SOFWARE PARA MONITORAÇÃO DO CONTEÚDO DO TRÁFEGO DE REDE EM AMBIENTE CORPORATIVO

Anderson Rodrigo Radtke Cardozo

Francisco Adell Péricas – Orientador

Roteiro da Apresentação

- Introdução
  - Objetivos do trabalho
  - Objetivos específicos do trabalho
- Fundamentação teórica
- Desenvolvimento
- Operacionalidade
- Resultados e discussão
- Conclusão
- Extensões

Introdução

- Vasto e diversificado conteúdo disponibilizado pela Internet
- Facilidade do acesso à Internet sem restrições ou controle nas empresas
- Interferência direta na produtividade do funcionário e da empresa
- Consumo dos recursos que a empresa dispõe
- Ferramentas centralizadas em servidores

Objetivos do trabalho

- O objetivo deste trabalho é desenvolver uma ferramenta agente e uma ferramenta gerente para monitoração dos acessos à Internet em um ambiente corporativo

Objetivos específicos do trabalho

- Disponibilizar nas estações da rede os agentes para registrar as informações dos acessos à Internet, armazenando as mesmas em um arquivo no disco rígido
- Disponibilizar uma ferramenta gerente para centralizar as informações colhidas dos agentes de cada estação da rede
- Disponibilizar a qualquer momento por meio da ferramenta gerente a consulta dos acessos à Internet realizados pelas estações da rede. Isso deve ser possível através de um agendamento ou de uma requisição feita pelo administrador da rede

Fundamentação teórica

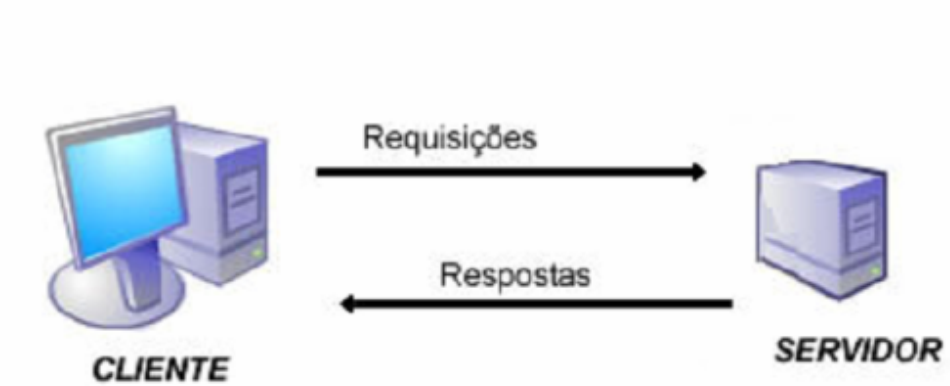
- Gerência de redes
  - Elementos gerenciados: São as estações que irão ser gerenciadas através do agente
  - Estação de gerência: É uma estação da rede que hospeda o software que gerencia a rede
  - Protocolo de gerência: É o idioma que permite a troca de informações entre o agente e o gerente
  - Informações de gerência: Definem os dados que podem ser referenciados em operações de protocolo de gerência

Fundamentação teórica

- O papel do gerente de redes
  - Avaliar o desempenho da sua equipe de suporte
  - Solicitar compra de equipamentos, aplicações ou outros recursos necessários
  - Providenciar treinamento adequado para a equipe
  - Reescalonar a solução de problemas para outros membros da equipe quando a solução demora

Fundamentação teórica

- Protocolo Session Message Block (SMB)
  - É um protocolo da IBM para compartilhar arquivos, impressoras, portas seriais e para comunicação entre computadores



Fundamentação teórica

- Aplicação Ntop
  - É um programa que monitora passivamente uma rede, coletando dados sobre os protocolos e sobre os hosts da rede
  - Foi escrito de uma forma portável com o objetivo de rodar em qualquer plataforma Unix e Win32
  - Possui um webserver integrado que permite consultas às informações através de um navegador
  - É distribuído sob uma licença pública geral, porém, a versão binária para Windows possui uma limitação de captura de mil pacotes

Fundamentação teórica

- Trabalhos correlatos
  - ISA Server: Não utiliza agentes. Controle total do acesso à internet dentro de uma rede baseada em computadores com sistema operacional Windows. Software Proprietário
  - Squid Web Proxy Cache: Não utiliza agentes. Permite o mesmo controle do anterior com a vantagem de ser gratuito e deve ser instalado em um servidor com sistema operacional Linux, porém, controla estações com qualquer sistema operacional
  - Web–Fi Server: Não utiliza agentes. É uma solução completa para uso corporativo mas requer o Microsoft Internet Explorer como navegador padrão. É um software proprietário
  - INCA: Utiliza agentes. Restringi o acesso do usuário a qualquer tipo de serviço de rede e é compatível apenas com a arquitetura Unix. Proprietário

Desenvolvimento – Requisitos

- Iniciar o aplicativo agente dentro da estação da rede toda vez que esta for inicializada (RF)
- Registrar da forma mais adequada em um arquivo, os acessos à Internet feitos na estação da rede (RF)
- Permitir que o administrador da ferramenta gerente agende um determinado dia da semana e horário para automaticamente solicitar os dados dos arquivos com os registros dos acessos à Internet de cada estação (RF)

