Redes de Computadores

Gerenciamento de Redes

Gerenciamento de Rede

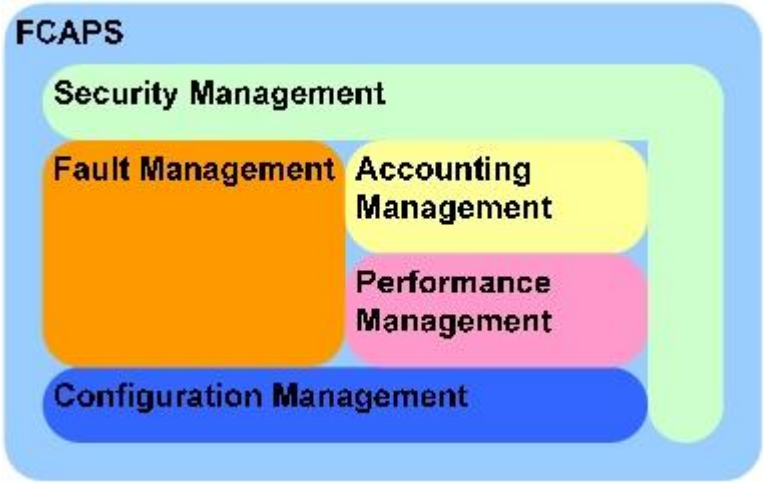
- Introdução
  - Uma rede consiste em inúmeros elementos complexos interagindo entre si
  - Esse elementos, ocasionalmente, apresentam defeitos
  - O administrador de rede deve manter a rede "viva e atuante"
    - Fazendo uso de ferramentas para monitorar, administrar e controlar a rede

Gerenciamento de Rede

- Definição
  - É o controle de qualquer objeto passível de ser monitorado numa estrutura de recursos físicos e lógicos de uma rede
  - Essencial para garantir a alta disponibilidade da rede
  - Satisfazer exigências operacionais
    - Desempenho
    - Qualidade de Serviço
    - Custo
  - Necessário o monitoramento, teste, configuração e diagnóstico dos componentes da rede

FCAPS

- Modelo de Gerenciamento de Rede
- Criado pela ISO e refinado pela ITU-T
- Divide o gerenciamento de redes em 5 tarefas
  - **F**ault Management
  - **C**onfiguration Management
  - **A**ccounting Management
  - **P**erformance Management
  - **S**ecurity Management



FCAPS

- Gerenciamento de Falhas (Fault Management)
  - Garantir o bom funcionamento de cada componente isolado ou interligado
    - Monitoramento da Rede
  - Falha
    - Condição anormal no sistema
      - Algum elemento ou serviço para de funcionar
      - Cria erros em excesso
    - Ex. enlace rompido, roteador danificado
  - Métodos
    - Reativo
    - Proativo

FCAPS

- Gerenciamento de Falhas (Fault Management)
  - Reativo
    - Detecção
      - Localização exata da falha
      - Automática ou Manual
    - Isolamento
      - Minimizar os efeitos da falha
      - Notificar os usuários afetados
    - Correção
      - Substituição ou reparo de componentes
    - Registro
      - Documentação da falha
      - Gera dados estatísticos para Gerencimanto de Desempenho

FCAPS

- Gerenciamento de Falhas (Fault Management)
  - Reativo
    - Soluções de curto prazo para as falhas
  - Proativo
    - Finalidade de monitorar comportamentos anormais
    - Tenta impedir a ocorrência de falhas
    - Soluções de longo prazo para as falhas

F**C**APS

- Gerenciamento de Configuração (Configuration Management)
  - Registro e manutenção dos parâmetros de configuração dos elementos e serviços da rede
  - Informações sobre cada entidade e sua relação com outras entidades da rede
  - Etapas
    - Reconfiguração
    - Documentação

FCAPS

- Gerenciamento de Configuração (Configuration Management)
  - Reconfiguração
    - Ajustar os componentes e as características da rede
    - Hardware
      - Não pode ser automatizado
    - Software
      - Maioria automatizada
    - Contas de usuário
      - Adição/remoção de contas
      - Verificação de privilégios de usuário
      - Até certo ponto automatizada

FCAPS

- Gerenciamento de Configuração (Configuration Management)
  - Documentação
    - Registro meticuloso de alterações na rede
    - Hardware
      - Diagramas
        - » Acompanha cada equipamento e sua conexão com a rede
        - » Ex. Relacionamento lógico e físico de cada elemento
      - Especificações
        - » Documentação de cada equipamento
        - » Ex. tipo de hardware, S/N, fornecedor

FCAPS

- Gerenciamento de Configuração (Configuration Management)
  - Documentação
    - Software
      - Especificação de cada ferramenta utilizada na rede
      - Ex. tipo de software, versão, hora de instalação
    - Contas de usuário
      - Registrados geralmente pelo próprio utilitário de gerenciamento
      - Ex. grupos de usuários, privilégios

