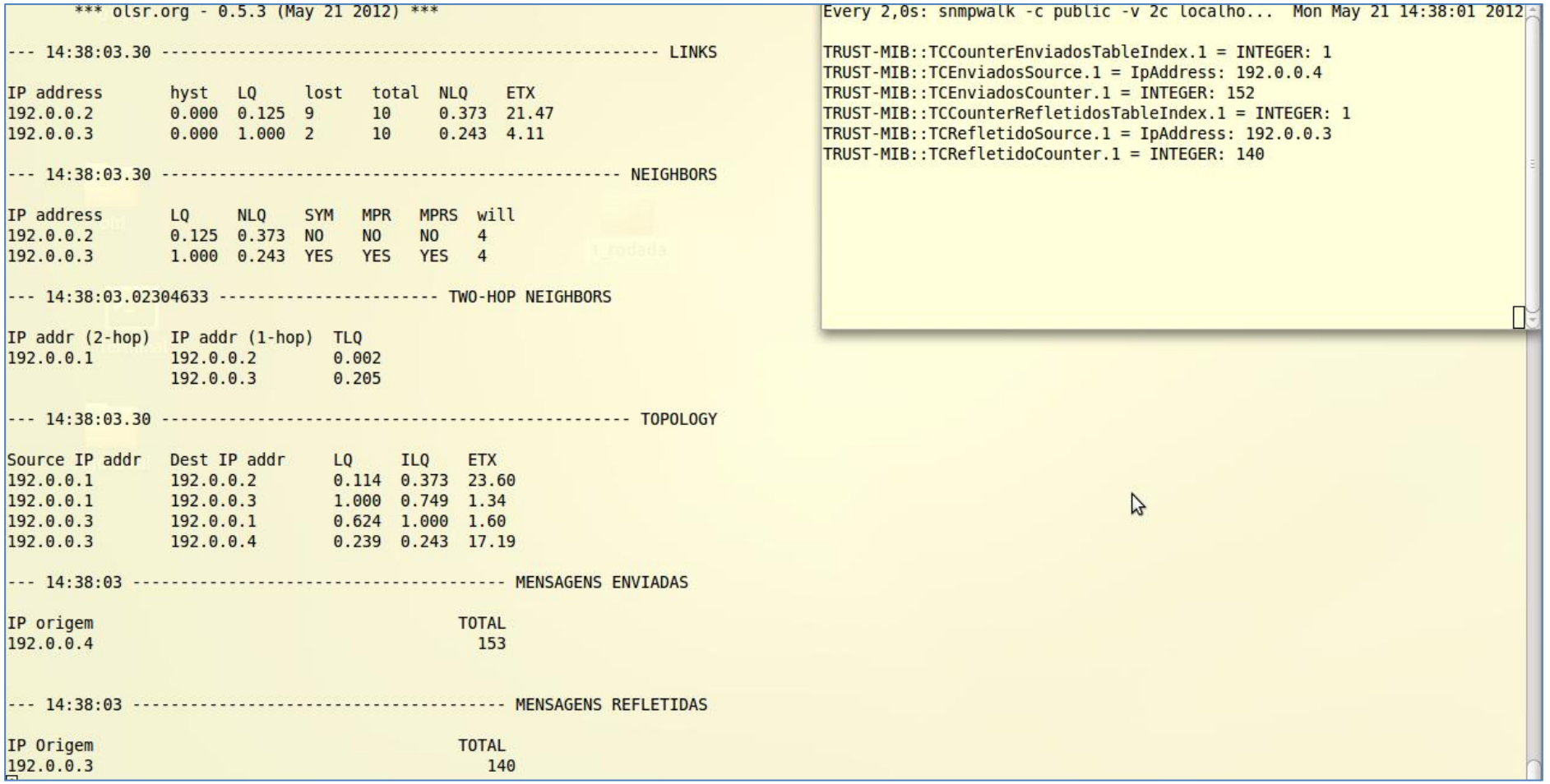

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:28:00.04 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:28:00.04 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:28:00.0240431 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.046
--- 14:28:00.04 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.624 6.70
192.0.0.1 192.0.0.3 0.239 0.624 6.70
192.0.0.2 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:28:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 40
--- 14:28:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 37
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:28:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 39
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 36

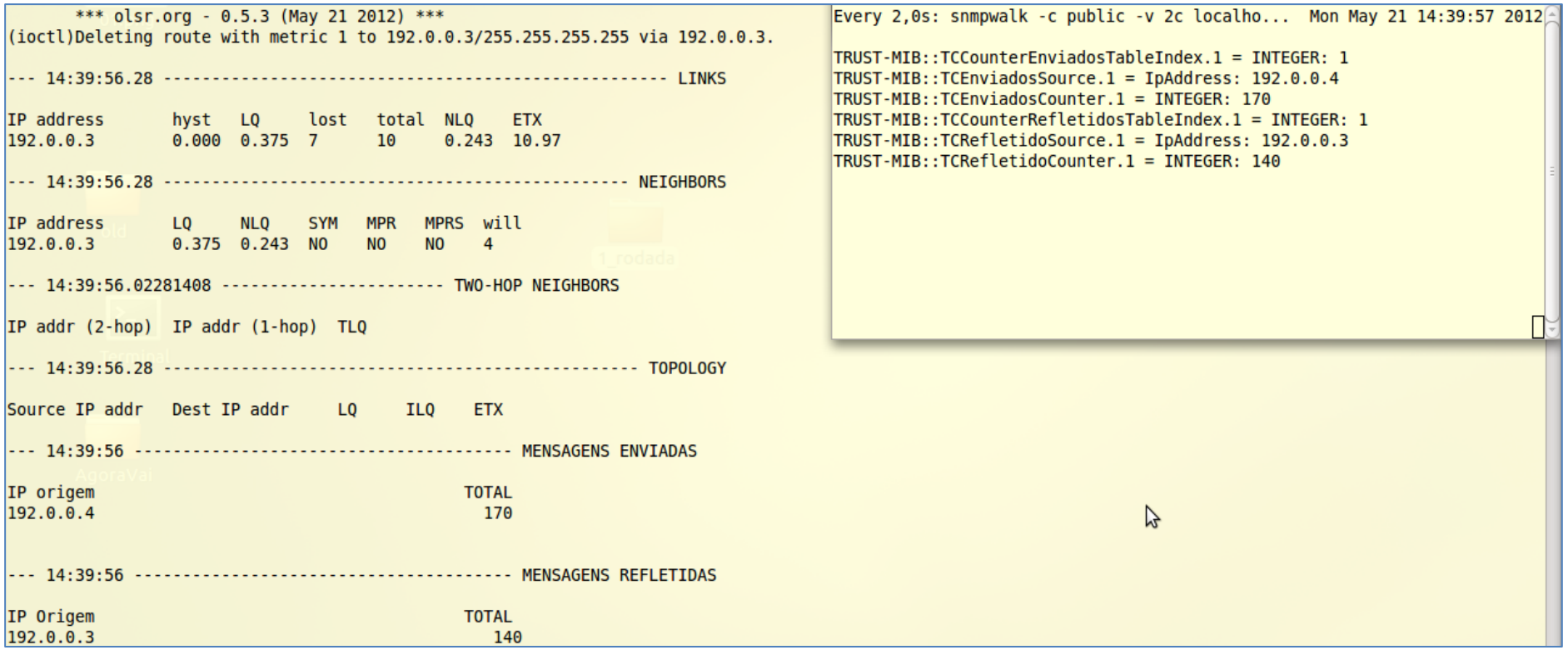

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:30:01.27 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.250 0 1 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:30:01.27 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.250 0.000 NO NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:30:01.02279049 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.074
--- 14:30:01.27 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.749 5.58
192.0.0.1 192.0.0.3 0.239 1.000 4.18
192.0.0.2 192.0.0.1 0.749 0.243 5.49
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:30:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 64
--- 14:30:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 60
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:29:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 63
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 59

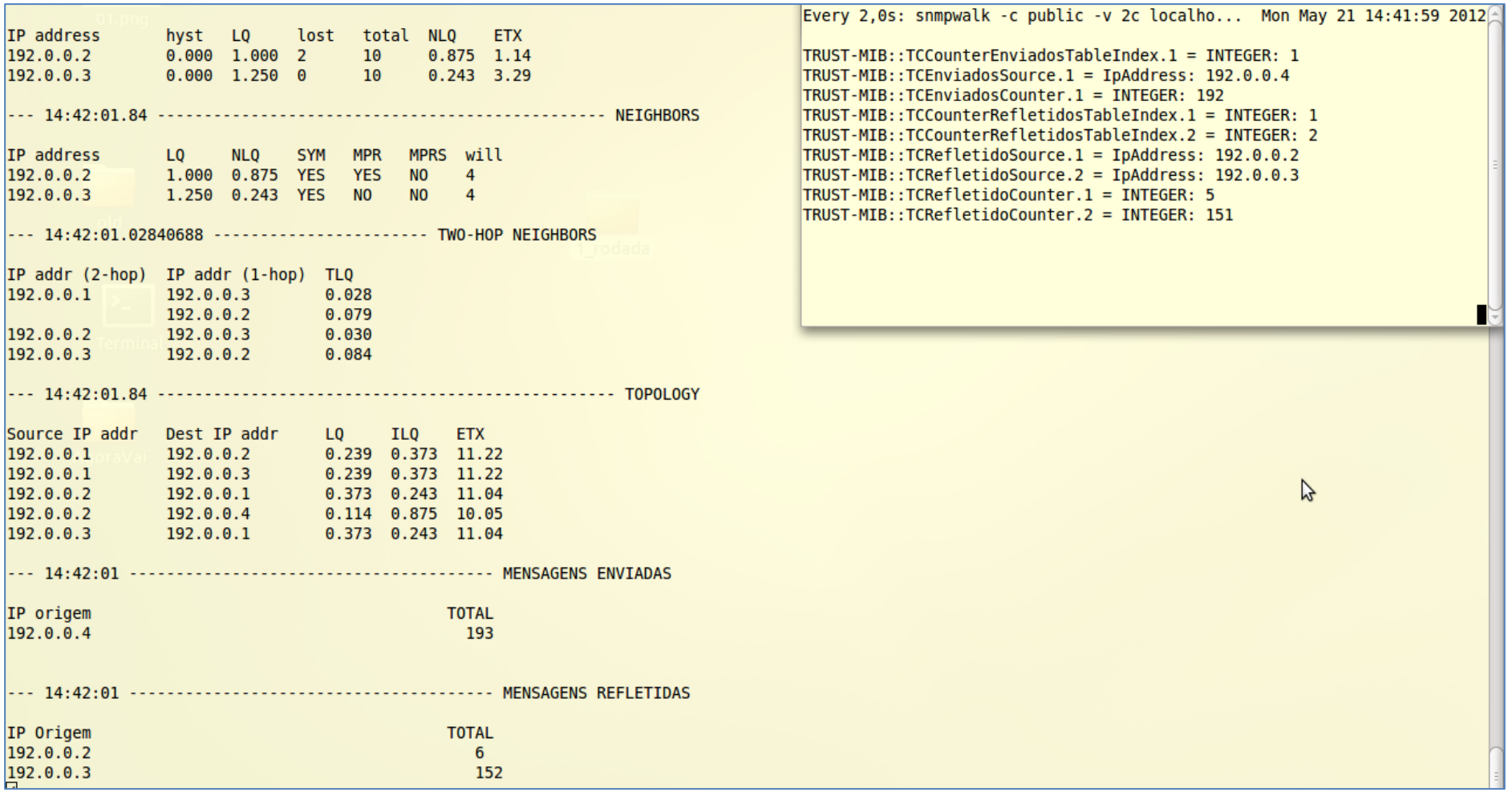

(ioctl)Deleting route with metric 3 to 192.0.0.1/255.255.255.255 via 192.0.0.3.
(ioctl)Adding route with metric 2 to 192.0.0.1/255.255.255.255 via 192.0.0.3/eth1.
--- 14:32:00.48 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:32:00.48 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:32:00.02481632 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.031
192.0.0.2 192.0.0.3 0.071
--- 14:32:00.48 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 1.000 0.875 1.14
192.0.0.2 192.0.0.1 0.749 0.875 1.53
192.0.0.2 192.0.0.3 0.749 0.875 1.53
192.0.0.3 192.0.0.1 0.247 1.000 4.05
192.0.0.3 192.0.0.2 0.749 0.875 1.53
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:32:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 87
--- 14:32:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 80
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:31:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 86
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 79

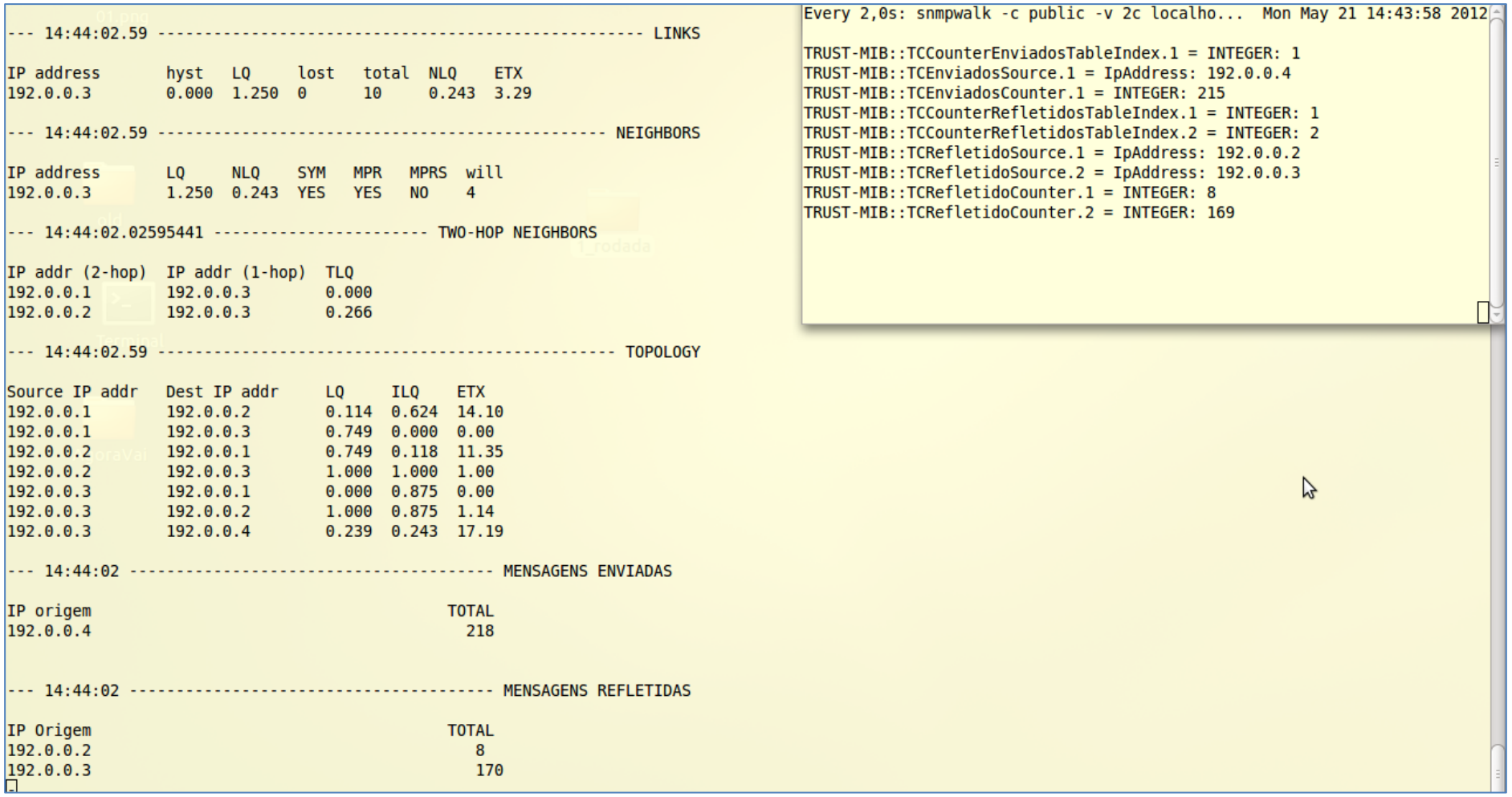

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:34:01.62 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.250 0 1 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:34:01.62 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.250 0.000 NO NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:34:01.02625439 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.132
--- 14:34:01.62 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.624 14.10
192.0.0.1 192.0.0.3 1.000 0.498 2.01
192.0.0.3 192.0.0.1 0.400 1.000 2.50
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 14:34:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 108
--- 14:34:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 102
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:33:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 107
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 101

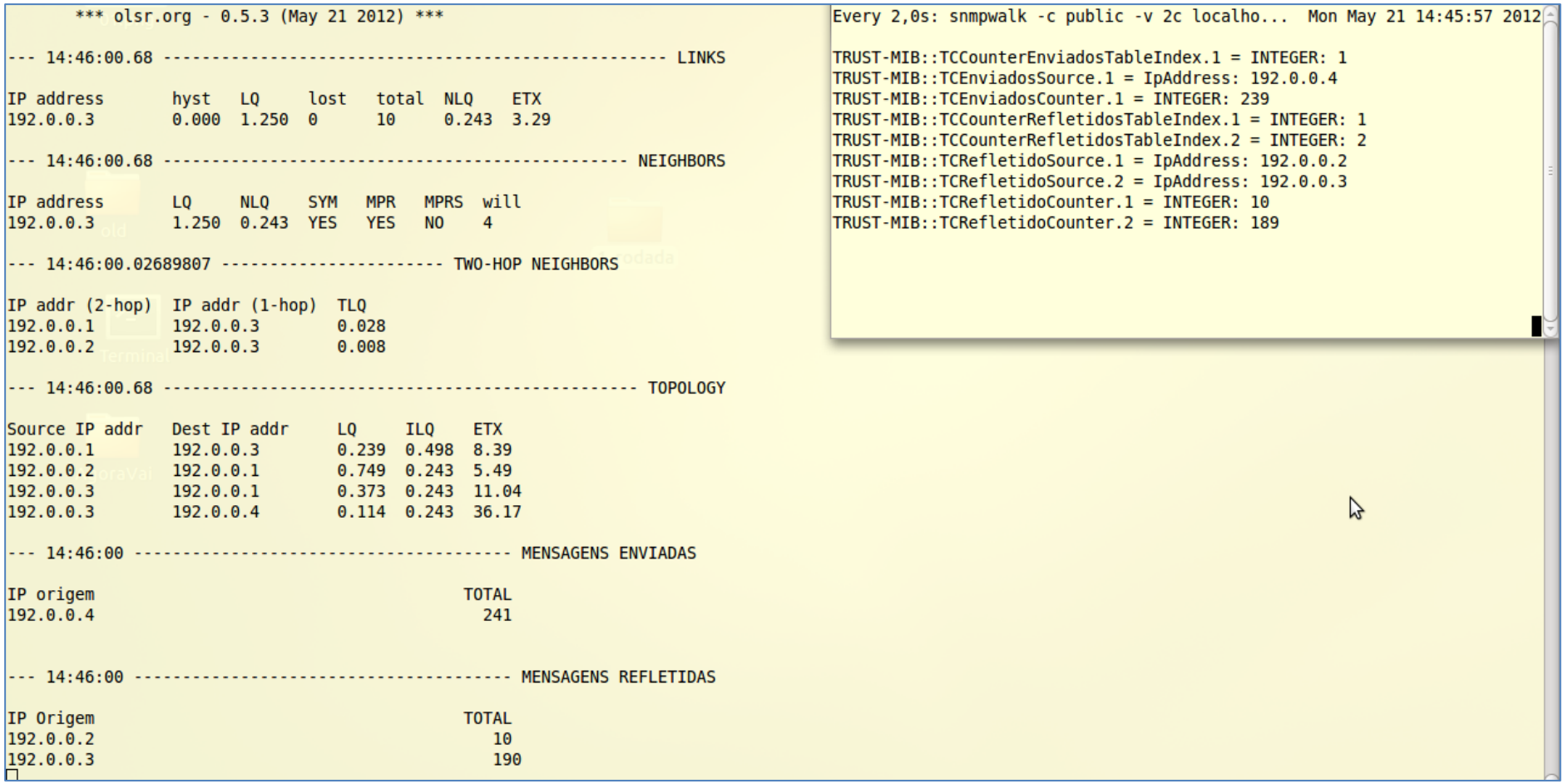

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:36:02.73 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 0 0 0.000 0.00
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 14:36:02.73 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.000 YES NO NO 4
192.0.0.3 1.125 0.243 YES YES NO 4
--- 14:36:02.02731071 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.059
--- 14:36:02.73 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.3 192.0.0.4 1.000 0.243 4.11
--- 14:36:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 130
--- 14:36:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 126
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:35:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 130
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 125

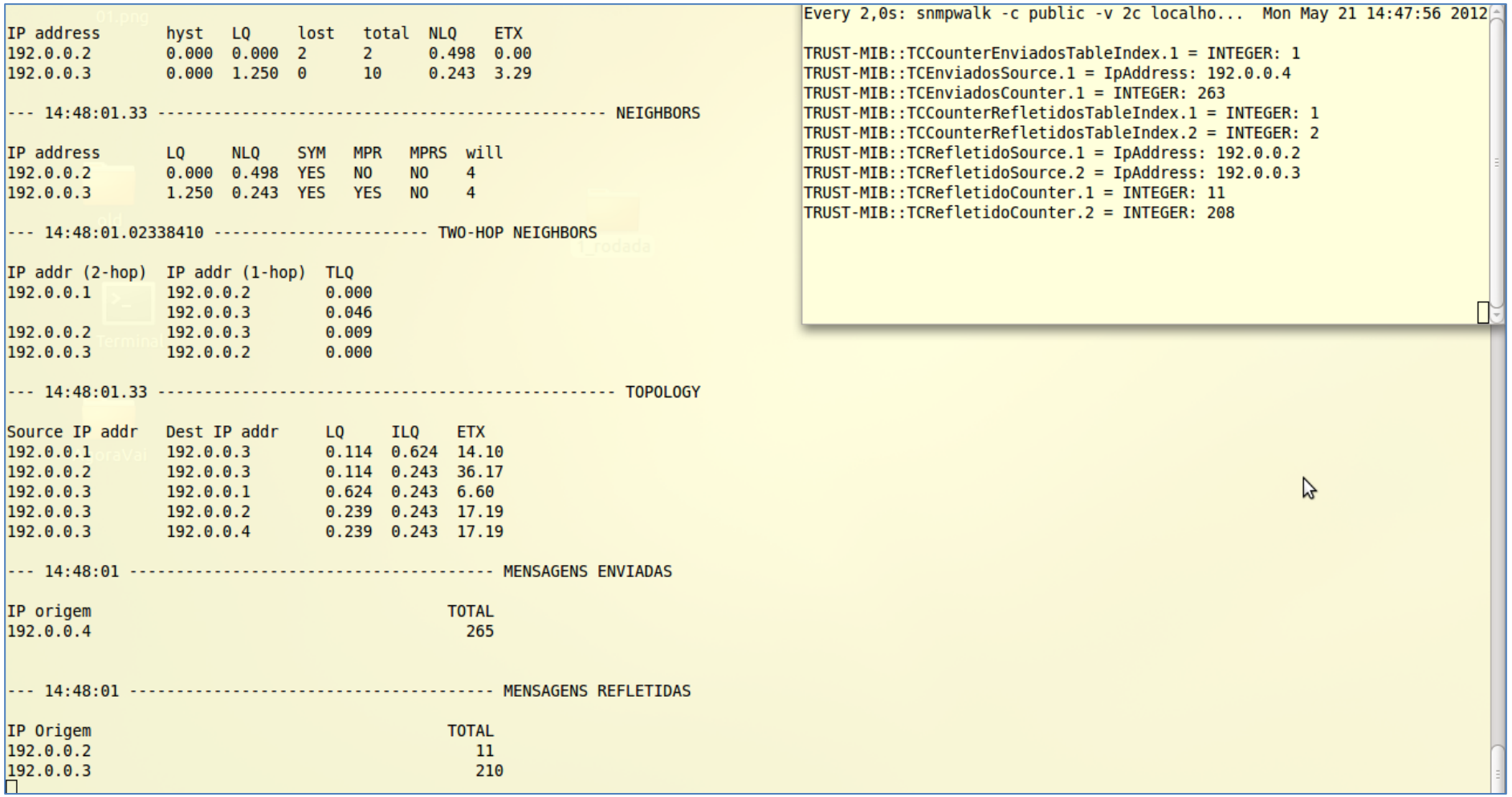

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:38:03.30 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.125 9 10 0.373 21.47
192.0.0.3 0.000 1.000 2 10 0.243 4.11
--- 14:38:03.30 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.125 0.373 NO NO NO 4
192.0.0.3 1.000 0.243 YES YES YES 4
--- 14:38:03.02304633 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.002
192.0.0.3 0.205
--- 14:38:03.30 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.373 23.60
192.0.0.1 192.0.0.3 1.000 0.749 1.34
192.0.0.3 192.0.0.1 0.624 1.000 1.60
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:38:03 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 153
--- 14:38:03 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 140
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:38:01 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 152
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 140

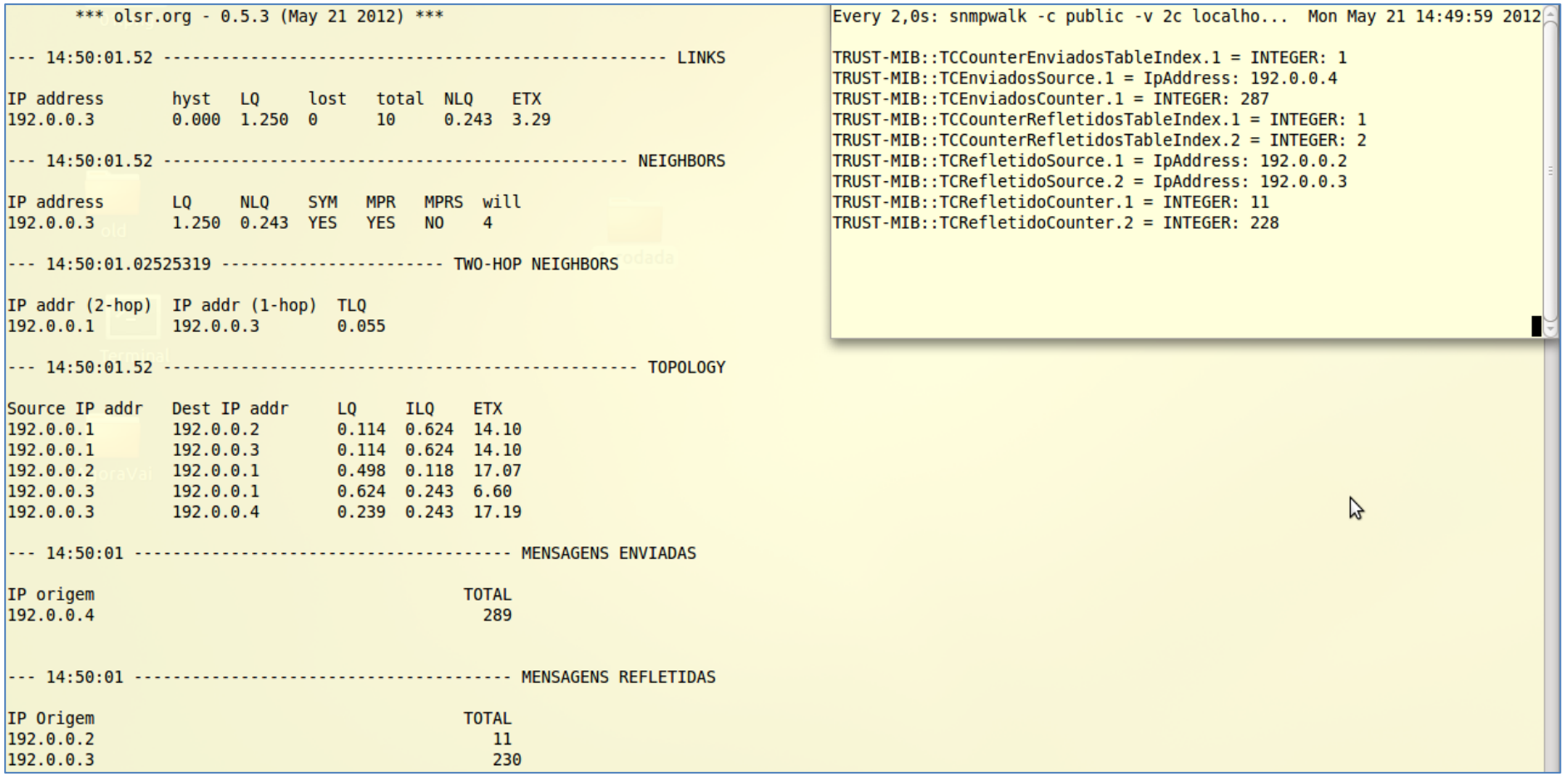

*** olsr.org - 0.5.3 (May 21 2012) ***
(ioctl)Deleting route with metric 1 to 192.0.0.3/255.255.255.255 via 192.0.0.3.
--- 14:39:56.28 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 0.375 7 10 0.243 10.97
--- 14:39:56.28 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 0.375 0.243 NO NO NO 4
--- 14:39:56.02281408 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 14:39:56.28 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 14:39:56 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 170
--- 14:39:56 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 140
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:39:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 170
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 140

