Estudo dirigido sobre o capítulo 9 – gerenciamento de rede

INSTITUTO FEDERAL
RIO GRANDE DO SUL

1. Descreva cenários que demonstrem a importância de se ter ferramentas de gerenciamento de redes.

- Detecção de falha em uma placa de interface em um hospedeiro ou roteador
  - Uma entidade de rede pode indicar ao administrador de rede que uma de suas interfaces não está funcionando
  - Antecipação ao problema: se o administrador notar um aumento de erros de somas de verificação em quadros que estão sendo enviados por uma placa de interface que está prestes a falhar
- Monitoração de hospedeiro – o administrador da rede pode verificar periodicamente se todos os hospedeiros da rede estão ativos e operacionais

1. Descreva cenários que demonstrem a importância de se ter ferramentas de gerenciamento de redes.

- Monitoração de tráfego para auxiliar o oferecimento de recursos
  - Exemplo: comutar servidores entre segmentos de LAN para diminuir o total de tráfego que passa por várias LANs
  - Monitorar a utilização de um enlace para determinar que um segmento de LAN ou enlace está sobrecarregado
  - Também o administrador poderia ser alertado quando o nível de congestionamento de um enlace ultrapassar determinado limite
- Detecção de mudanças rápidas em tabelas de roteamento – a alternância frequente de rotas pode indicar instabilidades no roteamento ou um roteador mal configurado

1. Descreva cenários que demonstrem a importância de se ter ferramentas de gerenciamento de redes.

- Monitoração de SLAs (Acordos de Nível de Serviços) – são contratos que definem parâmetros específicos de medida e níveis aceitáveis de desempenho do provedor da rede
  - É claro que, se há um contrato, então a medição e o gerenciamento do desempenho do sistema também serão de grande importância para o administrador
- Detecção de intrusos – um administrador vai querer ser avisado quando chegar tráfego de uma fonte suspeita ou quando se destinar tráfego a ela
  - Ele pode querer detectar a existência de certos tipos de tráfego

2. Descreva as cinco áreas de gerenciamento de rede segundo o modelo de gerenciamento de rede da ISO.

- Gerenciamento de desempenho – a meta é quantificar, medir, informar, analisar e controlar o desempenho de diferentes componentes da rede
  - Entre esses componentes estão dispositivos individuais, bem como abstrações fim a fim, como um trajeto pela rede
- Gerenciamento de falhas – o objetivo é registrar, detectar e reagir às condições de falha da rede
  - Pode-se considerar o gerenciamento de falhas como o tratamento imediato de falhas transitórias da rede (por exemplo, interrupção de serviço em enlaces, hospedeiros, ou em hardware e software de roteadores)

2. Descreva as cinco áreas de gerenciamento de rede segundo o modelo de gerenciamento de rede da ISO.

- Gerenciamento de configuração – permite que um administrador de rede saiba quais dispositivos fazem parte da rede administrada e quais são suas configurações de hardware e software
- Gerenciamento de contabilização – permite que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede
    - Quotas de uso, cobrança por utilização e alocação de acesso privilegiado a recursos fazem parte deste gerenciamento

2. Descreva as cinco áreas de gerenciamento de rede segundo o modelo de gerenciamento de rede da ISO.

- Gerenciamento de segurança – a meta é controlar o acesso aos recursos da rede de acordo com alguma política definida

3. O que é gerenciamento de rede?

- Gerenciamento de rede inclui a oferta, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável.

4. No contexto de gerenciamento de rede, o que é a entidade gerenciadora?

- É uma aplicação que, em geral, tem um ser humano no circuito e que é executada em uma estação central de gerência de rede na NOC (*Network Operation Center*)
  - É nela que são iniciadas ações para controlar o comportamento da rede e é aqui que o administrador humano interage com os dispositivos da rede

5. O que é um dispositivo gerenciado?

- É um equipamento de rede (incluindo seu software) que reside em uma rede gerenciada
  - Um dispositivo gerenciado pode ser um hospedeiro, um roteador, uma ponte, um *hub*, uma impressora ou um modem

6. O que são os objetos gerenciados?

- No interior de um dispositivo gerenciado pode haver diversos objetos gerenciados
  - Estes são, na verdade, as peças de hardware propriamente ditas que estão dentro do dispositivo gerenciado (uma placa de interface de rede) e os conjuntos de parâmetros de configuração para as peças de hardware e software (por exemplo, um protocolo de roteamento intradomínio, como o RIP)

