Medições, Monitoramento e Gerência de Redes e Serviços com ferramentas de código aberto

Alex Galhano Robertson[1,2]
Carlos Alberto Malcher Bastos[1]

1- Mestrado em Eng. de Telecomunicações da UFF
2- Rede Nacional de Ensino e Pesquisa - RNP

GTER-25
30-Mai-2008

Antes de começar ...

- Mestrando em Engenharia de Redes e Comunicação Multimídia pela UFF.

- Baseada em estudo para cliente do GTecCom
- Baseada em um capítulo da Tese de Mestrado
  - Orientador: Carlos Alberto Malcher Bastos

- No início: GTecCom/UFF
- Atualmente: RNP

Objetivo

- Objetivo
  - Esclarecer as diferenças entre Medir, Monitorar e Gerenciar, indicando situações onde cada ação se aplica melhor.
  - Ressaltar a importância e incentivar o uso e o desenvolvimento de bons Sistemas de Gerência de Redes, principalmente para aquelas que suportam serviços com requisitos rígidos.
  - Comparar Sistemas de Gerência de Redes de código aberto.

Agenda

- O que é medir?
- Medições Ativas
- Medições Passivas
- Medições para VoIP
- O que é monitorar?
- Monitorar o quê?
- Monitoração e Gerência
- NMS
- Itens importantes
- Modelos de Gerência
- ITIL e NMS
- IPv6 e NMS'es
- Comparação
- Conclusões

O que é medir? E medir o quê?

- Medir é ...
  - ... comparar grandezas de mesma espécie com um padrão.
- O que medir?
  - Os parâmetros importantes para o serviço prestado!
    - Atraso, Jitter, perda de pkts, consumo de banda.
      - Conte novidades!
    - Disponibilidade, desempenho, qualidade, custos, recursos, tempo de resposta em ações corretivas, tempos de execução de ações recorrentes, ...

Medições

- Medições Ativas
  - Precisa gerar tráfego na rede.
  - Geração de Tráfego Sintético
    - Simulação de aplicações

- Medições Passivas
  - Não precisa gerar tráfego na rede.
  - Ideal para identificar padrões e tendências de utilização dos recursos.

Ferramentas para medição

- Medição ativa
  - Ping, fping, traceroute, mtr, nmap, nessus, LG
  - D-ITG, mgen, iperf, pktgen
  - SIPp
- Medição passiva
  - tcpdump, wireshark, ntop, Snort
  - sFlow, NetFlow (protocolos)
  - **SNMP** (Protocolo)

SNMP

- SNMP – Simple Network Management Protocol
  - Protocolo utilizado por Sistemas de Gerência de Redes para resgatar informações de dispositivos na rede IP.
- Informação é transmitida com os comandos
  - GET, GETNEXT, GETBULK, SET, TRAP, INFORM
- Informação é definida pela MIB (Management Information Base)

Medições para VoIP

- Atraso, jitter, perda e consumo de banda
  - Reordenação de pkts, marcação de pacotes e frames, etc.
- Desempenho de proxies SIP
  - Individualmente ou um sistema inteiro.
- Experiência do usuário
  - Calculando MOS e Fator-R com parâmetros medidos na rede em tempo real, armazenados em CDR ou com tráfego sintético.

Quer mais sobre medições?

- Benchmarking for Network Interconnect Devices
  - RFC-2544 - Benchmarking Methodology
- Projeto GIGA
  - Infra-estrutura de medições em redes Ópticas
    - www.projetogiga.org.br e wiki.nuperc.unifacs.br
    - Desenvolvimento CactiSONAR/PerfSONAR
    - Ferramentas para Geração de Tráfego Sintético
    - Proposição de de protocolos alternativos ao TCP
    - Metodologias para alocação de caminhos

O que é monitorar? E por quê?

- O que é monitorar?
  - Acompanhar e avaliar.
  - Medir e comparar continuamente com valores pré-determinados.
    - Calculados ou medidos anteriormente.
- Por quê monitorar?
  - Assegurar-se de que a rede se encontra dentro de níveis normais e/ou aceitáveis.
  - Prever tendências para mudanças de perfis.
  - Permitir ações corretivas mais rápidas e acertadas.

Monitorar o que?

- Ambiente
  - Umidade, Temperatura, Acessos, ...
- Elementos de Rede
  - roteadores, firewalls, brigdes, switches, etc
    - Ocupação de enlaces, tipos de fluxos, classificação de serviços, compressão, fragmentação, filas, utilização de regras de FW e ACLs, etc.
- Servidores
  - Processos e serviços da Empresa, aplicações, vulnerabilidades, memória, espaço em disco, processos, arquivos abertos, conexões ativas e parâmetros particulares dos diversos serviços (impressões, acessos a sites, SMS enviados/recebidos, etc).