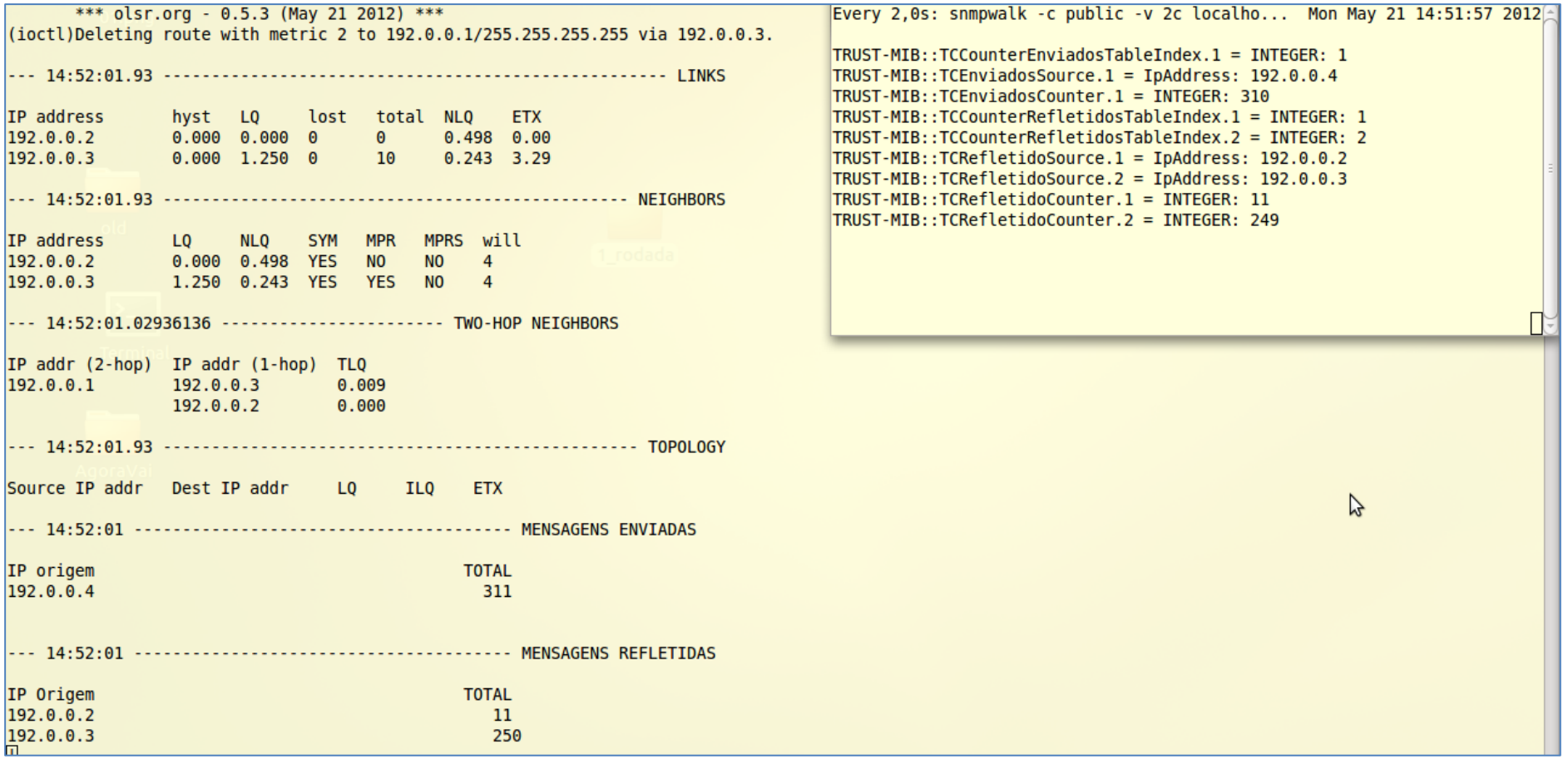

IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 1.000 2 10 0.875 1.14
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:42:01.84 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 1.000 0.875 YES YES NO 4
192.0.0.3 1.250 0.243 YES NO NO 4
--- 14:42:01.02840688 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.028
192.0.0.2 0.079
192.0.0.2 192.0.0.3 0.030
192.0.0.3 192.0.0.2 0.084
--- 14:42:01.84 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.373 11.22
192.0.0.1 192.0.0.3 0.239 0.373 11.22
192.0.0.2 192.0.0.1 0.373 0.243 11.04
192.0.0.2 192.0.0.4 0.114 0.875 10.05
192.0.0.3 192.0.0.1 0.373 0.243 11.04
--- 14:42:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 193
--- 14:42:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 6
192.0.0.3 152
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:41:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 192
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 5
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 151

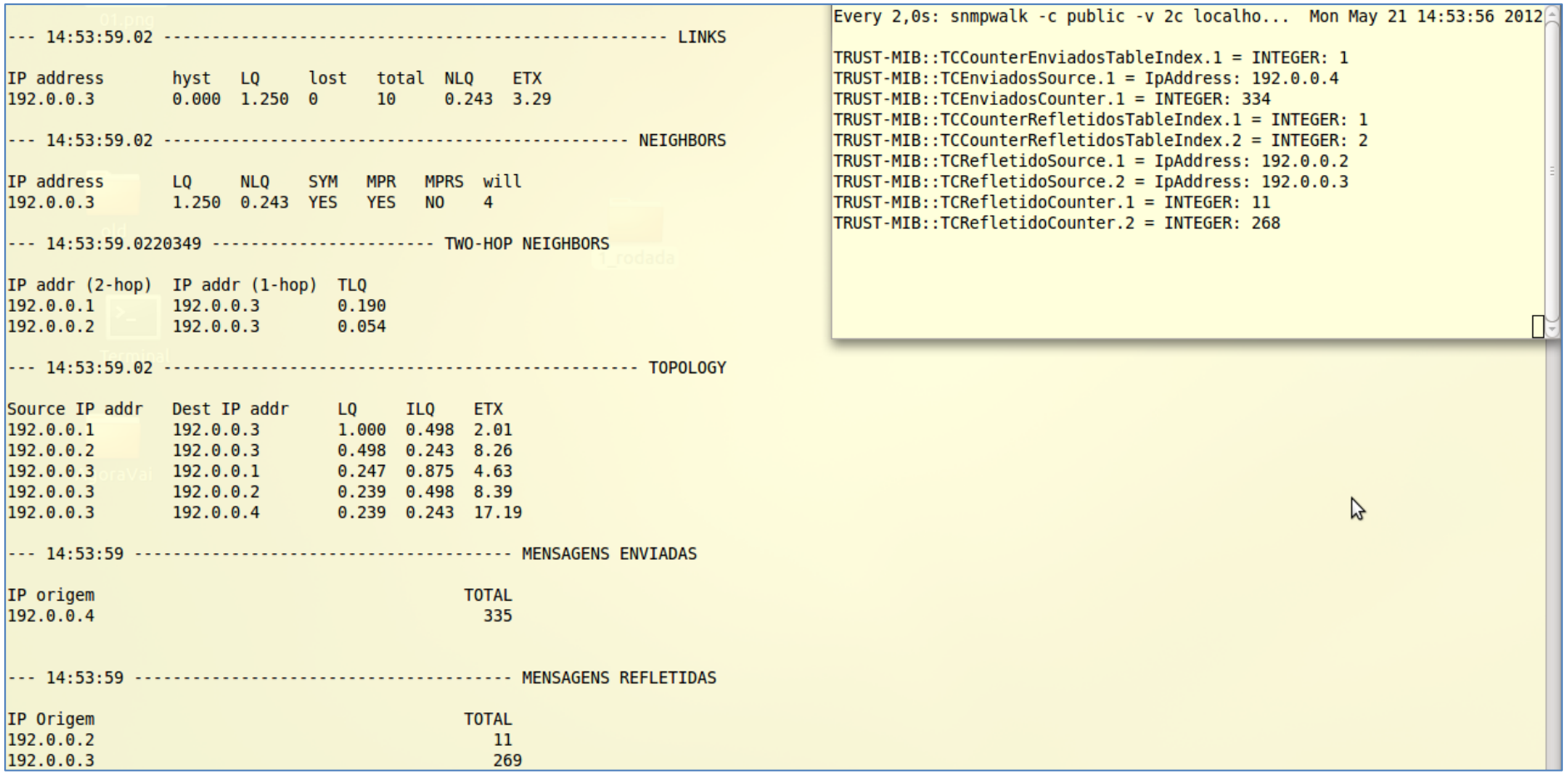

--- 14:44:02.59 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:44:02.59 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:44:02.02595441 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.000
192.0.0.2 192.0.0.3 0.266
--- 14:44:02.59 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.624 14.10
192.0.0.1 192.0.0.3 0.749 0.000 0.00
192.0.0.2 192.0.0.1 0.749 0.118 11.35
192.0.0.2 192.0.0.3 1.000 1.000 1.00
192.0.0.3 192.0.0.1 0.000 0.875 0.00
192.0.0.3 192.0.0.2 1.000 0.875 1.14
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:44:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 218
--- 14:44:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 8
192.0.0.3 170
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:43:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 215
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 8
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 169

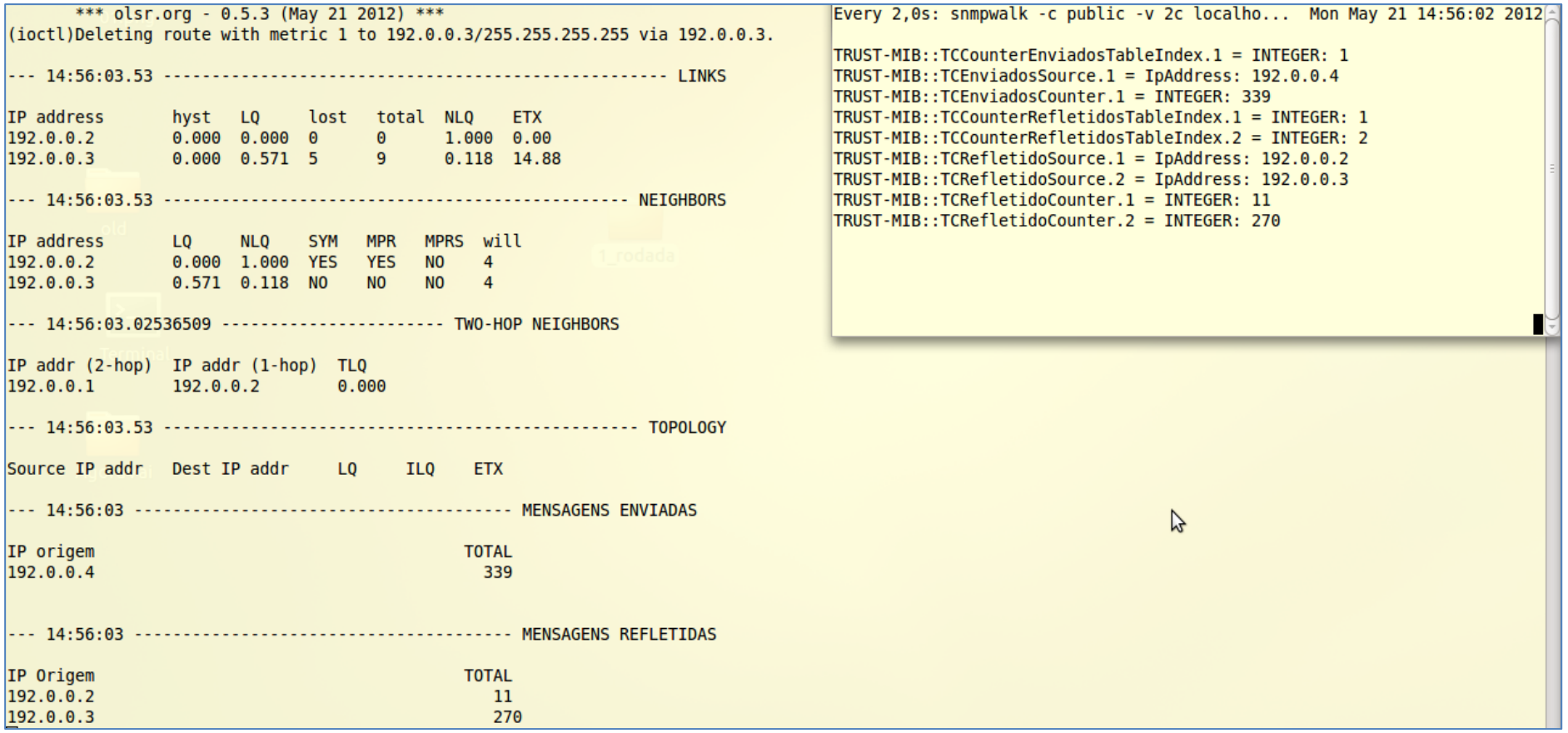

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:46:00.68 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:46:00.68 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:46:00.02689807 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.028
192.0.0.2 192.0.0.3 0.008
--- 14:46:00.68 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.498 8.39
192.0.0.2 192.0.0.1 0.749 0.243 5.49
192.0.0.3 192.0.0.1 0.373 0.243 11.04
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 14:46:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 241
--- 14:46:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 10
192.0.0.3 190
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:45:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 239
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 10
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 189


IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 2 2 0.498 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:48:01.33 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.498 YES NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:48:01.02338410 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.046
192.0.0.2 192.0.0.3 0.009
192.0.0.3 192.0.0.2 0.000
--- 14:48:01.33 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.624 14.10
192.0.0.2 192.0.0.3 0.114 0.243 36.17
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.2 0.239 0.243 17.19
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:48:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 265
--- 14:48:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 11
192.0.0.3 210
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:47:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 263
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 11
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 208


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 14:50:01.52 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:50:01.52 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:50:01.02525319 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.055
--- 14:50:01.52 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.624 14.10
192.0.0.1 192.0.0.3 0.114 0.624 14.10
192.0.0.2 192.0.0.1 0.498 0.118 17.07
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:50:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 289
--- 14:50:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 11
192.0.0.3 230
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:49:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 287
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 11
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 228

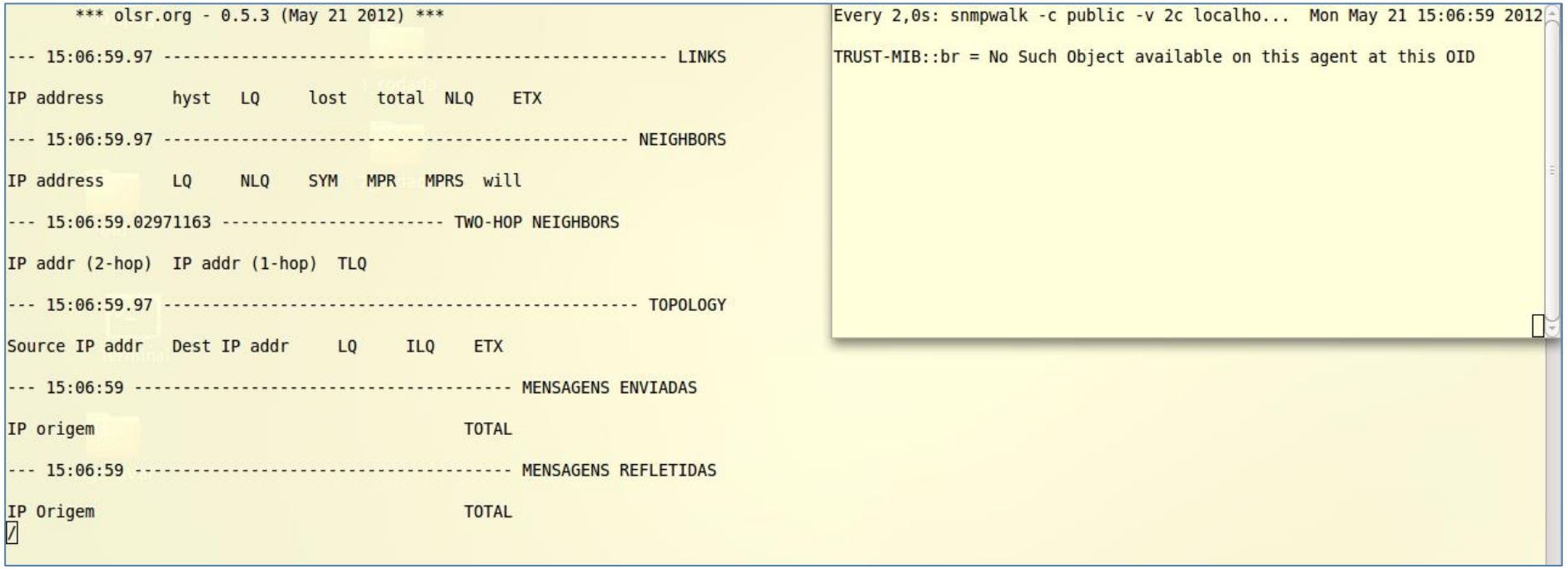

*** olsr.org - 0.5.3 (May 21 2012) ***
(ioctl)Deleting route with metric 2 to 192.0.0.1/255.255.255.255 via 192.0.0.3.
--- 14:52:01.93 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 0 0 0.498 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:52:01.93 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.498 YES NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:52:01.02936136 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.009
192.0.0.2 0.000
--- 14:52:01.93 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 14:52:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 311
--- 14:52:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 11
192.0.0.3 250
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:51:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 310
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 11
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 249

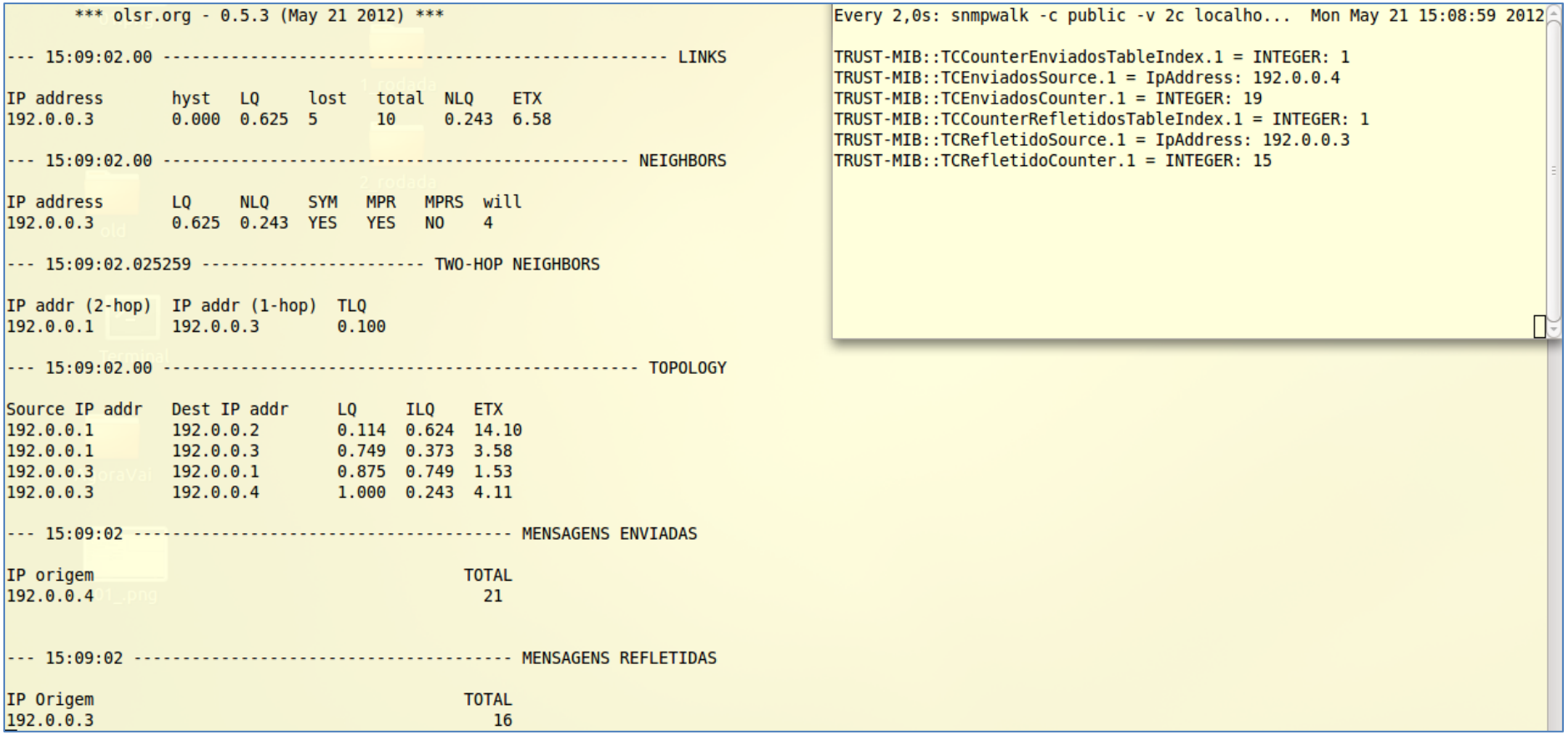

--- 14:53:59.02 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 14:53:59.02 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 14:53:59.0220349 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.190
192.0.0.2 192.0.0.3 0.054
--- 14:53:59.02 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 1.000 0.498 2.01
192.0.0.2 192.0.0.3 0.498 0.243 8.26
192.0.0.3 192.0.0.1 0.247 0.875 4.63
192.0.0.3 192.0.0.2 0.239 0.498 8.39
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 14:53:59 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 335
--- 14:53:59 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 11
192.0.0.3 269
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:53:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 334
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 11
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 268

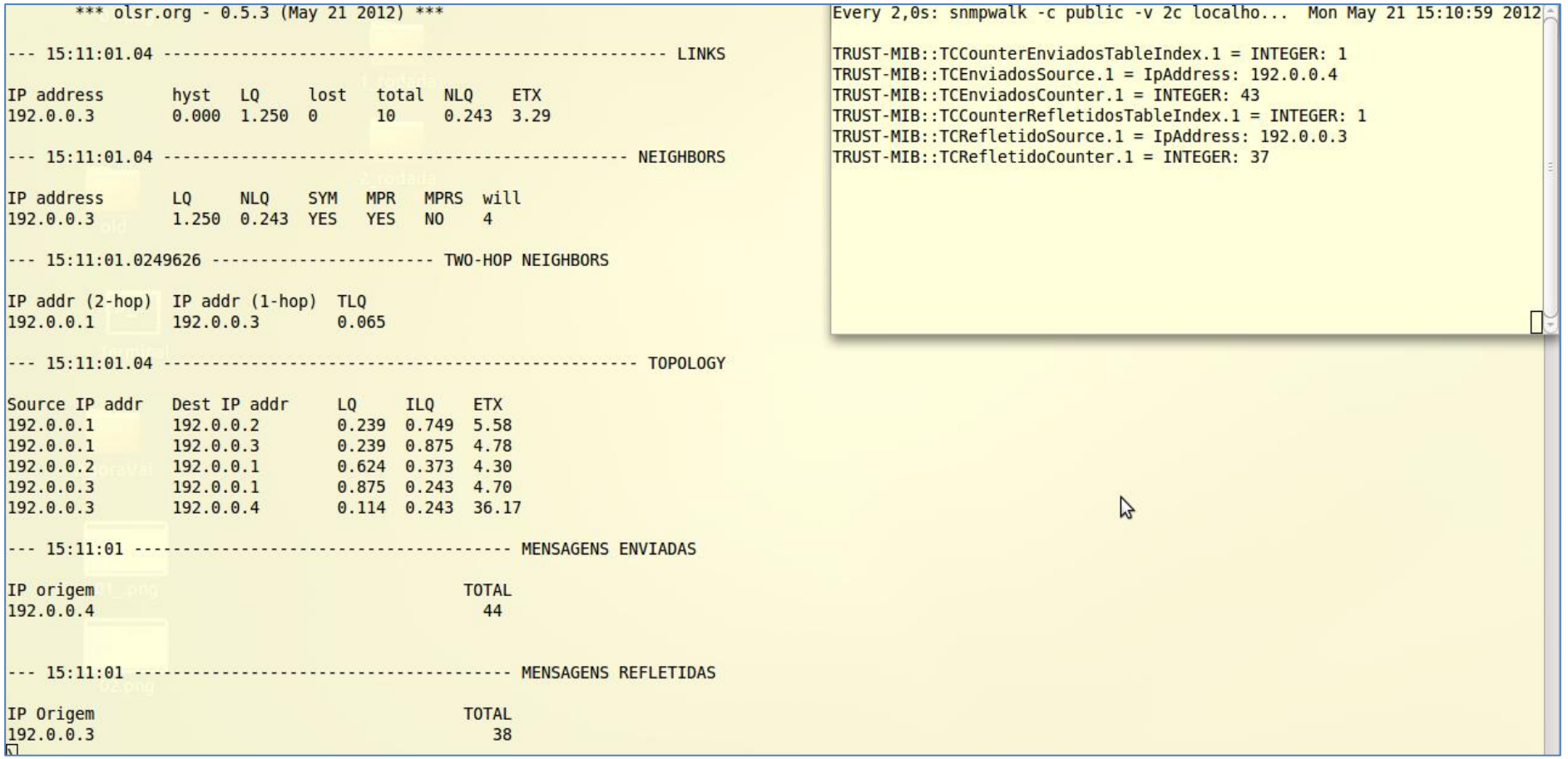

*** olsr.org - 0.5.3 (May 21 2012) ***
(ioctl)Deleting route with metric 1 to 192.0.0.3/255.255.255.255 via 192.0.0.3.
--- 14:56:03.53 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 0 0 1.000 0.00
192.0.0.3 0.000 0.571 5 9 0.118 14.88
--- 14:56:03.53 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 1.000 YES YES NO 4
192.0.0.3 0.571 0.118 NO NO NO 4
--- 14:56:03.02536509 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
--- 14:56:03.53 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 14:56:03 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 339
--- 14:56:03 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 11
192.0.0.3 270
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 14:56:02 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 339
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 11
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 270

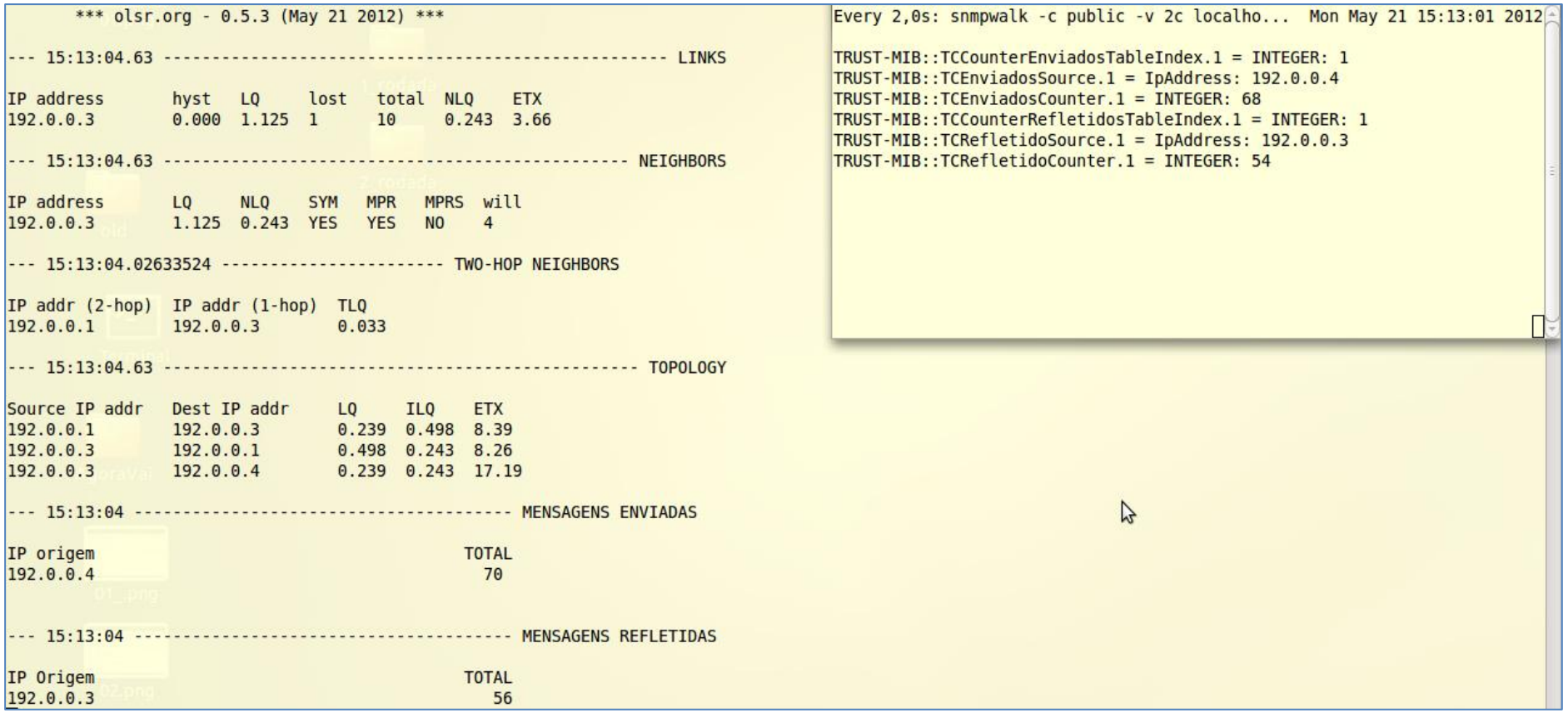
D - SIMULAÇÃO DA TRUST-MIB E OLSRD - Teste 02

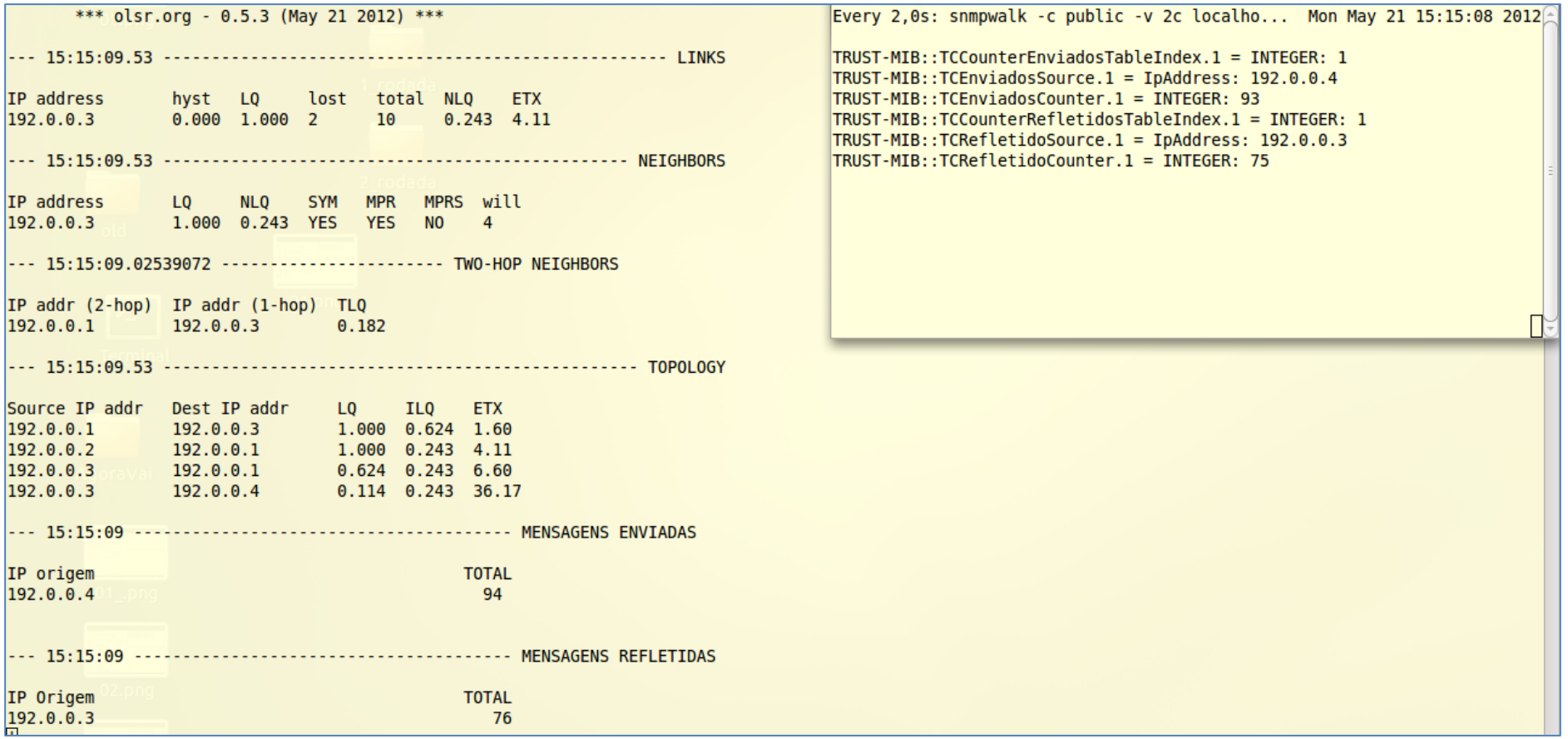
Telas do teste 02 da simulação realizada com o protocolo OLSRD e a TRUST-MIB.