FC**A**PS

- Gerenciamento de Contabilização (Accounting Management)
  - Quantificar o acesso e uso dos recursos da rede para fins de tarifação e/ou regulamentação
  - Pode ser utilizado para fins de orçamento
    - Em locais que não há tarifação, o termo “accounting” pode ser substituído por “administration”
  - Motivações de uso
    - Impedir o monopólio dos recursos da rede
    - Estimular o uso eficiente da rede
    - Elaborar planos com base na demanda
  - Protocolos para contabilização
    - TACACS, RADIUS, DIAMETER

FCAPS

- Gerenciamento de Desempenho (Performance Management)
  - Monitora e controla a rede para garantir que ela esteja rodando da forma mais eficiente possível
  - Está relacionado ao Gerenciamento de Falhas
  - Métricas
    - Capacidade
    - Tráfego
      - Interno
      - Externo
    - Throughtput
    - Tempo de resposta

FCAPS

- Gerenciamento de Segurança (Security Management)
  - Responsável pelo controle de acesso à rede tomando como base uma política predefinida
  - Geralmente faz uso de criptografia e autenticação
  - Conceitos
    - Authentication
    - Authorization
    - Auditing
  - Configuração de ferramentas

Gerenciamento de Redes

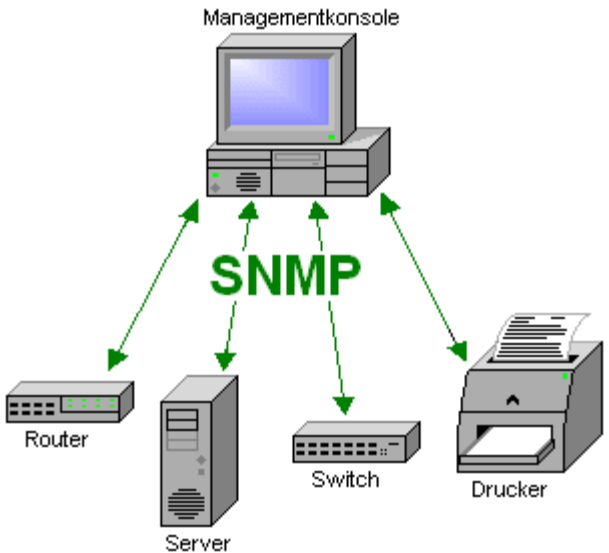
SNMP

SNMP

- Histórico
  - Redes de computadores eram baseadas em arquiteturas e protocolos patenteados
    - OSI - Teórico
    - TCP/IP – Prático
  - Devido ao crescimento das redes TCP/IP, surgiram dificuldades de gerência
    - Protocolos de gerência proprietários
  - O SNMP é apresentado como solução para padronização de gerenciamento de redes
    - Simples e baseado no TCP/IP

SNMP

- Simple Network Management Protocol
- Framework para o gerenciamento de rede utilizando o conjunto de protocolos TCP/IP
- Camada de aplicação
- Monitora dispositivos produzidos por diferentes fabricantes
- Não segue o modelo cliente – servidor convencional
- Padrão IETF

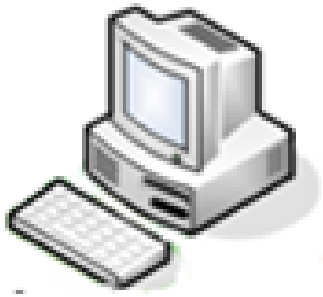


SNMP

- Componentes Básicos
  - Dispositivos Gerenciados
    - Nó da rede que possui um agente SNMP instalado
  - Agentes
    - Módulo de software de gestão de rede que fica armazenado em um dispositivo
  - Sistema de Gerenciamento de Redes (NMS - Network Management System)
    - Conjunto de aplicações que monitoram e controlam os dispositivos gerenciados

SNMP

- Personagens
  - Gerente
  - Agente
- Funcionalidades Básicas
  - GET
  - SET
  - TRAP



Gerente

Agente

SNMP

- Gerente/Entidade Gerenciadora
  - Normalmente é um host
  - Monitora e controla um conjunto de agentes
    - Realiza requisições de informações aos dispositivos gerenciados
      - Polling
    - Faz com que o agente realize certas ações
  - Recebe os alarmes gerados pelos agentes
    - Porta UDP/162
  - Realiza o maior processamento dos dados
    - Agente apenas provê a informação

SNMP

- Agente/Agente de Gerenciamento
  - Normalmente são roteadores
  - Mantém as informações de configuração e desempenho em um BD disponível ao gerente
    - 161/UDP
  - Podem estar localizados em diferentes pontos da internet
  - Realiza o envio de TRAP
    - Eventos excepcionais