Monitorar o que?

- A Rede
  - Atraso, jitter e perdas entre pontos estratégicos e ocupação de enlaces.
- PABX IP
  - CDR (tamanho, registros, bilhetagem), status do sistema, utilização de CPU e memória, ocupação de canais, motivos de desconexão, qualidade das ligações, etc
- Estações de usuários (!?!?)
  - Status, uso de CPU e memória, espaço em disco, processos, arquivos e programas utilizados, etc.

Sistemas de Monitoramento

- Qualquer sistema que retire informações da rede, dispositivos ou serviços e as armazene para posterior análise.
  - Snort (IDS – Intrusion Detection Systems)
  - Nessus (Security Scanners)
  - Ntop
  - Cacti
  - NFSen/NFDump
  - Nagios, Zabbix, OpenNMS, Zenoss

Até aqui ...

... sabemos que informação precisamos e como conseguí-la.

Agora, só falta nos organizar para poder tomar as decisões de forma
mais rápida e mais precisa.

Monitoramento não é Gerência!

- Monitoramento
  - Acompanhar e avaliar; Medir continuamente.
  - **Permite conhecer o estado instantâneo e o histórico. Permite calcular tendências.**
    -
- Gerência
  - Ação de gerir, de dirigir;
  - Administração.
  - **Ações de controle. Pode agir sobre a rede.**

Sistemas de Gerência de Redes

- O que são os NMS?
  - Network Management Systems
  - Sistemas que integram as informações necessárias para uma boa administração dos recursos da rede.
    - Monitoramento da rede, seus dispositivos e serviços
    - Gerência de recursos (inventário)
    - Gerência de alarmes
    - Gerência de atividades (trouble ticket / bug tracker)
    - Mapas interativos ou estáticos
    - Relatórios gerenciais
    - Integração com outros sistemas de medição

Boas Práticas

- Sistemas de Gerência podem (e devem?) seguir práticas recomendadas por entidades e organizações especializadas.

  - COBIT – Control Objectives for Information and related Technology
    - "… is a set of best practices (framework) for information technology (IT) management …"

  - SoGP – Standard Of Good Practices
    - "… is a detailed documentation of best practice for information security."

Modelos de Gerência

- TMN
  - Telecommunications Management Network
  - Desevolvido pelo ITU-T em maio de 1996 – M.3010
- FCAPS
  - Fault, Configuration, Accounting, Performance, Security
  - Desenvolvido pelo ITU-T em abril de 1997 – M.3400
- ITIL – Information Technology Infrastructure Library
  - "… is a set of concepts and techniques for managing information technology (IT) infrastructure, development, and operations."
  - UK Central Computer and Telecommunication Agency
  - Adoção em massa pelo meio dos anos 90.

ITIL – Últimas Versões

- ITIL v2
  - Service Delivery
  - Service Support
  - ICT Infra-Structure management
  - The business Perspective
  - Application Management
  - Software Asset Management
  - Planning to Implement Service Management
  - ITIL Small-Scale implementation
- ITIL v3 (disponibilizado em Maio de 2007)
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operation
  - Continual Service Improvement

Implementando Modelos de Gerência

- NMS em "sintonia" com o Modelo de Gerência adotado

  → **EMS (Enterprise Management System)** (Exemplo TVE-RJ)