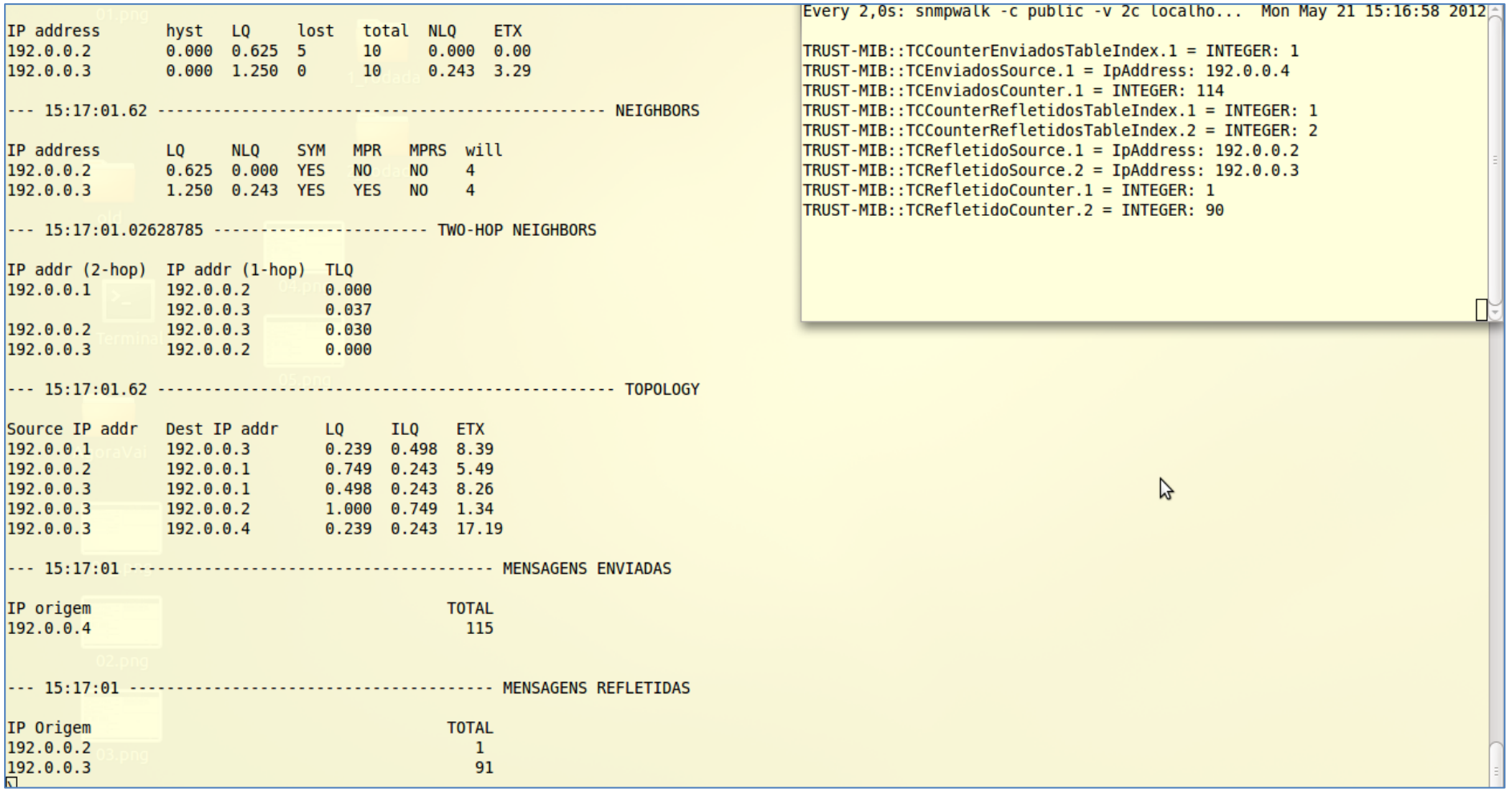


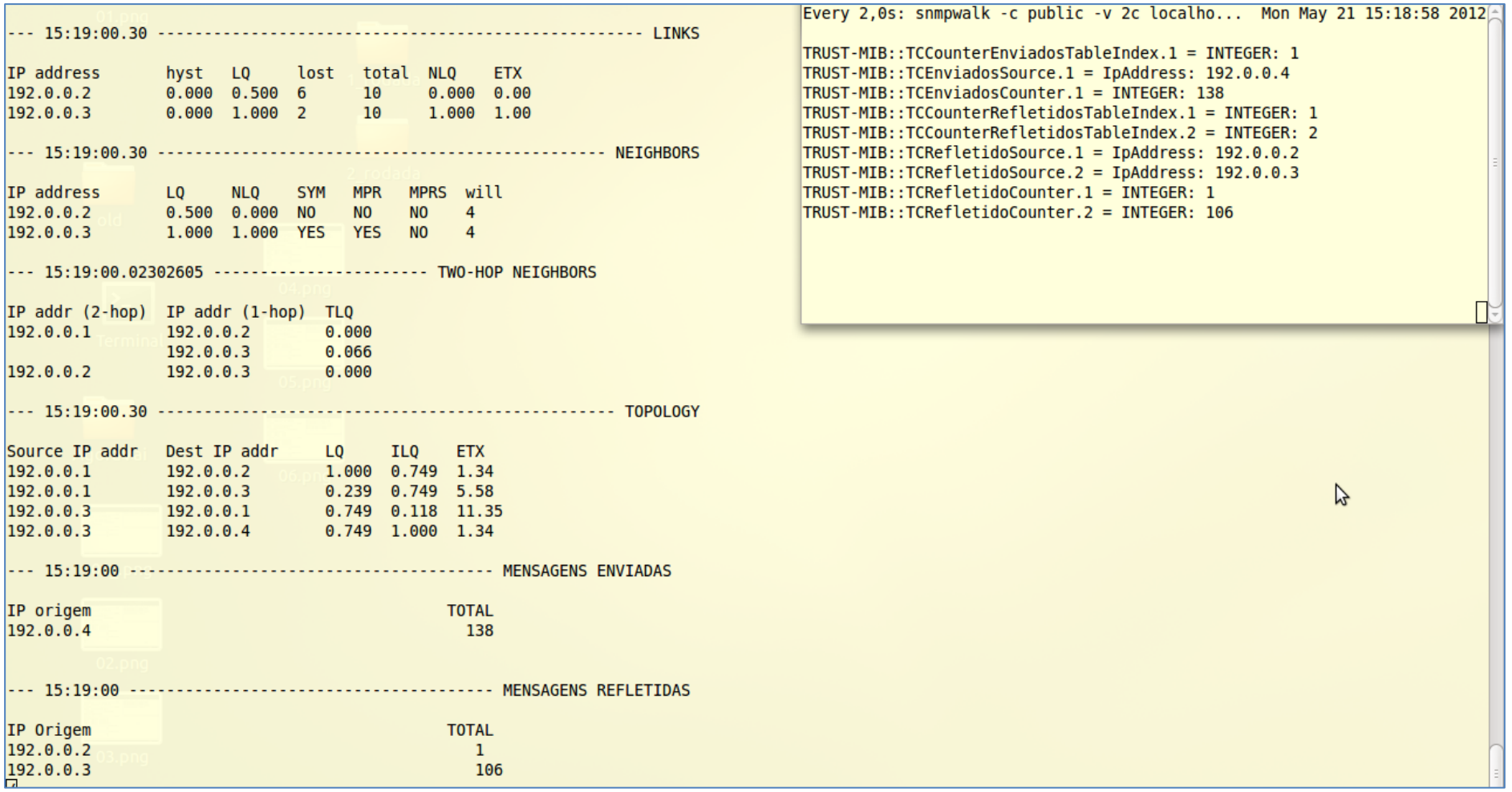

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:09:02.00 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 0.625 5 10 0.243 6.58
--- 15:09:02.00 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 0.625 0.243 YES YES NO 4
--- 15:09:02.025259 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.100
--- 15:09:02.00 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.624 14.10
192.0.0.1 192.0.0.3 0.749 0.373 3.58
192.0.0.3 192.0.0.1 0.875 0.749 1.53
192.0.0.3 192.0.0.4 1.000 0.243 4.11
--- 15:09:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 21
--- 15:09:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 16
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:08:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 19
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 15

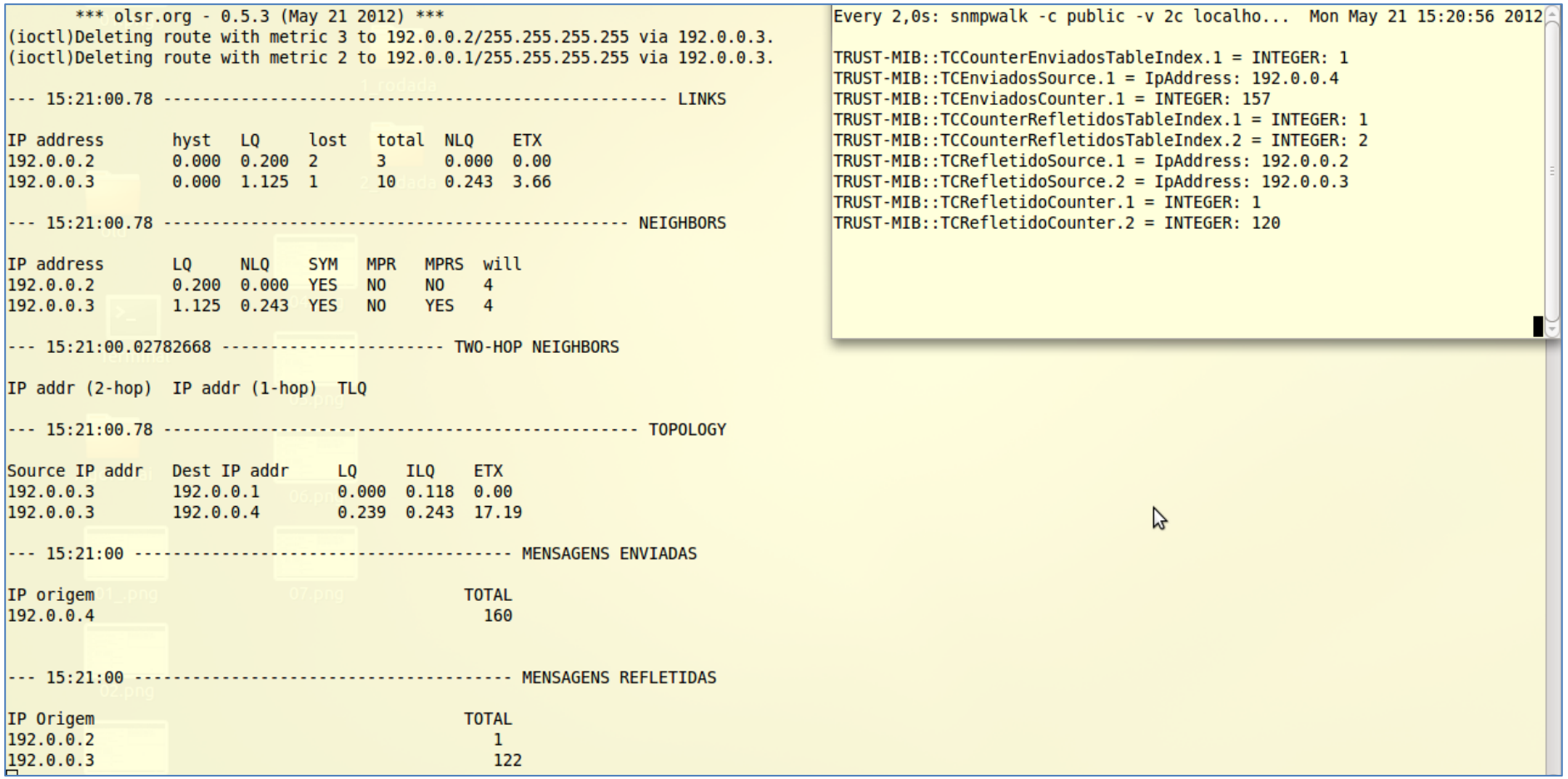

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:11:01.04 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:11:01.04 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:11:01.0249626 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.065
--- 15:11:01.04 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.749 5.58
192.0.0.1 192.0.0.3 0.239 0.875 4.78
192.0.0.2 192.0.0.1 0.624 0.373 4.30
192.0.0.3 192.0.0.1 0.875 0.243 4.70
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:11:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 44
--- 15:11:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 38
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:10:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 43
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 37

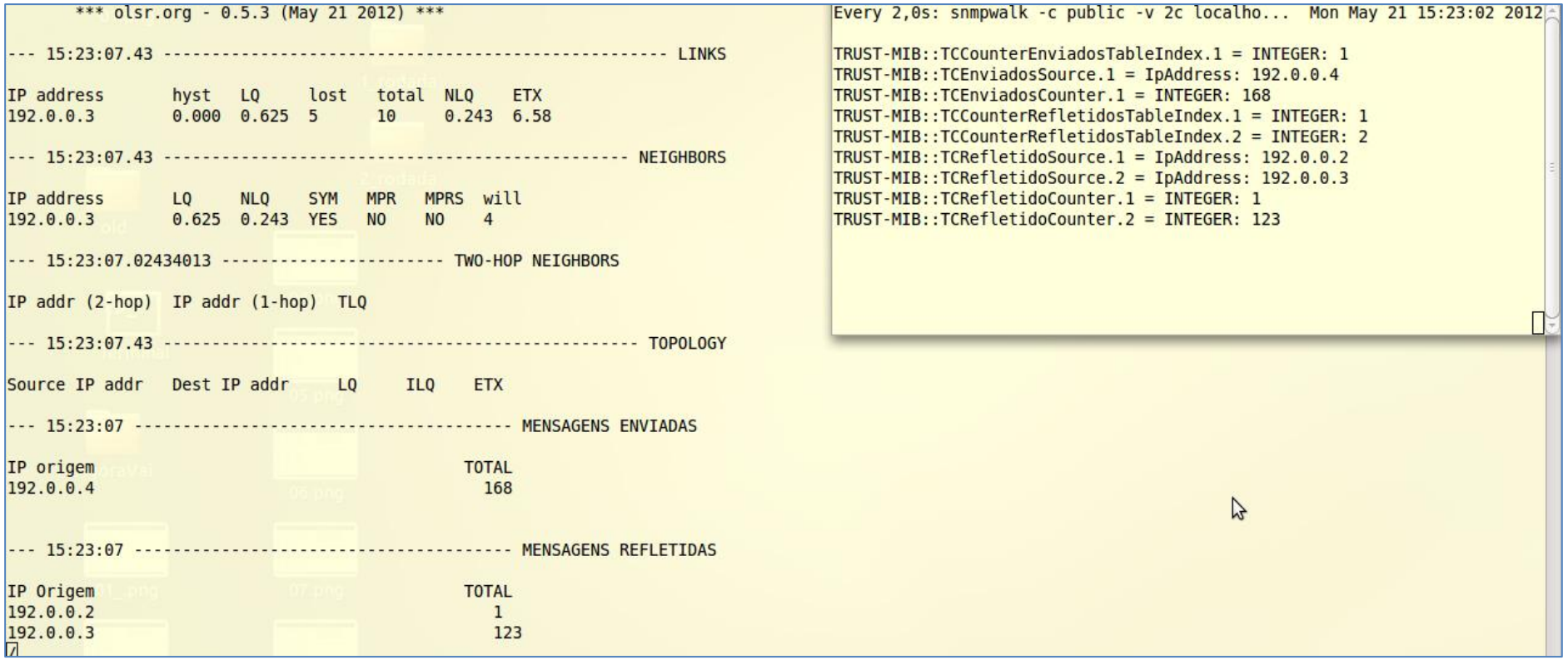

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:13:04.63 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 15:13:04.63 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 15:13:04.02633524 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.033
--- 15:13:04.63 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.498 8.39
192.0.0.3 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:13:04 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 70
--- 15:13:04 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 56
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:13:01 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 68
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 54

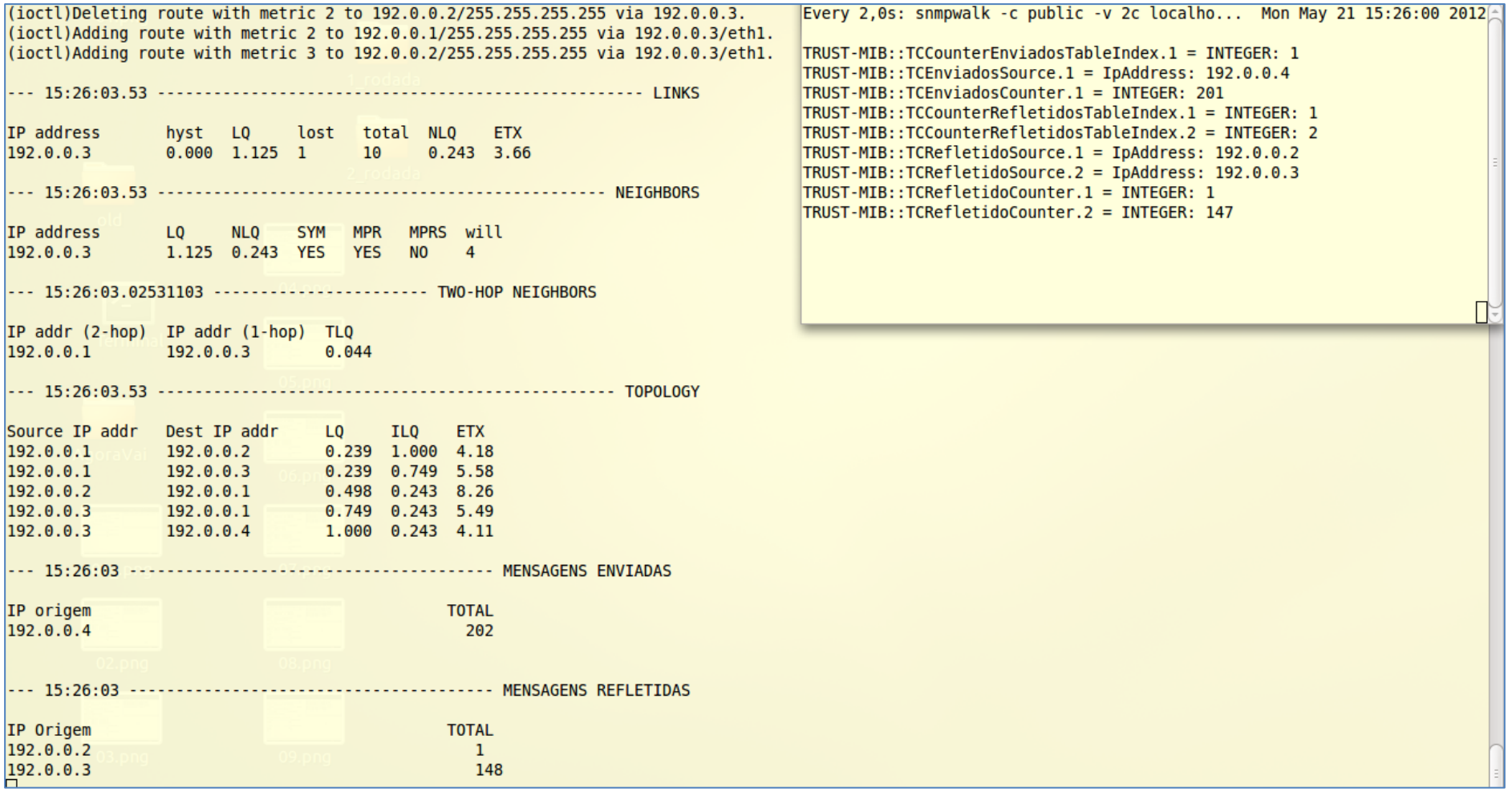

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:15:09.53 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.000 2 10 0.243 4.11
--- 15:15:09.53 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.000 0.243 YES YES NO 4
--- 15:15:09.02539072 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.182
--- 15:15:09.53 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 1.000 0.624 1.60
192.0.0.2 192.0.0.1 1.000 0.243 4.11
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:15:09 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 94
--- 15:15:09 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 76
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:15:08 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 93
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 75

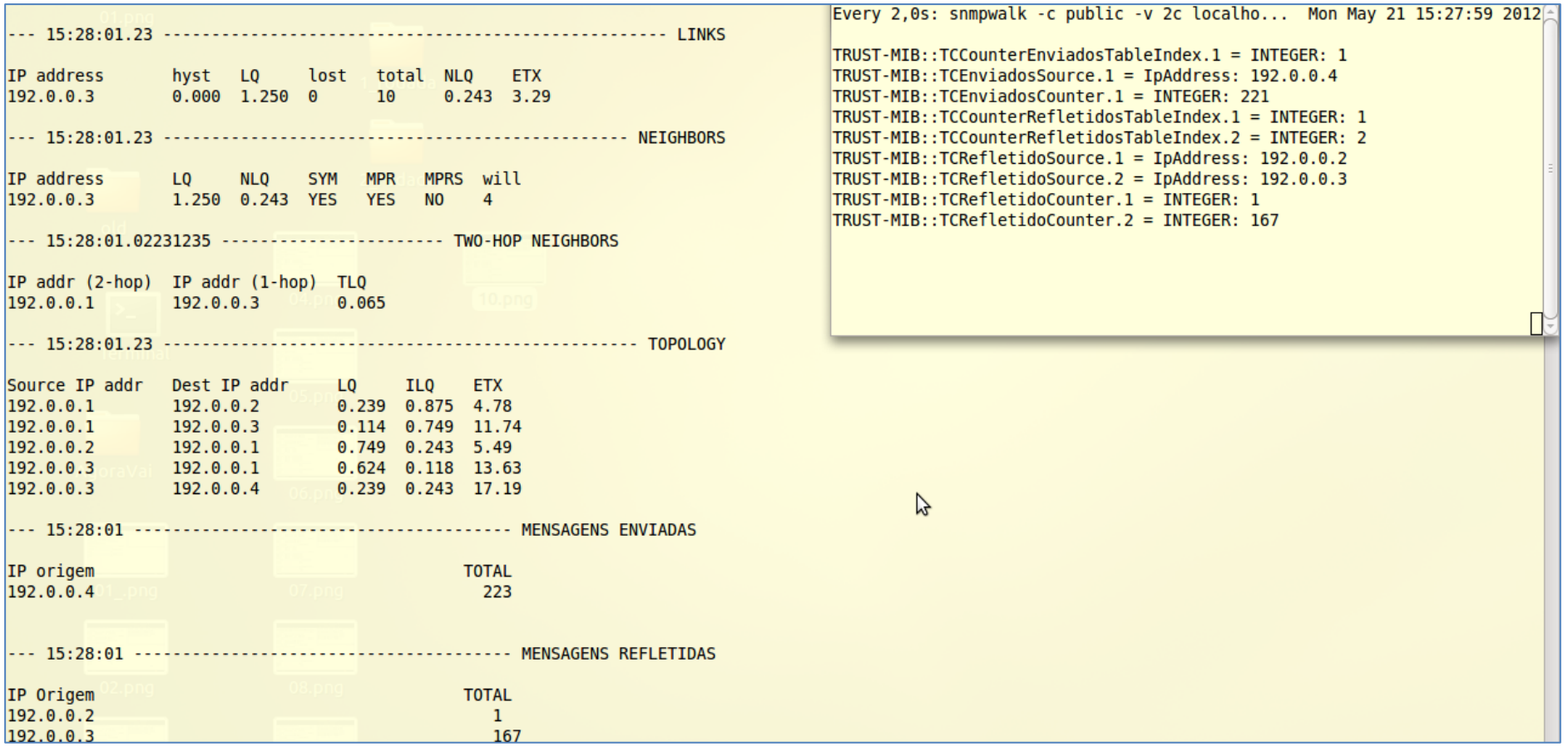

IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.625 5 10 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:17:01.62 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.625 0.000 YES NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:17:01.02628785 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.037
192.0.0.2 192.0.0.3 0.030
192.0.0.3 192.0.0.2 0.000
--- 15:17:01.62 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.498 8.39
192.0.0.2 192.0.0.1 0.749 0.243 5.49
192.0.0.3 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.2 1.000 0.749 1.34
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:17:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 115
--- 15:17:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 91
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:16:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 114
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 90

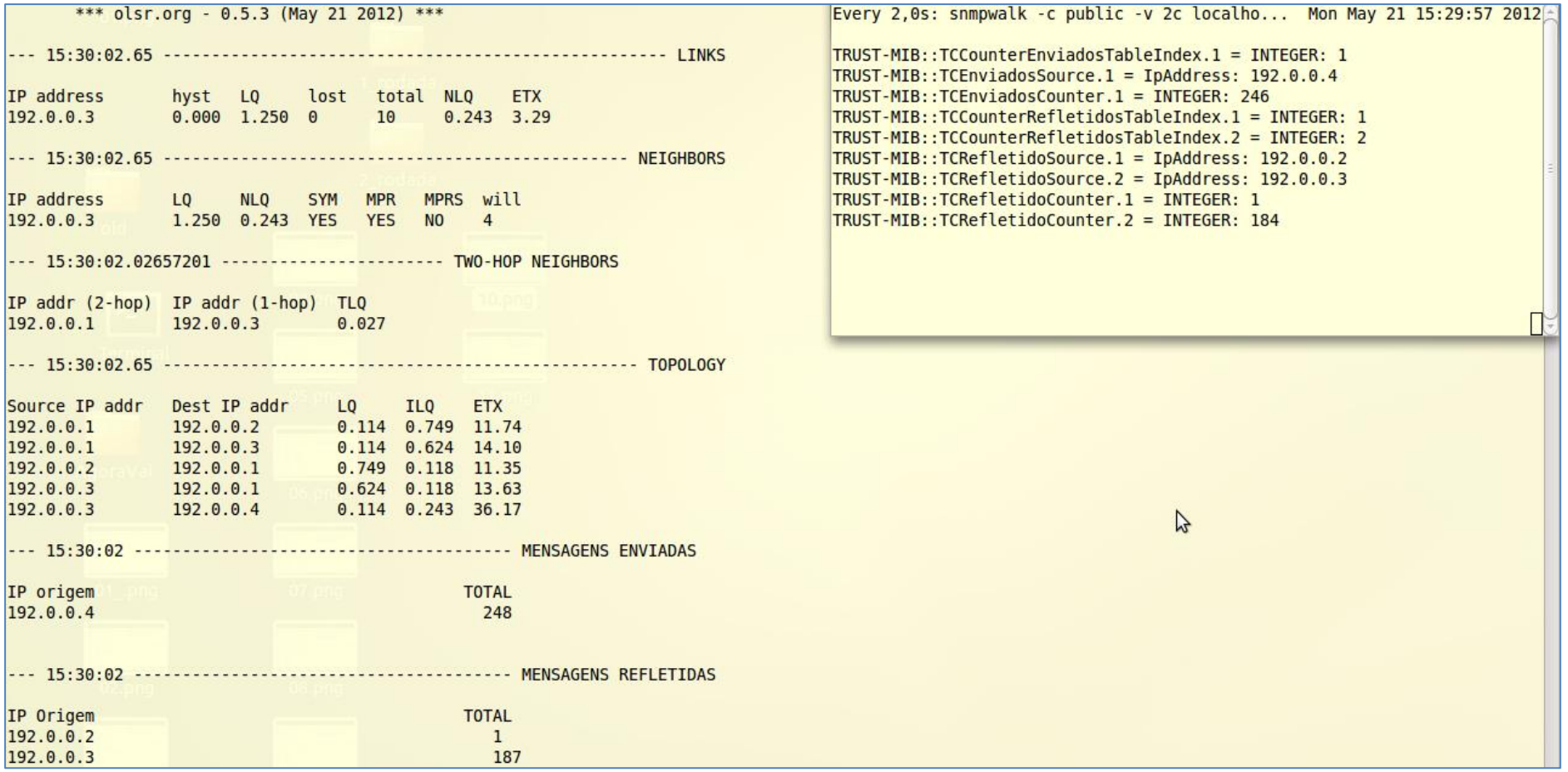

--- 15:19:00.30 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.500 6 10 0.000 0.00
192.0.0.3 0.000 1.000 2 10 1.000 1.00
--- 15:19:00.30 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.500 0.000 NO NO NO 4
192.0.0.3 1.000 1.000 YES YES NO 4
--- 15:19:00.02302605 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.066
192.0.0.2 192.0.0.3 0.000
--- 15:19:00.30 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 1.000 0.749 1.34
192.0.0.1 192.0.0.3 0.239 0.749 5.58
192.0.0.3 192.0.0.1 0.749 0.118 11.35
192.0.0.3 192.0.0.4 0.749 1.000 1.34
--- 15:19:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 138
--- 15:19:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 106
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:18:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 138
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 106

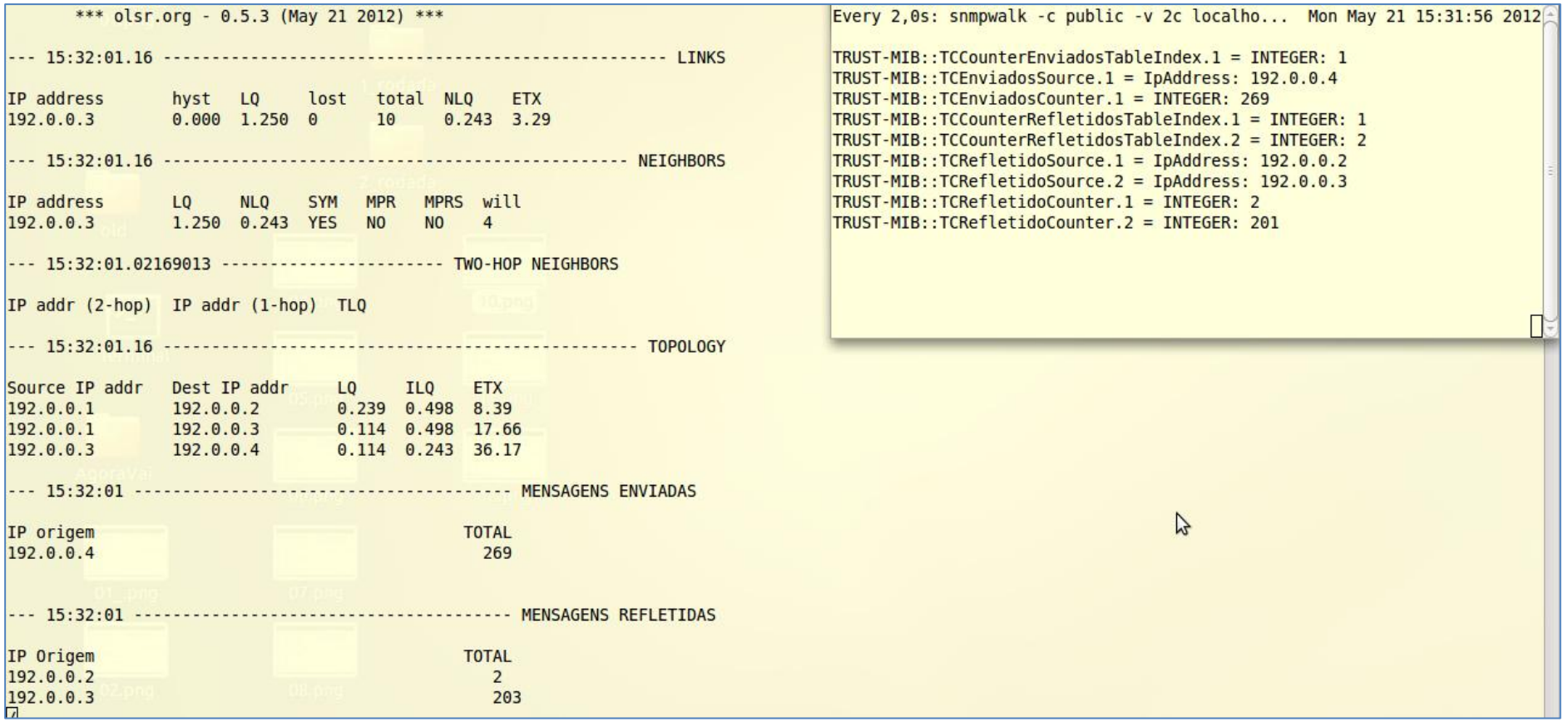

*** olsr.org - 0.5.3 (May 21 2012) ***
(ioctl)Deleting route with metric 3 to 192.0.0.2/255.255.255.255 via 192.0.0.3.
(ioctl)Deleting route with metric 2 to 192.0.0.1/255.255.255.255 via 192.0.0.3.
--- 15:21:00.78 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.200 2 3 0.000 0.00
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 15:21:00.78 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.200 0.000 YES NO NO 4
192.0.0.3 1.125 0.243 YES NO YES 4
--- 15:21:00.02782668 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 15:21:00.78 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.3 192.0.0.1 0.000 0.118 0.00
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:21:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 160
--- 15:21:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 122
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:20:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 157
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 120