SNMP

- Agente/Agente de Gerenciamento
  - Master Agent/Agente Principal
    - Software que interage com uma estação de gerenciamento
    - Equivalente a um software servidor ou daemon
  - Subagent/Sub-agente
    - Pequenos programas responsáveis pelo monitoramento de recursos específicos do dispositivo gerenciado
    - Passam informações específicas para o Agente Principal
    - Características
      - Responder a solicitações do software de gerência da rede
      - Coletar informações de objetos gerenciados
      - Configurar parâmetros destes objetos gerenciados
      - Gerar alarmes ou traps em determinadas situações

SNMP

- Agente Proxy
  - Lida com dispositivos mais antigos ou dispositivos que não suportam o SNMP
  - Atua como um tradutor
    - Traduz a comunicação entre um gerente SNMP e um dispositivo não SNMP
  - Permite o controle de redes com protocolos de gerenciamento heterogêneos

Questões de Aprendizagem

SNMP – Princípios

FCAPS

1. SNMP é um protocolo de

A. criptografia.

B. envio de mensagens de correio eletrônico.

C. gerência de redes.

D. segurança de redes.

E. sincronização.

1. SNMP é um protocolo de

A. criptografia.

B. envio de mensagens de correio eletrônico.

C. gerência de redes.

D. segurança de redes.

E. sincronização.

2. Simple Network Management Protocol (SNMP) é um framework para o gerenciamento de dispositivos de rede em uma internet que utiliza o conjunto de protocolos TCP/IP. O SNMP opera numa camada do modelo OSI/ISO e usa um host que controla e monitora um conjunto de roteadores.

A camada, os dispositivos que controlam e os que são controlados, recebem, respectivamente, as denominações de

A. física, gerente e agente

B. física, master e slave

C. aplicação, servidor e cliente

D. aplicação, master e slave

E. aplicação, gerente e agente

2. Simple Network Management Protocol (SNMP) é um framework para o gerenciamento de dispositivos de rede em uma internet que utiliza o conjunto de protocolos TCP/IP. O SNMP opera numa camada do modelo OSI/ISO e usa um host que controla e monitora um conjunto de roteadores.

A camada, os dispositivos que controlam e os que são controlados, recebem, respectivamente, as denominações de

A. física, gerente e agente

B. física, master e slave

C. aplicação, servidor e cliente

D. aplicação, master e slave

E. aplicação, gerente e agente

3. São características dos mecanismos de notificação empregados em ferramentas que usam o protocolo SNMP: o uso de pooling e protocolos de handshake (aperto de mãos).

4. O funcionamento das ferramentas para monitoramento de desempenho de serviços em redes fim a fim depende do controle de configuração de dispositivos, e essas ferramentas enquadram-se melhor como pertinentes à área P do modelo FCAPS.

5. RADIUS, TACACS+ e Diameter são protocolos que oferecem suporte a ferramentas pertinentes à área A do modelo FCAPS.

3. São características dos mecanismos de notificação empregados em ferramentas que usam o protocolo SNMP: o uso de pooling e protocolos de handshake (aperto de mãos).

4. O funcionamento das ferramentas para monitoramento de desempenho de serviços em redes fim a fim depende do controle de configuração de dispositivos, e essas ferramentas enquadram-se melhor como pertinentes à área P do modelo FCAPS.

5. RADIUS, TACACS+ e Diameter são protocolos que oferecem suporte a ferramentas pertinentes à área A do modelo FCAPS.

No que se refere a tecnologias de redes e seus equipamentos, bem como a gerenciamento de redes, julgue os próximos itens.

6. Uma rede gerenciada com o SNMP (simple network management protocol) possui três componentes chaves: os dispositivos gerenciados, os agentes e o NMS (networkmanagement system). O agente é definido como um software que reside em um dispositivo gerenciado e também no NMS.

No que se refere a tecnologias de redes e seus equipamentos, bem como a gerenciamento de redes, julgue os próximos itens.

6. Uma rede gerenciada com o SNMP (simple network management protocol) possui três componentes chaves: os dispositivos gerenciados, os agentes e o NMS (networkmanagement system). O agente é definido como um software que reside em um dispositivo gerenciado e também no NMS.

Com relação à gerência de redes SNMP, julgue os próximos itens.

7. A comunicação gerente-agente ocorre periodicamente, sendo iniciada pelo gerente, que recebe a resposta do agente. Em situações de alarmes e rompimento de limites, entretanto, o agente pode tomar a iniciativa da comunicação, acessando o gerente.

8. O SNMP utiliza as portas 161 e 162, sendo a primeira utilizada na comunicação iniciada pelo agente e a outra, na comunicação iniciada pelo gerente.