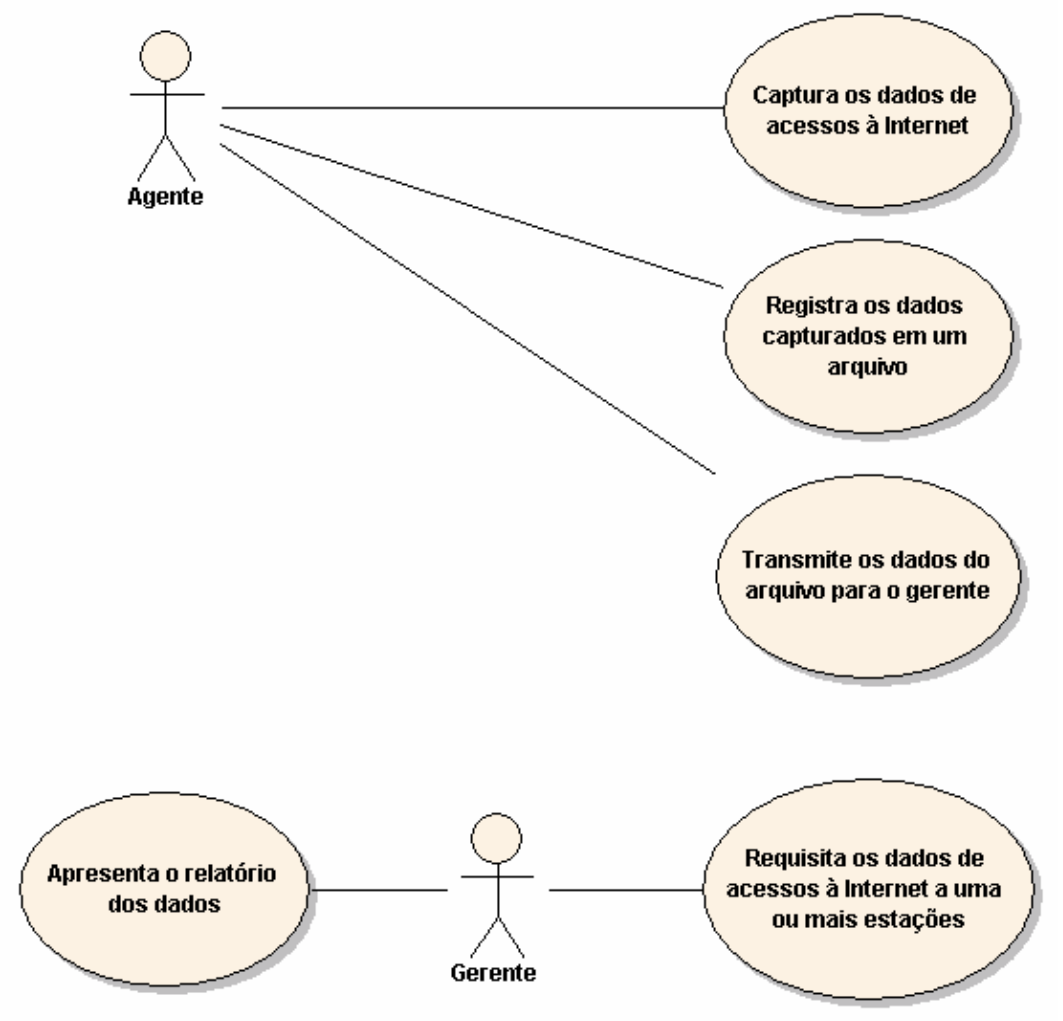
Desenvolvimento – Requisitos

- Possibilitar que o administrador da rede solicite o recolhimento dos dados dos arquivos com os registros dos acessos à Internet de uma estação específica ou de todas a qualquer momento (RF)
- Permitir a consulta das informações dos acessos à Internet de cada estação (RF)
- Serem implementados utilizando o ambiente de programação Delphi 7 da Borland (RNF)
- Serem compatíveis com os sistemas operacionais Windows 98, 98SE, 2000, ME e XP (RNF)

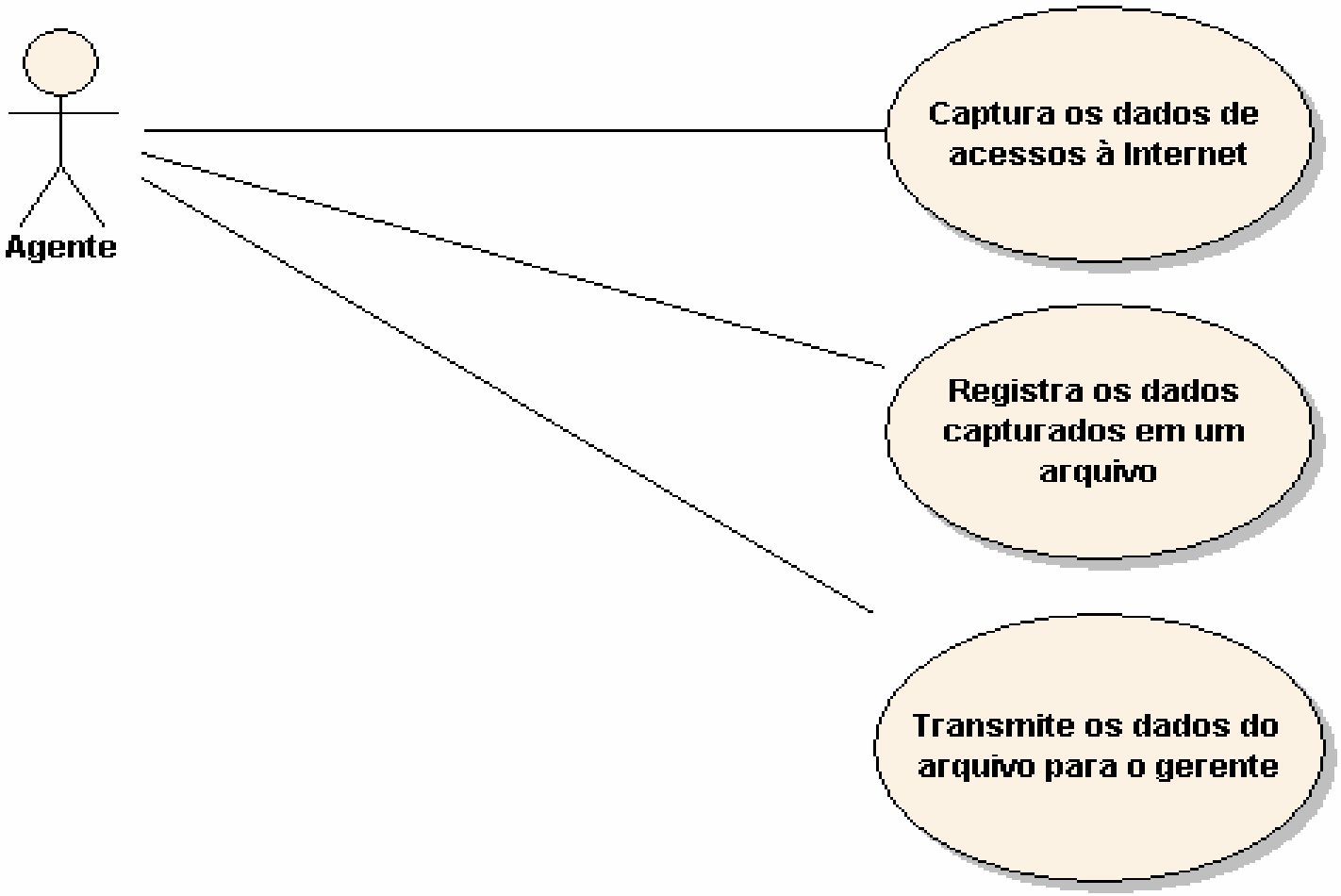
Especificação

- Técnicas e ferramentas utilizadas
  - Para especificação das ferramentas agente e gerente, foi utilizado a UML, usando os diagramas de casos de uso, de classe e de atividades. Para criação destes diagramas foi utilizado o software Enterprise Architect da Sparx Systems