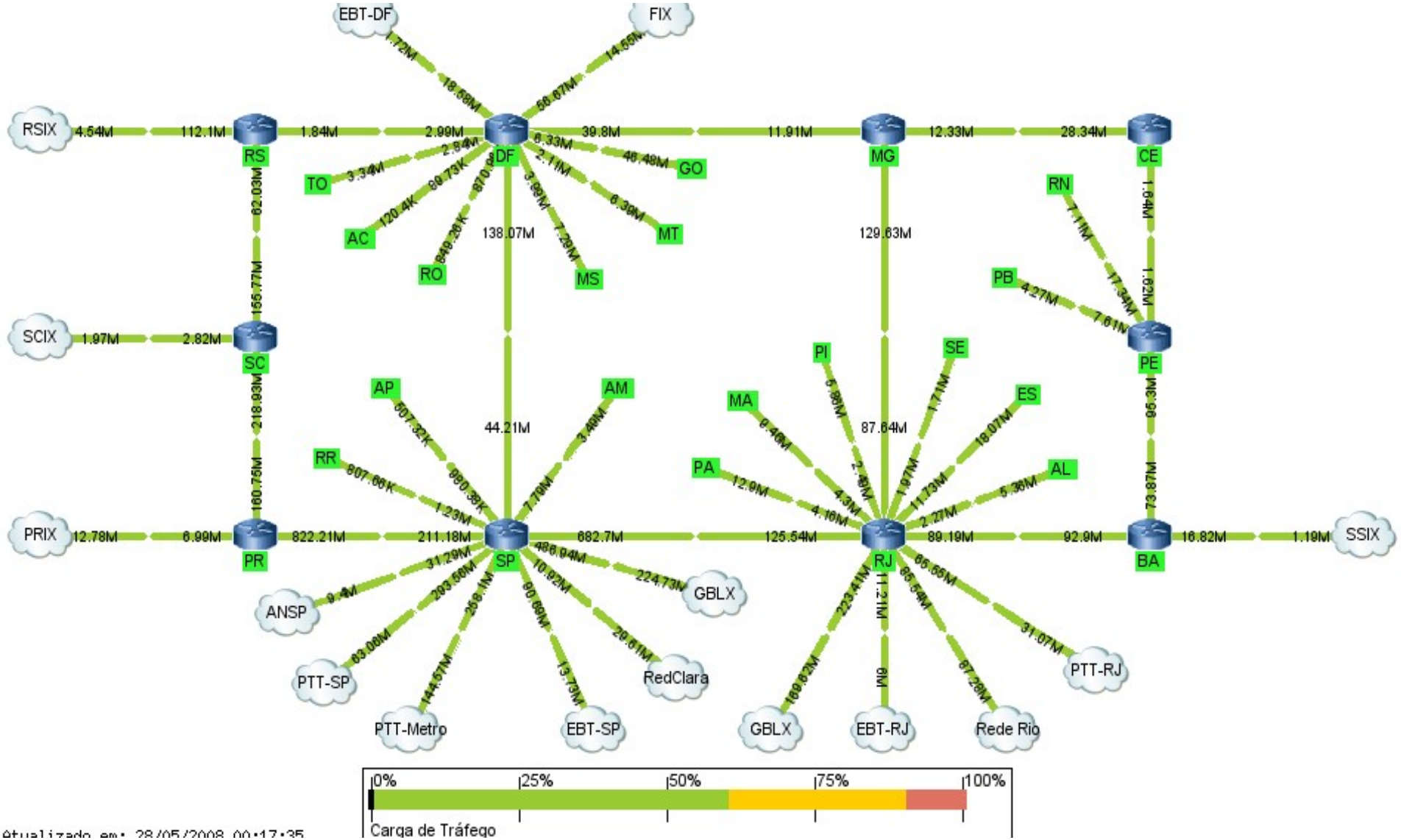
ITIL e NMS

- ITIL v3
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operation
  - Continual Service Improvement

Melhoram o processo de tomada de decisão

- NMS
  - Visão do todo (da rede e de cada serviço)
  - Perfis e tendências
  - Documentação e Históricos
  - Alarmes, diagnósticos e ações corretivas em tempo real
  - Conjunto de soluções + outras ferramentas de medição