9. A comunicação entre o gerente e o agente do elemento de rede gerenciado se dá por meio do protocolo SNMP, normalmente transportado pelo protocolo TCP.

Com relação à gerência de redes SNMP, julgue os próximos itens.

7. A comunicação gerente-agente ocorre periodicamente, sendo iniciada pelo gerente, que recebe a resposta do agente. Em situações de alarmes e rompimento de limites, entretanto, o agente pode tomar a iniciativa da comunicação, acessando o gerente.

8. O SNMP utiliza as portas 161 e 162, sendo a primeira utilizada na comunicação iniciada pelo agente e a outra, na comunicação iniciada pelo gerente.

9. A comunicação entre o gerente e o agente do elemento de rede gerenciado se dá por meio do protocolo SNMP, normalmente transportado pelo protocolo TCP.

10. SNMP ("Simple Network Management Protocol") é um protocolo que faz parte da pilha TCP/IP, sendo utilizado para obter informações de servidores, no trabalho de gerenciamento. No seu funcionamento, utiliza o conceito de MIB ("Management Information Base"), definido pelo RFC1066 como o conjunto de objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede. No funcionamento do protocolo SNMP ("Simple Network Management Protocol"), existem duas operações básicas e suas derivações descritas a seguir. I. utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento, previamente determinado. II. utilizada para ler o valor da variável; o gerente solicita ao agente que obtenha o valor da variável. As operações I e II são, respectivamente, conhecidas por:

A. LINK e GET

B. LINK e PUT

C. TRAP e SET

D. TRAP e PUT

E. TRAP e GET

10. SNMP ("Simple Network Management Protocol") é um protocolo que faz parte da pilha TCP/IP, sendo utilizado para obter informações de servidores, no trabalho de gerenciamento. No seu funcionamento, utiliza o conceito de MIB ("Management Information Base"), definido pelo RFC1066 como o conjunto de objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede. No funcionamento do protocolo SNMP ("Simple Network Management Protocol"), existem duas operações básicas e suas derivações descritas a seguir. I. utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento, previamente determinado. II. utilizada para ler o valor da variável; o gerente solicita ao agente que obtenha o valor da variável. As operações I e II são, respectivamente, conhecidas por:

A. LINK e GET

B. LINK e PUT

C. TRAP e SET

D. TRAP e PUT

E. TRAP e GET

Com relação a administração e gerência de redes, julgue os itens a seguir.

11. A gerência de configuração tem por finalidade garantir a melhor utilização dos recursos da rede, visando atender eficientemente a demandas.

12. A gerência de segurança tem por objetivo assegurar a legítima utilização dos recursos da rede, garantindo privacidade, confidencialidade e integridade à informação, enquanto exerce função de auditoria.

Com relação a administração e gerência de redes, julgue os itens a seguir.

11. A gerência de configuração tem por finalidade garantir a melhor utilização dos recursos da rede, visando atender eficientemente a demandas.

12. A gerência de segurança tem por objetivo assegurar a legítima utilização dos recursos da rede, garantindo privacidade, confidencialidade e integridade à informação, enquanto exerce função de auditoria.

13. Maria deseja utilizar os recursos do protocolo SNMP para gerenciar a rede local de computadores do TRF da 4a Região. Para tal, Maria deve instalar alguns módulos de serviços nos dispositivos envolvidos. Assim, para o dispositivo monitorado, Maria deve instalar um

A. Daemon Cliente.

B. Agente Mestre.

C. Daemon de Agente Mestre.

D. Sub-agente.

E. Proxy Cliente.

13. Maria deseja utilizar os recursos do protocolo SNMP para gerenciar a rede local de computadores do TRF da 4a Região. Para tal, Maria deve instalar alguns módulos de serviços nos dispositivos envolvidos. Assim, para o dispositivo monitorado, Maria deve instalar um

A. Daemon Cliente.

B. Agente Mestre.

C. Daemon de Agente Mestre.


D. Sub-agente.

E. Proxy Cliente.

No que se refere a administração e gerência de redes, julgue os próximos itens.

14. A gerência de configuração provê o controle da disposição física e do arranjo lógico dos objetos gerenciados.

15. A gerência de desempenho tem por finalidade reduzir congestionamento e inacessibilidade na rede, provendo aos usuários níveis de serviço consistentes.

16. A gerência de contabilização permite aumentar a confiabilidade, usando ferramentas para a rápida detecção e recuperação de problemas.

No que se refere a administração e gerência de redes, julgue os próximos itens.

14. A gerência de configuração provê o controle da disposição física e do arranjo lógico dos objetos gerenciados.

15. A gerência de desempenho tem por finalidade reduzir congestionamento e inacessibilidade na rede, provendo aos usuários níveis de serviço consistentes.