Diagrama de casos de uso



Casos de uso do agente



Casos de uso do gerente

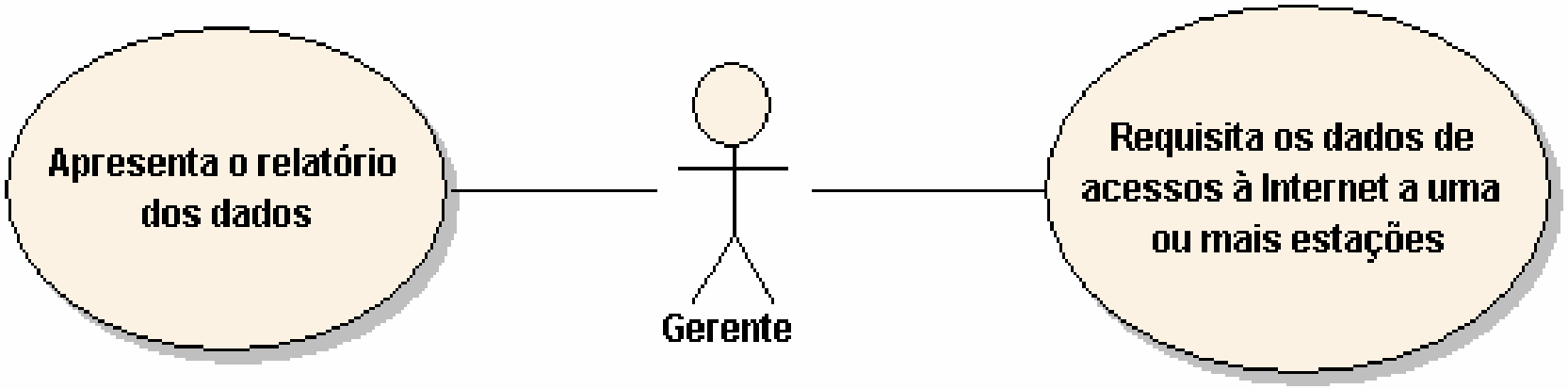
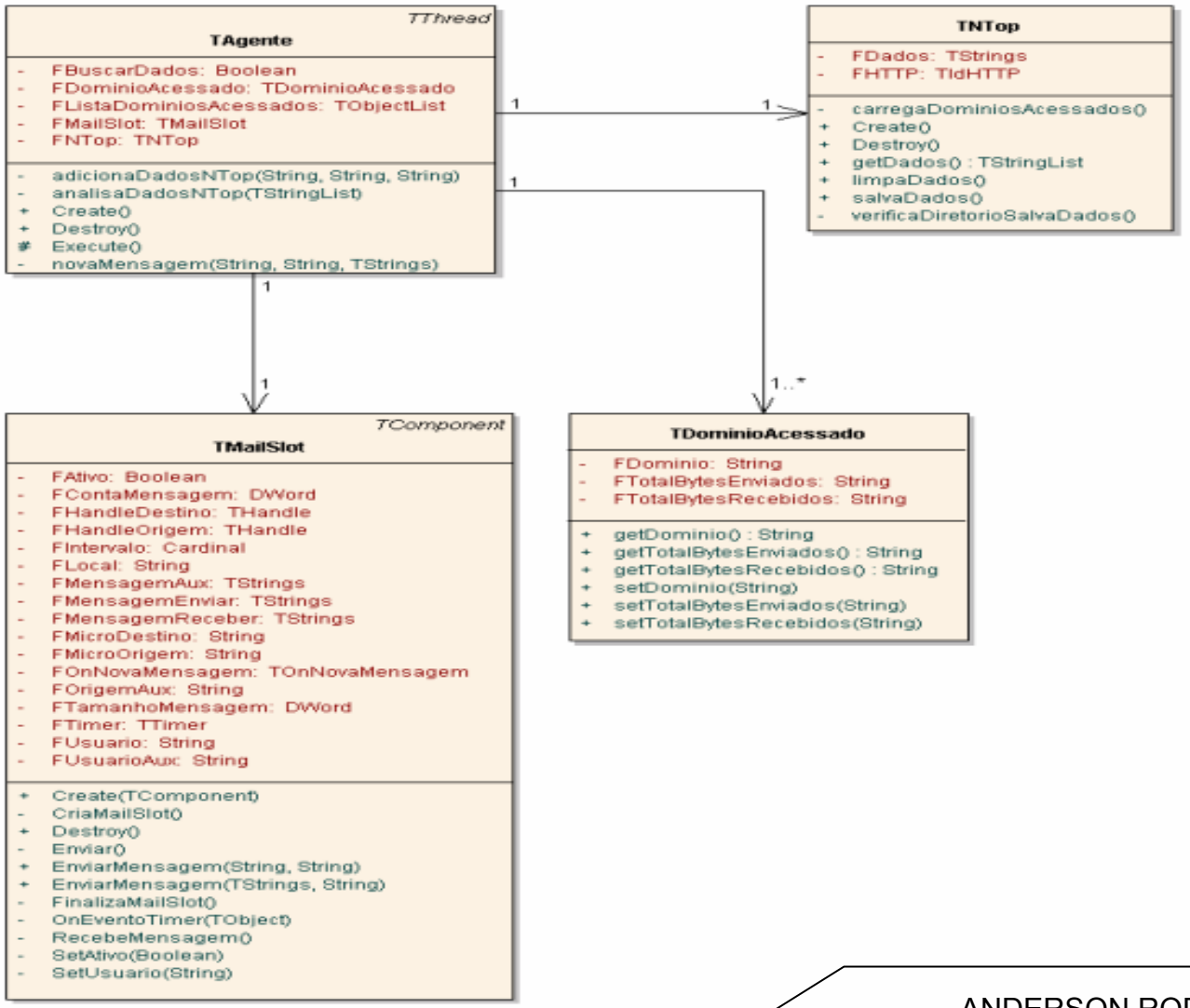
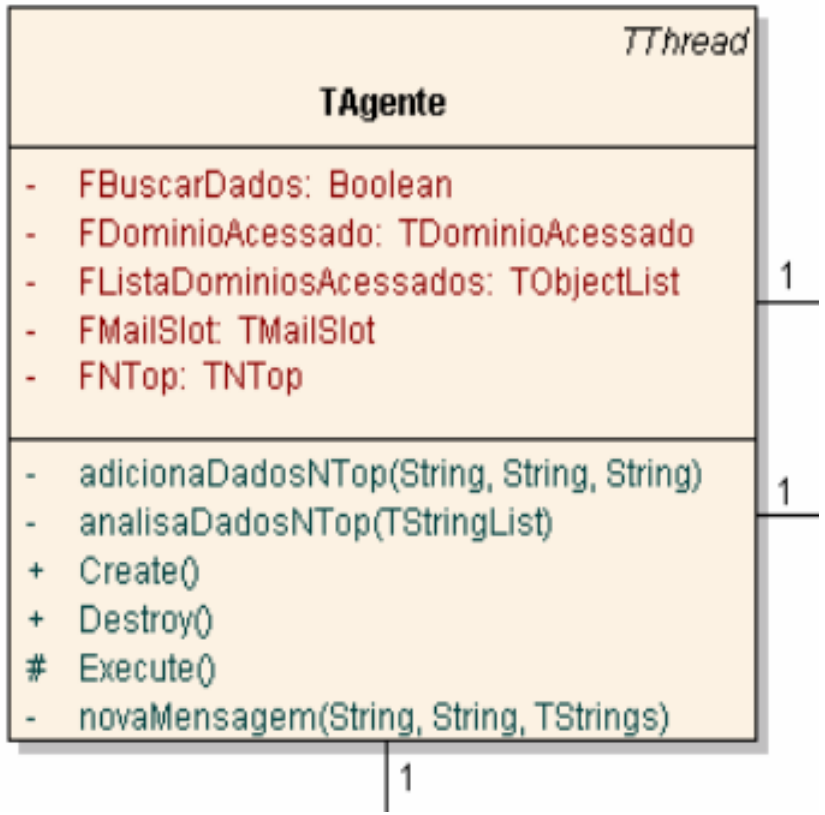