Visão do todo



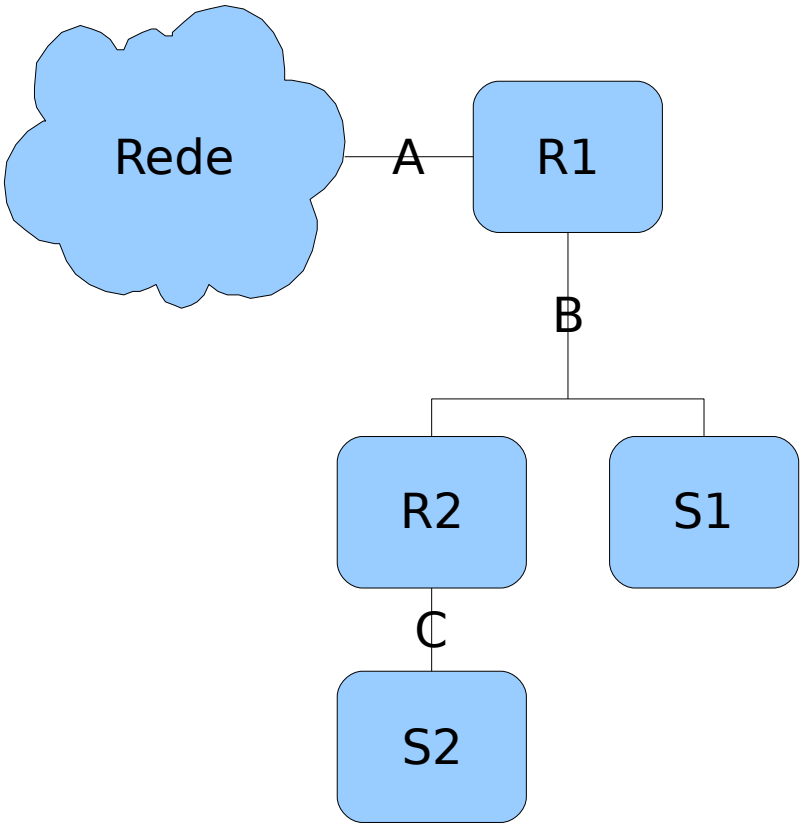
Históricos

- Possibilita investigação de acontecimentos passados
- Permite calcular **tendências** futuras
  - **Previne falhas** simples, pois ajuda a evitar a escassez de recursos.
- Estabeleça "**Linhas de Base**"
  - Associação permite o cálculo da **disponibilidade dos recursos**.
  - Possibilita a verificação do cumprimento dos acordos de SLA.

Alarmes

- A maioria dos NMS recebem alarmes por Traps SNMP.
- Alarmes de eventos isolados ajudam, mas dizem pouco sobre um problema real.
- Correlacionamento de alarmes e eventos melhora muito o diagnóstico.
  - Hierarquia de elementos na rede.
  - Aviso ou ação só é disparado se ocorrer uma sequência específica de eventos.

Correlacionamento de Eventos



- Hierarquia
  - Problema em A não deve disparar alarmes de R2, S1 e S2.
- Serviços S1 e S2 são relacionados
  - Alarme só dispara se trigger atingir níveis específicos nos dois servidores.

Operador Virtual

- Monitora
  - Medição e armazenamento
- Processa as informações
- Age!
  - Modifica LSPs ou tabelas de rotas, aumenta limite de emails na fila, recarrega configurações, desliga chamadas presas, etc
  - Envia notificações e registra as modificações

Relatórios

- Fornece um panorama da infra-estrutura de redes e dos serviços monitorados.
  - Devem ser emitidos regularmente.
- Publico alvo: Gerentes e Administradores
- É possível obter relatórios com detalhes de algum serviço
  - Geralmente, emitidos por demanda.
  - Arquivos de log são relatórios detalhados?

Relatórios importantes

- Gerentes
  - Disponibilidade de serviços prestados **por** terceiros
  - Disponibilidade de serviços prestados **para** terceiros
  - As 'N' maiores causas de indisponibilidade
- Administrador (Resp. pela operação)
  - Circuitos com alta ocupação
  - Servidores com alto uso de disco ou memória
  - Os 'N' problemas mais comuns

Recursos humanos

- O profissional é parte integrante da solução!
  - É recomendável haver pelo menos um funcionário especificamente para administrar e operar o SGR.
    - O profissional DEVE ser capaz de instalar, configurar e operar o conjunto de ferramentas que compõe o Sistema de Gerência de Redes.
  - Dependendo da atividade ou do tamanho da empresa, pode ser necessário uma equipe de gerência.

Comunicação

- Sim, comunicação!
  - Apresentação da informação com clareza, de forma organizada e compreensível
    - Gráficos e relatórios
  - Forma eficiente de transferir conhecimento
    - e delegar tarefas
- Documentação
  - Descrição de procedimentos
  - Manuais de operação de sistemas e equipamentos

Profissionais da operação precisam de informações!

Funções desejáveis

- Gerência de inventário
- Gerência de alarmes
- Gerência de eventos
- Integração com CRM
- Integração com outras ferramentas de medição
- Suporte ao serviço de Telefonia sobre IP

IPv6 e NMS'es

- Até pouco tempo, a maioria dos NMSes ainda não possuia suporte a IPv6.

- Felizmente, todos já estão implementando.

  Se não na versão estável, pelo menos na versão *beta.*

- Versões comerciais já suportam v6.