16. A gerência de contabilização permite aumentar a confiabilidade, usando ferramentas para a rápida detecção e recuperação de problemas.

GABARITO

1. C
2. E
3. E
4. E
5. C
6. E
7. C
8. E
9. E
10. E
11. E
12. C
13. D
14. C
15. C
16. E

SNMP

- Arquitetura de Gerenciamento na Internet
  - SMI (Structure of Management Information)
    - Estrutura de informações de gerenciamento
    - Impõe regras para a construção da base de dados
  - MIB (Management Information Base)
    - Base de informações de gerenciamento
    - Contém as informações sobre objetos gerenciados
  - SNMP (Simple Network Management Protocol)
    - Protocolo de comunicação

SMI - Structure of Management Information

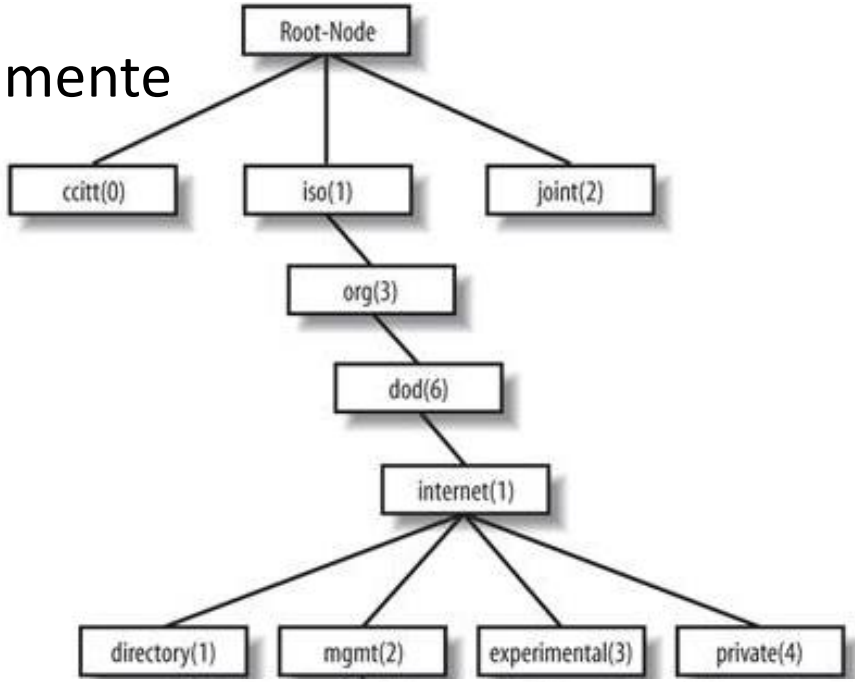
- Estrutura de Informações de Gerenciamento
  - Define os tipos de dados que podem residir em uma entidade gerenciada
  - Versão 2
  - Define regras para atribuição de nomes a objetos
  - Estabelece tipos de objetos
  - Mostra como codificar objetos e valores
  - Não define o número de objetos gerenciáveis por uma entidade
  - Não atribui nome aos objetos
  - Não estabelece associações entre um objeto e seus valores

SMI - Structure of Management Information

- 3 atributos são necessários para a identificação de um objeto
  - Nome do objeto
    - Object ID (OID)
    - Nomeação hierárquica e universal
  - Tipo(s) de dado(s)
    - Inteiro, Contador, String
  - Método de codificação
    - Basic Encoding Rules (BER)