Diagrama de classes



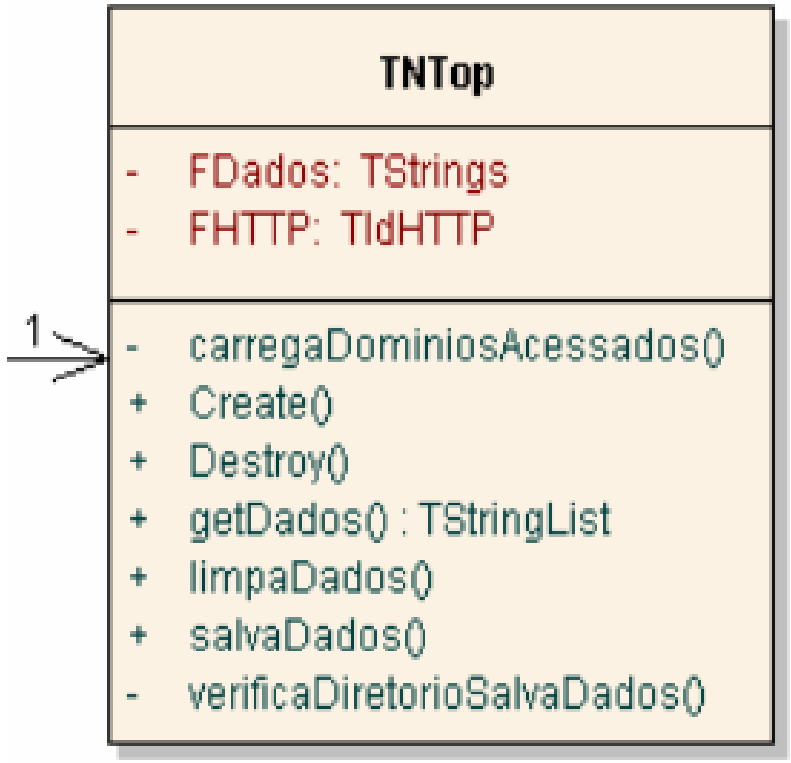
Classe TAgente

- Principal classe da ferramenta agente sendo ela uma thead responsável por instanciar cada uma das demais classes



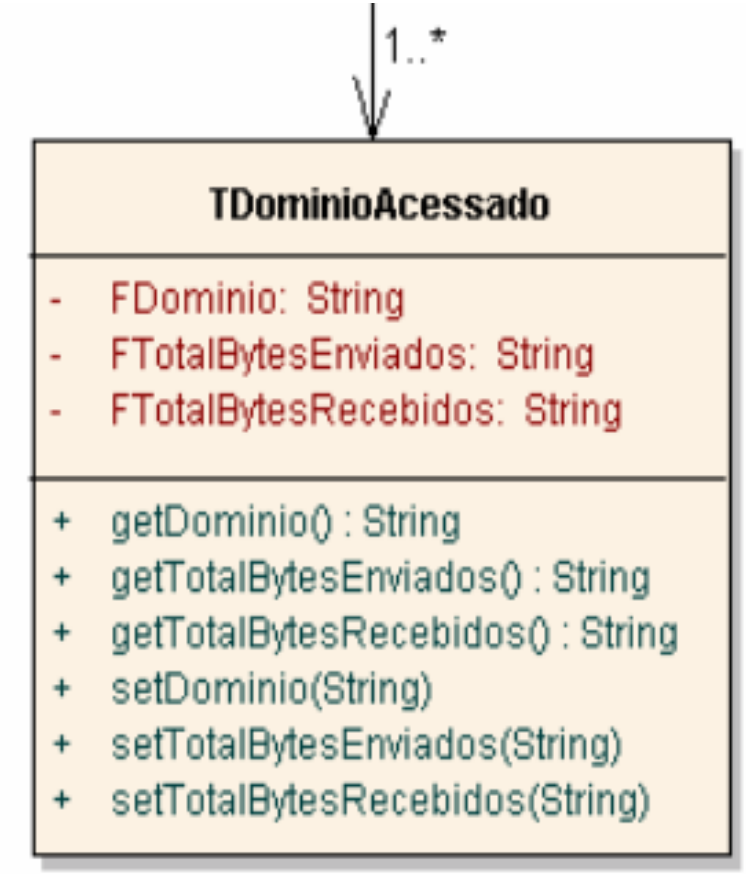
Classe TNTop

- Classe responsável por coletar os dados de acessos à Internet da aplicação Ntop



