Gestão
Resumo Arquiteturas de Comunicação

Universidade de Aveiro

Sebastian D. González,

Gestão
Resumo Arquiteturas de Comunicação

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

sebastian.duque@ua.pt(103690)

23 de janeiro de 2024

Conteúdo

Lista de Figuras

Glossário

HTTP Hypertext Transfer Protocol.

MIB Management Information Base.

NMS Network Management System.

OID Object Identifier.

PDP Policy Decision Points.

PEP Policy Enforcement Points.

SNMP Simple Network Management Protocol.

Warning!!

Isto são apenas uns apontamentos realizados por uma pobre alma de MIECT, feitas a partir dos slides da disciplina e outras fontes 😈. Por favor, não usem apenas estes apontamentos como material de estudo se pretendem obter uma nota minimamente aceitável.

Dito isto, boa sorte a todos e ámen CT 🙏.

Agradecimentos aos Professores Paulo Salvador e Rui Aguiar por todo material fornecido nas aulas.

Introdução

Porquê gestão de Redes e Sistemas?

1. **Custo Inferior:** a gestão manual é dispendiosa.
2. **Mais Eficiência:** Sistemas automáticos permitem um planeamento eficiente e mecanismos para prever as tendências de utilização, reduzindo erros e acelerando a atuação.
3. **Melhor Serviço:** O gerente é informado simultaneamente ao cliente e pode realizar uma verificação automática da situação.
4. **Conhecimento Ampliado:** Mais informações disponíveis sobre a rede possibilitam melhores decisões e planeamento.

Por que não intervenção humana?

A complexidade crescente das tarefas de gestão e a evolução rápida da tecnologia impulsionam a busca por alternativas automatizadas. Descrever responsabilidades claramente é desafiador, e a velocidade das mudanças na tecnologia e nos sistemas de gestão supera muitas vezes a capacidade humana de resposta. A falta de recursos técnicos, como especialistas em gestão, também limita a eficácia da intervenção humana. Assim, a automação e sistemas inteligentes oferecem respostas mais rápidas e adaptáveis às demandas em constante mudança.

Alternativas de Gestão

1. **Scope**
   - **Gestão de Sistemas -** Abrange todos os aspetos da empresa.
   - **Gestão de Redes -** Centra-se principalmente nos aspetos de rede, sistemas de comunicação e equipamentos.
2. **Communication Protocol**

- **Protocolos Dedicados -** Específicos para redes.
- **Sistemas Baseados na Web -** Utilizam modelos HTTP, recentemente comuns.

3. **Decision Model**

- **Modelos Centralizados -** Modelo agente-gerente.
- **Modelos Distribuídos -** Compartilhamento das responsabilidades de gestão.
- **Modelos Hierárquicos -** Estrutura hierárquica com informação centralizada na raiz.

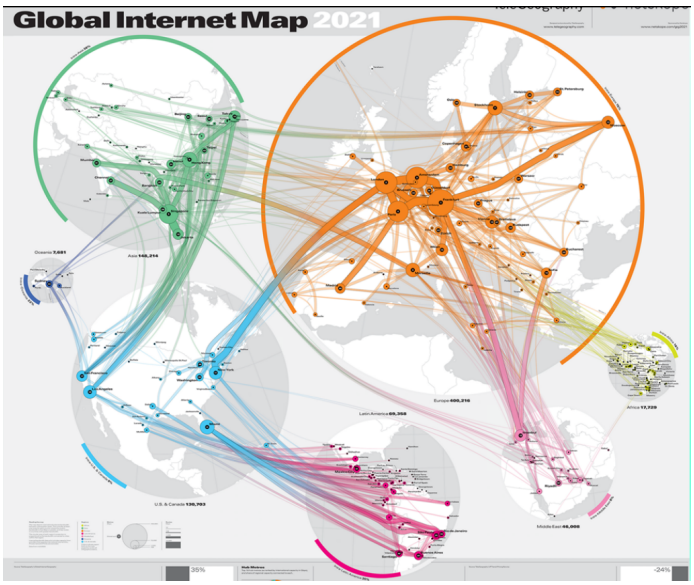

Figura 1.1: Global Internet Map 2021

SNMP

Simple Network Management Protocol (SNMP) é um protocolo para gerir e monitorizar de redes de computadores. Ele é parte integrante de protocolos TCP/IP, e sua principal função é permitir aos administradores monitorizarem e controlem dispositivos de rede remotamente. SNMP é uma arquitetura cliente-servidor, onde os dispositivos geridos (como routers, switches, entre outros) são configurados para enviar informações para um servidor SNMP, conhecido como Network Management System (NMS).