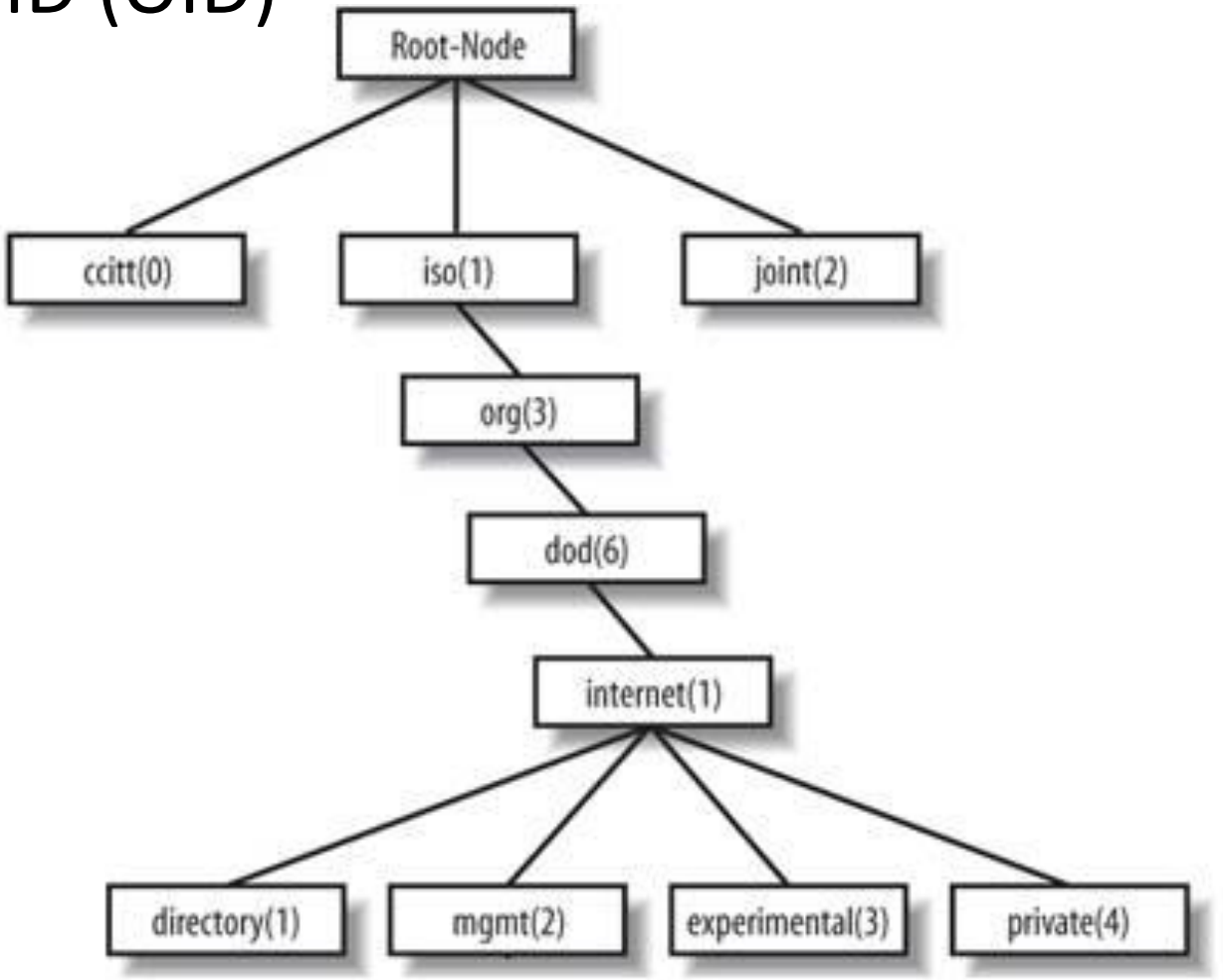
SMI - Structure of Management Information

- Object ID (OID)
  - Cada objeto gerenciável dentro da MIB deve conter um nome exclusivo e padronizado
  - Reaproveita a padronização de nomes da ISO
    - Árvore global de objetos
  - Objetos nomeados hierarquicamente
  - Cada nó da árvore contém um nome e um número
    - Ex. mgmt(2)
      - 1.3.6.1.2
      - iso.org.dod.internet.mgmt



SMI - Structure of Management Information

- Object ID (OID)

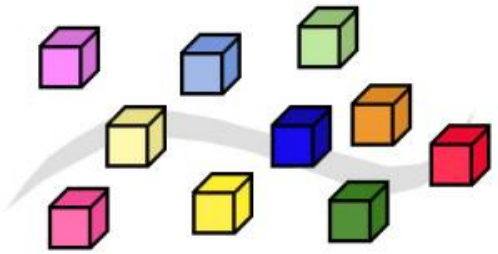


SMI - Structure of Management Information

- Tipos de dados
  - Reaproveita alguns tipos de dados do ASN.1
    - ASN.1 (Abstract Syntax Notation 1)
      - Descreve as estruturas de dados para representação, codificação, transmissão e decodificação dos dados em redes
  - Cria novos tipos de dados específicos para gerenciamento de rede
  - Categorias dos dados
    - Simples
    - Estruturada

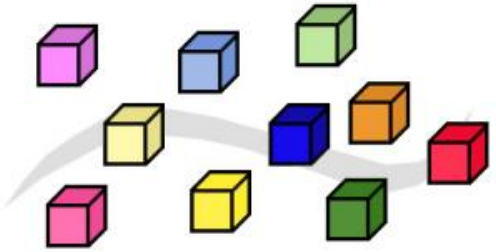
SMI - Structure of Management Information

- Tipos de dados – Simples
  - ASN.1
    - INTEGER (4 bytes)
      - Inteiro com valor entre -2^31 a 2^31-1
    - Integer32 (4 bytes)
      - Idem ao INTEGER
    - Unsigned32 (4 bytes)
      - Sem sinal com valor entre 0 a 2^32-1
    - OCTET STRING (variável)
      - String de bytes com até 65.535 bytes de comprimento
    - OBJECT IDENTIFIER (variável)
      - Identificador do objeto