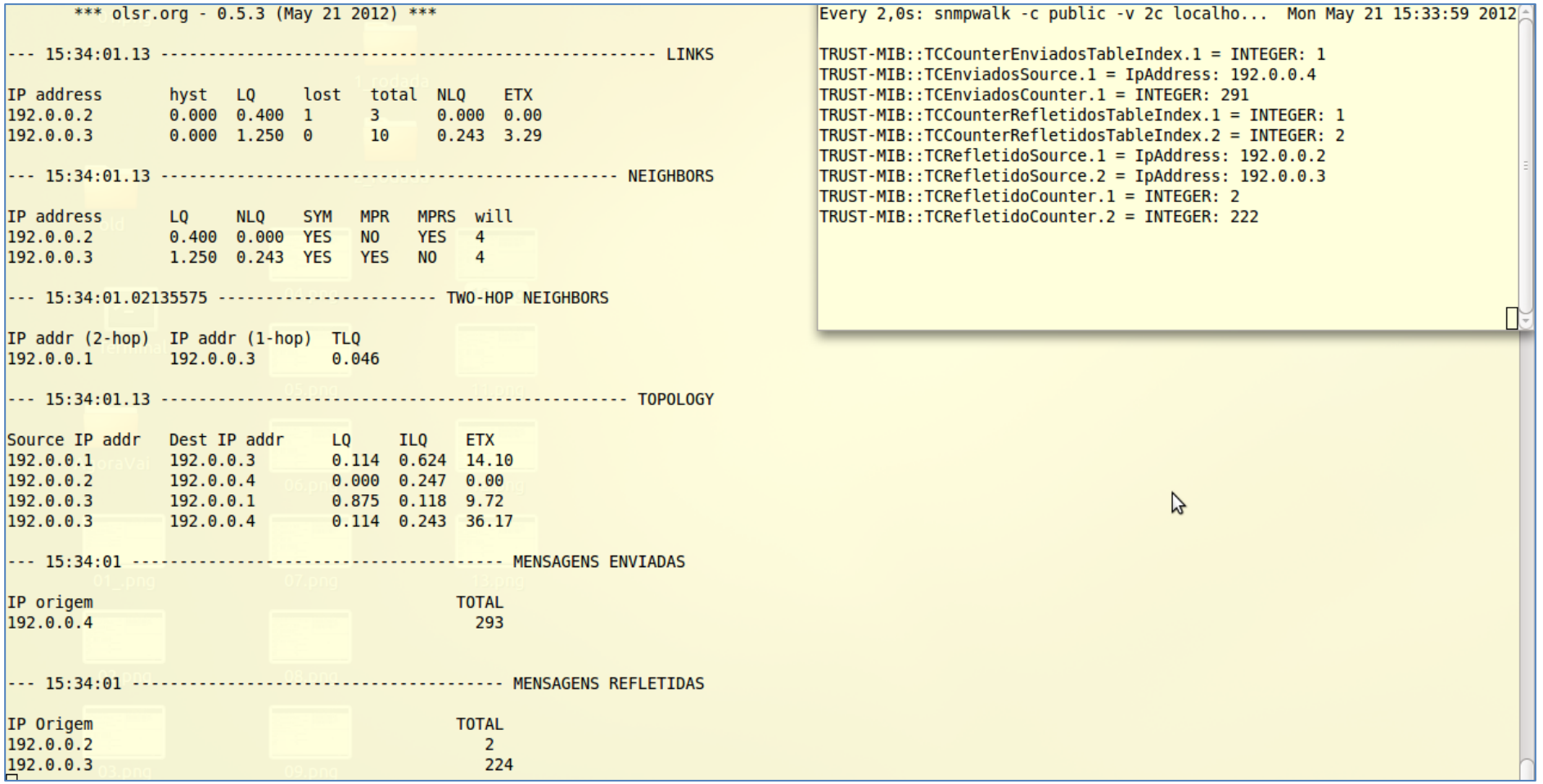

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:23:07.43 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 0.625 5 10 0.243 6.58
--- 15:23:07.43 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 0.625 0.243 YES NO NO 4
--- 15:23:07.02434013 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 15:23:07.43 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 15:23:07 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 168
--- 15:23:07 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 123
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:23:02 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 168
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 123

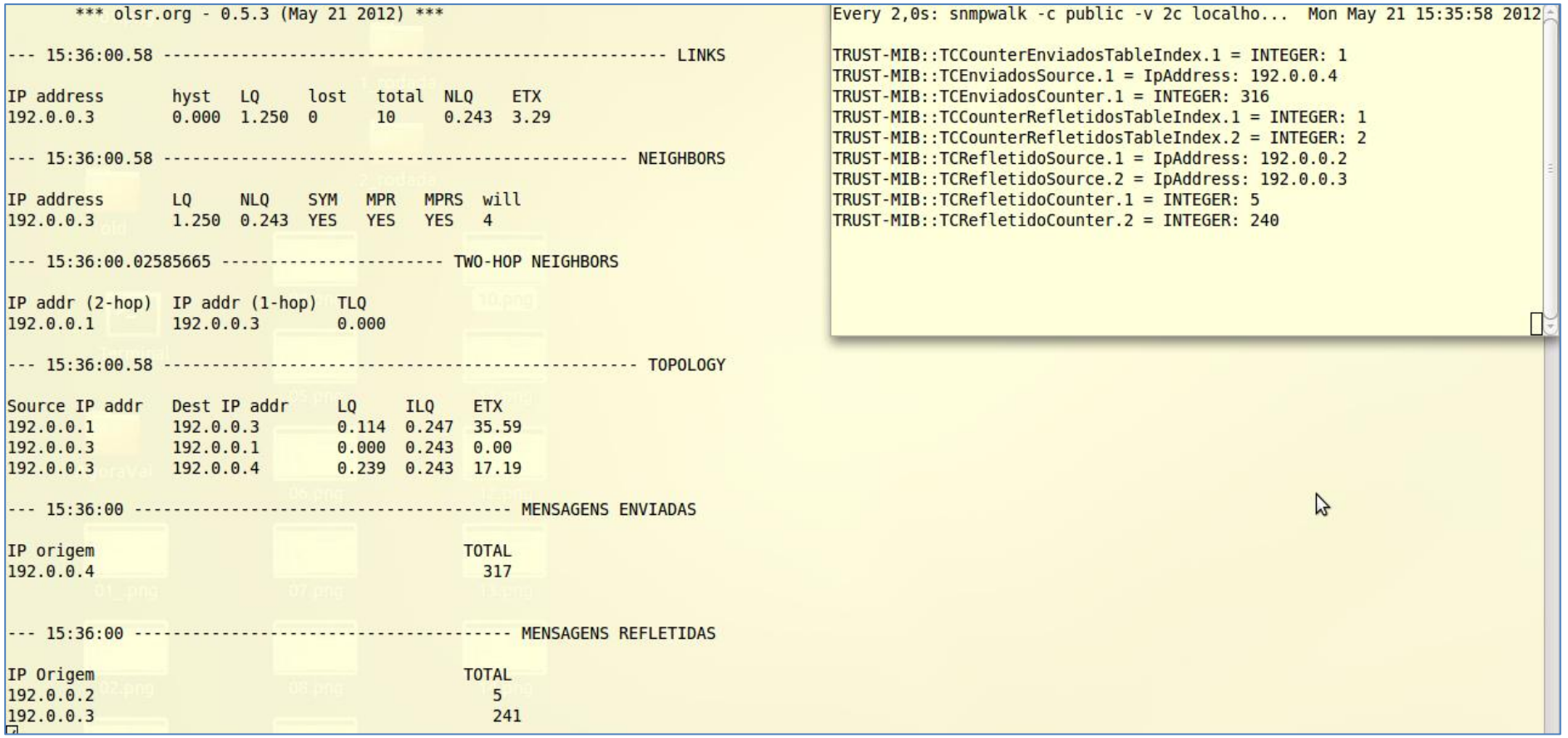

(ioctl)Deleting route with metric 2 to 192.0.0.2/255.255.255.255 via 192.0.0.3.
(ioctl)Adding route with metric 2 to 192.0.0.1/255.255.255.255 via 192.0.0.3/eth1.
(ioctl)Adding route with metric 3 to 192.0.0.2/255.255.255.255 via 192.0.0.3/eth1.
--- 15:26:03.53 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 15:26:03.53 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 15:26:03.02531103 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.044
--- 15:26:03.53 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 1.000 4.18
192.0.0.1 192.0.0.3 0.239 0.749 5.58
192.0.0.2 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.1 0.749 0.243 5.49
192.0.0.3 192.0.0.4 1.000 0.243 4.11
--- 15:26:03 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 202
--- 15:26:03 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 148
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:26:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 201
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 147

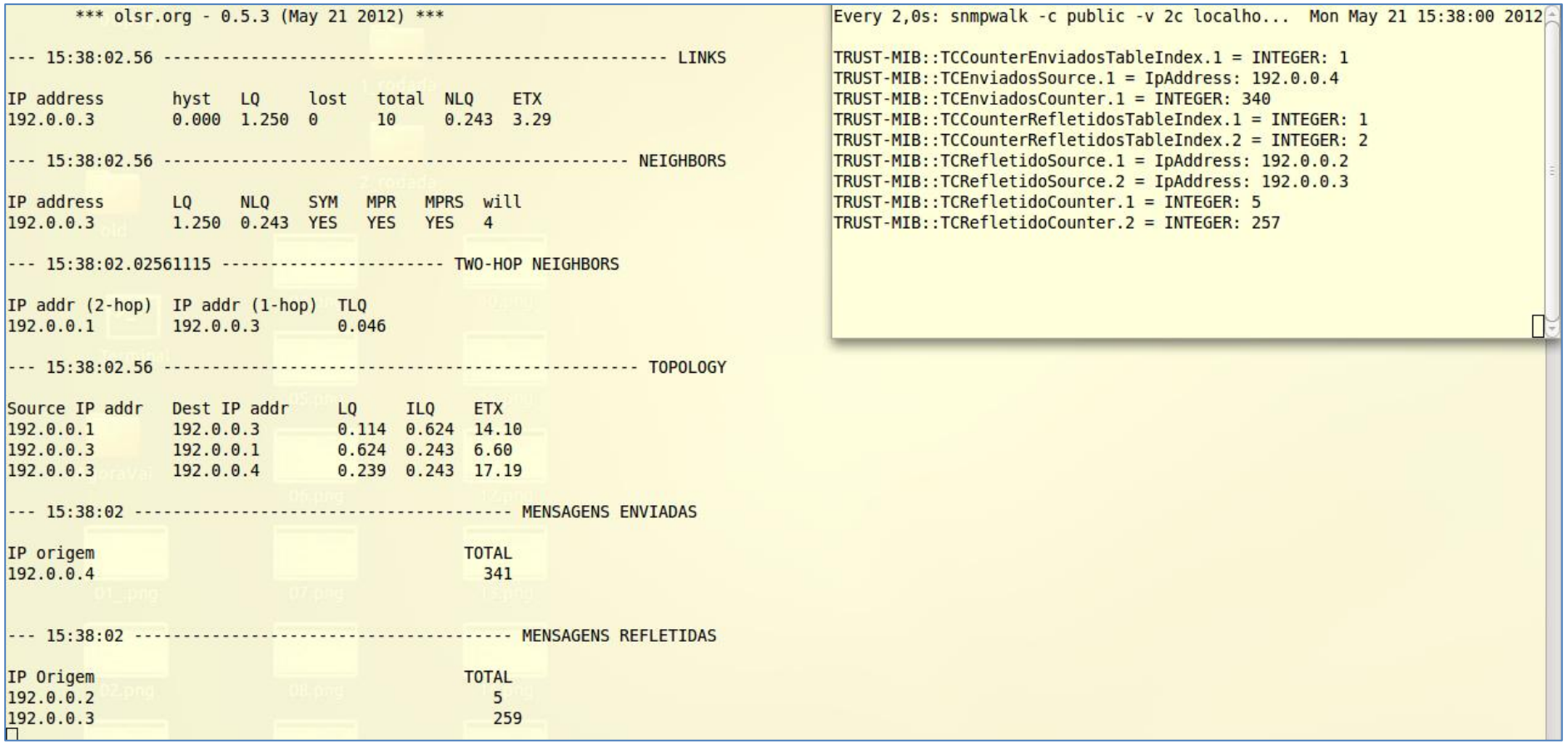

--- 15:28:01.23 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:28:01.23 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:28:01.02231235 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.065
--- 15:28:01.23 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.875 4.78
192.0.0.1 192.0.0.3 0.114 0.749 11.74
192.0.0.2 192.0.0.1 0.749 0.243 5.49
192.0.0.3 192.0.0.1 0.624 0.118 13.63
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:28:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 223
--- 15:28:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 167
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:27:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 221
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 167

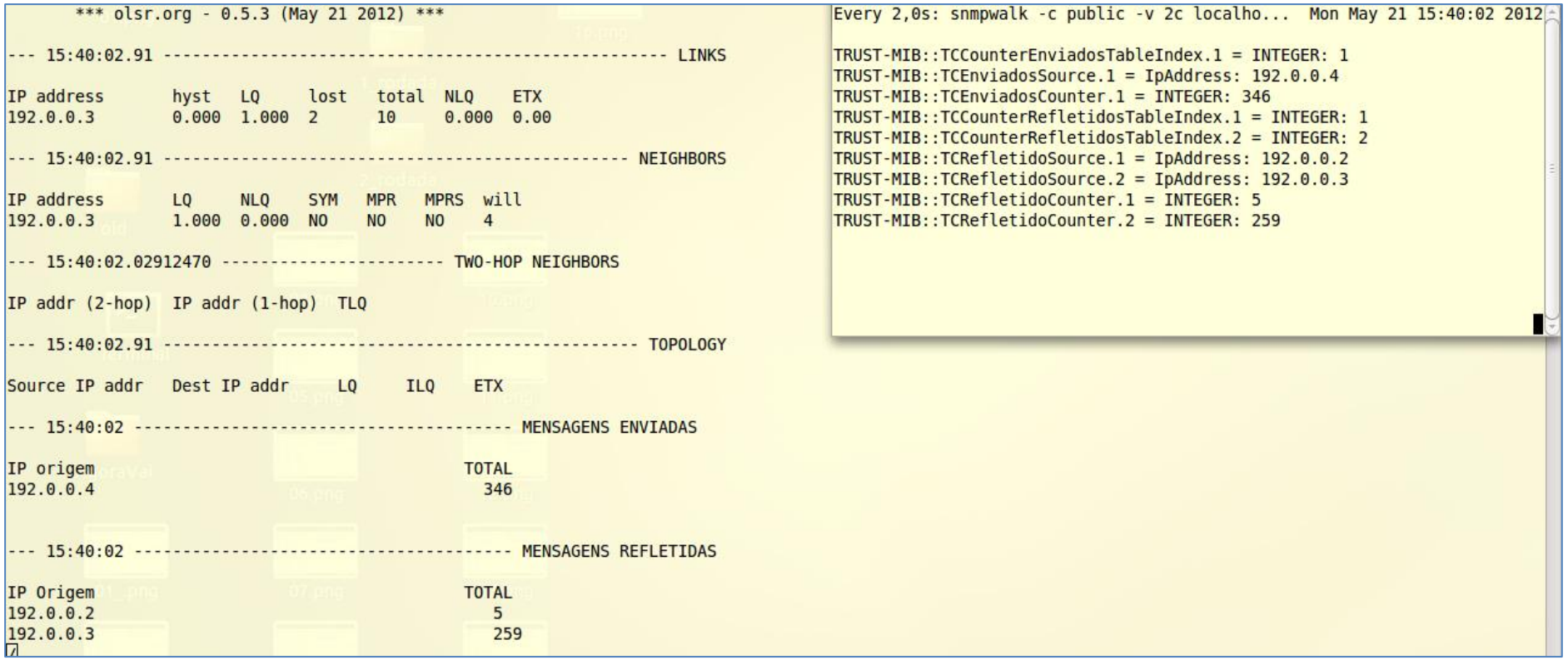

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:30:02.65 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:30:02.65 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:30:02.02657201 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.027
--- 15:30:02.65 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.749 11.74
192.0.0.1 192.0.0.3 0.114 0.624 14.10
192.0.0.2 192.0.0.1 0.749 0.118 11.35
192.0.0.3 192.0.0.1 0.624 0.118 13.63
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:30:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 248
--- 15:30:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 187
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:29:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 246
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 184


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:32:01.16 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:32:01.16 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES NO NO 4
--- 15:32:01.02169013 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 15:32:01.16 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.498 8.39
192.0.0.1 192.0.0.3 0.114 0.498 17.66
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:32:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 269
--- 15:32:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 2
192.0.0.3 203
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:31:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 269
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 2
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 201


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:34:01.13 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.400 1 3 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:34:01.13 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.400 0.000 YES NO YES 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:34:01.02135575 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.046
--- 15:34:01.13 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.624 14.10
192.0.0.2 192.0.0.4 0.000 0.247 0.00
192.0.0.3 192.0.0.1 0.875 0.118 9.72
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:34:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 293
--- 15:34:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 2
192.0.0.3 224
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:33:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 291
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 2
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 222

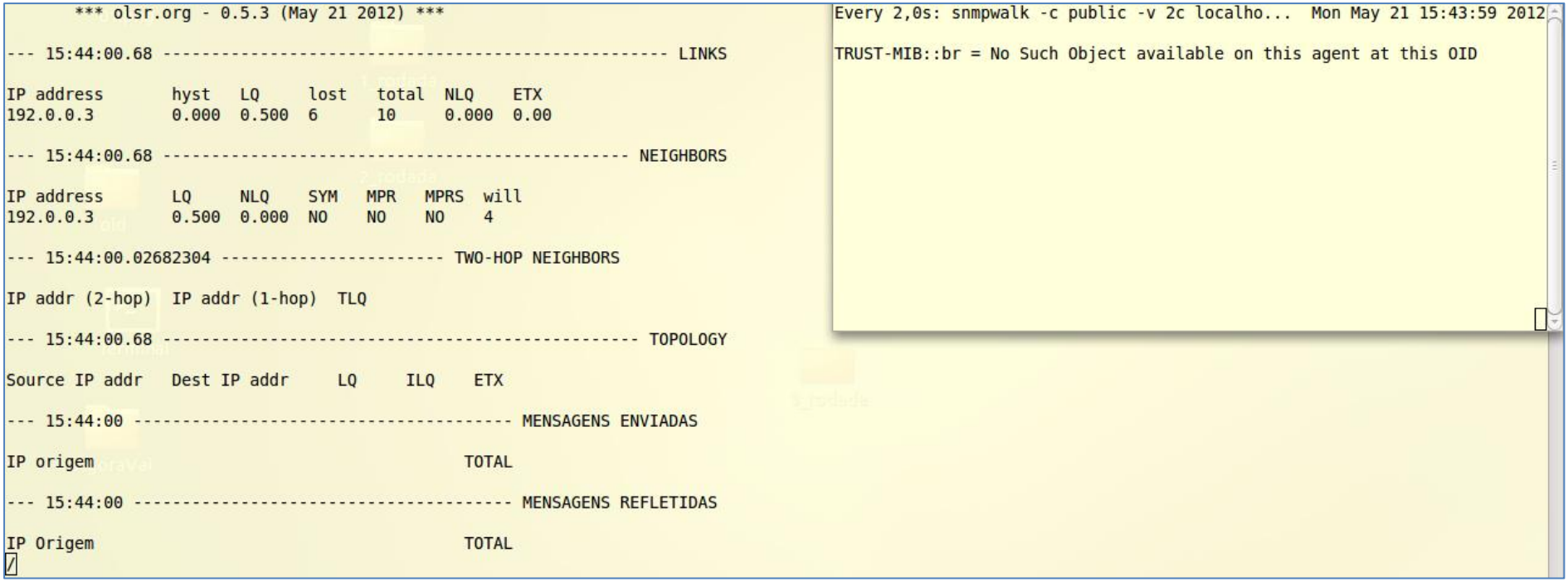

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:36:00.58 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:36:00.58 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES YES 4
--- 15:36:00.02585665 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.000
--- 15:36:00.58 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.247 35.59
192.0.0.3 192.0.0.1 0.000 0.243 0.00
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:36:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 317
--- 15:36:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 5
192.0.0.3 241
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:35:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 316
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 5
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 240

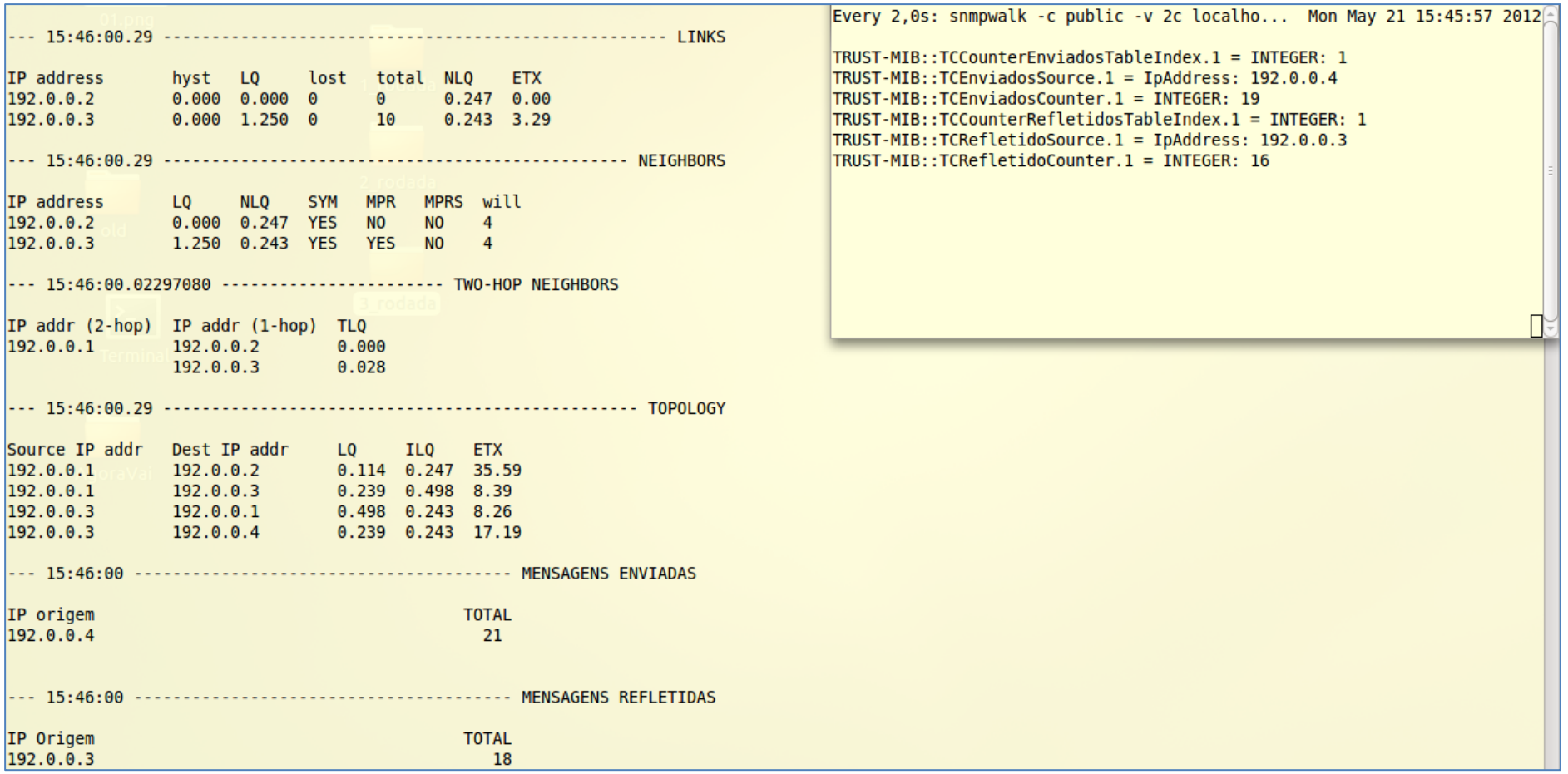

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:38:02.56 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:38:02.56 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES YES 4
--- 15:38:02.02561115 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.046
--- 15:38:02.56 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.624 14.10
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:38:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 341
--- 15:38:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 5
192.0.0.3 259
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:38:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 340
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 5
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 257

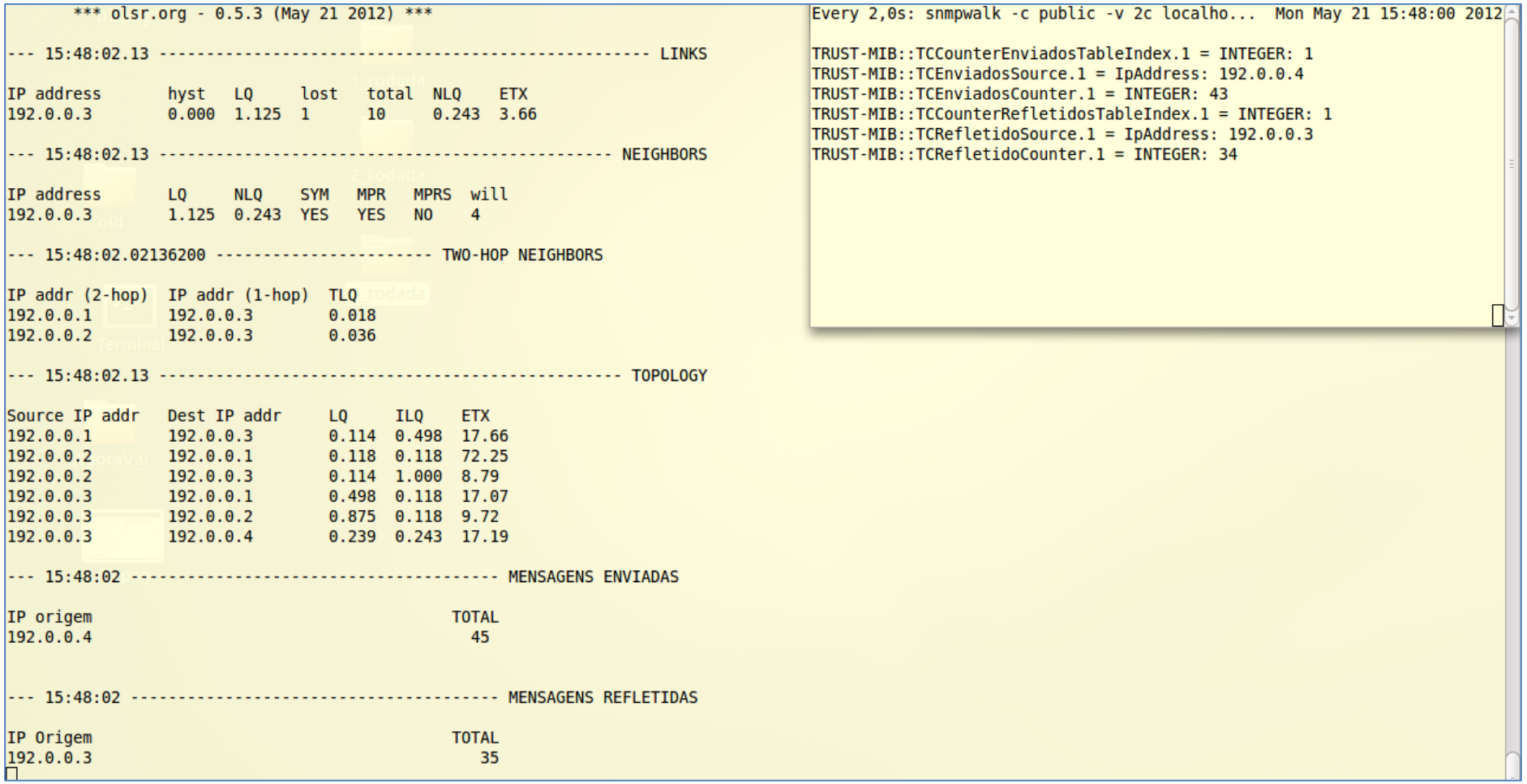

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:40:02.91 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.000 2 10 0.000 0.00
--- 15:40:02.91 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.000 0.000 NO NO NO 4
--- 15:40:02.02912470 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 15:40:02.91 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 15:40:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 346
--- 15:40:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 5
192.0.0.3 259
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:40:02 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 346
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 5
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 259

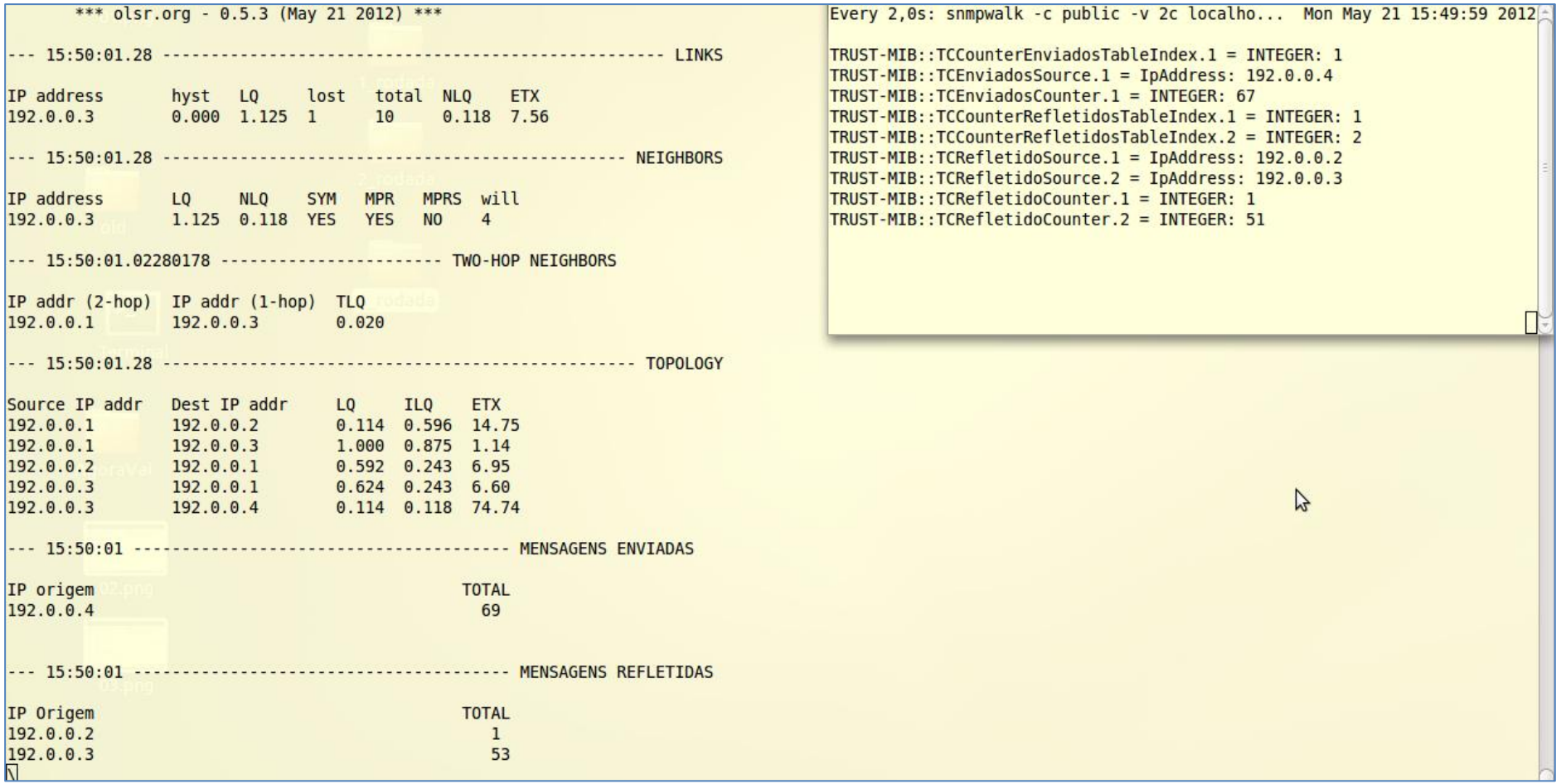
E - SIMULAÇÃO DA TRUST-MIB E OLSRD - Teste 03