Classe TDominioAcessado

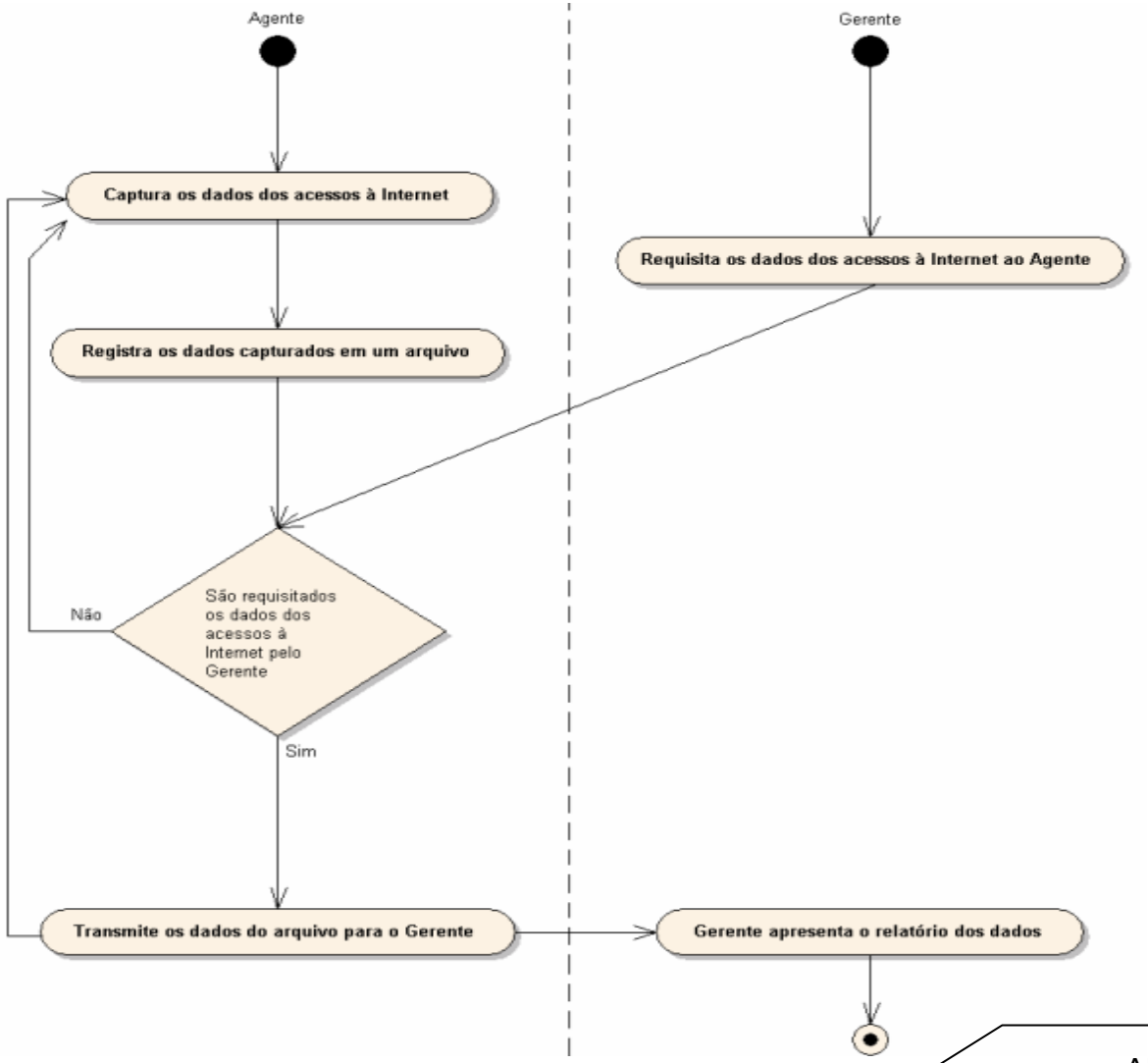
- Armazena os dados coletados pela classe TNTop



Classe TMailSlot

- Esta classe é um componente da classe TAgente e tem o objetivo de enviar e receber dados utilizando o protocolo SMB

Diagrama de atividades



Implementação

- Técnicas e ferramentas utilizadas
  - Para implementação das ferramentas foi utilizado o ambiente de programação Delphi 7 da Borland
  - Foi utilizada a aplicação Ntop e quando a mesma é iniciada é criado um webserver e todos os dados monitorados pela mesma podem ser acessados através de qualquer navegador da Internet pois o sistema de arquivos é formado por páginas em HTML
  - O agente captura os dados monitorados pela aplicação Ntop da página HTML gerada pela aplicação Ntop responsável somente pelos domínios acessados e armazena em um arquivo

Implementação

- O agente procura por um conjunto de identificadores (relacionados abaixo) que se refere às páginas acessadas, repetindo este processo até que localize todos os domínios e demais dados necessários dos acessos à Internet da estação

```
const
   cDominio      = '?dom=';
   cALIGNRIGHT   = '<TD  ALIGN=RIGHT>';
   cIgual        = '=';
   cFechaTag     = '>';
   cAbreTag      = '<';
   cEComercial   = '&';
   cPercentual   = '%';
```

Implementação

```
procedure TAgente.analisaDadosNTop(Dados: TStringList);
var
   wStrAux, wDominio, wBytesRec, wBytesEnv : String;
   wPos, wCont                             : Integer;
begin
   try
      try
         for wCont := 147 to Dados.Count - 1 do
            begin
               wStrAux := Dados.Strings[wCont];
               wPos    := Pos(cDominio,wStrAux);
               if wPos <> 0 then
                  begin
                     // Localiza Domínio
                     wDominio  := copy(wStrAux,wPos,length(wStrAux));
                     wDominio  := copy(wDominio,Pos(cIgual,wDominio)+1,length(wDominio));
                     wDominio  := copy(wDominio,0,Pos(cFechaTag,wDominio)-1);
                     // Localiza Bytes Enviados
                     wPos      := Pos(cALIGNRIGHT,wStrAux);
                     wBytesEnv := copy(wStrAux,wPos,length(wStrAux));
                     wBytesEnv := copy(wBytesEnv,Pos(cFechaTag,wBytesEnv)+1,length(wBytesEnv));
                     wBytesEnv := copy(wBytesEnv,0,Pos(cAbreTag,wBytesEnv)-1);
                     wPos      := Pos(cEComercial,wBytesEnv);
                     if wPos <> 0 then
                        wBytesEnv := copy(wBytesEnv,0,wPos-1);
                        if Pos('.',wBytesEnv) <> 0 then
                           wBytesEnv := wBytesEnv + ' KBytes'
                        else
                           wBytesEnv := wBytesEnv + ' Bytes';
```

Implementação

```
                    // Localiza Bytes Recebidos
                    wPos      := Pos(cPercentual,wStrAux) + 1;
                    wBytesRec := copy(wStrAux,wPos,length(wStrAux));
                    wPos      := Pos(cALIGNRIGHT,wBytesRec);
                    wBytesRec := copy(wBytesRec,wPos,length(wBytesRec));
                    wBytesRec := copy(wBytesRec,Pos(cFechaTag,wBytesRec)+1,length(wBytesRec));
                    wBytesRec := copy(wBytesRec,0,Pos(cAbreTag,wBytesRec)-1);
                    wPos      := Pos(cEComercial,wBytesRec);
                    if wPos <> 0 then
                       wBytesRec := copy(wBytesRec,0,wPos-1);
                    if Pos('.',wBytesRec) <> 0 then
                       wBytesRec := wBytesRec + ' KBytes'
                    else
                       wBytesRec := wBytesRec + ' Bytes';
                    Self.adicionaDadosNTop(wDominio,wBytesEnv,wBytesRec);
                 end;
           end;
        finally
     end;
  end;
end;
```

Implementação

- O protocolo SMB é implicitamente utilizado através dos comandos CreateMailSlot, CreateFile, WriteFile e ReadFile que são nativos de uma biblioteca do Microsoft Windows e de uso exclusivo para o protocolo SMB

```
// Procedimento que cria uma caixa de correio do SMB
procedure TMailSlot.CriaMailSlot;
begin
   Self.FLocal := '\\.\mailslot\' + cMailBox;
   Self.FHandleOrigem := CreateMailslot(PChar(Self.FLocal),0,0,nil);
   if Self.FHandleOrigem = INVALID_HANDLE_VALUE then
      Self.SetAtivo(False);
end;
```

