Desafios de Gerência e Segurança de Redes

Elias Procópio Duarte Jr.
DInfo /UFPR
Itaipu - Julho de 2003

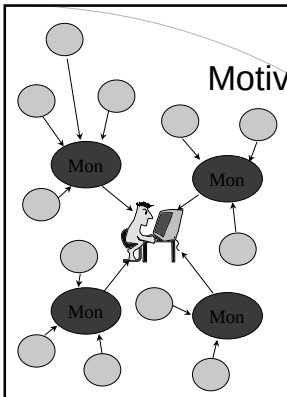
Roteiro

- Sistemas Integrados de Gerência de Redes
- Funcionalidade
- O Desafio da Segurança
- Paradigmas de Gerência
- O *framework* SNMP
- Conclusões

Sistemas de Gerência de Redes

- "As redes e as organizações que as possuem tem se tornado indistinguíveis"
- O custo de falhas, problemas de segurança, desempenho é cada vez mais alto
- Por outro lado: as redes estão cada vez maiores e mais complexas...
- Solução: usar ferramentas automatizadas para monitorar e controlar a rede

Motivação



- Uma plataforma que integra ferramentas
- Uma interface única para monitoração e controle (via Web)
- Um sistema integrado, independente de hardware ou sistema operacional

Funcionalidade de Gerência

- *Gerência de*
  - Falhas
  - Desempenho
  - Configuração
  - Contabilização
  - Segurança

Gerência de Falhas

- Motivação: o que fazer quando a rede não está funcionando corretamente?
- Talvez a função mais importante
- Consiste em localizar e resolver problemas ou falhas da rede
- Um bom sistema de gerência de falhas tem consequência direta no um aumento da confiabilidade da rede em si

Etapas na Gerência de Falhas

- Inicialmente: identificar a falha (*através de monitoração ou recebimento de alarme)*
- Em seguida: isolar a falha (*o que exatamente está causando o problema?)*
- Finalmente: corrigir a falha *(se possível)*

Gerência de Desempenho

- A rede está lenta? Por que?
- Monitorar a performance, o desempenho na rede
- Parâmetros usuais: throughput, utilização
- É importante estabelecer metas, ex.: o que é um “bom tempo de resposta”?
- As vezes para melhorar o desempenho basta aumentar o buffer de alguns dispositivos...

Análise de Performance da Rede

- Inicialmente: coletar dados sobre a utilização de máquinas e links: *util%=(bits enviados+bits recebidos)/banda*
- Procurar gargalos e isolar problemas de desempenho (*usando ferramentas*)
- Alarmes podem indicar problemas de performance, ao invés de falhas

Gerência de Configuração

- Permite *controlar* a rede a partir da estação de gerência
- Permite a configuração de hardware (ex: roteadores) e software (ex: protocolos)
- Permite também a troca de software instalado em dispositivos da rede
- Deve incluir um rígido esquema de segurança para impedir ataques danosos

Passos na Configuração

- Inicialmente é importante obter o estado corrente de todos os dispositivos
- Esta informação é então usada para, eventualmente, modificar a configuração da rede
- É importante manter um inventário, usando ferramenta que permita sua manutenção

Gerência de Contabilização

- Quanto cada usuário usou a rede? E cada departamento? Quanto deve pagar pelo uso?
- A contabilidade envolve
  - medir o uso da rede
  - o estabelecimento de métricas
  - a checagem de cotas
  - a determinação de custos
  - e mandar a conta para os usuários

Ferramentas para Contabilização

- Inicialmente coletam estatísticas sobre a utilização da rede
- Métricas: quantidade de bytes transferidos, transações distribuídas, tempo...
- Ajudam o gerente na tomada de decisões a respeito da configuração da rede e alocação de recursos

Gerência de Segurança

- Envolve o controle do acesso a informação armazenada
- Não inclui ferramentas de segurança a nível de aplicação, sistema operacional ou físico
- O quinhão específico da gerência envolve a configuração, monitoração e controle do acesso