7. O que é uma Base de Informações de Gerenciamento?

- Os objetos gerenciados têm informações associadas a eles que são coletadas dentro de uma base de informações de gerenciamento (MIB)
  - Os valores dessas informações estão disponíveis para a entidade gerenciadora (e, em muitos casos, podem ser ajustados por ela)

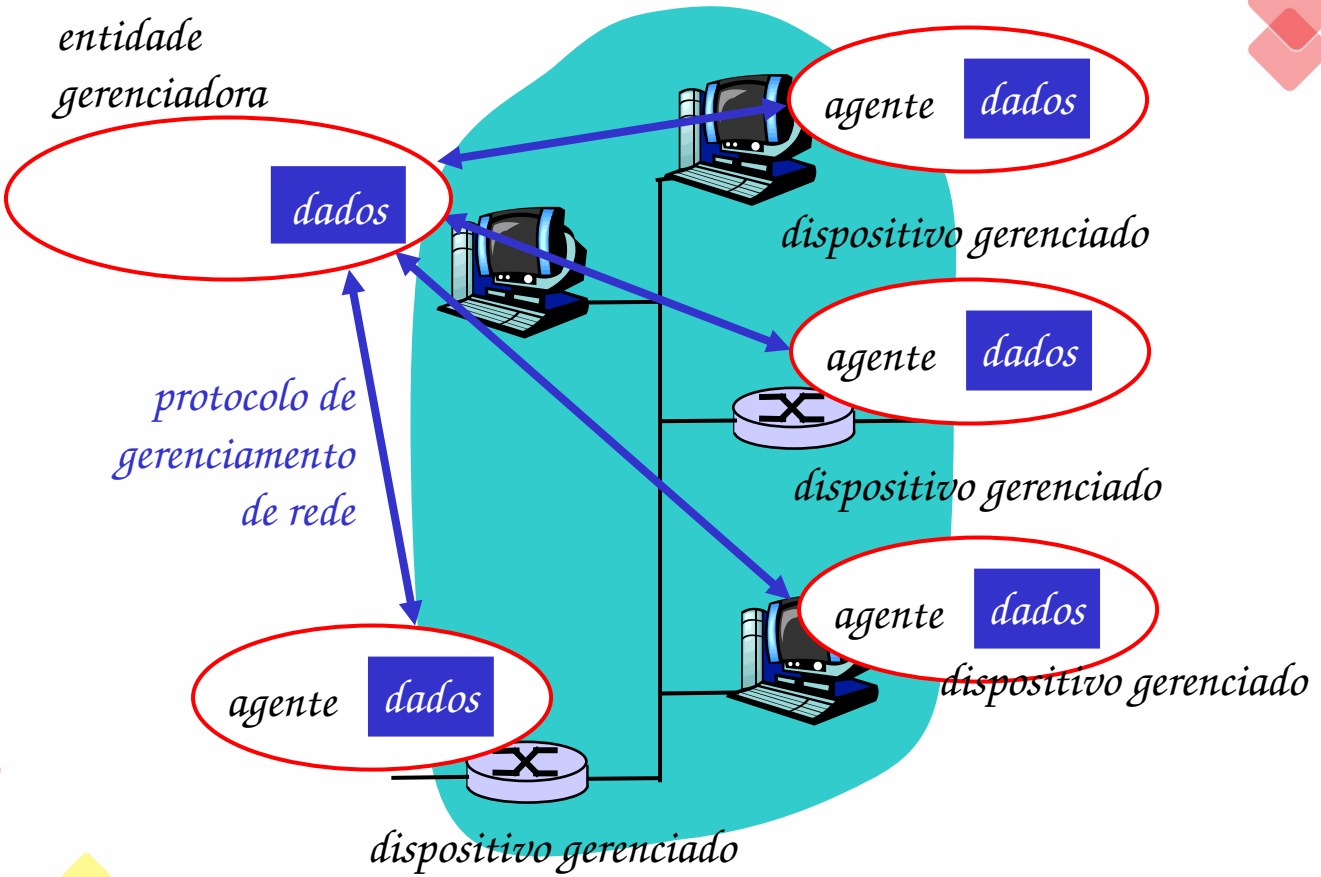
8. O que é um agente de gerenciamento de rede?