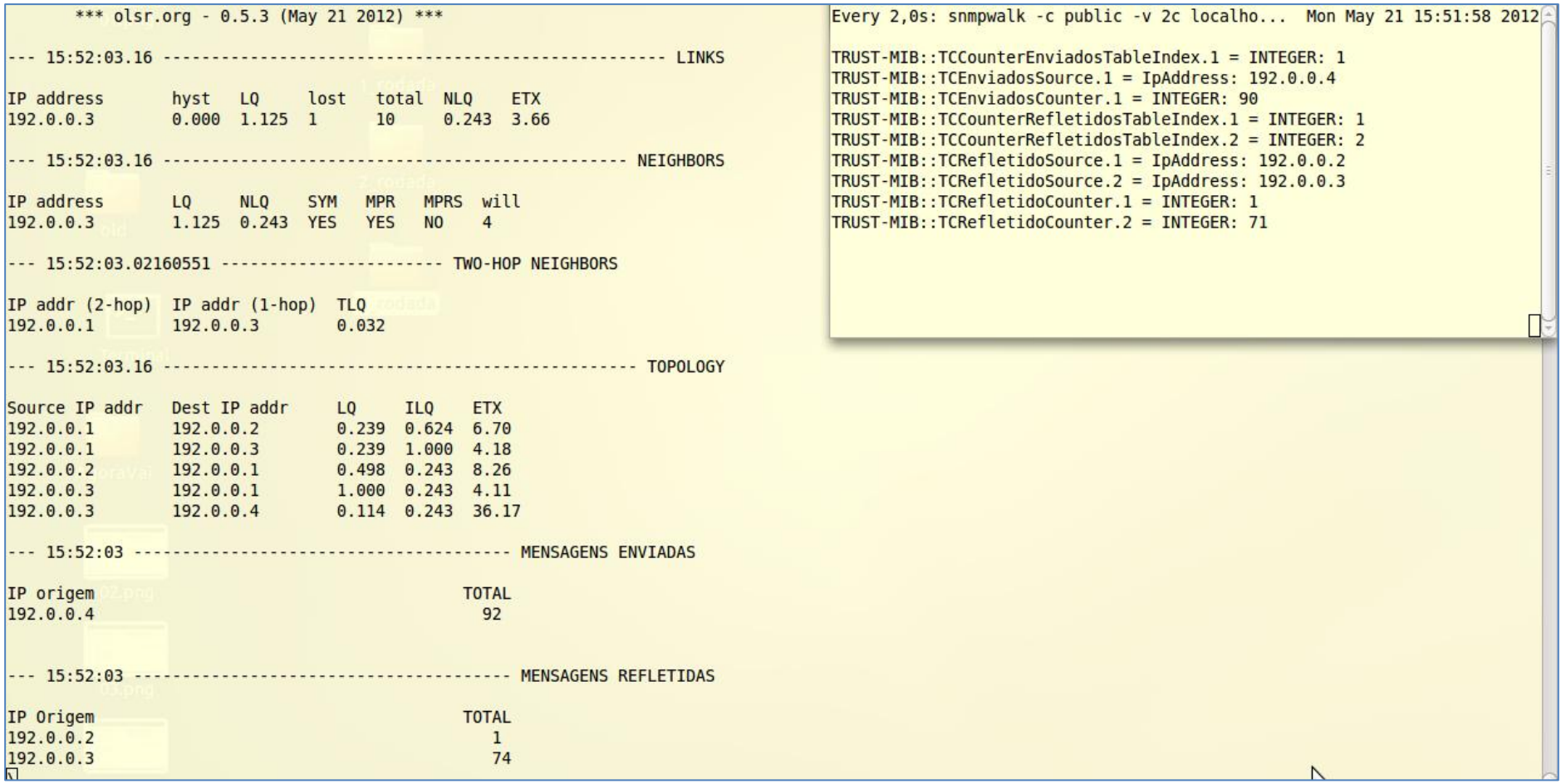
Telas do teste 03 da simulação realizada com o protocolo OLSRD e a TRUST-MIB.

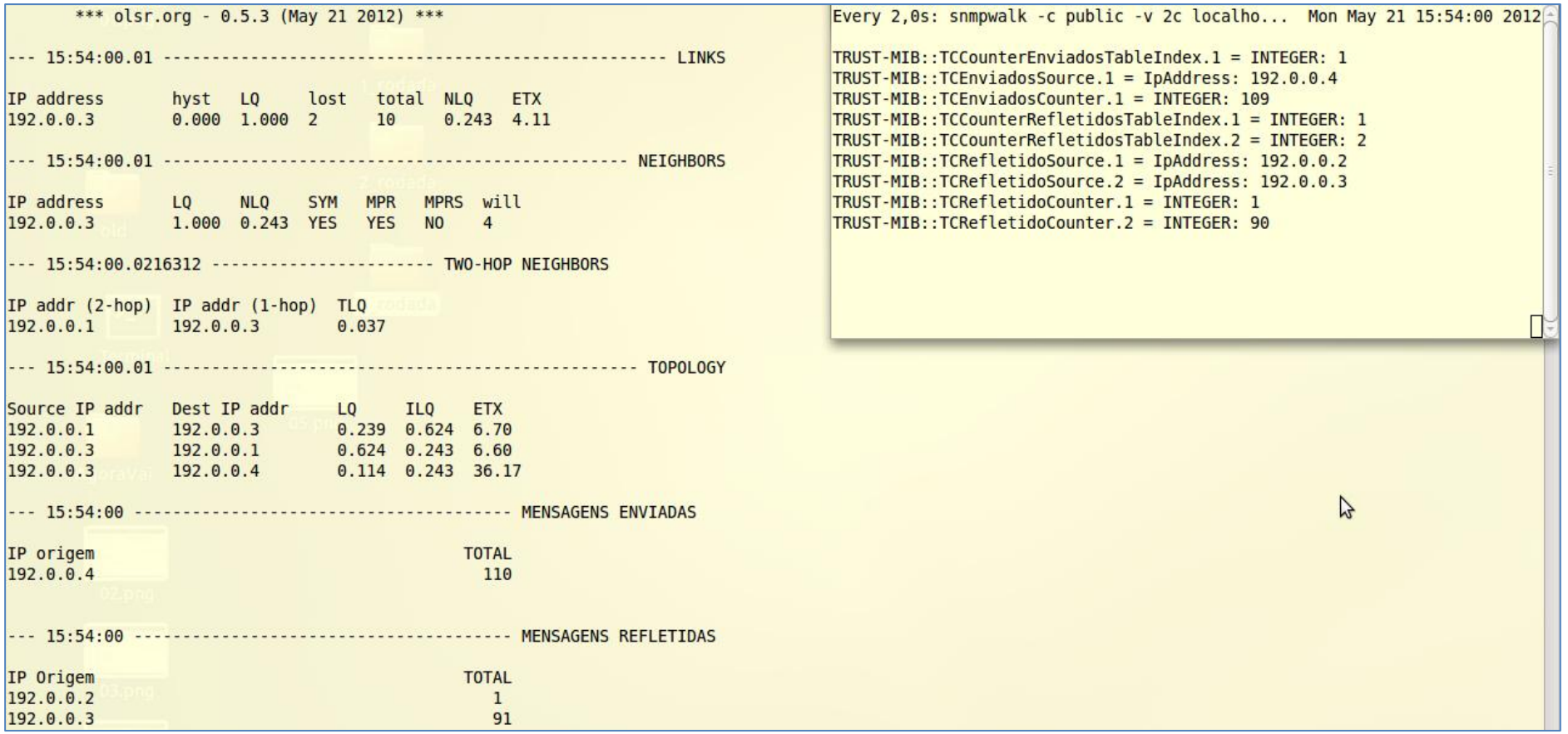


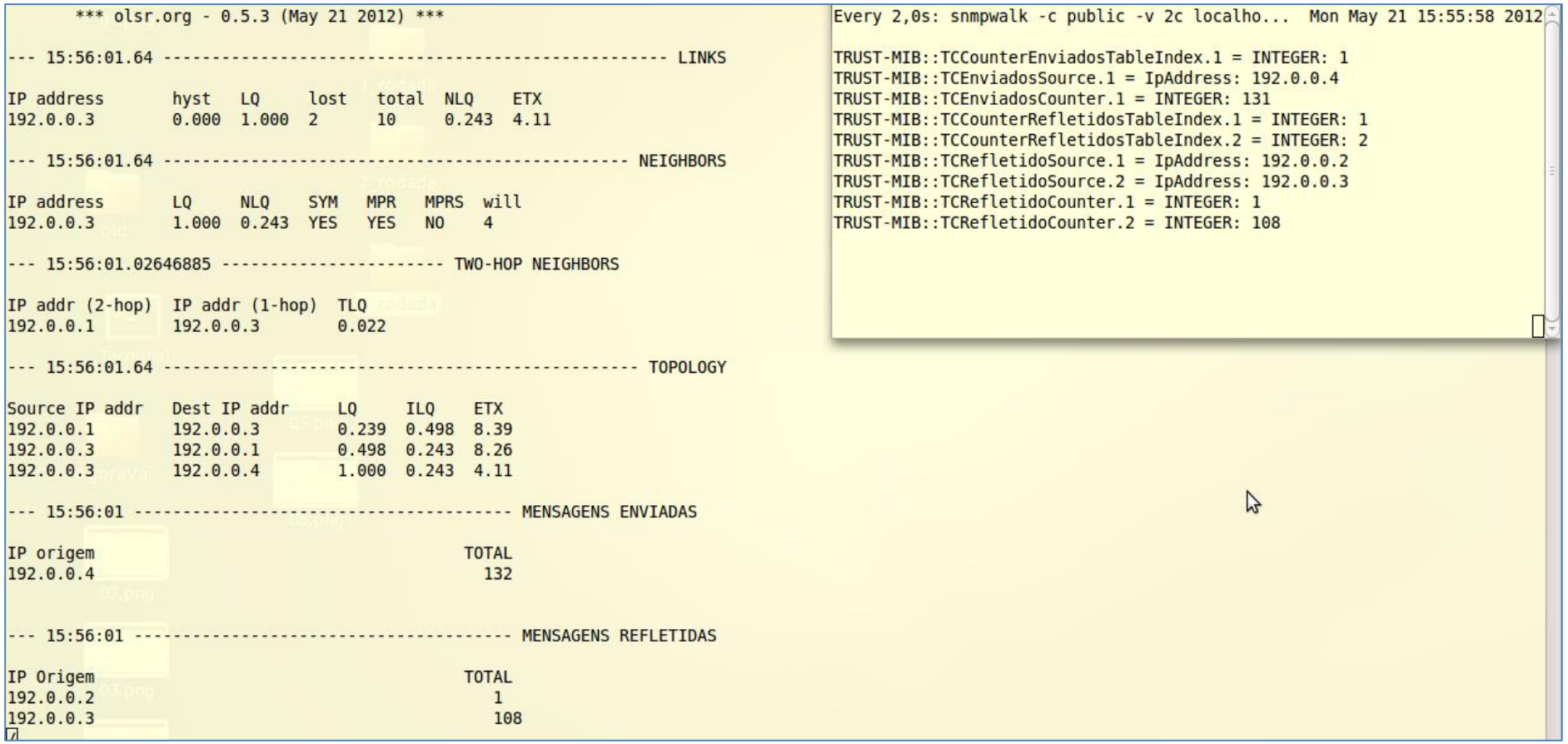

--- 15:46:00.29 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 0 0 0.247 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:46:00.29 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.247 YES NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:46:00.02297080 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.028
--- 15:46:00.29 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.247 35.59
192.0.0.1 192.0.0.3 0.239 0.498 8.39
192.0.0.3 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:46:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 21
--- 15:46:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 18
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:45:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 19
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 16

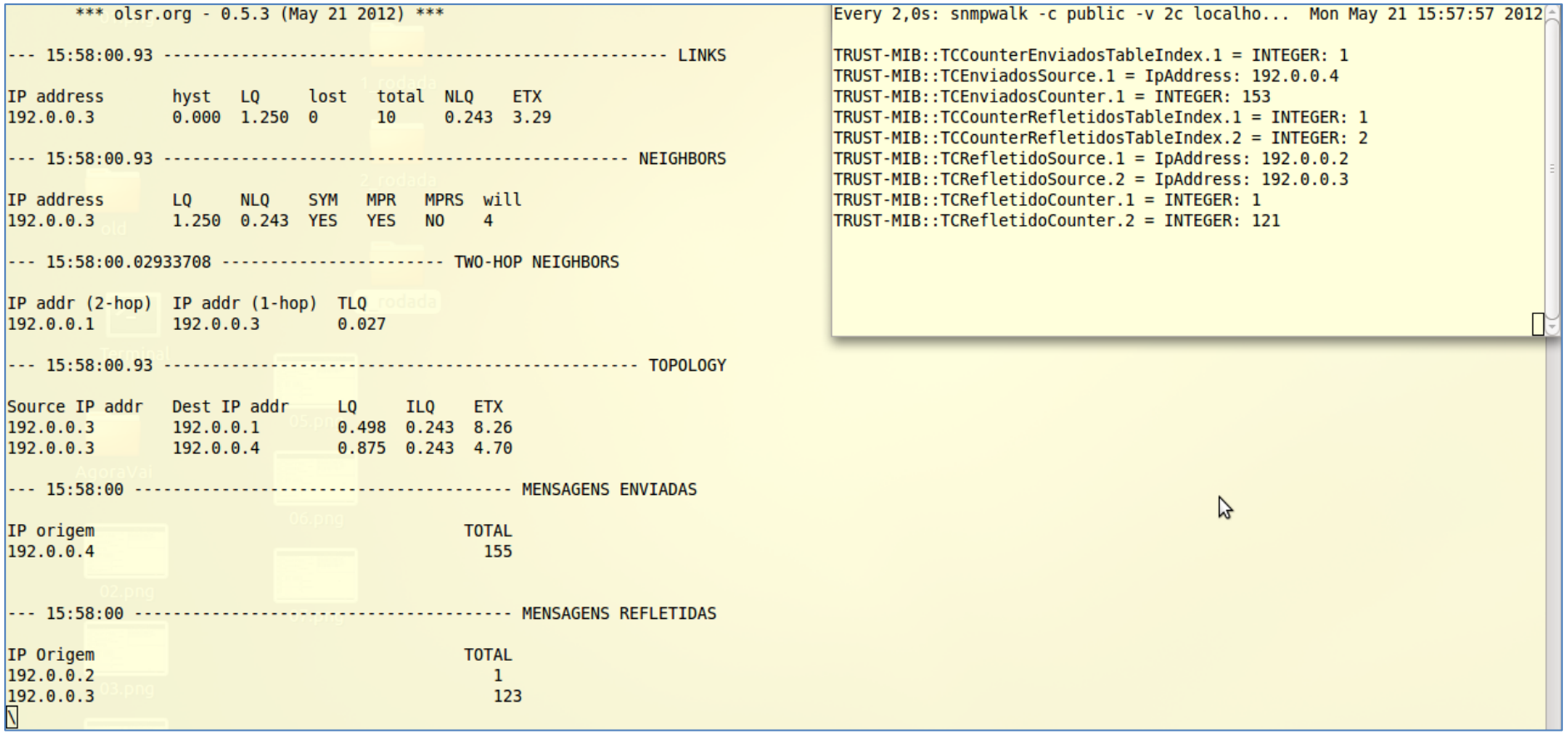

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:48:02.13 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 15:48:02.13 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 15:48:02.02136200 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.018
192.0.0.2 192.0.0.3 0.036
--- 15:48:02.13 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.498 17.66
192.0.0.2 192.0.0.1 0.118 0.118 72.25
192.0.0.2 192.0.0.3 0.114 1.000 8.79
192.0.0.3 192.0.0.1 0.498 0.118 17.07
192.0.0.3 192.0.0.2 0.875 0.118 9.72
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 15:48:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 45
--- 15:48:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 35
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:48:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 43
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 34

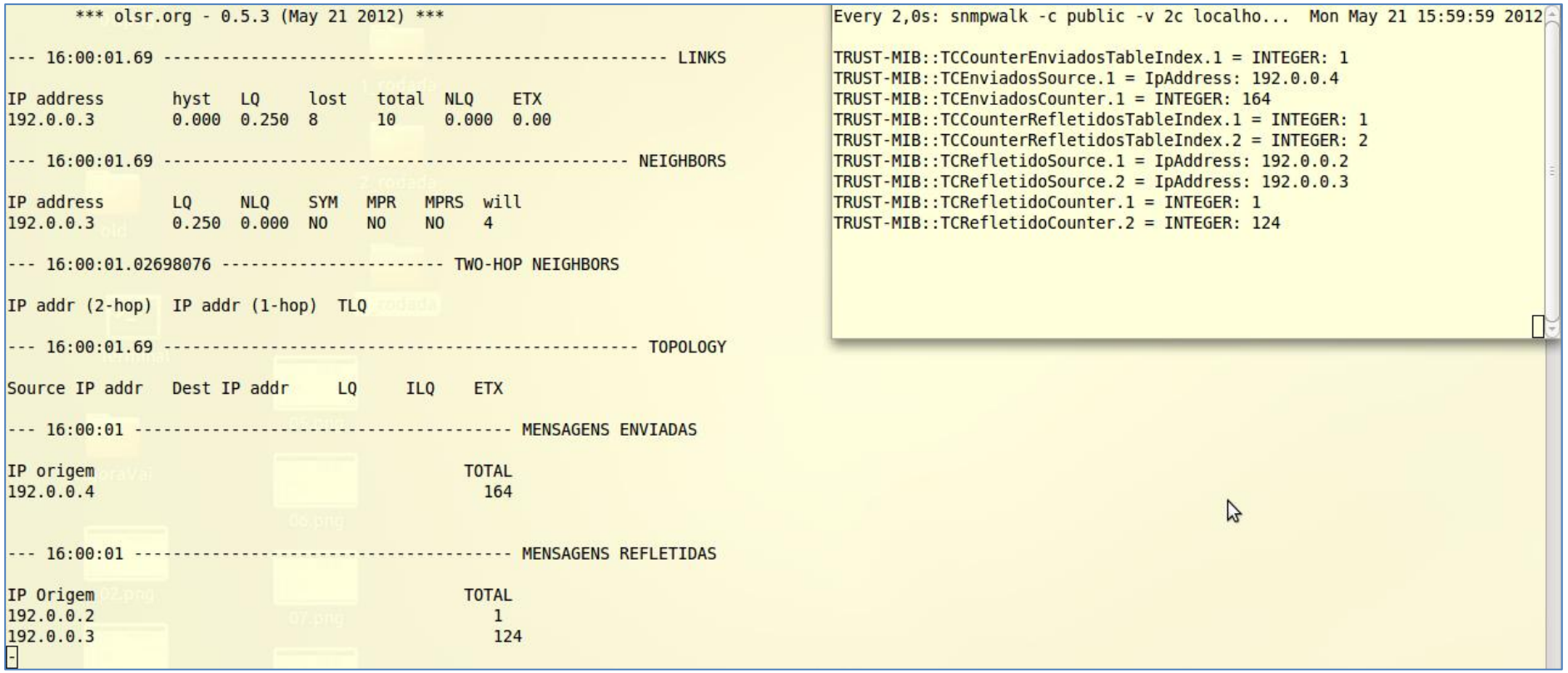

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:50:01.28 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.118 7.56
--- 15:50:01.28 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.118 YES YES NO 4
--- 15:50:01.02280178 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.020
--- 15:50:01.28 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.596 14.75
192.0.0.1 192.0.0.3 1.000 0.875 1.14
192.0.0.2 192.0.0.1 0.592 0.243 6.95
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.4 0.114 0.118 74.74
--- 15:50:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 69
--- 15:50:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 53
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:49:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 67
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 51

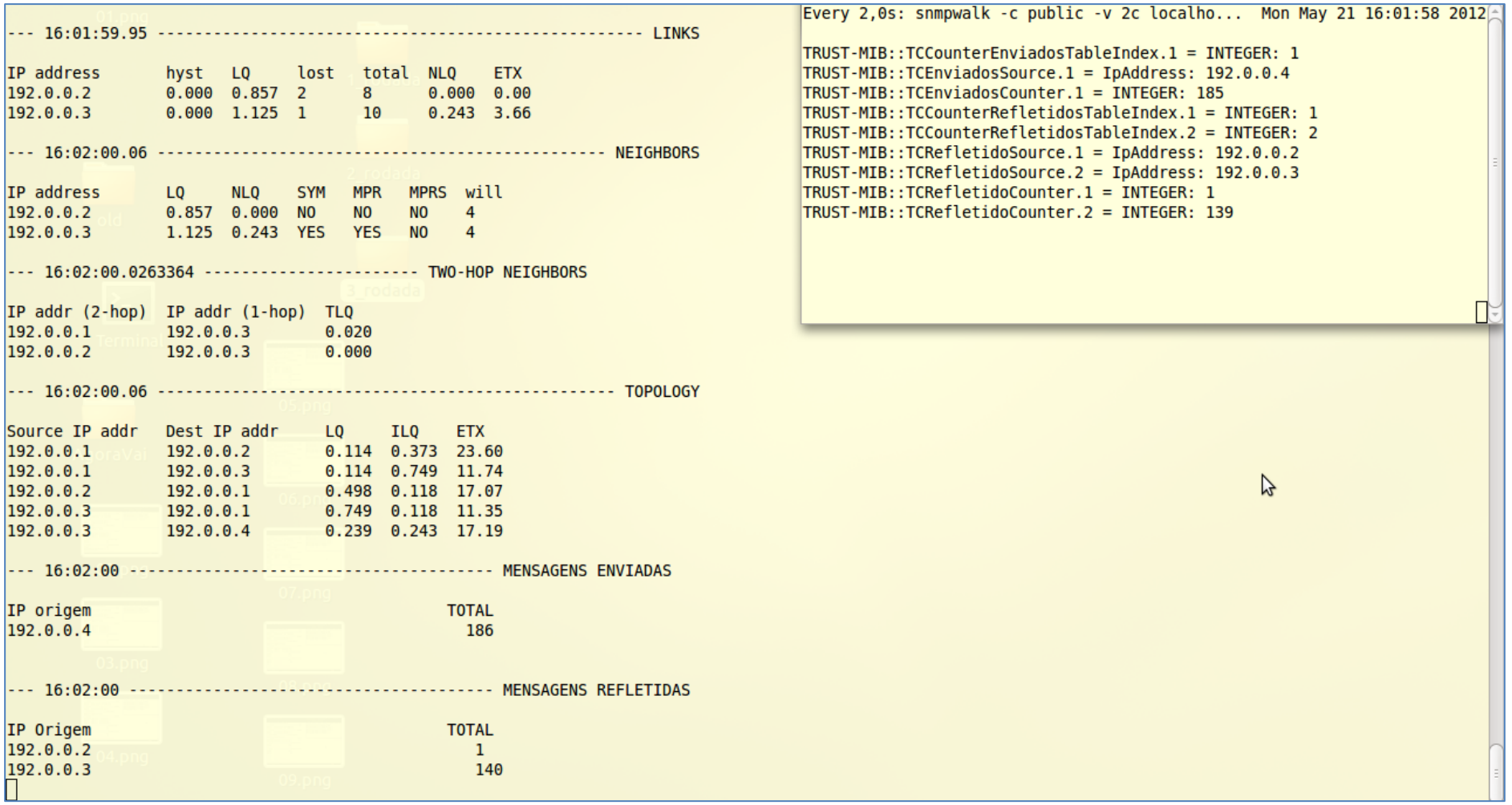

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:52:03.16 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 15:52:03.16 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 15:52:03.02160551 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.032
--- 15:52:03.16 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.624 6.70
192.0.0.1 192.0.0.3 0.239 1.000 4.18
192.0.0.2 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.1 1.000 0.243 4.11
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:52:03 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 92
--- 15:52:03 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 74
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:51:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 90
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 71

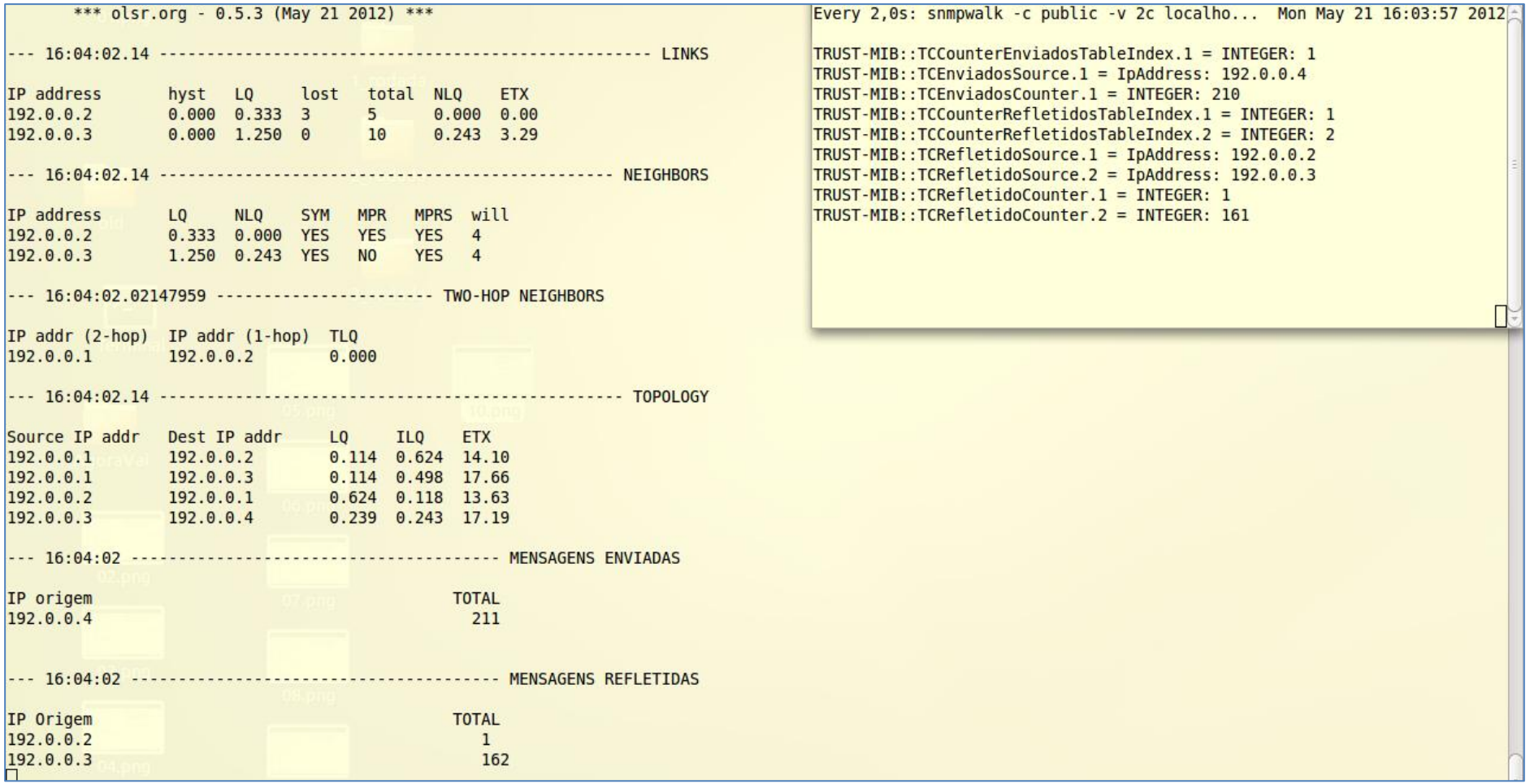

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:54:00.01 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.000 2 10 0.243 4.11
--- 15:54:00.01 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.000 0.243 YES YES NO 4
--- 15:54:00.0216312 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.037
--- 15:54:00.01 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.624 6.70
192.0.0.3 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 15:54:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 110
--- 15:54:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 91
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:54:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 109
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 90

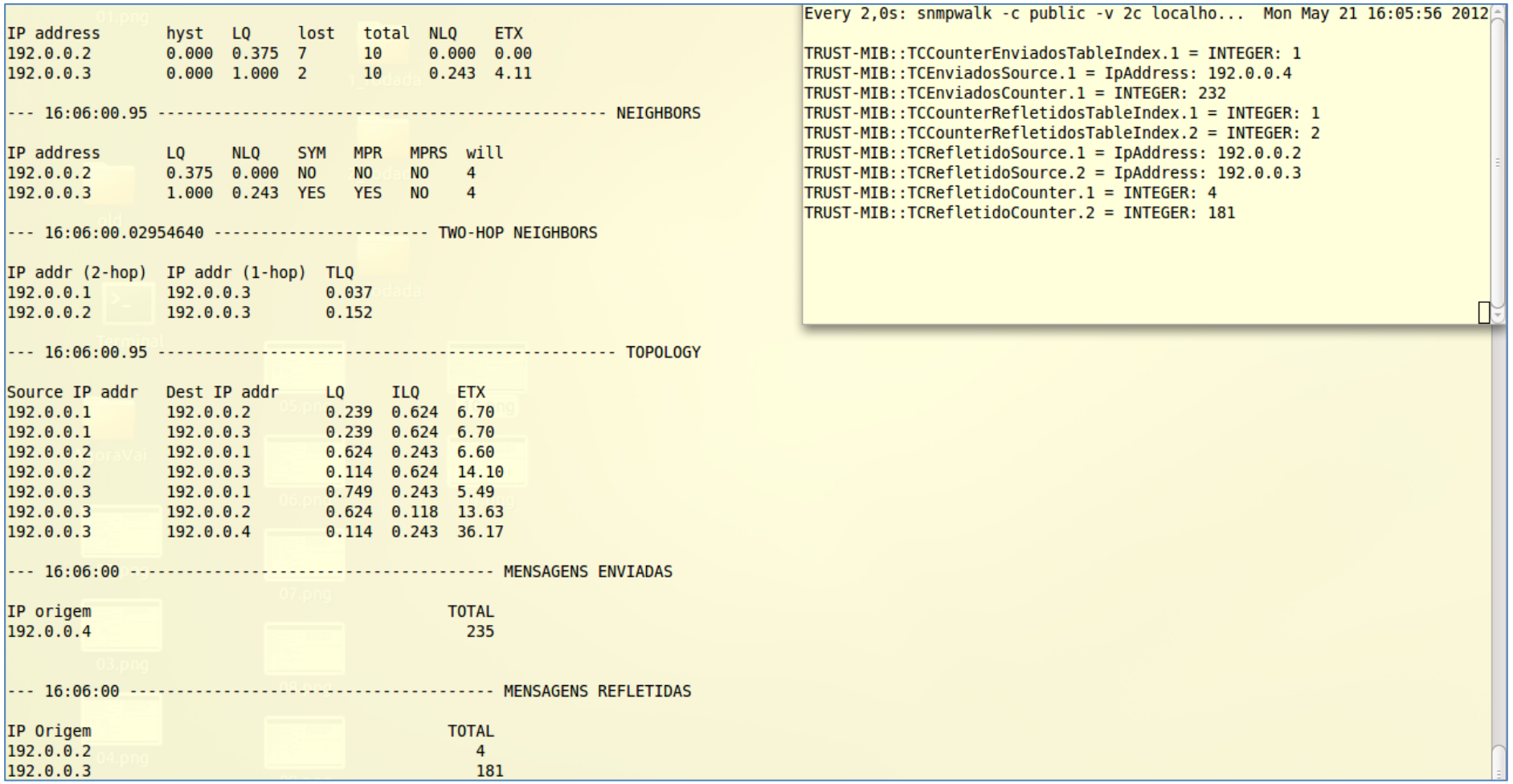

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:56:01.64 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.000 2 10 0.243 4.11
--- 15:56:01.64 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.000 0.243 YES YES NO 4
--- 15:56:01.02646885 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.022
--- 15:56:01.64 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.498 8.39
192.0.0.3 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.4 1.000 0.243 4.11
--- 15:56:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 132
--- 15:56:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 108
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:55:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 131
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 108