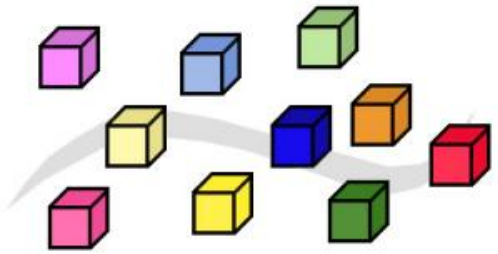
SMI - Structure of Management Information

- Tipos de dados – Simples
  - Definidos pelo SMI
    - IPAddress (4 bytes)
      - Endereço IP composto por 4 inteiros
    - Counter32 (4 bytes)
      - Inteiro cujo valor pode ser incrementado de 0 a 2^32
      - Quando atinge seu valor máximo, recomeça do zero
    - Counter64 (8 bytes)
      - Idem ao Counter32 só que com 8 bytes
      - Introduzido no SMIv2 (SNMPv2)



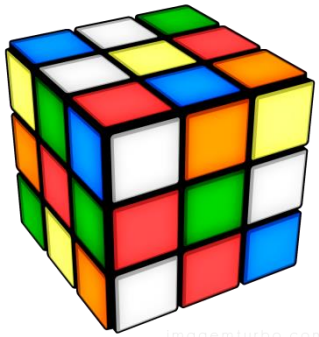
SMI - Structure of Management Information

- Tipos de dados – Simples
  - Definidos pelo SMI
    - Gauge32 (4 bytes)
      - Idem ao Counter32, mas quando atinge seu valor máximo, ele não reinicia do zero, mas permanece nesse valor até ser reiniciado
    - TimeTicks (4 bytes)
      - Valor de contagem que registra o tempo em 1/100s
    - BITS (variável)
      - String de bits
      - Permite o acesso bit a bit
      - Introduzido no SMIv2 (SNMPv2)



SMI - Structure of Management Information

- Tipos de dados – Estruturados
  - Sequence
    - Combinação de tipos de dados simples
    - Não necessariamente do mesmo tipo
  - Sequence of
    - Combinação de tipos de dados simples
    - Geralmente do mesmo tipo
    - Combinação de tipos de dados Sequence do mesmo tipo



SMI - Structure of Management Information

- Método de Codificação
  - Formatação dos dados que serão transmitidos pela rede
  - BER (Basic Encoding Rules)
    - Codificação em trinca
    - Marca (Tag)
      - Define o tipo de dado
    - Comprimento (Length)
      - Tamanho do dado
      - Permite comprimentos variáveis
    - Valor (Value)
      - Dado a ser enviado