- Reside em cada dispositivo gerenciado um agente de gerenciamento de rede, um processo que é executado no dispositivo, que se comunica com a entidade gerenciadora e que executa ações locais nos dispositivos gerenciados

9. O que é o protocolo de gerenciamento de rede?

- É executado entre a entidade gerenciadora e o agente de gerenciamento de rede dos dispositivos gerenciados
  - Permite que a entidade gerenciadora investigue o estado dos dispositivos gerenciados e, indiretamente, execute ações sobre eles mediante seus agentes
  - O protocolo de gerenciamento em si não gerencia a rede

9. O que é o protocolo de gerenciamento de rede?



10. Quais são os dois padrões mais importantes de gerenciamento de rede?

- O OSI CMISE/CMIP (*Common Management Service Element/ Common Management Information Protocol*) e o SNMP (*Simple Network Management Protocol*) emergiram como os dois padrões mais importantes
- Como o SNMP foi projetado e oferecido rapidamente em uma época em que a necessidade de gerenciamento de rede começava a ficar premente, ele encontrou uma ampla aceitação
  - Hoje, esse protocolo é a estrutura de gerenciamento de rede mais amplamente usada e disseminada

11. Quais são as quatro partes que constituem a estrutura de gerenciamento padrão da Internet?

- Definições dos objetos de gerenciamento de rede, conhecidos como objetos MIB
  - As informações de gerenciamento são representadas como uma coletânea de objetos gerenciados que, juntos, formam um banco virtual de informações virtuais conhecidas como MIB
  - Um objeto MIB pode ser um contador tal como o número de datagramas IP descartados em um roteador
    - um conjunto de informações descritivas como a versão do software que está sendo executado em um servidor DNS
    - informações de estado como se um determinado dispositivo está funcionando corretamente
    - ou informações específicas de protocolos, como um caminho de roteamento até um destino

11. Quais são as quatro partes que constituem a estrutura de gerenciamento padrão da Internet?

- Objetos MIB relacionados são reunidos em módulos MIB
- Uma linguagem de definição de dados, conhecida como SMI (*Structure of Management Information*) usada para especificar objetos MIB
- Um protocolo SNMP – usado para transmitir informações e comandos entre uma unidade gerenciadora e um agente que os executa em nome da entidade dentro de um dispositivo de rede gerenciado
- Capacidades de segurança e de administração – um aprimoramento do SNMP versão 3

12. O que pode ser um objeto MIB? O que objetos MIB definem?

- Um objeto MIB pode ser um contador tal como o número de datagramas IP descartados em um roteador
  - um conjunto de informações descritivas como a versão do software que está sendo executado em um servidor DNS
  - informações de estado como se um determinado dispositivo está funcionando corretamente
  - ou informações específicas de protocolos, como um caminho de roteamento até um destino
- Os objetos MIB definem as informações de gerenciamento mantidas por um dispositivo gerenciado

13. Descreva a linguagem SMI.

- Define os tipos de dados, um modelo de objeto e regras para escrever e revisar informações de gerenciamento
- Objetos MIB são especificados nessa linguagem de definição de dados

14. Qual é o uso do protocolo SNMP?

- É usado para transmitir informações e comandos entre uma unidade gerenciadora e um agente que os executa em nome da entidade dentro de um dispositivo de rede gerenciado

15. Liste os 11 tipos básicos de dados definidos para a SMI.

- Integer
- Integer32
- Unsigned32
- Octet string
- Object identifier
- Endereço ip
- Counter32
- Counter64
- Gauge32
- Timeticks
- opaque

16. Dê um exemplo de uso da construção OBJECT TYPE. Explique o exemplo.

IpSystemStatsInDelivers OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION ...