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 15:58:00.93 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 15:58:00.93 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 15:58:00.02933708 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.027
--- 15:58:00.93 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.3 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.4 0.875 0.243 4.70
--- 15:58:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 155
--- 15:58:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 123
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:57:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 153
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 121


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:00:01.69 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 0.250 8 10 0.000 0.00
--- 16:00:01.69 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 0.250 0.000 NO NO NO 4
--- 16:00:01.02698076 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 16:00:01.69 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 16:00:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 164
--- 16:00:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 124
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 15:59:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 164
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 124

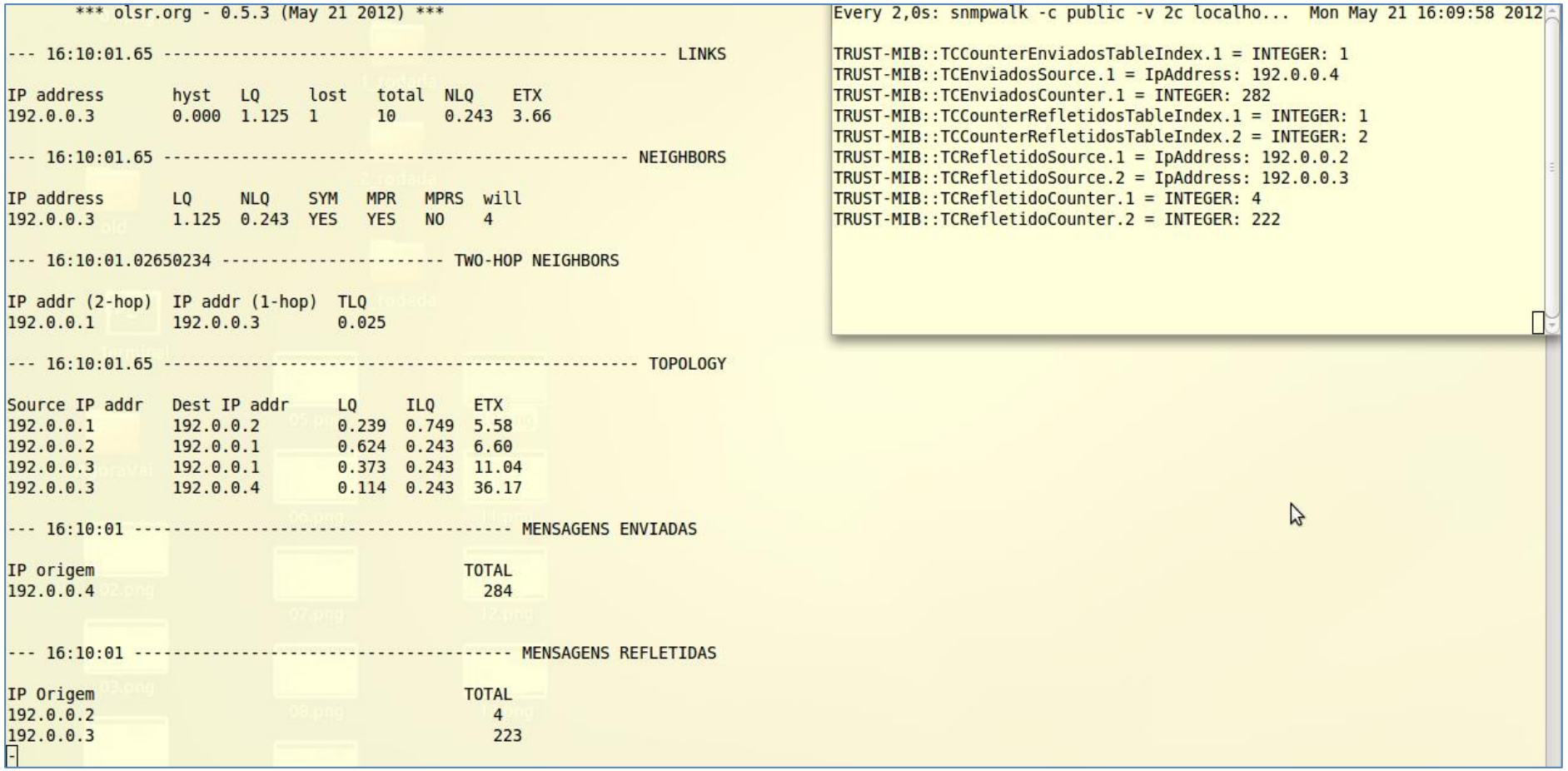

--- 16:01:59.95 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.857 2 8 0.000 0.00
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:02:00.06 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.857 0.000 NO NO NO 4
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:02:00.0263364 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.020
192.0.0.2 192.0.0.3 0.000
--- 16:02:00.06 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.373 23.60
192.0.0.1 192.0.0.3 0.114 0.749 11.74
192.0.0.2 192.0.0.1 0.498 0.118 17.07
192.0.0.3 192.0.0.1 0.749 0.118 11.35
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:02:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 186
--- 16:02:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 140
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:01:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 185
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 139

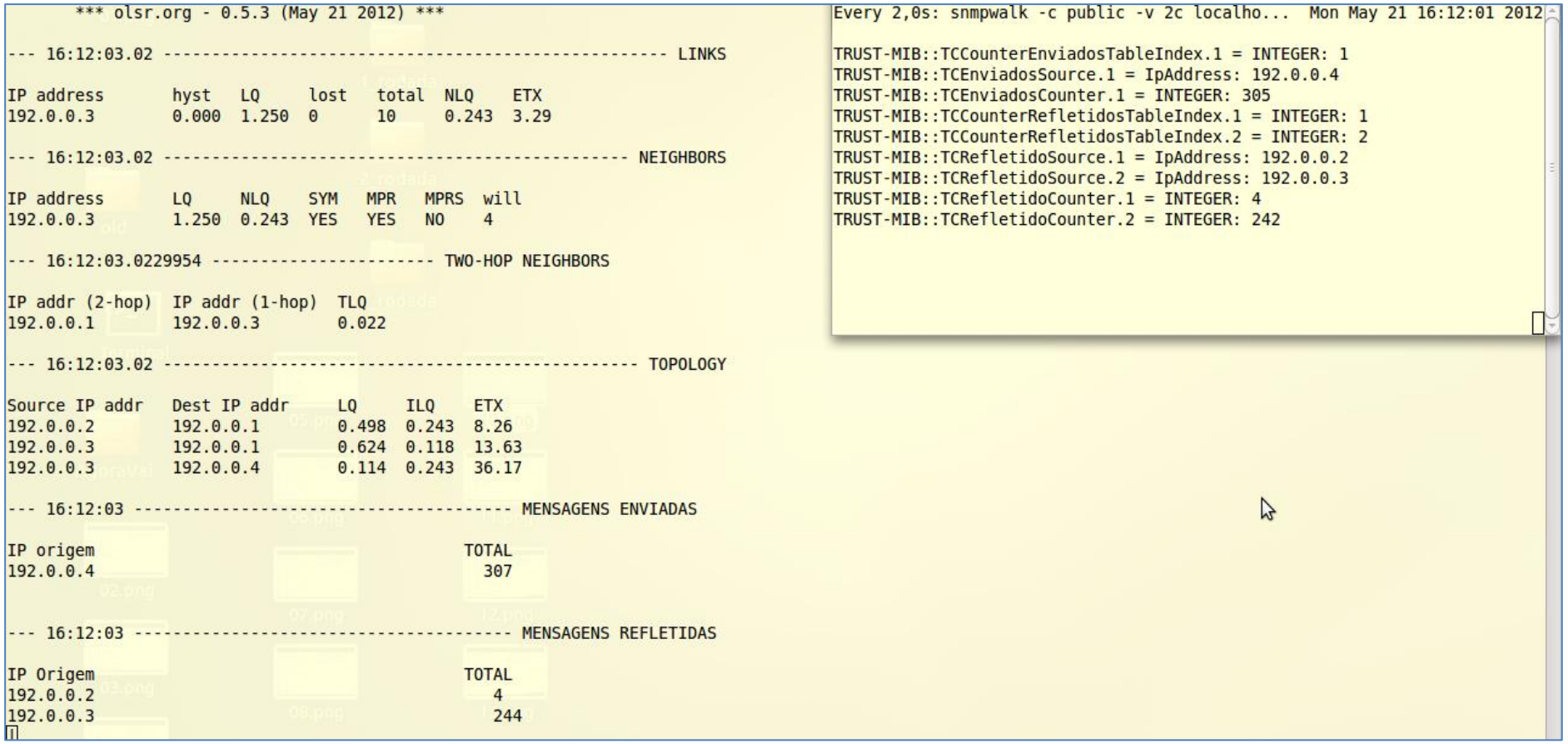

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:04:02.14 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.333 3 5 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:04:02.14 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.333 0.000 YES YES YES 4
192.0.0.3 1.250 0.243 YES NO YES 4
--- 16:04:02.02147959 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
--- 16:04:02.14 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.624 14.10
192.0.0.1 192.0.0.3 0.114 0.498 17.66
192.0.0.2 192.0.0.1 0.624 0.118 13.63
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:04:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 211
--- 16:04:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 1
192.0.0.3 162
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:03:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 210
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 1
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 161

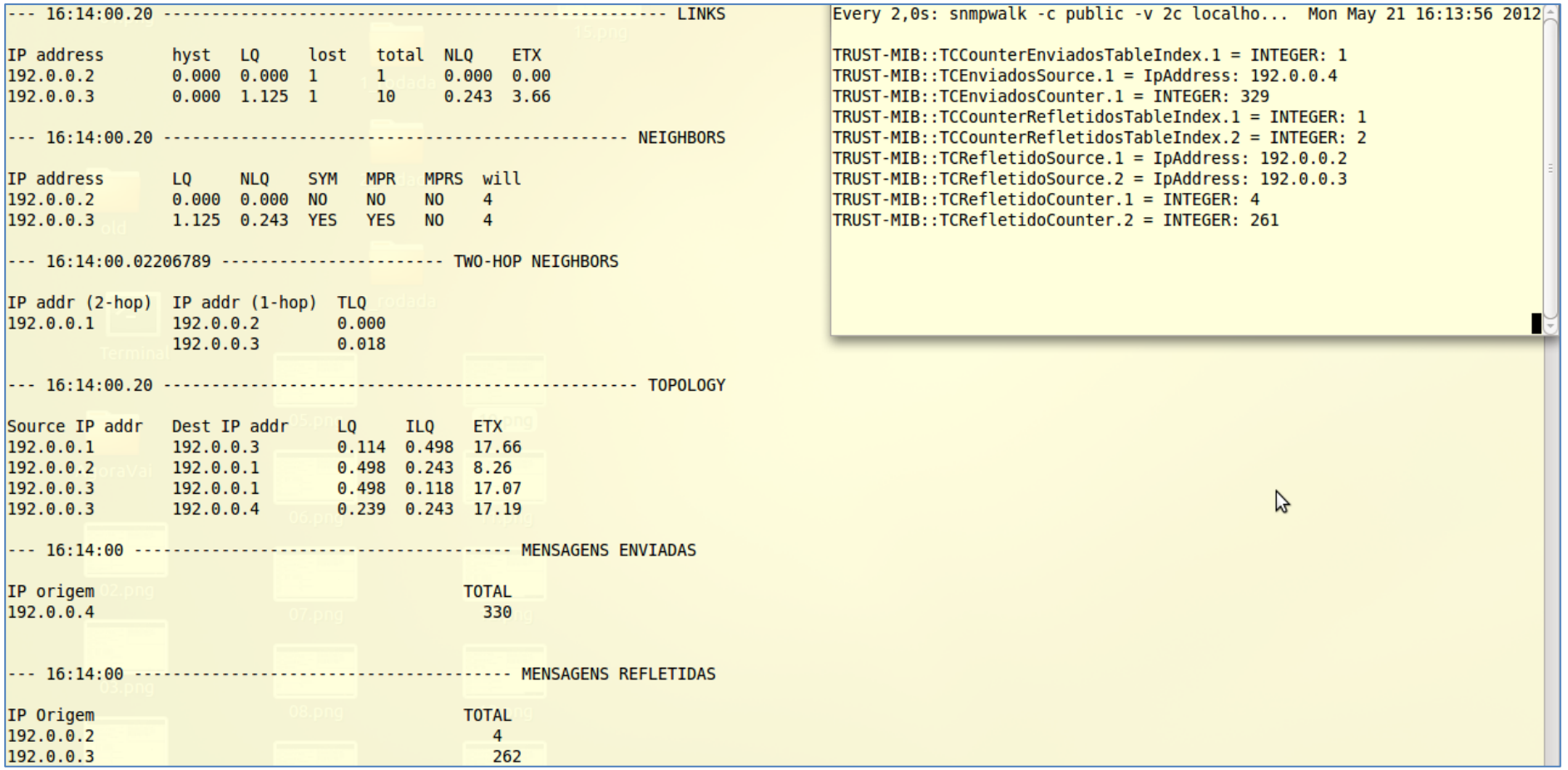

IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.375 7 10 0.000 0.00
192.0.0.3 0.000 1.000 2 10 0.243 4.11
--- 16:06:00.95 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.375 0.000 NO NO NO 4
192.0.0.3 1.000 0.243 YES YES NO 4
--- 16:06:00.02954640 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.037
192.0.0.2 192.0.0.3 0.152
--- 16:06:00.95 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.624 6.70
192.0.0.1 192.0.0.3 0.239 0.624 6.70
192.0.0.2 192.0.0.1 0.624 0.243 6.60
192.0.0.2 192.0.0.3 0.114 0.624 14.10
192.0.0.3 192.0.0.1 0.749 0.243 5.49
192.0.0.3 192.0.0.2 0.624 0.118 13.63
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:06:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 235
--- 16:06:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 4
192.0.0.3 181
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:05:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 232
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 4
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 181

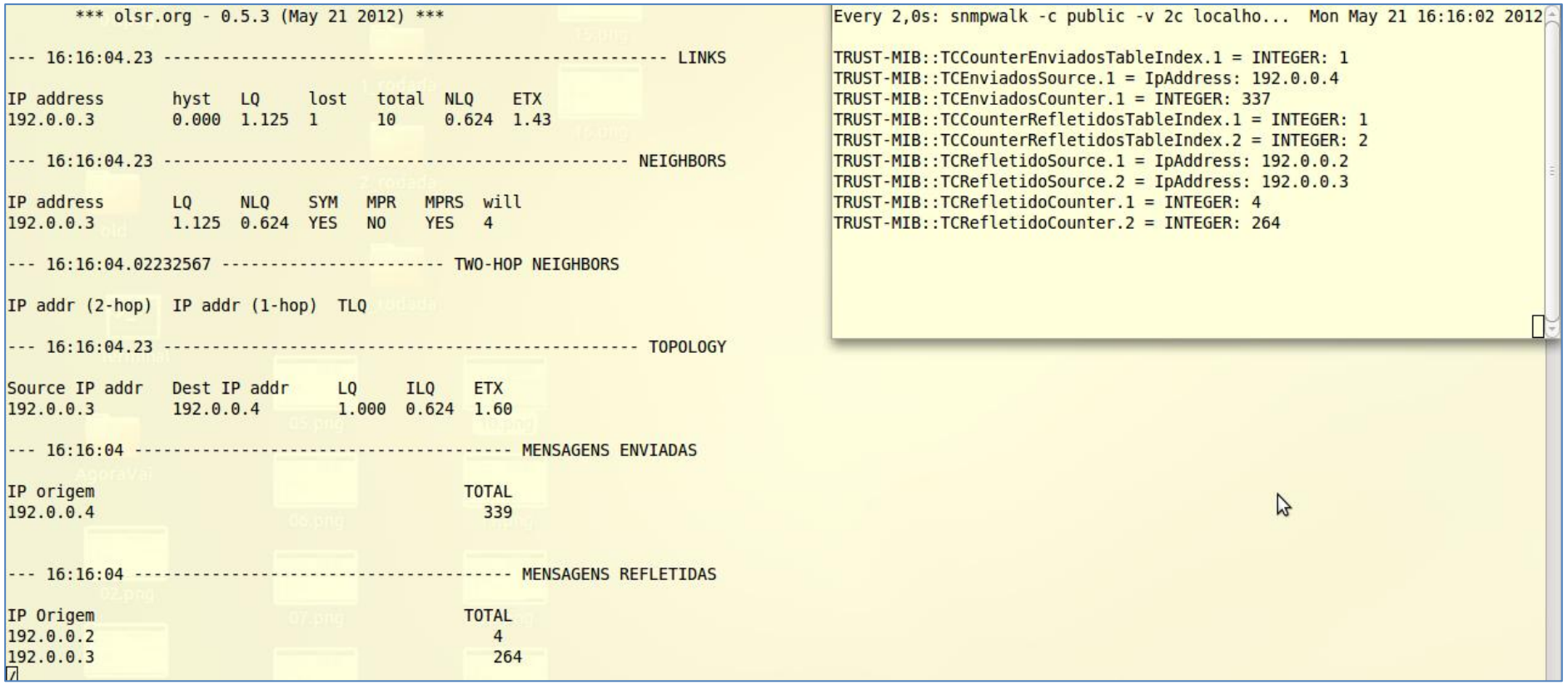
```
IP address       hyst   LQ     lost   total  NLQ    ETX
192.0.0.2        0.000  0.000  1      1      0.000  0.00
192.0.0.3        0.000  1.250  0      10     0.243  3.29

--- 16:08:01.32 ------------------------------------------------ NEIGHBORS

IP address       LQ     NLQ    SYM   MPR   MPRS  will
192.0.0.2        0.000  0.000  NO    NO    NO    4
192.0.0.3        1.250  0.243  YES   YES   NO    4

--- 16:08:01.02328088 ---------------------- TWO-HOP NEIGHBORS

IP addr (2-hop)  IP addr (1-hop)  TLQ
192.0.0.1        192.0.0.3        0.228
192.0.0.2        192.0.0.3        0.009
192.0.0.3        192.0.0.2        0.000

--- 16:08:01.32 ------------------------------------------------ TOPOLOGY

Source IP addr   Dest IP addr   LQ     ILQ    ETX
192.0.0.1        192.0.0.3        1.000  0.749  1.34
192.0.0.2        192.0.0.1        0.498  0.118  17.07
192.0.0.2        192.0.0.3        0.114  0.243  36.17
192.0.0.3        192.0.0.1        0.749  1.000  1.34
192.0.0.3        192.0.0.2        0.239  0.118  35.53
192.0.0.3        192.0.0.4        0.239  0.243  17.19

--- 16:08:01 ------------------------------------- MENSAGENS ENVIADAS

IP origem                                TOTAL
192.0.0.4                                  259


--- 16:08:01 ------------------------------------ MENSAGENS REFLETIDAS

IP Origem                                TOTAL
192.0.0.2                                  4
192.0.0.3                                  202
```

```
Every 2,0s: snmpwalk -c public -v 2c localho...  Mon May 21 16:07:59 2012

TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 259
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 4
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 202
```


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:10:01.65 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:10:01.65 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:10:01.02650234 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.025
--- 16:10:01.65 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.749 5.58
192.0.0.2 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.1 0.373 0.243 11.04
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:10:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 284
--- 16:10:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 4
192.0.0.3 223
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:09:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 282
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 4
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 222

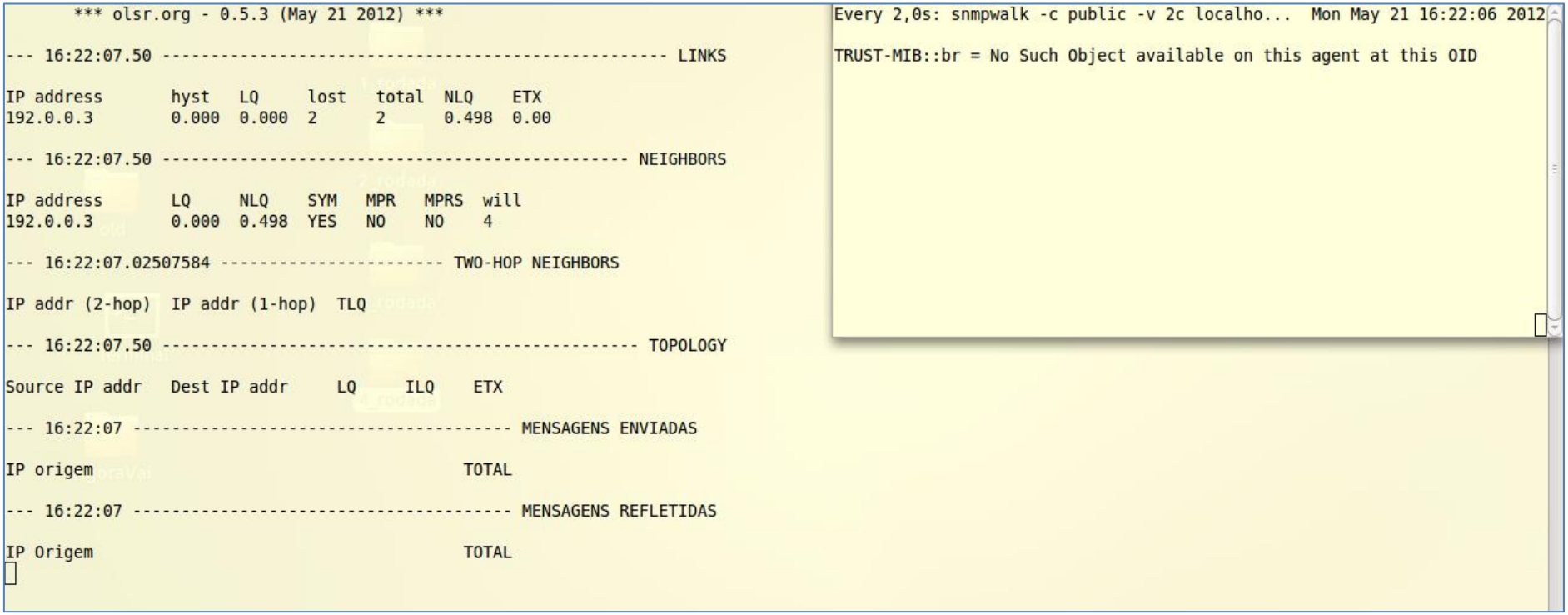

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:12:03.02 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:12:03.02 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:12:03.0229954 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.022
--- 16:12:03.02 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.2 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.1 0.624 0.118 13.63
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:12:03 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 307
--- 16:12:03 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 4
192.0.0.3 244
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:12:01 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 305
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 4
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 242

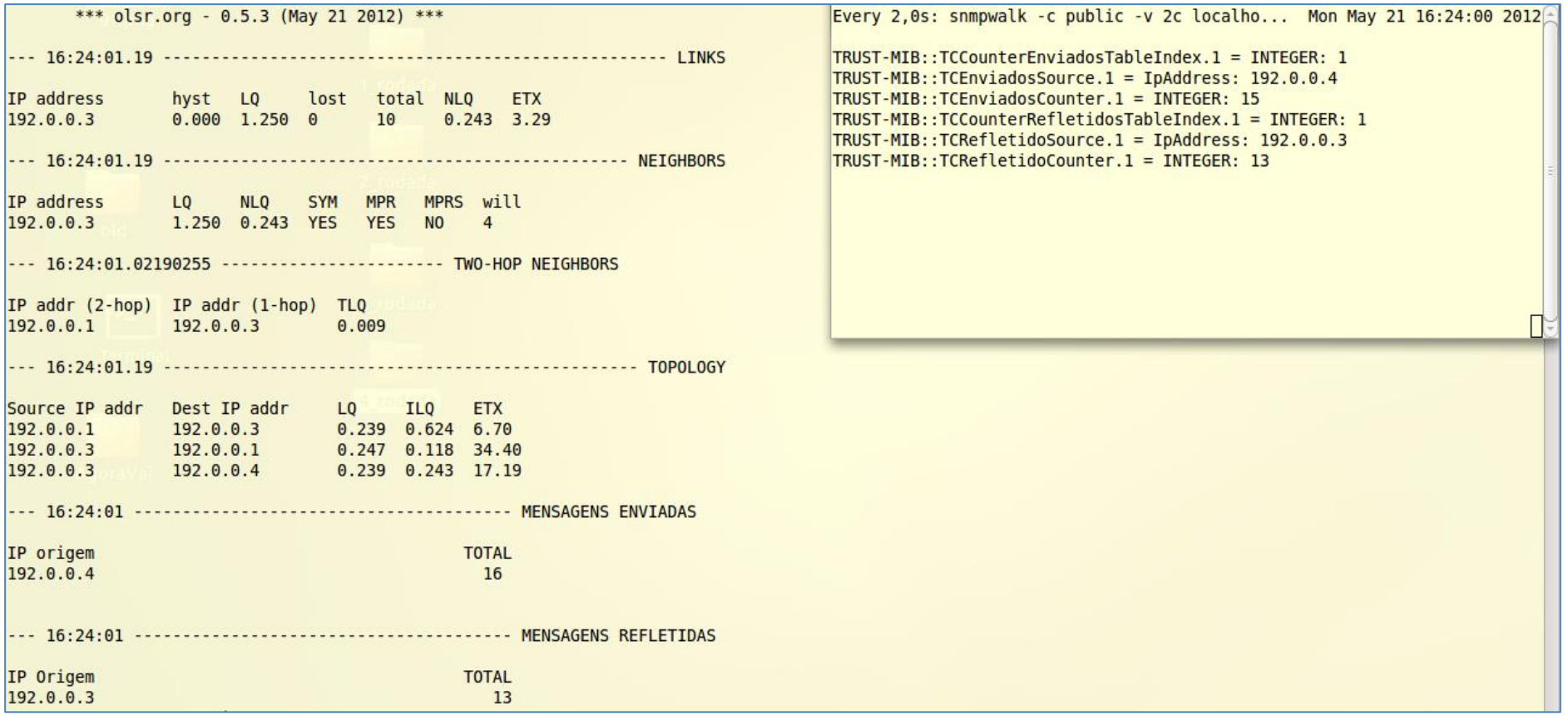

--- 16:14:00.20 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 1 1 0.000 0.00
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:14:00.20 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.000 NO NO NO 4
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:14:00.02206789 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.018
--- 16:14:00.20 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.498 17.66
192.0.0.2 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.1 0.498 0.118 17.07
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:14:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 330
--- 16:14:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 4
192.0.0.3 262
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:13:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 329
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 4
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 261

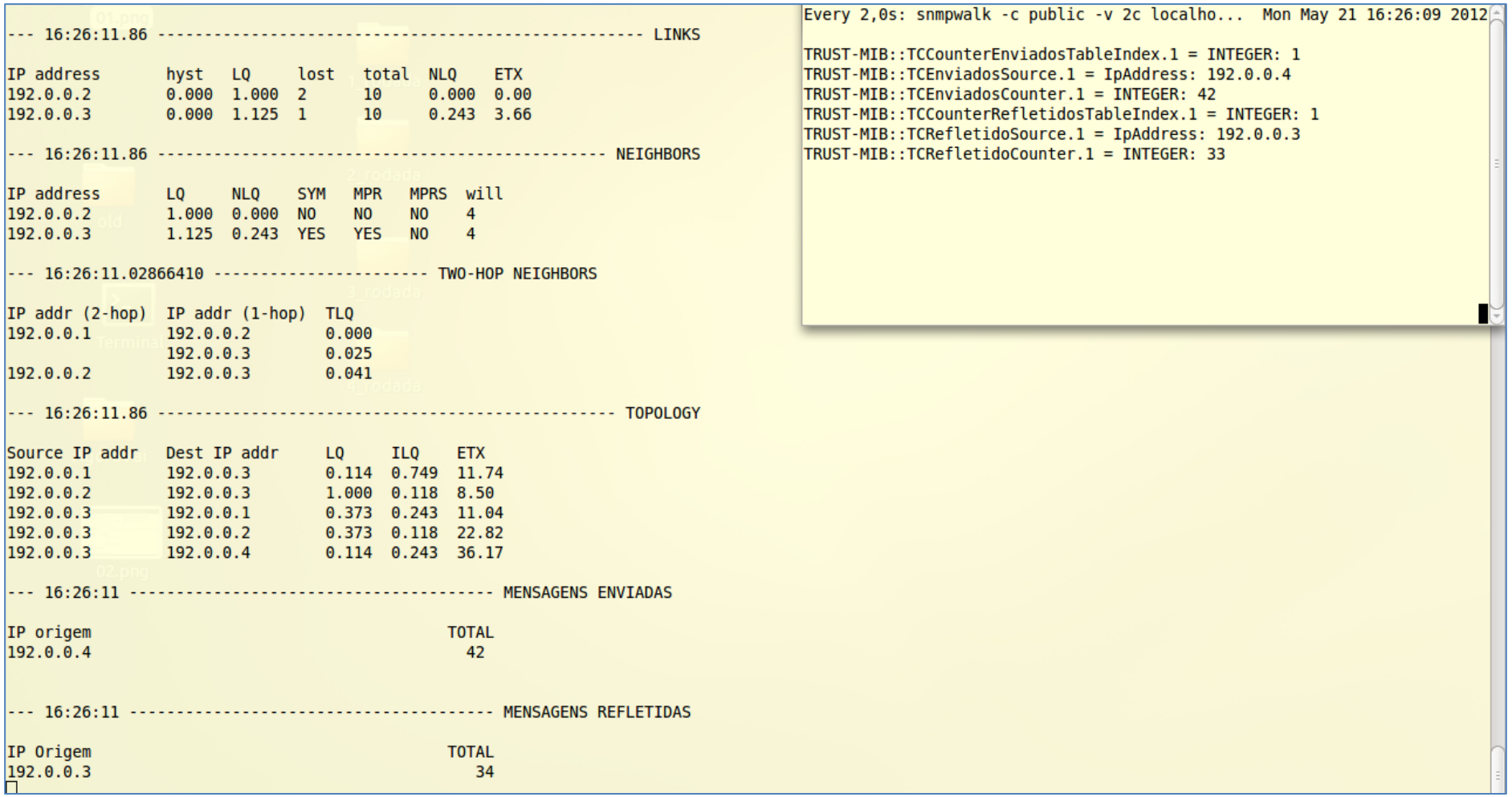

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:16:04.23 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.624 1.43
--- 16:16:04.23 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.624 YES NO YES 4
--- 16:16:04.02232567 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 16:16:04.23 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.3 192.0.0.4 1.000 0.624 1.60
--- 16:16:04 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 339
--- 16:16:04 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 4
192.0.0.3 264
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:16:02 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 337
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 4
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 264

