



# DETERMINAÇÃO DO PERFIL DE ATAQUES A REDE DE COMPUTADORES



Autor(a): Michelle Marques Pfeifer ( [pfeifer\\_michelle@gmail.com](mailto:pfeifer_michelle@gmail.com) )

Orientador(a): André Franceschi de Angelis ( [andre@ft.unicamp.br](mailto:andre@ft.unicamp.br) )

FT – Faculdade de Tecnologia

CNPq – Conselho Nacional de Desenvolvimento Científico e Tecnológico.

Programa de Iniciação Científica Júnior – PIC Jr.

Palavras-chaves: Redes de computadores, Ataques



## Introdução

No mundo atual, as redes de computadores são essenciais. Mantê-las em bom funcionamento é um grande desafio para técnicos e estudiosos. As redes estão sujeitas a diversos problemas, incluindo ataques intencionais. Os ataques vem aumentando em número e evoluindo em sofisticação (Figura 1). Abordagens preventivas tem o intuito de detectar a ocorrência de ataques antes que eles causem danos significativos a rede. Tais abordagens proativas majoritariamente baseiam-se em técnicas estatísticas e, dentre elas, o uso de cartas de Controle Estatístico de Processos (CEP). Este projeto visa aos primeiros esforços no sentido de determinar o perfil estatístico dos ataques mais frequentes, quando observados em cartas (CEP), integrando-se às investigações em curso na Faculdade de Tecnologia.

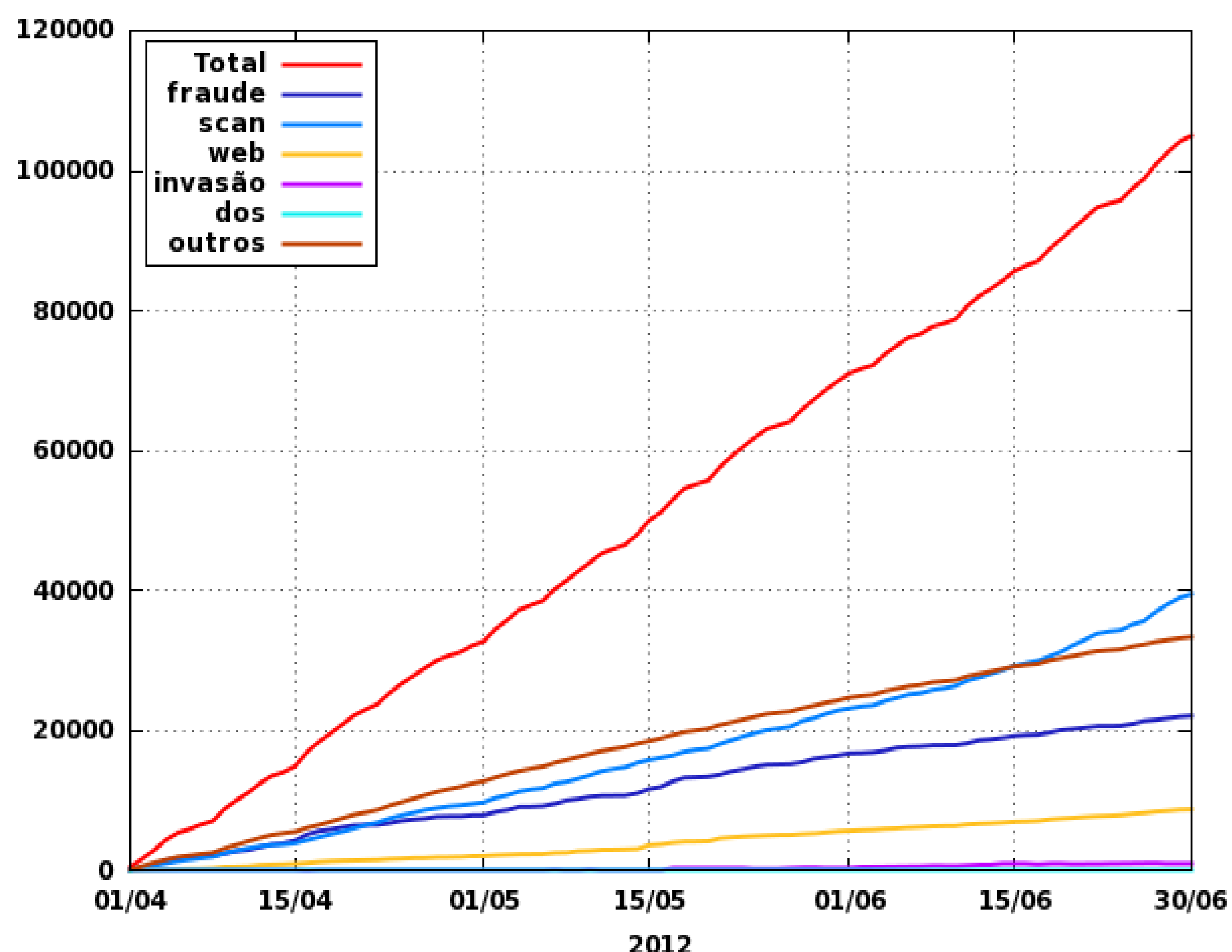


Fig. 1: Incidentes Reportados ao CERT.br -- Abril a Junho de 2012.