Etapas da Gerência da Segurança

- Identificar qual informação deve ser protegida, e de que forma
- Determinar os pontos de acesso à rede
- Introduzir métodos de segurança nos pontos de acesso (ex.: fazer *log* de acessos, auditoria)
- Gerenciar o conjunto de medidas de segurança espalhadas pela rede

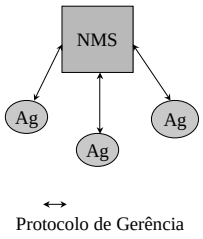
Uma Ferramenta de Gerência de Segurança

- Monitoração de *firewall*: emitindo alarmes sempre que pacotes são descartados
- Monitoração de servidores: *logging*
- Análise de Tráfego: na busca de padrões que indiquem um comportamento suspeito
- Auditoria: sistemas que façam uma varredura de *logs* na busca de eventos de segurança

Gerência da Internet Redes TCP/IP

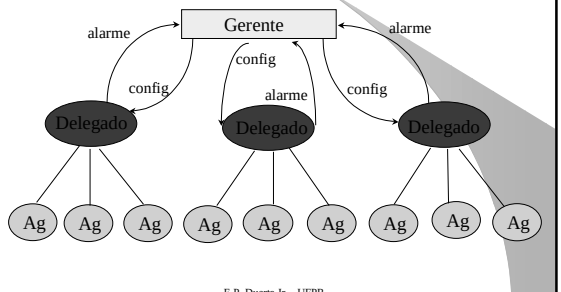
- O Protocolo SNMP
- *Simple Network Management Protocol*
- Padrão TCP/IP/Internet, hoje na versão 3
- Aplicação UDP/IP
- Vastamente implementado: disponível virtualmente para todo dispositivo de rede
- Software de Domínio Público: Net-SNMP http://www.net-snmp.org

O Paradigma Gerente/Agente



- O gerente (NMS - “Network Managemen Station”) se comunica, usando um protocolo de gerência de redes, com
- Agentes, espalhados pela rede, cada um responsável por um elemento da rede

Gerência Distribuída



Gerentes & Agentes

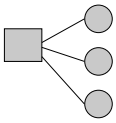
- O gerente humano monitora e controla a rede a partir do NMS
- É importante que a interface seja gráfica e intuitiva
- Diversos aplicativos de gerência podem estar presentes
- O agente tem um banco de dados com informações do objeto gerenciado
- O gerente pode requisitar informações do agente *(polling)* ou
- O agente pode emitir alarmes ao gerente

Os Padrões SNMP Definem

- Entidades de Gerência
  - Estações de Gerência em Vários Níveis
  - Nodos (“Unidades”) Gerenciados
- Estrutura e Sintaxe das Informações de Gerência
- Protocolo de Gerência
- Mecanismos de Segurança

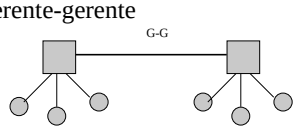
O Protocolo

- Usado para o gerente comunicar com agentes
- As operações básicas definidas são:
  - **get** (ler objetos)
  - **set** (escrever objetos)
  - **trap** (reportar alarmes)



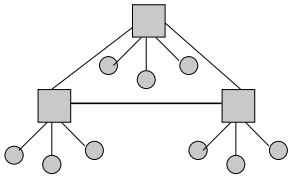
SNMPv2

- Inclui algumas novas operações: *getbulk*...
- Elabora mecanismos de segurança
- Antes apenas a COMUNIDADE (senha)
- Acrescenta mecanismos de comunicação gerente-gerente



SNMPv3

- Facilita a gerência distribuída
- Elabora mecanismos de segurança



O Agente

- snmpd (servidor)
- Cada agente tem uma MIB (*Management Information Base*)
- Existe uma série de MIBs padrão, que descrevem protocolos, maquinas, aplicativos
- Cada MIB contém uma série de objetos de gerência têm identificadores padrão