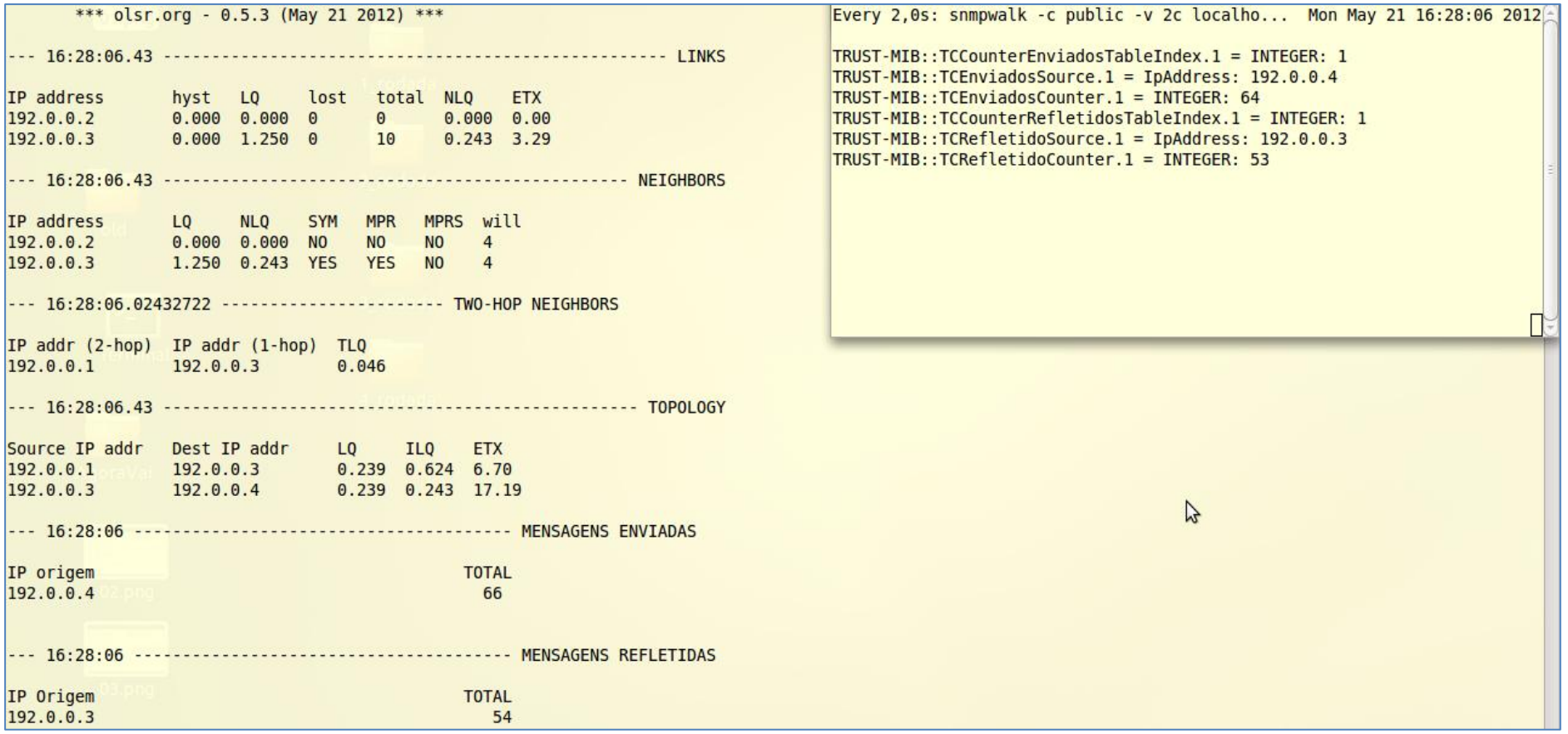
F - SIMULAÇÃO DA TRUST-MIB E OLSRD - Teste 04

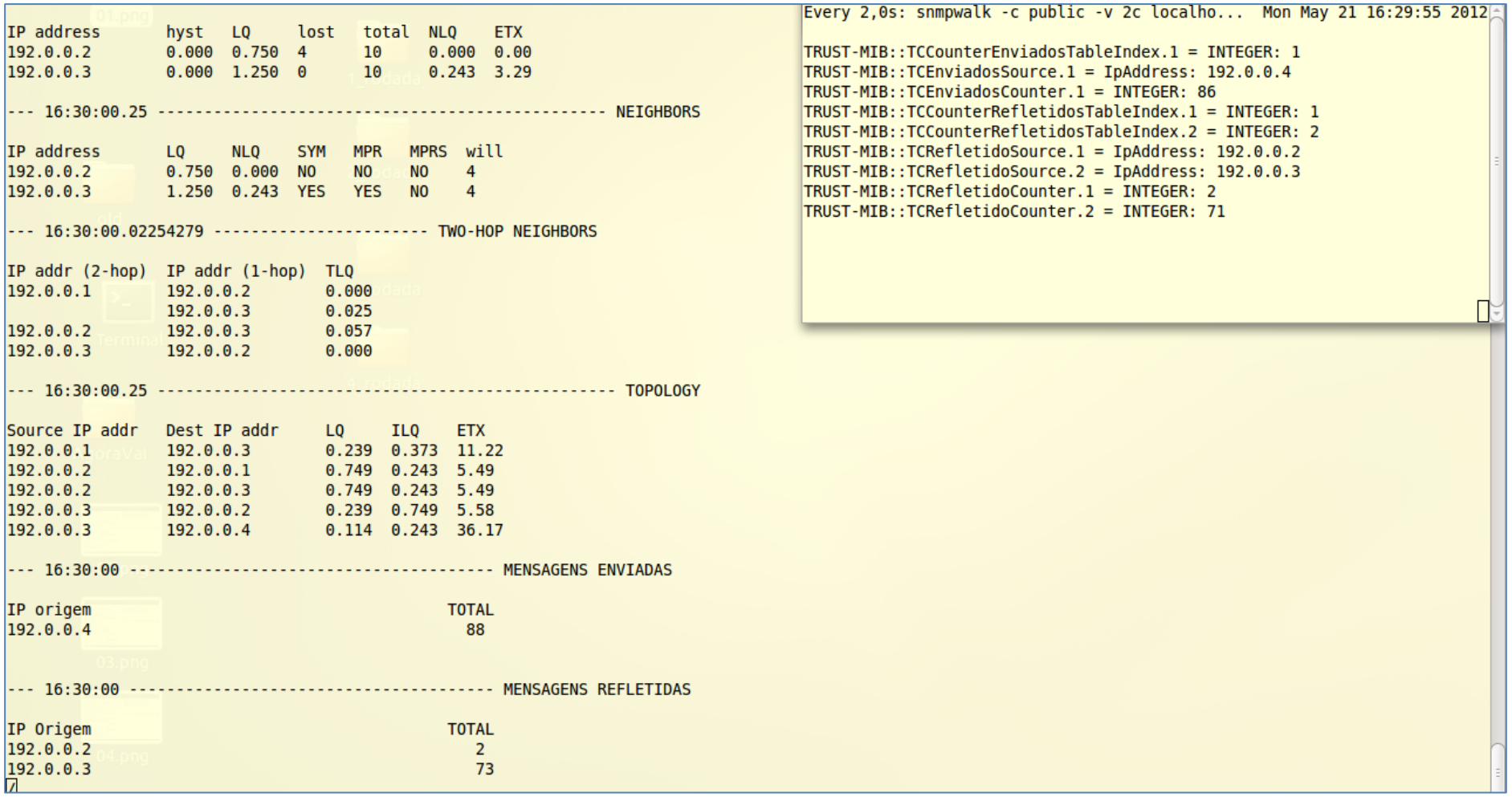
Telas do teste 04 da simulação realizada com o protocolo OLSRD e a TRUST-MIB.

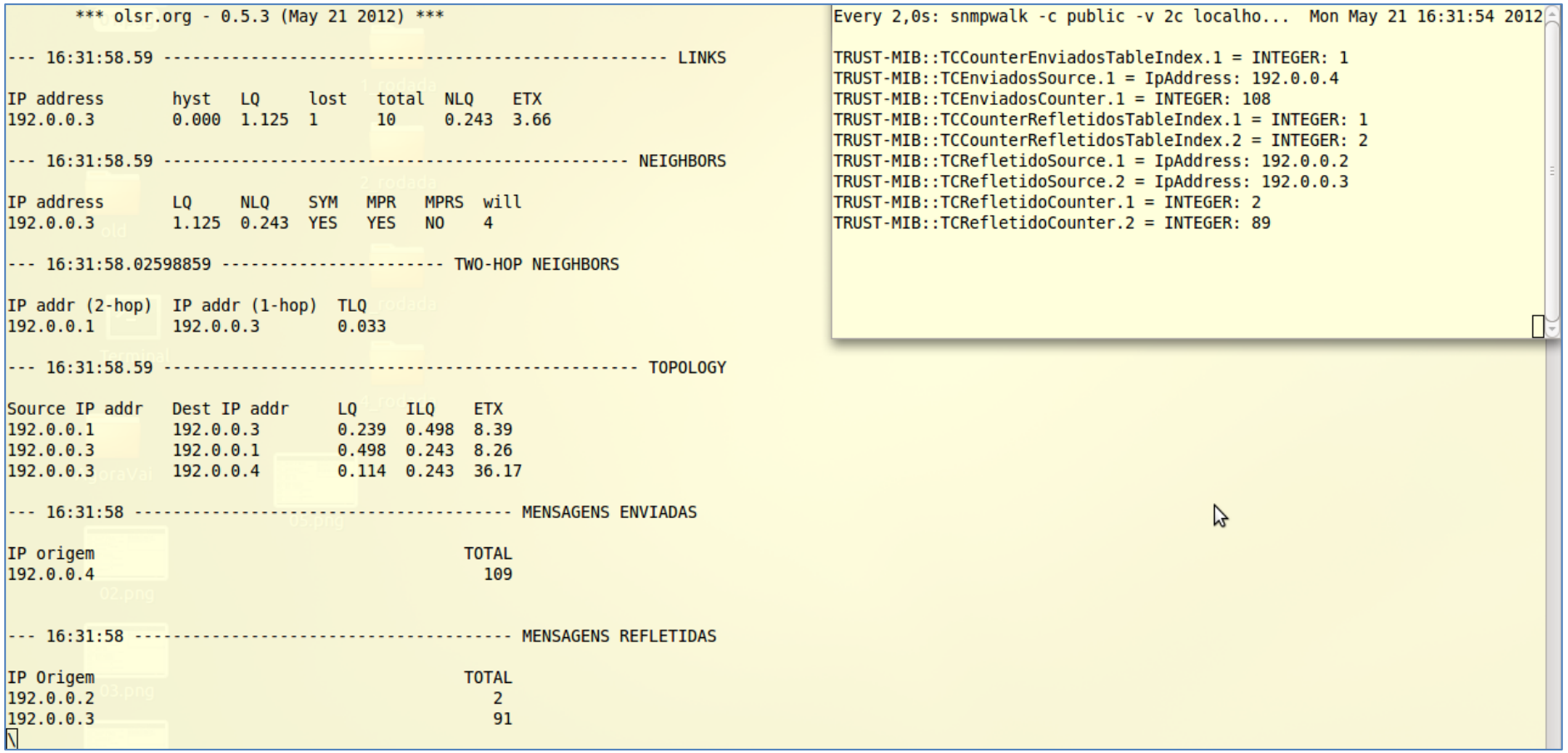


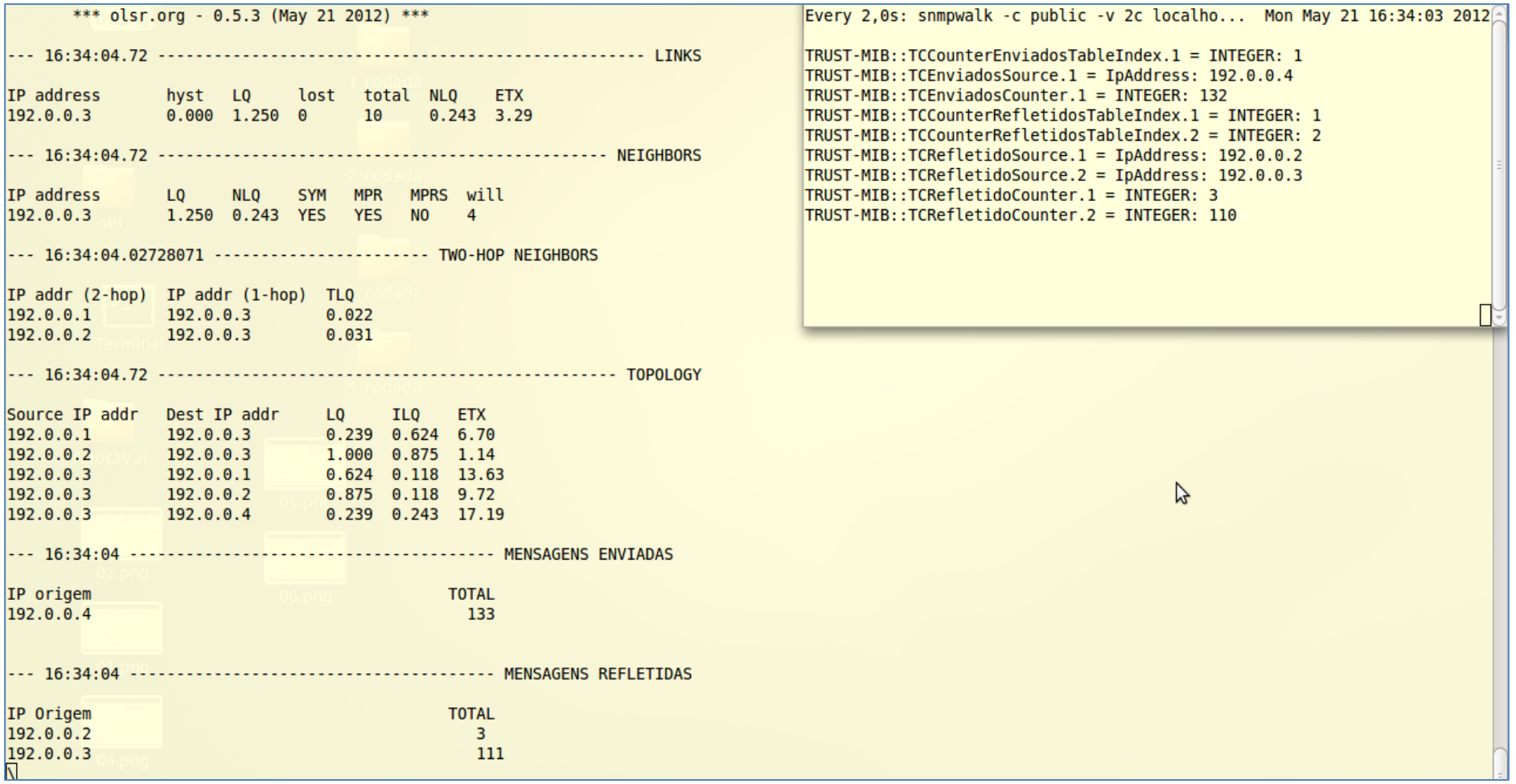

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:24:01.19 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:24:01.19 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:24:01.02190255 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.009
--- 16:24:01.19 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.624 6.70
192.0.0.3 192.0.0.1 0.247 0.118 34.40
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:24:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 16
--- 16:24:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 13
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:24:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 15
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 13

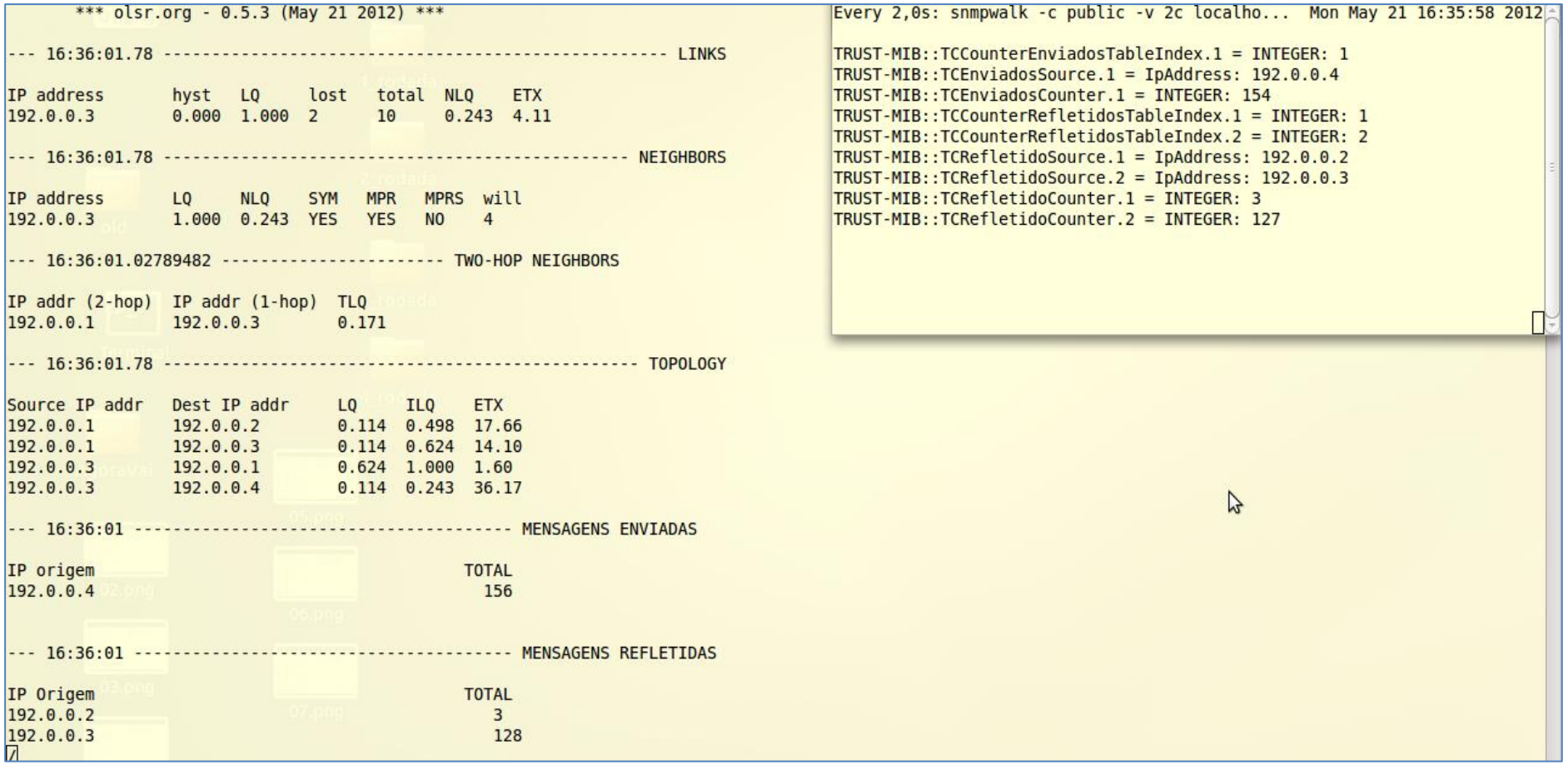

--- 16:26:11.86 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 1.000 2 10 0.000 0.00
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:26:11.86 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 1.000 0.000 NO NO NO 4
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:26:11.02866410 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.025
192.0.0.2 192.0.0.3 0.041
--- 16:26:11.86 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.749 11.74
192.0.0.2 192.0.0.3 1.000 0.118 8.50
192.0.0.3 192.0.0.1 0.373 0.243 11.04
192.0.0.3 192.0.0.2 0.373 0.118 22.82
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:26:11 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 42
--- 16:26:11 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 34
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:26:09 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 42
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 33

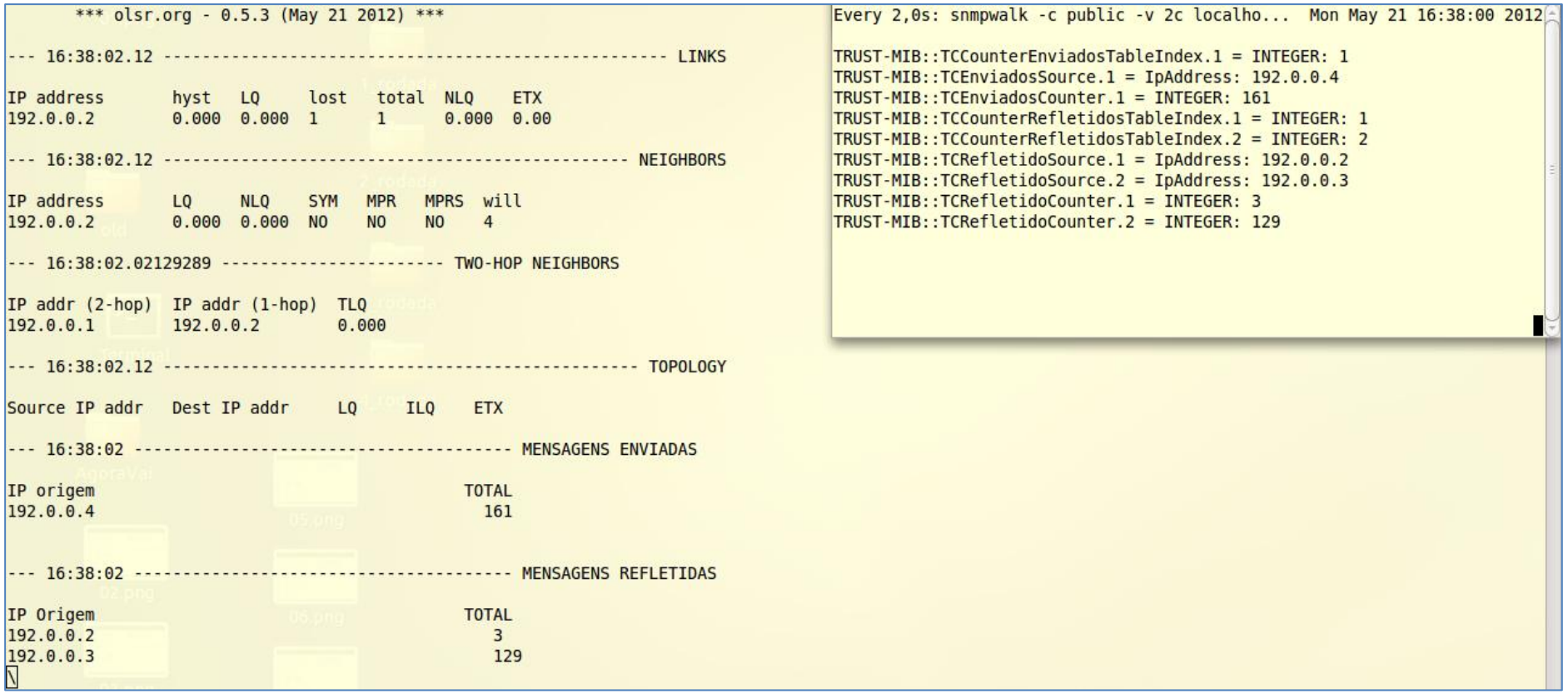

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:28:06.43 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 0 0 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:28:06.43 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.000 NO NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:28:06.02432722 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.046
--- 16:28:06.43 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.624 6.70
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:28:06 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 66
--- 16:28:06 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.3 54
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:28:06 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 64
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 53

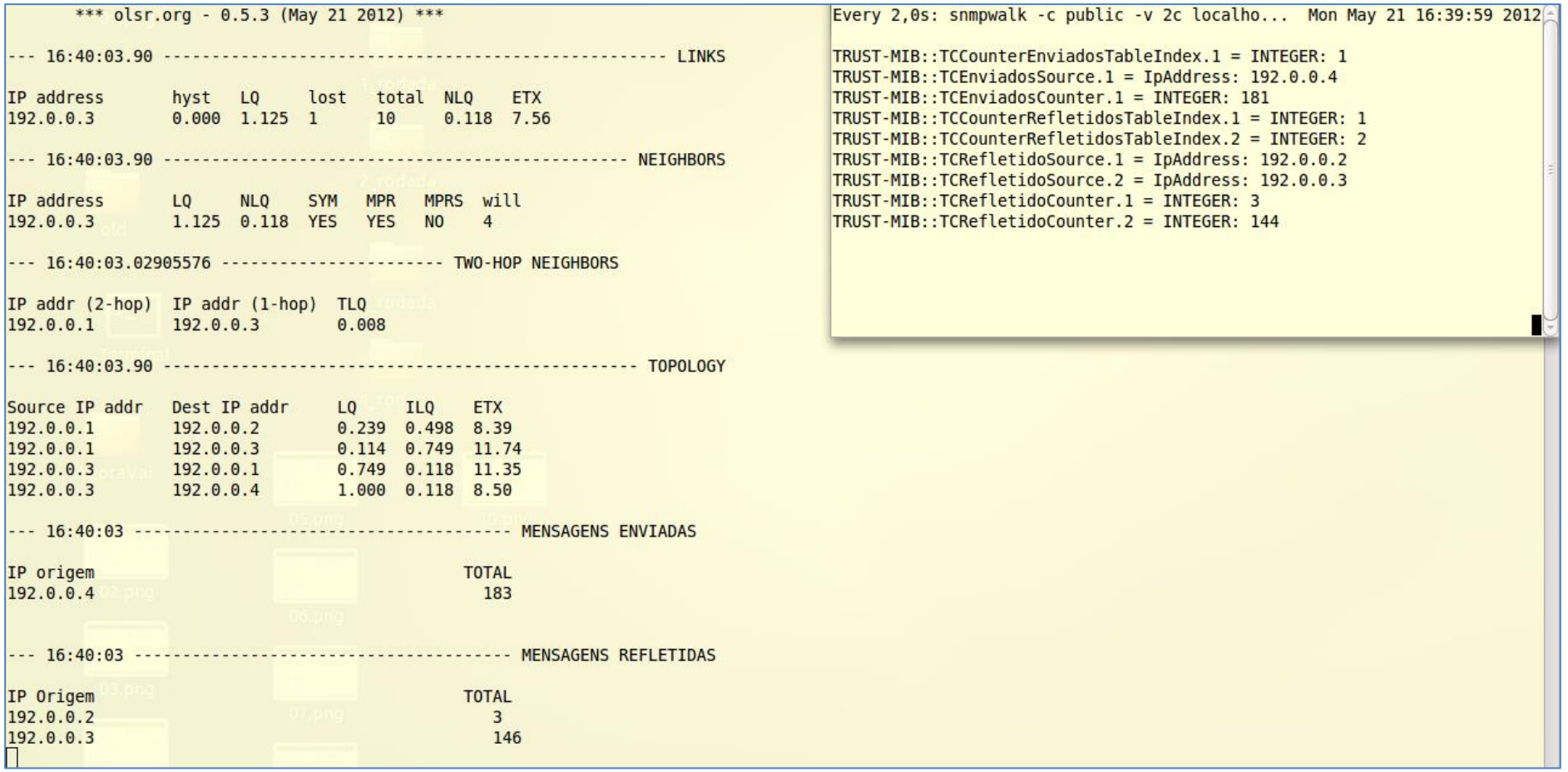

IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.750 4 10 0.000 0.00
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:30:00.25 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.750 0.000 NO NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:30:00.02254279 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
192.0.0.3 0.025
192.0.0.2 192.0.0.3 0.057
192.0.0.3 192.0.0.2 0.000
--- 16:30:00.25 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.373 11.22
192.0.0.2 192.0.0.1 0.749 0.243 5.49
192.0.0.2 192.0.0.3 0.749 0.243 5.49
192.0.0.3 192.0.0.2 0.239 0.749 5.58
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:30:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 88
--- 16:30:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 2
192.0.0.3 73
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:29:55 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 86
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 2
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 71

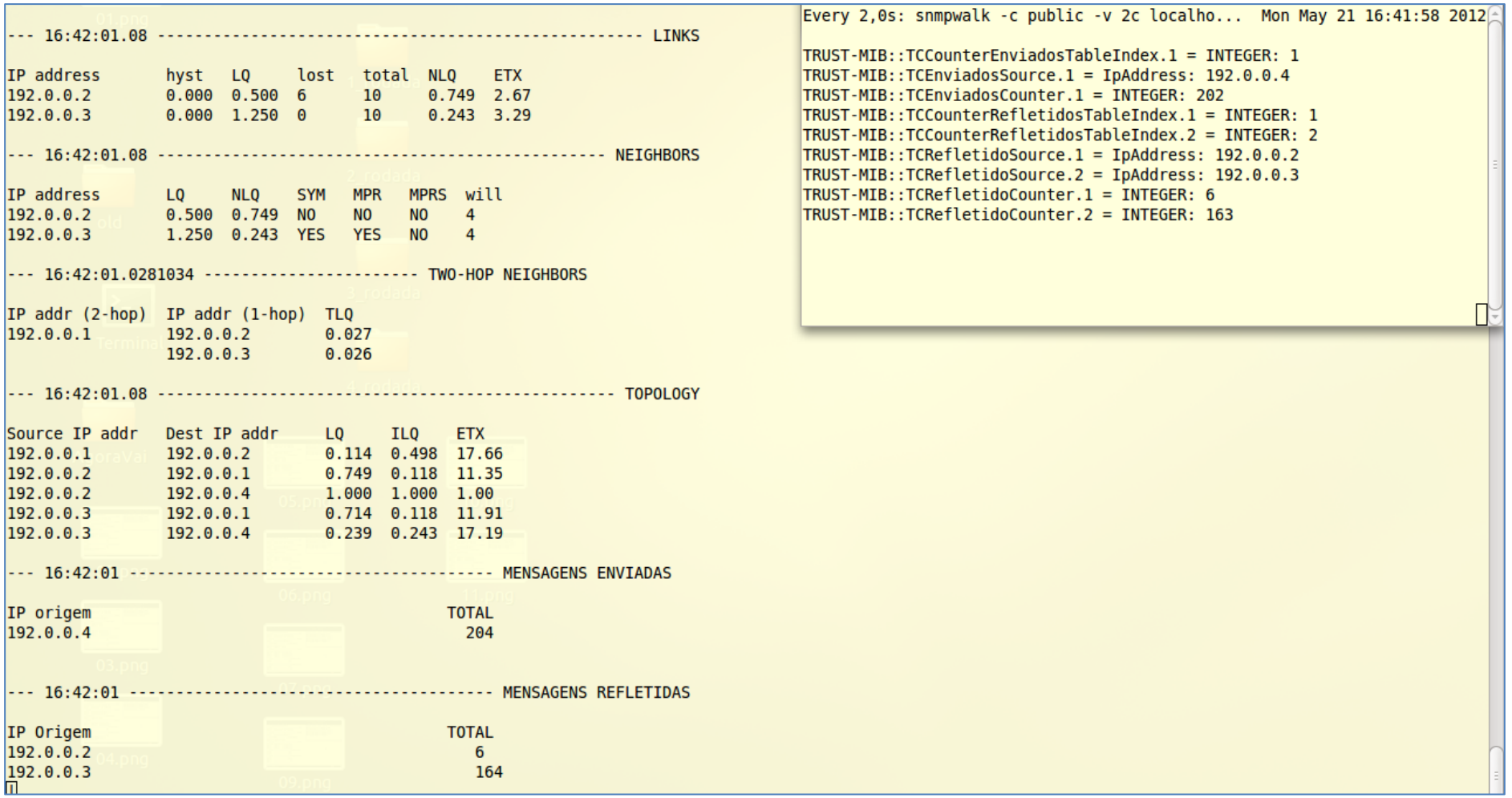

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:31:58.59 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:31:58.59 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:31:58.02598859 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.033
--- 16:31:58.59 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.498 8.39
192.0.0.3 192.0.0.1 0.498 0.243 8.26
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:31:58 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 109
--- 16:31:58 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 2
192.0.0.3 91
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:31:54 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 108
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 2
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 89