- **SNMP agent:** Um módulo de software que reside em elementos de rede; recolhe e armazena informações de gestão especificadas nos módulos MIB suportados. O agente SNMP responde a pedidos SNMP de uma estação NMS para informações e ações. O agente SNMP pode enviar notificações de falha proativamente para o gestor SNMP.
- **Managed object:** Uma representação de algo que pode ser gerido. Os objetos geridos diferem das variáveis, que são instâncias específicas de objetos.
- **Management Information Base (MIB):** É uma base de dados virtual que contém informações sobre os dispositivos geridos numa rede. Essas informações são organizadas hierarquicamente e podem incluir dados como configurações, status, estatísticas e outros parâmetros relevantes.
- **Syntax notation:** Uma linguagem usada para descrever objetos geridos num formato independente de máquina. Sistemas de gestão baseados em SNMP utilizam um subconjunto da Notação de Sintaxe Abstrata 1 (ASN.1) da Organização Internacional de Normalização (ISO) para definir tanto os pacotes trocados pelo protocolo de gestão quanto os objetos a serem geridos.
- **Structure of Management Information (SMI):** Define as regras para descrever informações de gestão (a MIB).

2.1 Polling

O gestor de rede pergunta, periodicamente, ao agente, por nova informação.

- 😋 Vantagem: O gestor controla totalmente o equipamento e conhece todos os detalhes da rede.
- 😩 Desvantagem: Atraso entre o evento e a sua entrada no sistema, e sobrecarga de comunicação desnecessária:
  - **Polling lento, resposta lenta aos eventos:** Atraso na verificação periódica e demora na resposta aos eventos.
  - **Polling rápido, reação rápida, mas grande desperdício de largura de banda:** Verificação rápida e resposta ágil aos eventos, mas com um uso substancial de largura de banda.

2.2 Traps

Acontece um evento →enviada uma Trap. A `Trap` contém informações adequadas, como o nome do equipamento, o instante de tempo do evento e o tipo de evento.

- 🥳 Vantagem: Informação apenas é gerada quando necessário.
- 😭 Desvantagem: Mais recursos necessários no equipamento gerido e as `Trap`, por vezes, podem ser inúteis:
  - **Polling lento, resposta lenta aos eventos:**Se muitos eventos ocorrerem simultaneamente, a largura de banda pode ser desperdiçada com todos os `Traps`(limites podem resolver). Como o agente tem apenas um escopo limitado na rede, o NMS pode já estar ciente dos eventos[1].

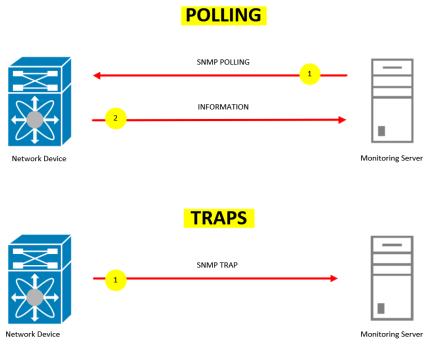

Figura 2.1: Polling e Traps

2.3 Traps&Polling

Ocorre um evento, o que resulta no envio de um `Trap`. O gestor realiza um polling periódico para obter o restante das informações. Além disso, o gestor realiza pollings periódicos regulares como uma medida de backup.

2.4 SNMPv1

O SNMPv1 (*Simple Network Management Protocol version 1*) utiliza o conceito de "SNMP community string" para autorização e autenticação. A `community string` é uma sequência de caracteres que identifica e define as permissões de acesso de uma máquina ao agente SNMP (dispositivo gerido). Existem duas palavras-chave principais associadas às `community strings`:

- `public`): Geralmente configurado como "read-only" (somente leitura). Permite que a máquina que usa esta "community string" acesse informações e leia dados do agente SNMP, mas não permite alterações.
- `private`: Geralmente configurado como "read-write" (leitura e escrita). Permite que a máquina que usa esta "community string" acesse informações, leia dados e faça alterações no agente SNMP.