Implementação

```
// Procedimento que envia mensagem para uma caixa de correio do SMB
procedure TMailSlot.Enviar;
var
   wBytes   : DWord;
   wDestino : String;
begin
   wDestino := '\\' + Self.FMicroDestino + '\mailslot\' + cMailBox;
   Self.FhandleDestino := CreateFile(PChar(wDestino),GENERIC_WRITE,FILE_SHARE_READ,nil,
                                     CREATE_ALWAYS,FILE_ATTRIBUTE_NORMAL,0);
   try
      if Self.FHandleDestino = INVALID_HANDLE_VALUE then
         exit
      else
         WriteFile(Self.FHandleDestino,Pointer(Self.FMensagemEnviar.Text)^,
                   length(Self.FMensagemEnviar.Text),wBytes,nil);
   finally
      CloseHandle(Self.FHandleDestino);
   end;
end;
```

Implementação

- Para transmissão das informações pela rede, elas tiveram que ser quebradas em partes quando a seqüência era superior a 255 bytes

```
procedure TMailSlot.EnviarMensagem(Destino: String; Mensagem: TStrings);
var
   wContador, wTamanho : Integer;
begin
   if length(TrimLeft(TrimRight(Destino))) = 0 then
      exit;
   Self.FMicroDestino := Destino;
   wTamanho := length(Mensagem.Text);
   if wTamanho <= 255 then
      begin
         with Self.FMensagemEnviar do
            begin
               Clear;
               AddStrings(Mensagem);
               Insert(0,Self.FMicroOrigem);
               Insert(1,Self.FUsuario);
            end;
         Self.Enviar;
      end
   else
```

Implementação

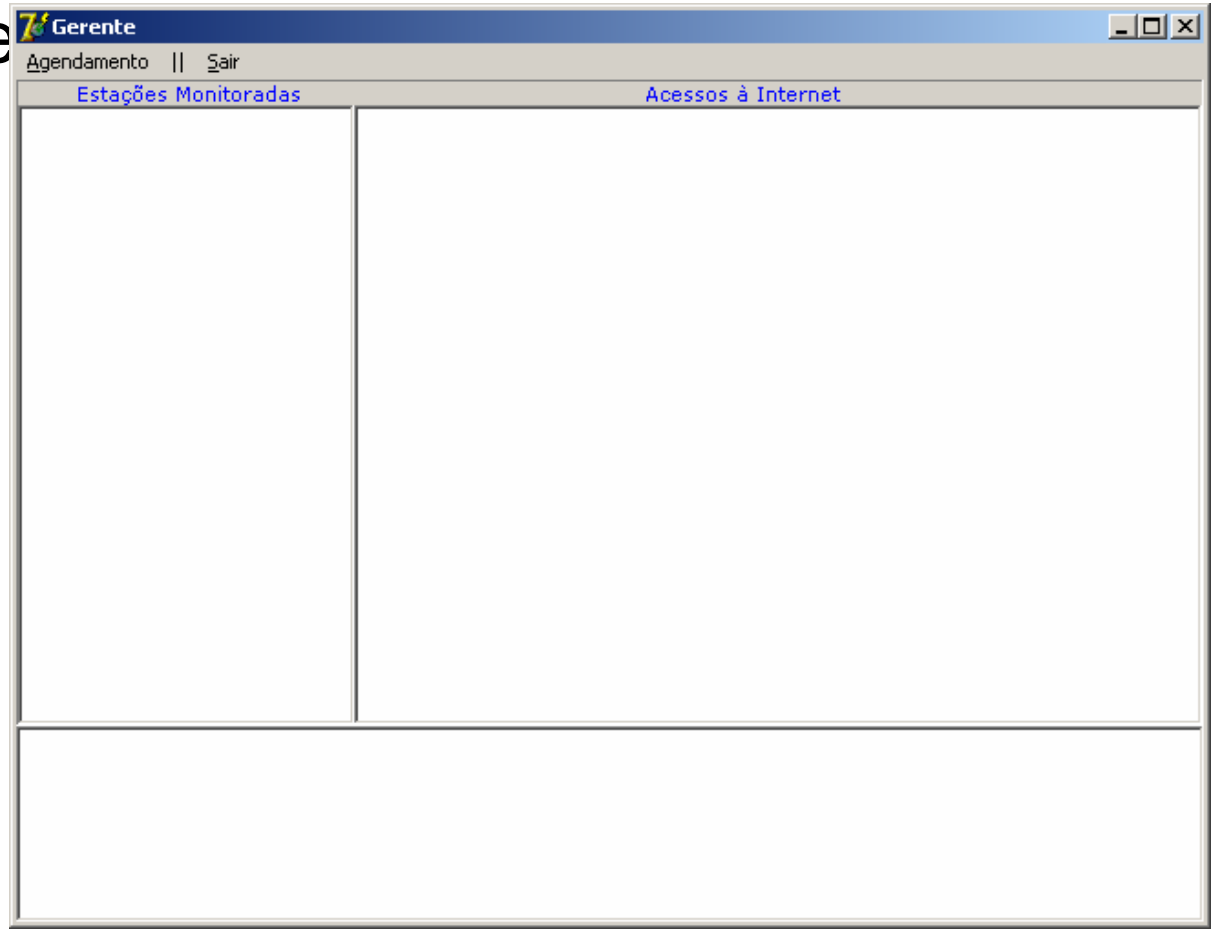
```
      begin
         with Self.FMensagemEnviar do
            begin
               Clear;
               Add('#INICIO#');
               Insert(0,Self.FMicroOrigem);
               Insert(1,Self.FUsuario);
               Self.Enviar;
               for wContador := 0 to Mensagem.Count - 1 do
                  begin
                     Clear;
                     Add(Mensagem.Strings[wContador]);
                     Insert(0,Self.FMicroOrigem);
                     Insert(1,Self.FUsuario);
                     Insert(2,'#CONTINUA#');
                     Self.Enviar;
                  end;
               Clear;
               Add('#FIM#');
               Insert(0,Self.FMicroOrigem);
               Insert(1,Self.FUsuario);
               Self.Enviar;
            end;
      end;
end;
```

Operacionalidade

- Primeiramente é importante destacar que o software é executado em duas partes distintas, o agente e o gerente
- É necessária a instalação e configuração do aplicativo Ntop na estação
- Também é necessária a instalação da ferramenta agente na estação
- É importante colocar tanto o Ntop quanto o agente no menu iniciar para que executem no momento em que o sistema operacional da estação for carregado
- O gerente deve ser executado antes de qualquer agente