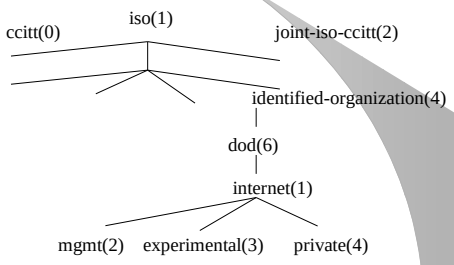
Objetos de Gerência

- Variáveis de uma MIB
- Escalares ou tabelas
- Tipos de Dados:
  - Counter, Gauge
  - Time Ticks (1/100 segundo)
  - DisplayString, PhysAddress,.....
- Identificadores são cuidadosamente assinalados/estruturados

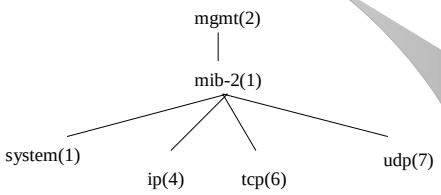
SMI: Structure of Manament Information

- Informação é componente chave dos sistemas de gerência, no SNMP:
  - monitorar um sistema => ler objetos
  - controlar um sistema => escrever objetos
- Escrito em um subconjunto do ASN.1
- Abstract Syntax Notation 1: linguagem ISO/OSI para definir a sintaxe de dados a nível de aplicação

SMI: Structure of Management Information - Árvore de Identificadores



Continuação da Árvore de Identificadores de Objetos



Exemplos de Objetos

- 1.3.6.1.2.1.1.1 é o **system.sysDescr**, string que descreve o agente

```
lostPackets OBJECT TYPE
    SYNTAX Counter32
    MAXACCESS read-only
    STATUS current
    DESCRIPTION
        "pacotes perdidos desde o último boot"
    ::= {experimental 20}
```

Os Grupos da MIB-II

- Objetos padronizados para gerenciar protocolos, interfaces de rede, ...
- São 9 grupos:
  - System, Interfaces, IP, ICMP
  - TCP, UDP, EGP, SNMP
  - Transmission

SNMPv3: Cont.

- Elabora um esquema de seguraça (autenticação - autorização) unificado
- *View Based Access Control Method*
- Permite assim uma maior capacidade de configuração remota de dispositivos da rede
- RFC's publicados em janeiro/98:
  - RFC's 2271-3
- As operações do protocolo se mantém as mesmas da versão 2

Tolerância a Falhas

- Um sistema *tolerante a falhas* continua funcionando corretamente mesmo na presença de falhas de alguns de seus componenentes, ainda que com desempenho degradado;
- Como organizar um sistema de monitoração totalmente tolerante a falhas?

Gerência de Redes Tolerante a Falhas

- Paradoxo da Gerência
- É importante que o sistema de gerência continue funcionando na presença de falhas
- Aplicações Distribuídas implementadas em SNMP
- Algoritmos de Monitoração para LAN e WAN
- Replicação, Proxies de Roteamento

Diagnóstico em Nível de Sistema

- Estratégias que permitem monitoração totalmente distribuída
- A monitoração continua, mesmo na presença de falhas na rede
- Eficientes para implementação SNMP
- Interface Web

IEEE LANOMS'2003

- O IEEE dá o suporte técnico para várias conferências mundias em gerência de redes
- IM, NOMS, APNOMS e LANOMS
- Neste ano o LANOMS vai acontecer em

Foz do Iguaçu, de 4 a 6 de setembro de 2003

LANOMS em Foz

- Foram 60 artigos submetidos de todo o mundo (record do evento)
- Palestrantes Convidados confirmados:
  - Dr. Masayoshi Ejiri (Fujitsu, Japão)
  - Dr. German Goldszmith (IBM, EUA)
  - Prof. Mehmet Ulema (EUA)
  - Prof. Guy Pujole (França)

LANOMS - WGRS

- Em conjunto com o LANOMS vamos ter o Workshop de Gerência de Redes e Serviços
- Apenas palestras convidadas:
  - Empresas produtoras de software de gerência
  - Empresas grandes usuárias de gerência
  - Empresas provedoras de comunicações
  - Representantes de Redes Latino Americanas e da Internet2 americana

Conclusões

- Gerência = Monitoração & Controle
- Sistemas Integrados de Gerência: 5 funções principais
- SNMP: diversos produtos disponíveis, comerciais e de domínio público
- Abordagens Distribuídas Confiáveis
- Futuro: *self-management*