2.5 SNMPv2

O `SNMPv2` (*Simple Network Management Protocol version 2*) é uma evolução do `SNMPv1`. O `SNMPv2` trouxe melhorias significativas para o gerenciamento de redes. Entre as principais características, destaca-se a otimização da estrutura `MIB` para representar informações de forma mais eficiente, a introdução da variante `SNMPv2c` mantendo melhorias na `MIB`, aprimoramentos nas armadilhas `SNMP` para comunicação eficiente de eventos assíncronos, e a definição de métodos de transporte flexíveis (`SNMPv2-TM`). Além disso, houve melhorias nas operações de protocolo e nas convenções textuais para mensagens `SNMP`. Embora tenha trazido avanços, o `SNMPv2` enfrentou desafios de segurança, levando ao desenvolvimento posterior do `SNMPv3`, que incorporou recursos avançados de segurança.

2.6 SNMPv3

O `SNMPv3` (*Simple Network Management Protocol version 3*) representou uma evolução significativa em relação às versões anteriores, incorporando recursos avançados de segurança para enfrentar as limitações percebidas no `SNMPv1` e `SNMPv2`. Algumas melhorias notáveis incluem:

- **Novo Formato de Mensagem:** O `SNMPv3` trouxe um novo formato de mensagem, proporcionando maior flexibilidade e eficiência na comunicação entre sistemas de gestão e agentes `SNMP`.

- **Segurança da Mensagem:** Uma das características mais destacadas das extensões do `SNMPv3` é a ênfase na segurança. Foram introduzidos mecanismos robustos de autenticação e criptografia para garantir a integridade, autenticidade e confidencialidade das mensagens `SNMP`.
- **Controle de Acesso:** As extensões do `SNMPv3` implementaram controlos de acesso aprimorados, permitindo uma configuração mais granular e baseada em funções. Os administradores podem definir políticas de acesso específicas para utilizadores individuais, garantindo que apenas as operações necessárias sejam permitidas.

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Figura 2.2: Versões SNMP

2.7 SNMP Operations

O `SNMP` fornece as seguintes cinco operações básicas:

1. **Operação Get:** Pedido enviado pelo NMS ao agente para recuperar um ou mais valores do agente.
2. **Operação GetNext:** Pedido enviado pelo NMS para recuperar o valor do próximo OID na árvore.
3. **Operação Set:** Pedido enviado pelo NMS ao agente para definir um ou mais valores do agente.
4. **Operação de Resposta:** Resposta enviada pelo agente ao NMS.
5. **Operação de Armadilha (Trap):** Resposta não solicitada enviada pelo agente para notificar o NMS dos eventos ocorridos.

No SNMPv3, as operações de obtenção (Get) são realizadas com autenticação e criptografia.

2.8 SNMP Names (numbers/OID)

Para nomear todos os objetos possíveis (protocolos, dados, etc.), é utilizado uma árvore de MIB da ISO:

- Nomenclatura hierárquica de objetos
- Cada folha da árvore possui um nome e número.

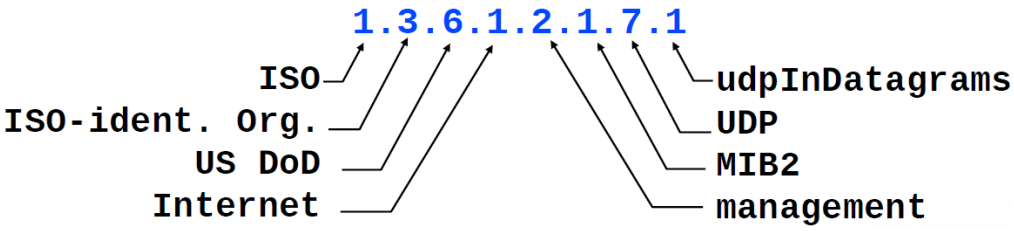

Figura 2.3: SNMP numbers

2.9 SNMP MIBs

Management Information Base (MIB) é um conjunto de objetos geridos, utilizado para definir informações provenientes de equipamentos, criado pelo fabricante.