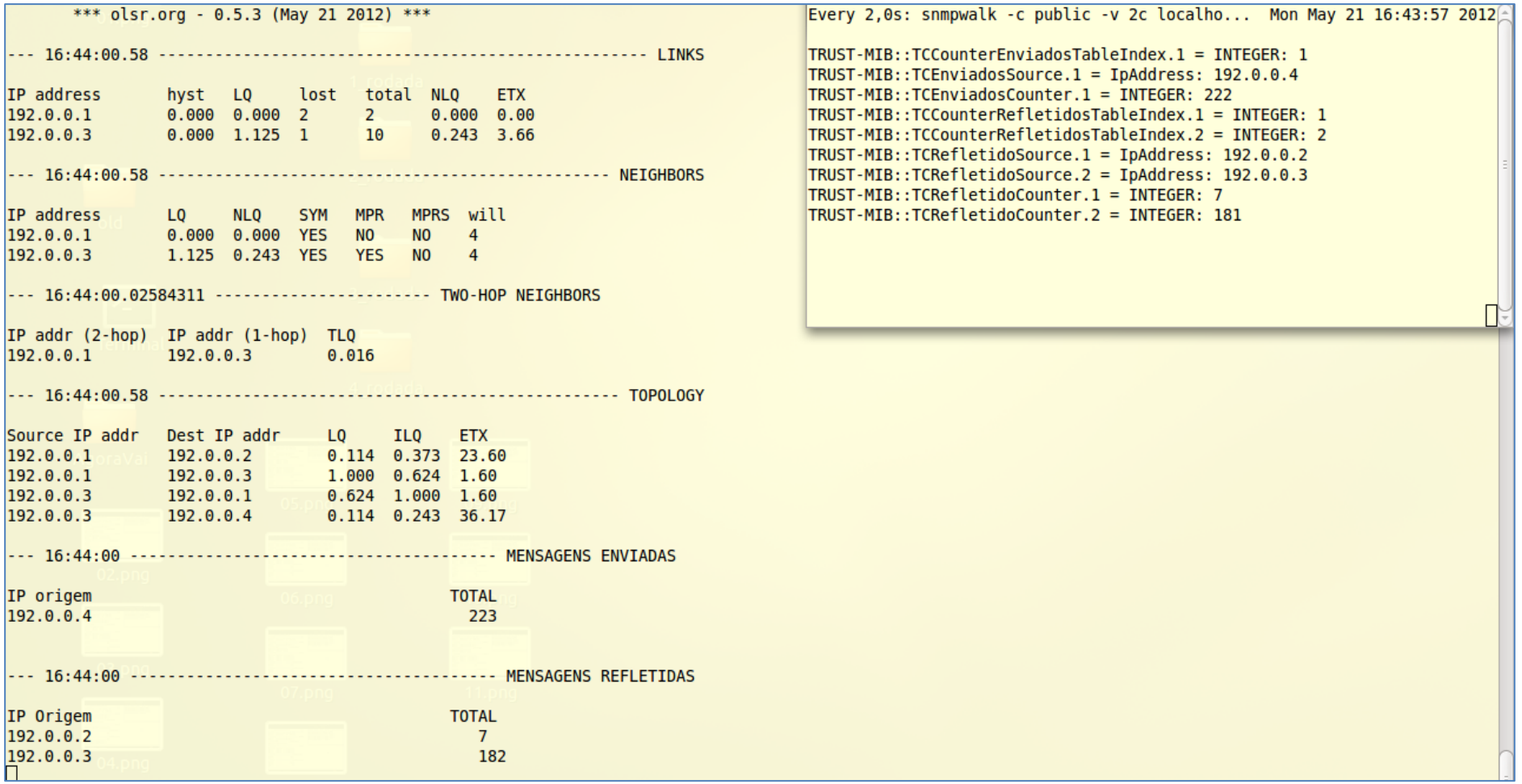

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:34:04.72 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:34:04.72 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:34:04.02728071 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.022
192.0.0.2 192.0.0.3 0.031
--- 16:34:04.72 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.239 0.624 6.70
192.0.0.2 192.0.0.3 1.000 0.875 1.14
192.0.0.3 192.0.0.1 0.624 0.118 13.63
192.0.0.3 192.0.0.2 0.875 0.118 9.72
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:34:04 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 133
--- 16:34:04 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 3
192.0.0.3 111
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:34:03 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 132
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 110

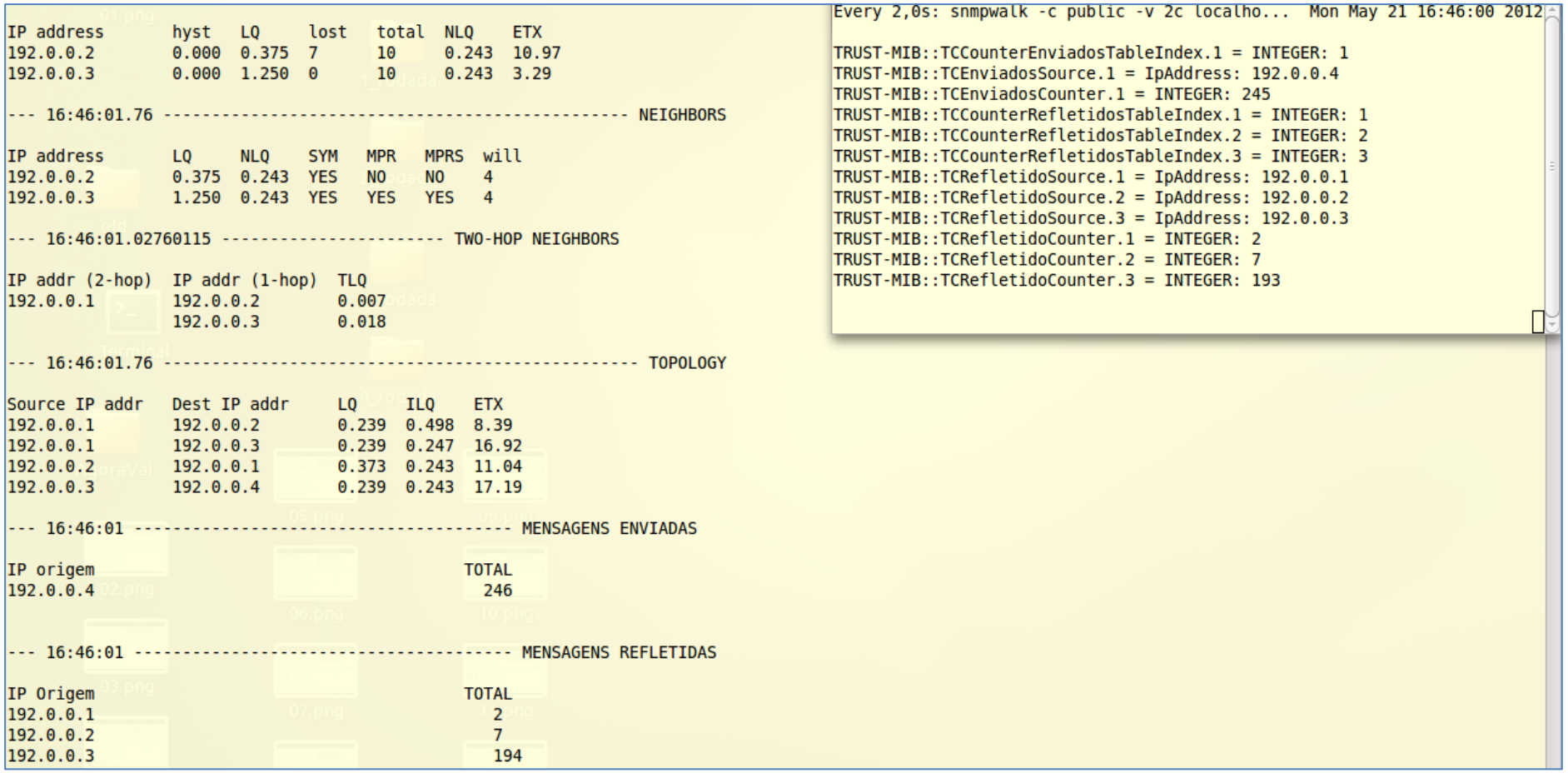

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:36:01.78 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.000 2 10 0.243 4.11
--- 16:36:01.78 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.000 0.243 YES YES NO 4
--- 16:36:01.02789482 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.171
--- 16:36:01.78 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.498 17.66
192.0.0.1 192.0.0.3 0.114 0.624 14.10
192.0.0.3 192.0.0.1 0.624 1.000 1.60
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:36:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 156
--- 16:36:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 3
192.0.0.3 128
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:35:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 154
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 127

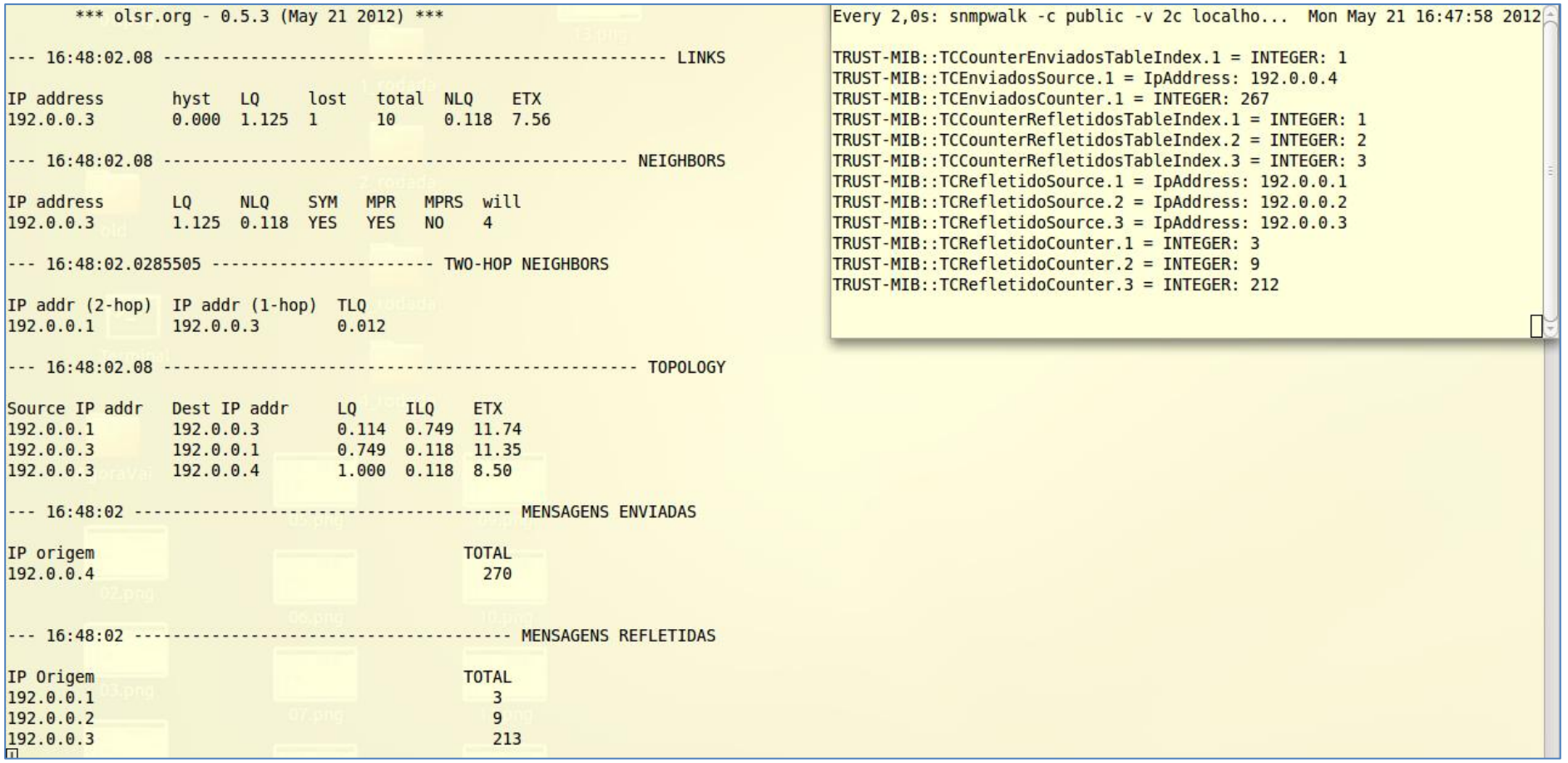

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:38:02.12 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 1 1 0.000 0.00
--- 16:38:02.12 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.000 NO NO NO 4
--- 16:38:02.02129289 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.000
--- 16:38:02.12 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 16:38:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 161
--- 16:38:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 3
192.0.0.3 129
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:38:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 161
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 129

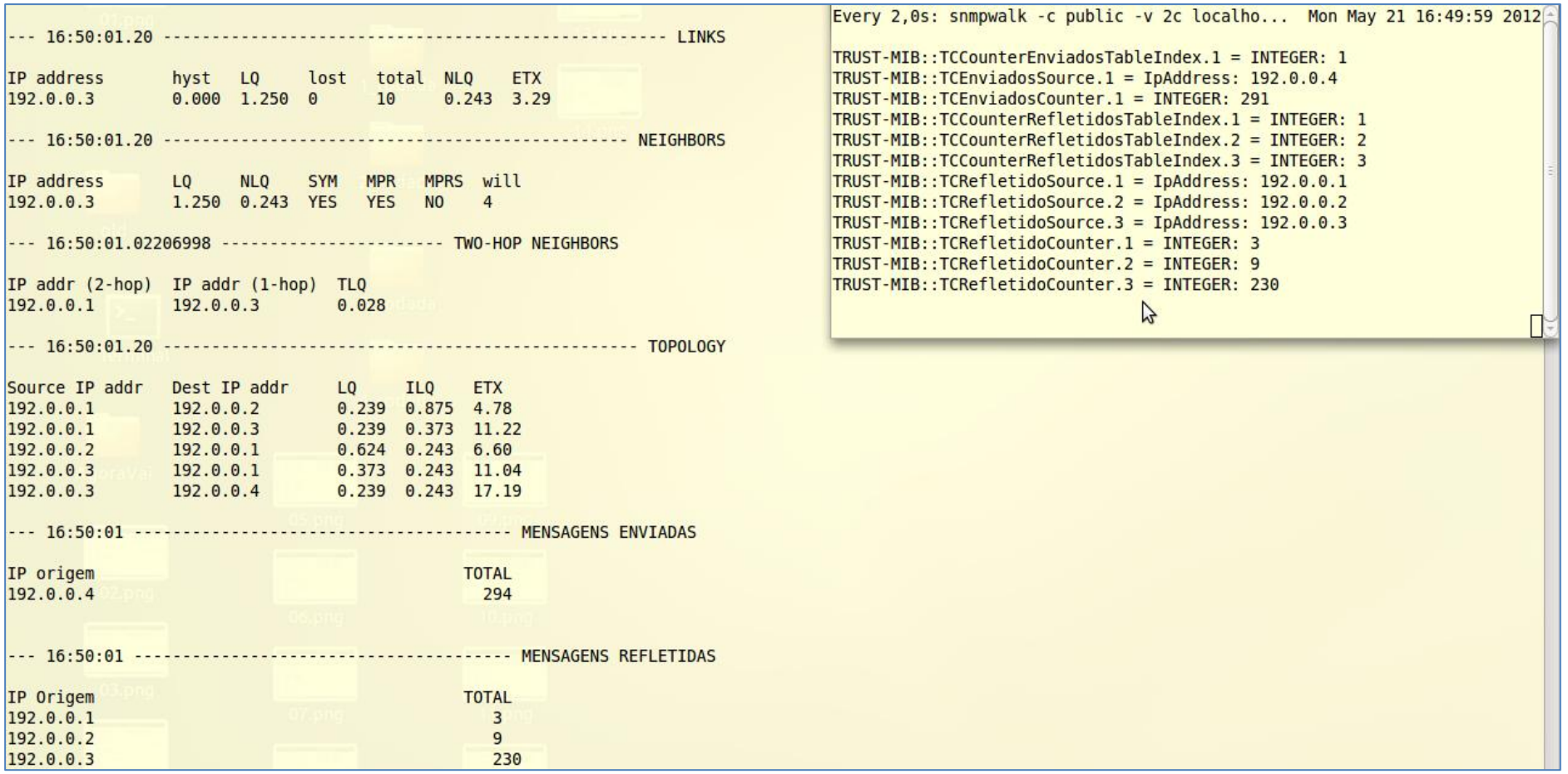

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:40:03.90 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.118 7.56
--- 16:40:03.90 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.118 YES YES NO 4
--- 16:40:03.02905576 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.008
--- 16:40:03.90 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.498 8.39
192.0.0.1 192.0.0.3 0.114 0.749 11.74
192.0.0.3 192.0.0.1 0.749 0.118 11.35
192.0.0.3 192.0.0.4 1.000 0.118 8.50
--- 16:40:03 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 183
--- 16:40:03 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 3
192.0.0.3 146
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:39:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 181
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 144

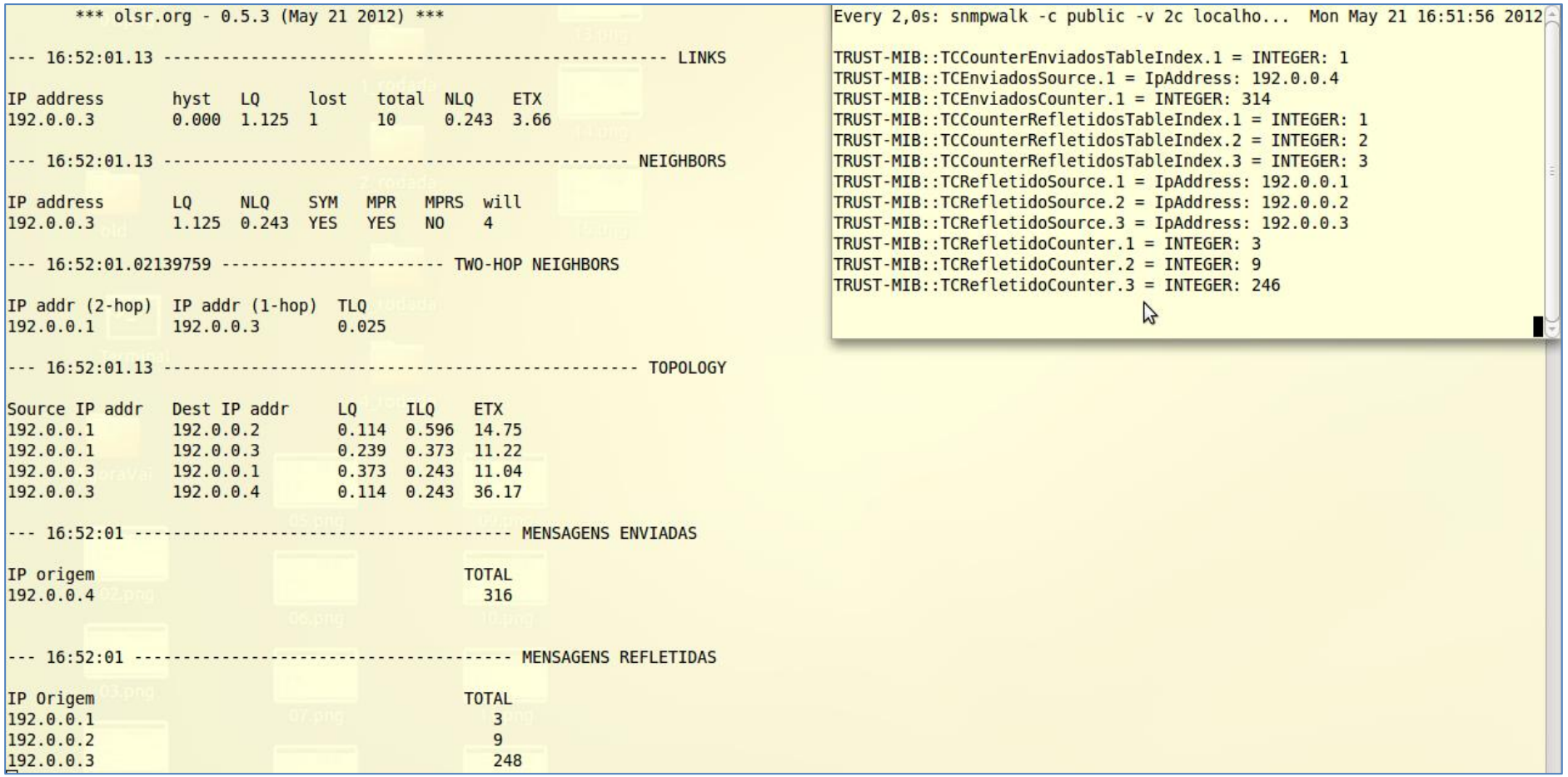

--- 16:42:01.08 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.500 6 10 0.749 2.67
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:42:01.08 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.500 0.749 NO NO NO 4
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:42:01.0281034 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.027
192.0.0.3 0.026
--- 16:42:01.08 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.498 17.66
192.0.0.2 192.0.0.1 0.749 0.118 11.35
192.0.0.2 192.0.0.4 1.000 1.000 1.00
192.0.0.3 192.0.0.1 0.714 0.118 11.91
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:42:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 204
--- 16:42:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 6
192.0.0.3 164
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:41:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 202
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 6
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 163

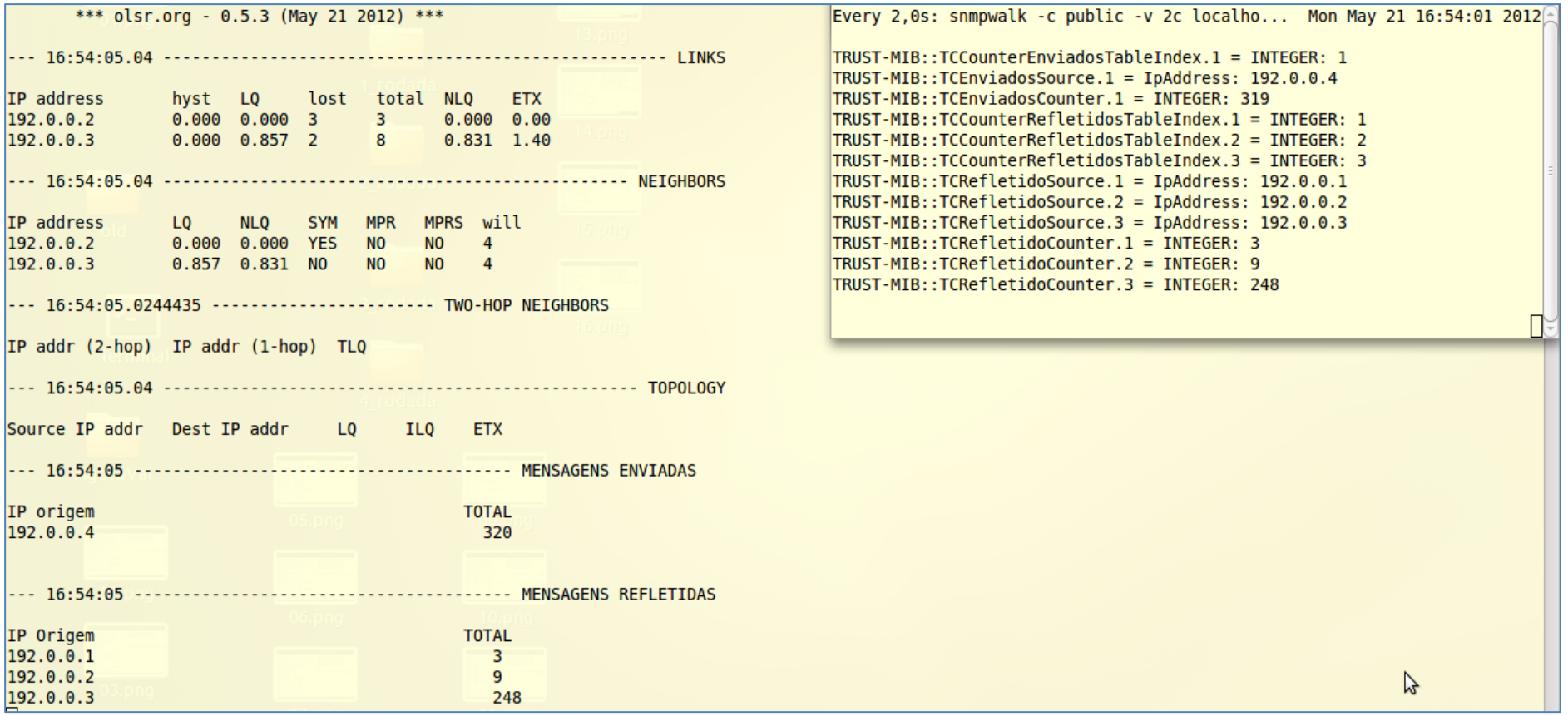

*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:44:00.58 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.1 0.000 0.000 2 2 0.000 0.00
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:44:00.58 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.1 0.000 0.000 YES NO NO 4
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:44:00.02584311 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.016
--- 16:44:00.58 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.373 23.60
192.0.0.1 192.0.0.3 1.000 0.624 1.60
192.0.0.3 192.0.0.1 0.624 1.000 1.60
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:44:00 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 223
--- 16:44:00 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.2 7
192.0.0.3 182
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:43:57 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 222
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 7
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 181


IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.375 7 10 0.243 10.97
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:46:01.76 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.375 0.243 YES NO NO 4
192.0.0.3 1.250 0.243 YES YES YES 4
--- 16:46:01.02760115 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.2 0.007
192.0.0.3 0.018
--- 16:46:01.76 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.498 8.39
192.0.0.1 192.0.0.3 0.239 0.247 16.92
192.0.0.2 192.0.0.1 0.373 0.243 11.04
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:46:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 246
--- 16:46:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.1 2
192.0.0.2 7
192.0.0.3 194
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:46:00 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 245
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCCounterRefletidosTableIndex.3 = INTEGER: 3
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.1
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.3 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 2
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 7
TRUST-MIB::TCRefletidoCounter.3 = INTEGER: 193


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:48:02.08 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.118 7.56
--- 16:48:02.08 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.118 YES YES NO 4
--- 16:48:02.0285505 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.012
--- 16:48:02.08 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.3 0.114 0.749 11.74
192.0.0.3 192.0.0.1 0.749 0.118 11.35
192.0.0.3 192.0.0.4 1.000 0.118 8.50
--- 16:48:02 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 270
--- 16:48:02 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.1 3
192.0.0.2 9
192.0.0.3 213
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:47:58 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 267
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCCounterRefletidosTableIndex.3 = INTEGER: 3
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.1
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.3 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 9
TRUST-MIB::TCRefletidoCounter.3 = INTEGER: 212


--- 16:50:01.20 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.250 0 10 0.243 3.29
--- 16:50:01.20 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.250 0.243 YES YES NO 4
--- 16:50:01.02206998 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.028
--- 16:50:01.20 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.239 0.875 4.78
192.0.0.1 192.0.0.3 0.239 0.373 11.22
192.0.0.2 192.0.0.1 0.624 0.243 6.60
192.0.0.3 192.0.0.1 0.373 0.243 11.04
192.0.0.3 192.0.0.4 0.239 0.243 17.19
--- 16:50:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 294
--- 16:50:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.1 3
192.0.0.2 9
192.0.0.3 230
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:49:59 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 291
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCCounterRefletidosTableIndex.3 = INTEGER: 3
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.1
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.3 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 9
TRUST-MIB::TCRefletidoCounter.3 = INTEGER: 230


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:52:01.13 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.3 0.000 1.125 1 10 0.243 3.66
--- 16:52:01.13 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.3 1.125 0.243 YES YES NO 4
--- 16:52:01.02139759 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
192.0.0.1 192.0.0.3 0.025
--- 16:52:01.13 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
192.0.0.1 192.0.0.2 0.114 0.596 14.75
192.0.0.1 192.0.0.3 0.239 0.373 11.22
192.0.0.3 192.0.0.1 0.373 0.243 11.04
192.0.0.3 192.0.0.4 0.114 0.243 36.17
--- 16:52:01 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 316
--- 16:52:01 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.1 3
192.0.0.2 9
192.0.0.3 248
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:51:56 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 314
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCCounterRefletidosTableIndex.3 = INTEGER: 3
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.1
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.3 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 9
TRUST-MIB::TCRefletidoCounter.3 = INTEGER: 246


*** olsr.org - 0.5.3 (May 21 2012) ***
--- 16:54:05.04 ---------- LINKS
IP address hyst LQ lost total NLQ ETX
192.0.0.2 0.000 0.000 3 3 0.000 0.00
192.0.0.3 0.000 0.857 2 8 0.831 1.40
--- 16:54:05.04 ---------- NEIGHBORS
IP address LQ NLQ SYM MPR MPRS will
192.0.0.2 0.000 0.000 YES NO NO 4
192.0.0.3 0.857 0.831 NO NO NO 4
--- 16:54:05.0244435 ---------- TWO-HOP NEIGHBORS
IP addr (2-hop) IP addr (1-hop) TLQ
--- 16:54:05.04 ---------- TOPOLOGY
Source IP addr Dest IP addr LQ ILQ ETX
--- 16:54:05 ---------- MENSAGENS ENVIADAS
IP origem TOTAL
192.0.0.4 320
--- 16:54:05 ---------- MENSAGENS REFLETIDAS
IP Origem TOTAL
192.0.0.1 3
192.0.0.2 9
192.0.0.3 248
Every 2,0s: snmpwalk -c public -v 2c localho... Mon May 21 16:54:01 2012
TRUST-MIB::TCCounterEnviadosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCEnviadosSource.1 = IpAddress: 192.0.0.4
TRUST-MIB::TCEnviadosCounter.1 = INTEGER: 319
TRUST-MIB::TCCounterRefletidosTableIndex.1 = INTEGER: 1
TRUST-MIB::TCCounterRefletidosTableIndex.2 = INTEGER: 2
TRUST-MIB::TCCounterRefletidosTableIndex.3 = INTEGER: 3
TRUST-MIB::TCRefletidoSource.1 = IpAddress: 192.0.0.1
TRUST-MIB::TCRefletidoSource.2 = IpAddress: 192.0.0.2
TRUST-MIB::TCRefletidoSource.3 = IpAddress: 192.0.0.3
TRUST-MIB::TCRefletidoCounter.1 = INTEGER: 3
TRUST-MIB::TCRefletidoCounter.2 = INTEGER: 9
TRUST-MIB::TCRefletidoCounter.3 = INTEGER: 248

G - PUBLICAÇÕES REALIZADAS DURANTE O MESTRADO

1.	David, B. M.; Santana, B. C.; Peotta, L.; Holtz, M. D.; de Sousa Jr, R. T. (2010). A Context-Dependent Trust Model for the MAC Layer in LR-WPANs. International Journal on Computer Science and Engineering. Vol. 02, No. 09, pp 3007-3016**.**