- Esse objeto define um contador de 32 bits que monitora o número de datagramas IP que foram recebidos no dispositivo gerenciado e entregues com sucesso a um protocolo de camada superior

17. Para que serve a construção MODULE-IDENTITY.

- A construção MODULE-IDENTITY permite que os objetos relacionados entre si sejam agrupados, como conjunto, dentro de um módulo
- Além de conter as definições OBJECT-TYPE dos objetos gerenciados dentro do módulo, a construção MODULE-IDENTITY contém cláusulas para documentar informações de contato do autor do módulo, a data da última atualização, um histórico de revisões e uma descrição textual do módulo

18. Descreva as construções NOTIFICATION-TYPE, MODULE-COMPLIANCE e AGENT-CAPABILITIES.

- NOTIFICATION-TYPE é usada para especificar informações referentes a mensagens SNMPv2 Trap e Information Request geradas por um agente ou por uma entidade gerenciadora
- A MODULE-COMPLIANCE define o conjunto de objetos gerenciados dentro de um módulo que um agente deve implementar
- A construção AGENT-CAPABILITIES especifica as capacidades dos agentes relativas às definições de notificação de objetos e de eventos

19. O que é o modo comando-resposta do SNMP?

- A entidade gerenciadora SNMPv2 envia uma requisição a um agente SNMPv2, que a recebe, realiza alguma ação e envia uma resposta à requisição

20. O que é uma mensagem trap do SNMP?

- É para um agente enviar uma mensagem não solicitada à entidade gerenciadora
- São usadas para notificar uma entidade gerenciadora de uma situação excepcional que resultou em mudança nos valores dos objetos MIB
- O administrador da rede pode querer receber uma mensagem trap quando uma interface cai, quando o congestionamento atinge um nível predefinido ou quando ocorre qualquer evento notável

21. Descreva sucintamente os tipos de PDUs do SNMP.

- As PDUS *GetRequest*, *GetNextRequest* e *GetBulkRequest* são enviadas de uma entidade gerenciadora a um agente para requisitar o valor de um ou mais objetos MIB no dispositivo gerenciado do agente
  - Em todos os três casos, o agente responde com uma PDU *response* que contém os identificadores de objetos e seus valores associados
- A PDU *SetRequest* é usada por uma entidade gerenciadora para estabelecer o valor de um ou mais objetos MIB em um dispositivo gerenciado
  - Um agente responde com uma PDU *response* que contém uma mensagem *Error Status "noError"* para confirmar que o valor na verdade foi estabelecido
- A PDU *InformRequest* é usada por uma entidade gerenciadora para comunicar a outra entidade gerenciadora informações MIB remotas à entidade receptora

21. Descreva sucintamente os tipos de PDUs do SNMP.

- O tipo final de SNMPv2-PDU é a mensagem *trap*
  - Mensagens *trap* são geradas assincronamente, isto é, não são geradas em resposta a uma requisição recebida, mas em resposta a um evento para o qual a entidade gerenciadora requer notificação

22. Onde está a principal mudança do SNMPv3 em relação ao SNMPv2?

- Nas áreas de administração e segurança

23. Em que consistem as aplicações SNMP?

- As denominadas aplicações SNMP consistem em um gerador de comandos, um receptor de notificações e um transmissor *proxy* (na entidade gerenciadora); um elemento respondedor de comandos e um originador de notificações (no agente)

24. O que é fornecido, em termos de segurança, pelo SNMPv3?

- Criptografia, autenticação, proteção contra ataques de reprodução e controle de acesso

25. O que é a ASN.1?

- A ASN.1 é um padrão originado na ISO, usado em uma série de protocolos relacionados à Internet, particularmente na área de gerenciamento de rede
- As variáveis MIB do SNMP estão inextricavelmente ligada à ASN.1

26. O que são *little-endian* e *big-endian* e o que estes termos têm a ver com um serviço de apresentação?

- A ordem de armazenamento *big-endian* armazena primeiramente os bytes mais significativos (nos endereços de armazenamento mais baixos)
- A ordem *little-endian* armazena primeiramente os bytes menos significativos
- Visto que diferentes computadores armazenam e representam dados de modo diferente, como os protocolos de rede devem enfrentar o problema?
- Uma alternativa é ter um método independente de máquina, de sistema operacional e de linguagem para descrever números inteiros e outros tipos de dados (isto é, uma linguagem de descrição de dados) e regras que estabeleçam como cada um destes tipos de dados devem ser transmitidos pela rede
  - Tanto a SMI quanto a ASN.1 adotam esta alternativa

Contextualização

- ***Zabbix*** – instalação e uso inicial
  - https://www.zabbix.com/download
- **Nagios** – instalação e uso inicial no Raspberry PI
  - https://www.filipeflop.com/blog/monitore-a-rede-local-com-nagios-e-raspberry-pi/