Um MIB armazena informações sobre os dispositivos de rede, como routers, switches, servidores, entre outros. Essas informações são organizadas em uma árvore de hierarquia, e cada informação específica é identificada por um número único chamado Object Identifier (OID)

2.10 RMON - Remote monitoring

O RMON é um conjunto de informações geridas utilizado para medir o tráfego de rede. Ele envolve agentes, interfaces de gestão e sondas para análise de rede, frequentemente configuradas para tipos específicos de dados. Aqui estão alguns pontos chave sobre o RMON:

- **Agentes e Interfaces de Gerenciamento:** O RMON utiliza agentes para fornecer uma interface de gerenciamento remota. Esses agentes coletam informações e estatísticas sobre o tráfego de rede para monitoramento.
- **Probes para Análise de Rede:** Probes, ou probes, são equipamentos utilizados para a análise de rede. Elas operam em modo promíscuo, capturando e analisando todo o tráfego na rede. Normalmente, são configuradas para tipos específicos de dados.

- **Operação Offline:** suporta operação offline, o que significa que as Probes podem operar separadas da rede, o que facilita a análise de dados fora do ambiente de produção.
- **Monitorização Preemptive:** Fornece monitoramento preemptivo, antecipando problemas e oferecendo uma visão abrangente da rede.
- **Suporte a Múltiplos Gestores e Probes:** Pode ser configurado para suportar vários gestoress e Probes, permitindo monitorização em diferentes locais da rede.
- **Detecção e Relato de Problemas:** O RMON é projetado para detetar e relatar problemas na rede, incluindo o uso de nove grupos distintos: Estatísticas, Histórico, Alarme, Host, HostTopN, Matriz, Filtro, Captura de Pacotes e Evento. PBM

Policy Based Management PBM

Partes conceptuais:

- **Ferramentas de política de gestão:**
  - Utilizadas para criar as regras de política.
- **Repositório de políticas:**
  - Armazena as regras das políticas.
- **Consumidores de políticas - Policy Decision Points (PDP):**
  - Tomam decisões e transferem as regras de política para os alvos de política.
- **Alvos de política - Policy Enforcement Points (PEP):**
  - Elementos funcionais afetados pelas regras de política.

3.1 PEP-PDP Model

O Modelo `PEP-PDP` (Policy Enforcement Point - Policy Decision Point) envolve ferramentas de política de gestão (usadas para criar regras), um repositório de políticas (para armazenar regras), consumidores de políticas (PDPs, que tomam decisões e transferem regras para alvos), e alvos de política (PEPs, elementos afetados pelas regras). PEP executa a política, enquanto PDP toma decisões sobre quais políticas aplica

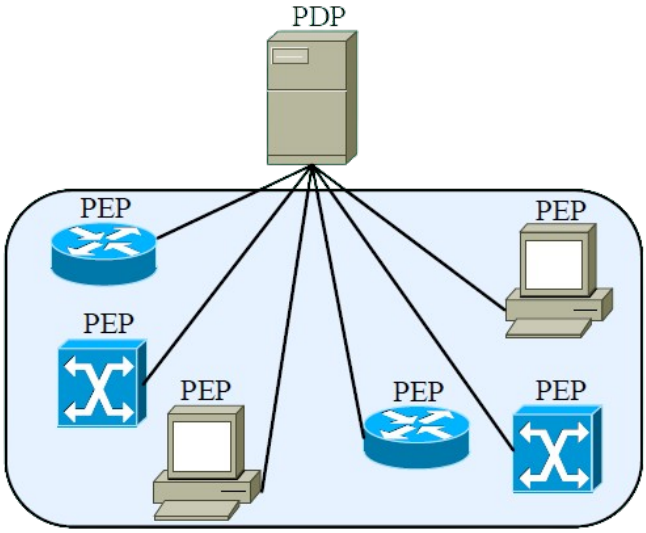

Figura 3.1: PEP-PDP Model

Common Open Policy Service
COPS

É protocolo de pergunta/resposta para interação PDP-PEP é baseado em TCP, o que assegura a sincronização de estado para recuperação de falhas e manutenção de estado com keep-alive. O PDP pode enviar notificações para o PEP, inicialmente concebidas para suporte e controlo de QoS. Além disso, o PDP pode receber políticas através de LDAP e SNMP. O sistema suporta dois tipos de clientes: RSVP, no modelo de terceirização, e Diff-serv, no modelo de configuração.

Bibliografia

[1] cordero.me, *SNMP Polling vs Traps*, `https://cordero.me/snmp-polling-vs-traps/`, 2023.