Fonte: <http://www.cert.br/stats/incidentes/2012-apr-jun/tipos-ataque-acumulado.html>

## Metodologia

Este trabalho prevê um estudo das redes de computadores e seus protocolos, por meio de levantamento bibliográfico fortemente baseado em livros da área. Na etapa seguinte, deverá ser realizada uma análise dos principais ataques a redes de computadores, a partir de artigos e pesquisas em sites especializados. A última etapa é determinar o perfil estatístico de um ataque ou um subconjunto de ataques a redes, quando considerada a observação de seu tráfego. A partir deste perfil, tráfego sintético de ataques poderá ser gerado e incorporado a bases de dados para a avaliação de ferramentas de proteção a rede.

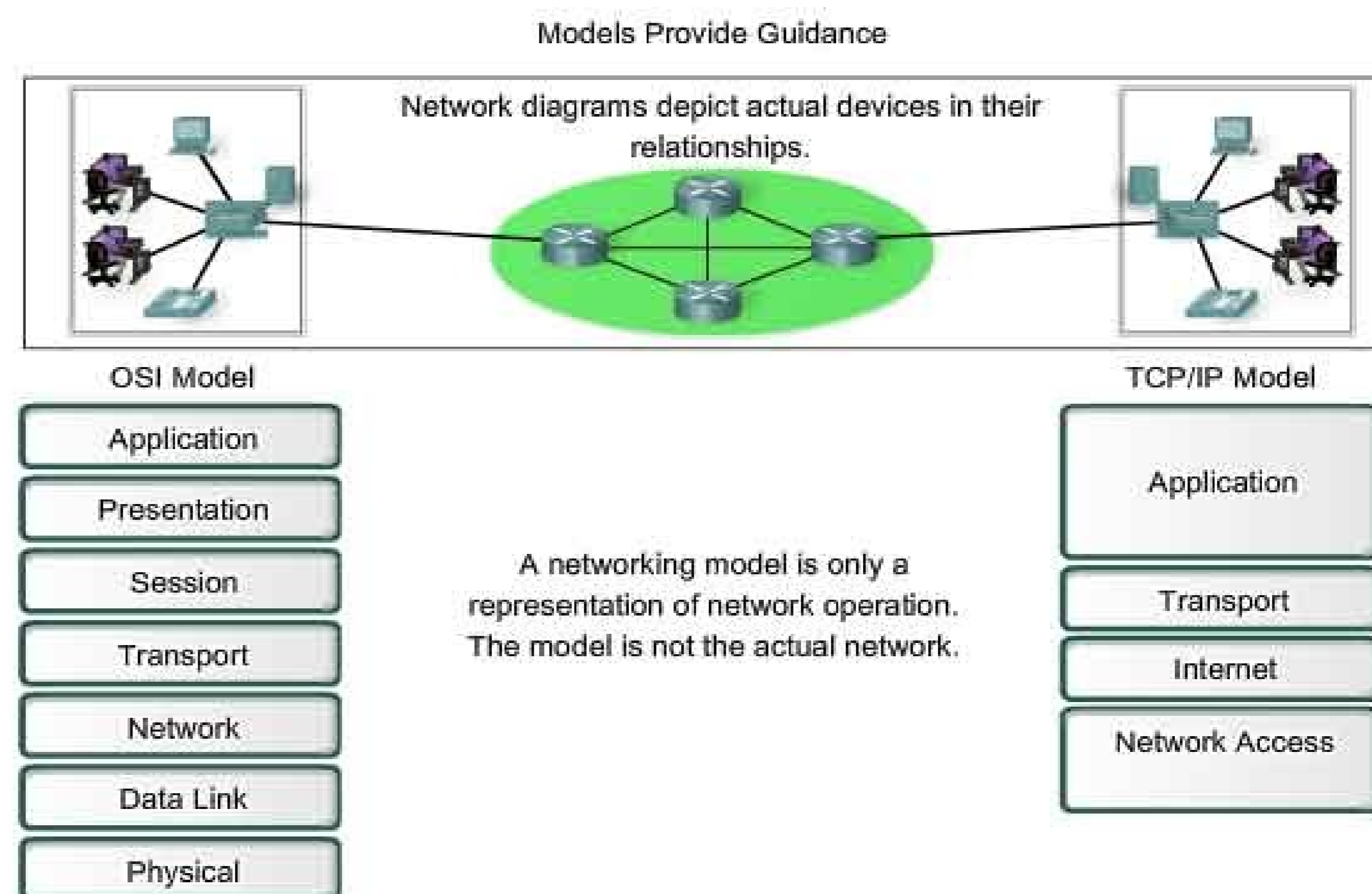


Fig. 2: Modelos OSI e TCP/IP

Fonte: [http://www.highteck.net/EN/Communicating/Communicating\\_over\\_the\\_Network.html](http://www.highteck.net/EN/Communicating/Communicating_over_the_Network.html)