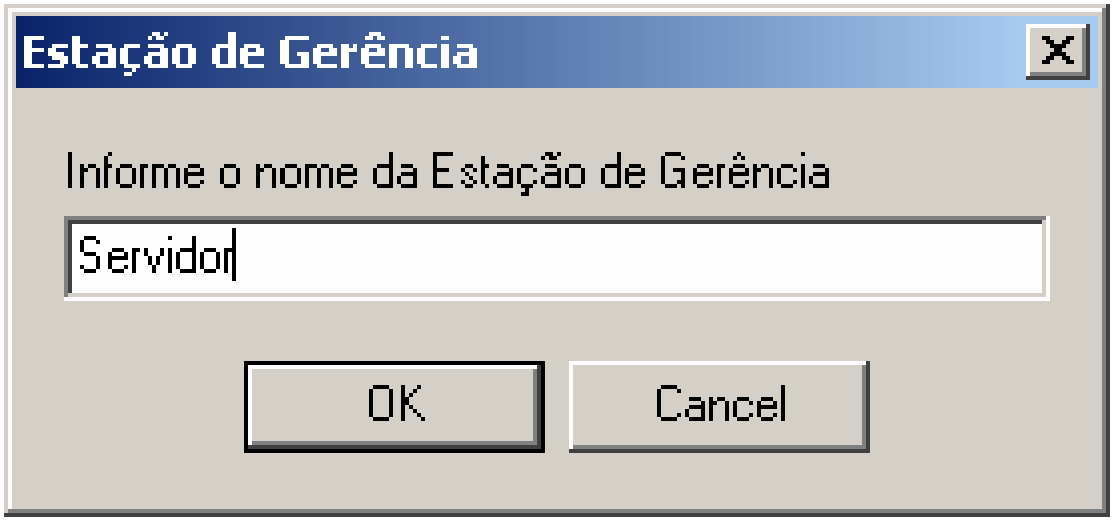
Operacionalidade

- Aplicação gerente antes da inicialização dos agentes



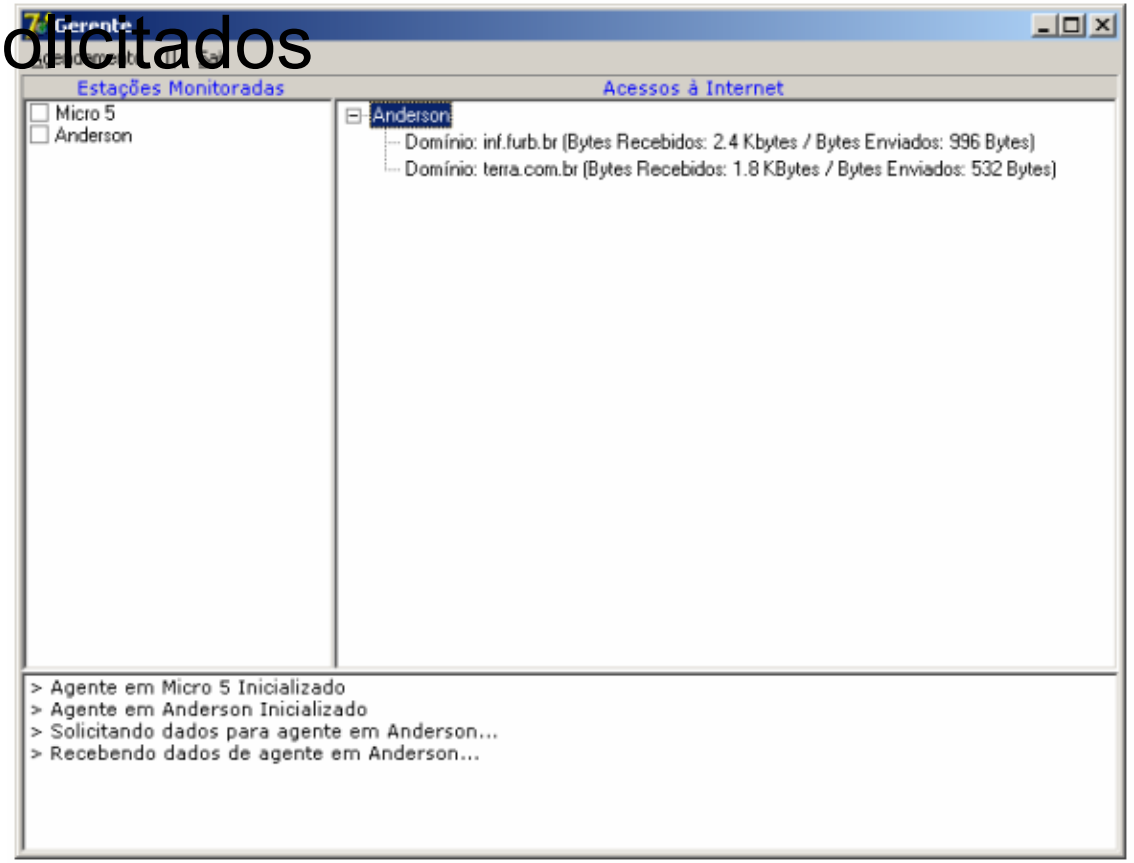
Operacionalidade

- Aplicação agente caso nunca tenha sido informado o nome da estação de gerência



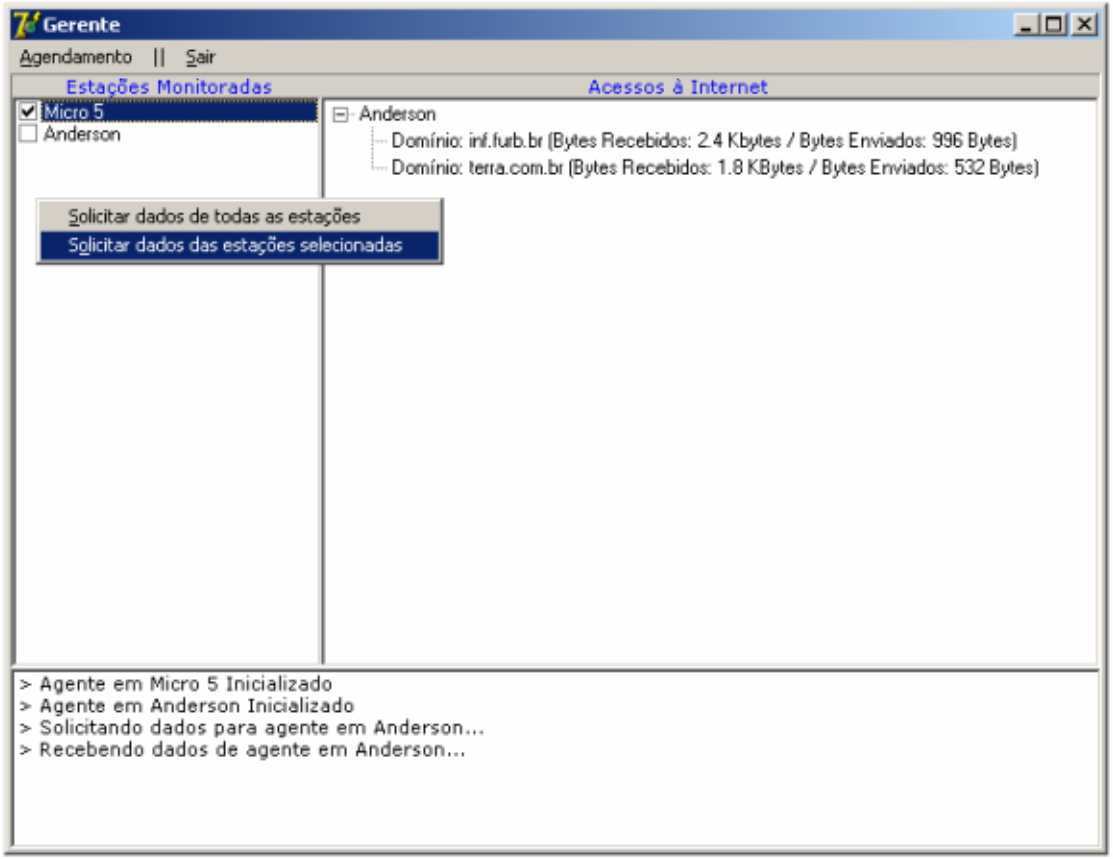
Operacionalidade

- Aplicação gerente com dois agentes inicializados sendo que o agente da estação Anderson teve seus dados solicitados



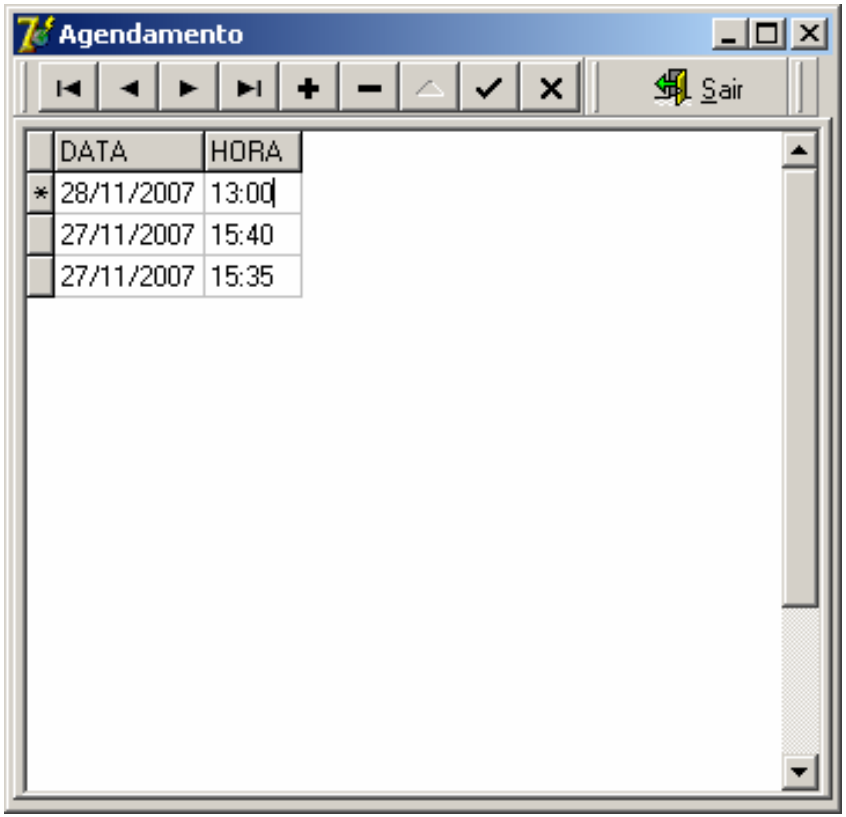
Operacionalidade

- Aplicação gerente solicitando dados do agente da estação Micro 5 que foi previamente selecionada



Operacionalidade

- Aplicação gerente agendando datas e horários para solicitar os dados dos agentes das estações



Resultados e discussão

- Observando o funcionamento das ferramentas agente e gerente, todas as informações são apresentadas no gerente no mesmo momento em que os dados são solicitados aos agentes
- É possível fazer uma análise mais detalhada verificando o registro gerado pelo agente no rodapé, neste local são apresentadas as inicializações dos agentes como também as solicitações e recebimentos dos dados

Resultados e discussão

- Comparação entre os trabalhos correlatos e o trabalho implementado

	ISA Server	Squid Web Proxy Cache	Web-Fi Server	INCA	Trabalho Implementado
Aplicação	Desktop	Desktop	Web	Desktop	Desktop
Configuração	Simples	Complexa	Simples	Simples	Simples
Dependência de outro software	Não	Não	Não	Não	Sim
Licença	Proprietária	Gratuita	Proprietária	Proprietária	Gratuita
Operacionalidade	Simples	Complexa	Simples	Simples	Simples
Plataforma	Windows	Linux	Windows	Unix, Linux ou Solaris	Windows
Processamento centralizado	Sim	Sim	Sim	Não	Não
Vulnerabilidade	Baixa	Baixa	Média	Baixa	Alta

Conclusões