Comparação I

	Código Aberto			
	Zabbix	**Nagios**	**OpenNMS**	**Zenoss**
Versão Gratuita (G) e/ou Comercial (C)	Gratuita	Gratuita	Gratuita	Gratuita e Comercial (3)
Comercializa dispositivo específico para gerência de redes	Não	Sim	Não	Sim
Comercializa serviço de monitoramento remoto	Não	Não	Não	Não
Documentação e suporte on line (aberta)	Boa	Muito boa	Muito boa	Muito boa
Possui suporte on site	Sim	Sim	Não	Sim
Possui serviço de consultoria	Sim	Sim	Sim	Sim
Possui treinamento	Sim	Não	Sim	Sim
Possui parceiros no Brasil	Não	2 parceiros	Não	1 parceiro

Comparação II

	Código Aberto			
	Zabbix	**Nagios**	**OpenNMS**	**Zenoss**
Sistema Operacional	AIX, X-BSD, HP-UX, Linux, MacOS X, Solaris, Tru64/OS	Linux	Linux, Windows, BSD, PPC64, Solaris	Linux, VMWare
Interface	Web	Web	Web	Web
Calcula disponibilidade	Sim	Não	Sim	Sim
Calcula Tendências	Sim	Não	Não	Sim
Gerência de inventário	Não	Não	Não	Sim
Auto-Discovery	Sim	Sim. Por sw de terceiros	Sim	Sim
Monitora dispositivos e serviços novos e/ou de terceiros	Sim. Utilizando complementos.	Sim. Utilizando Plugins	Sim. Configurações específicas.	Sim. Utilizando ZenPacks
Reconhece Traps SNMP nativamente	Sim	Não. Precisa de Patch	Sim	Sim
Desenha mapa lógico da rede (auto - manual)	Não informado	Automático	Não. Trabalho em Progresso	Automático
Mapeia os dispositivos geograficamente	Sim	Não	Não	Sim
Correlacionamento de eventos	Sim	Não	Sim	Sim
Suporte a NetFlow	Não	Não	Sim. Integração com outro SW	Não
Ferramentas específicas para VoIP	Não	Não	Sim. Adaptação para Cisco	Não
Suporte a IPv6	Ainda em Beta, para próxima versão.	Sim	Não	Não

Últimas versões

- Nagios
  - Em 19-05-2008
- Zenoss
  - Em 15-05-2008
- OpenNMS
  - Em 07-05-2008
- Zabbix
  - Em 25-03-2008

Comentários

- **Nagios** é, sem dúvida, o NMS de código aberto mais utilizado, apesar de não ser o mais completo.
- **Zenoss** é o sistema de código aberto com maior apelo comercial.
  - Talvez isso faça dele o mais completo e mais amigável.
- **OpenNMS** mostra preocupações mais gerenciais (procura seguir FCAPS). Manuseio não parece ser muito fácil.
- **Zabbix** está sendo bastante comentado e começa a aparecer com força. Aparentemente, possui interface bem amigável, mas documentação e suporte deixam a desejar.

Conclusões

- Gerência ≠ Monitoramento
- … muito importante manter um Sistema de Gerência de Redes.
  - Tão simples quanto apenas monitoramento e alarmes para enlaces e serviços.
  - Tão complexo quanto se queira.
- O profissional ou equipe que opera o sistema é um componente importante.
  - Deve ser suficientemente capacitado.

Conclusões

- “O” Sistema de Gerência de Redes ...
  - ... não existe!
  - Será necessário utilizar ferramentas de medições auxiliares, realizar adequações, juntar sistemas , programar, programar e programar.
  - Pode-se criar um Framework para unir as ferramentas necessárias para a prestação de serviços específicos.

Conclusões - VoIP

- Certifique-se que sua rede suporta a demanda.
  - Faça medições antes de oferecer serviços críticos
- Apesar dos PBX IP disponibilizarem informações via SNMP, nenhum NMS de código aberto possui suporte a VoIP.
  - Não monitoram todos os parâmetros.
  - Não interpretam os resultados.
- Para o monitoramento adequado de redes VoIP ainda é preciso utilizar outros softwares ou desenvolver complementos.
  - Informações úteis estão na rede, nos dispositivos e no CDR.
- O mesmo pode se dizer sobre vídeo.

Trabalhos Futuros

- Adequar NMS aos modelos de gerência
  - EMS - Enterprise Management System
- Implementar suporte a VoIP nos NMS
  - Medições, interpretações e alarmes.
  - Construir um “Medidor de Qualidade” específico para Voz (e Vídeo) sobre IP.
- Incluir suporte a NetFlow e Sflow nos NMS
  - Integração com outros softwares
  - Suporte nativo
- Integrar ferramentas de medições nos NMS

Obrigado!

Alex Galhano Robertson
alexgr@rnp.br