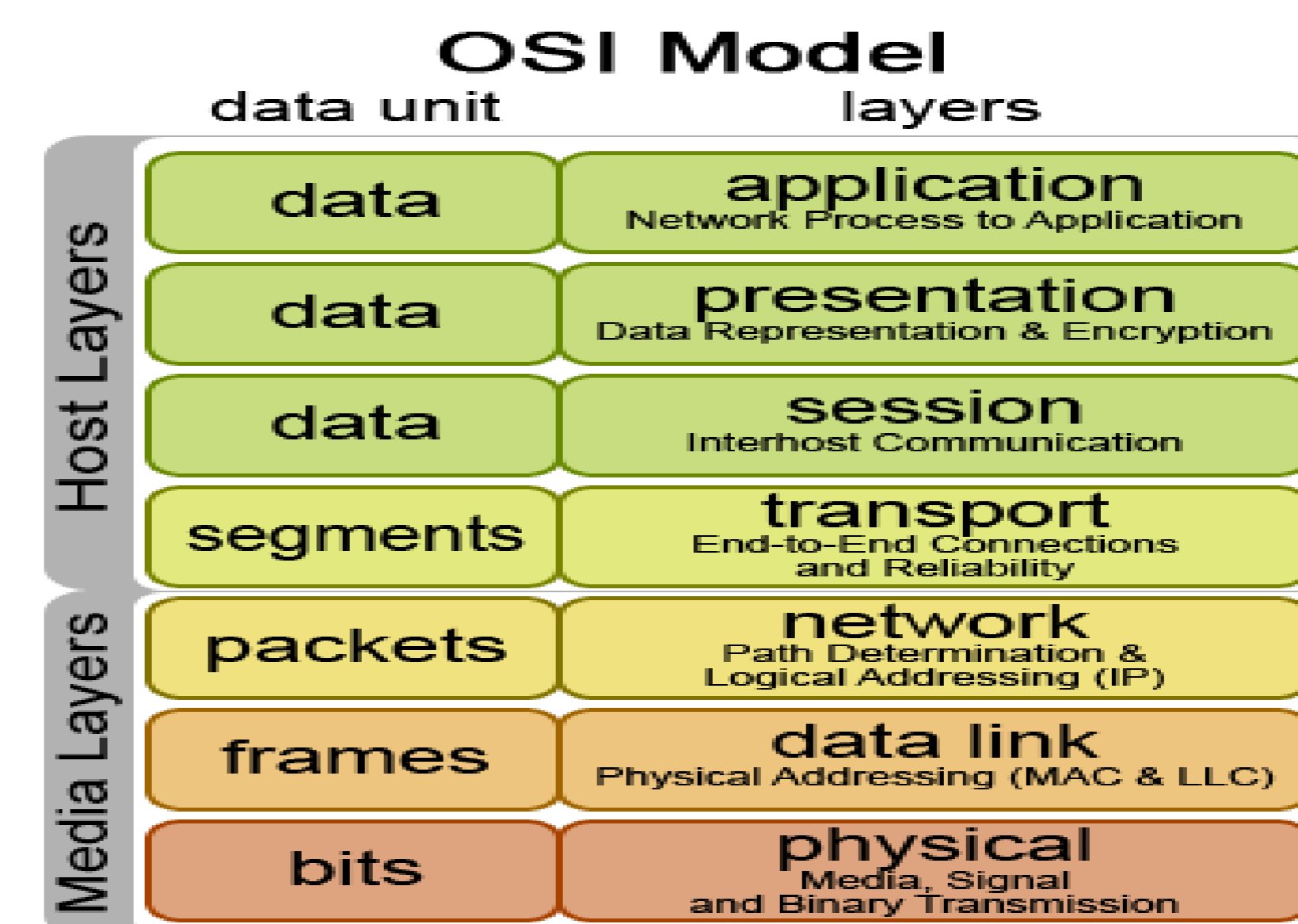


Fig. 3: Camadas do modelo OSI

Fonte: [http://encycl.opentopia.com/term/OSI\\_model](http://encycl.opentopia.com/term/OSI_model)

## Resultados e discussões

Foi concluída a primeira fase do trabalho, iniciado em julho de 2012, correspondente ao estudo das redes. Foi possível entender o funcionamento das redes de computadores, desde o modelo OSI/ISO (Figs. 2 e 3) até a suíte de protocolos TCP/IP, usada na Internet. Adicionalmente, foram vistos e manipulados equipamentos de infraestrutura, tais como placas de redes, conectores, cabos, *hubs*, *switches* e roteadores. A partir de outubro de 2012, serão realizadas as próximas etapas do trabalho.

## Referências bibliográficas

CYCLADES. **Guia Internet de Conectividade**. São Paulo: SENAC, 2000.  
TENENBAUM, Andrew S. **Computer Networks**. Rio de Janeiro: Campus, 2003.