- Com os estudos e implementações que foram feitos neste trabalho, concluí que é bem simples gerenciar o acesso à Internet das estações de uma rede de forma descentralizada, porque existem diversos protocolos que auxiliam neste gerenciamento
- Todos os requisitos foram supridos com o software, que visa apresentar de modo simples e rápido os acessos à Internet realizados pelas estações de uma rede

Conclusões

- A captura dos dados monitorados pelo Ntop foi bastante simples, já que o mesmo oferece os arquivos em HTML e sendo assim bastou rastrear determinados identificadores
- Apresentar os dados capturados com o agente do Ntop de maneira legível foi fácil e rápido pois o ambiente de programação Delphi possui vários recursos que ajudam neste aspecto
- A transmissão dos dados utilizando o protocolo SMB atendeu perfeitamente todos os requisitos. O tempo de resposta é bastante satisfatório, bem como a confiabilidade de transmissão das informações

Limitações

- Não foi possível garantir que os agentes não possam ser finalizados nas estações
- A segurança do arquivo que armazena os acessos à Internet em cada estação não pode ser garantida
- A versão para Windows do aplicativo Ntop possui uma limitação de captura de mil pacotes
- Não foi possível retirar o agente da lista de estações do gerente quando o mesmo é finalizado na estação

Extensões

- Criar uma segurança por meio de criptografia para o arquivo que guarda os acessos à Internet da estação ou persistir estes dados no gerente, eliminando a necessidade do arquivo na estação
- Apresentar na ferramenta gerente outros dados além do domínio, bytes enviados e bytes recebidos
- Aprimorar a parte gerencial, ou seja, permitir a impressão de relatórios
- Incorporar o código fonte do Ntop na aplicação agente e retirar a limitação de mil pacotes
- Garantir que o agente não possa ser finalizado na estação sem o consentimento do administrador