SNMP

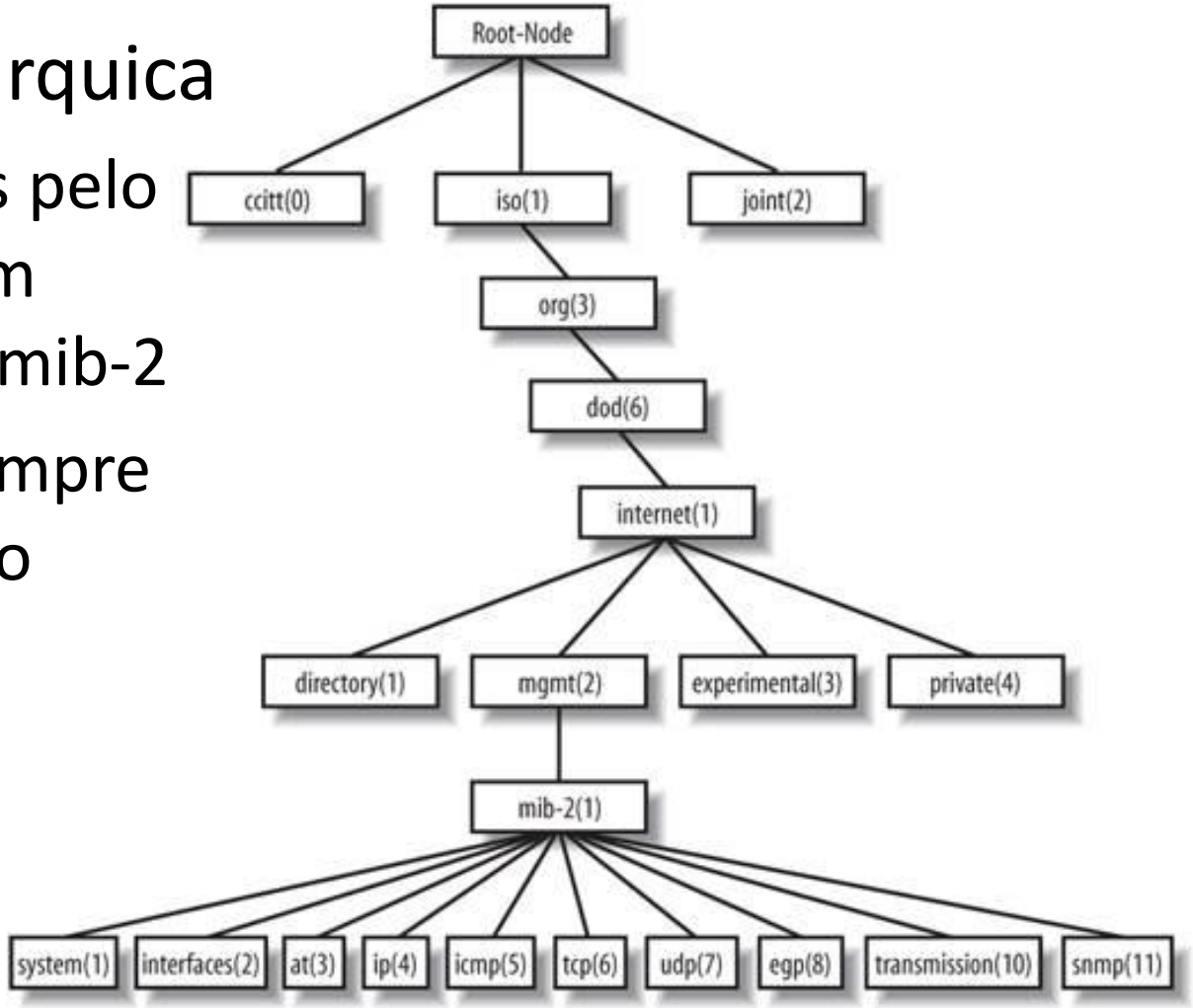
- Arquitetura de Gerenciamento na Internet
  - SMI (Structure of Management Information)
    - Estrutura de informações de gerenciamento
    - Impõe regras para a construção da base de dados
  - MIB (Management Information Base)
    - Base de informações de gerenciamento
    - Contém as informações sobre objetos gerenciados
  - SNMP (Simple Network Management Protocol)
    - Protocolo de comunicação

MIB - Management Information Base

- Base de Informações de Gerenciamento
  - É o banco de dados que contêm os objetos (variáveis) disponíveis para o gerenciamento do dispositivo
  - Versão 2
  - Possui um conjunto de objetos com nome, tipo e relações entre si pertencentes a um dispositivo gerenciado
  - Define o número de objetos que uma entidade pode gerenciar
  - Atribui nomes aos objetos
    - Respeitando as regras do SMI
  - Associa um tipo a cada objeto nomeado
  - Cada agente tem sua própria MIB-2

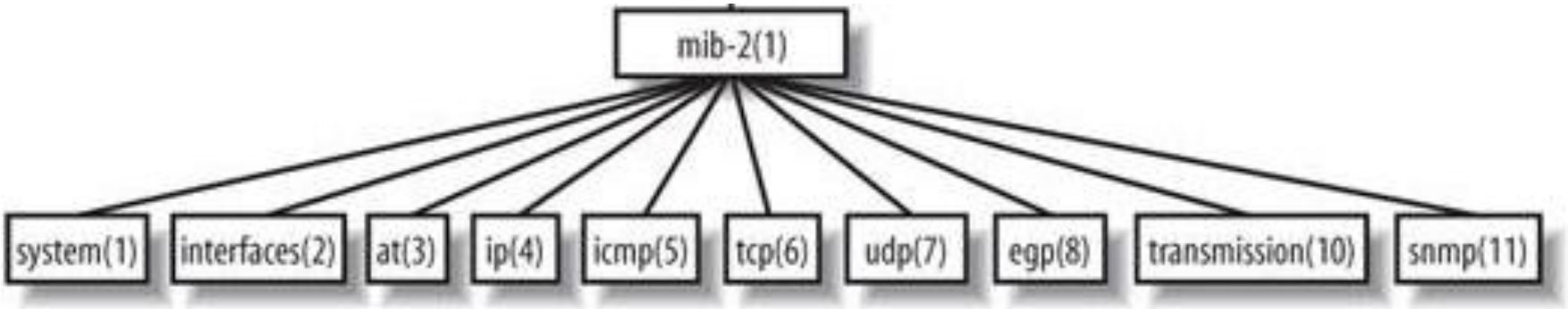
MIB - Management Information Base

- Organização hierárquica
  - Objetos utilizados pelo SNMP se localizam abaixo do objeto mib-2
  - Objetos SNMP sempre utilizarão o prefixo 1.3.6.1.2.1



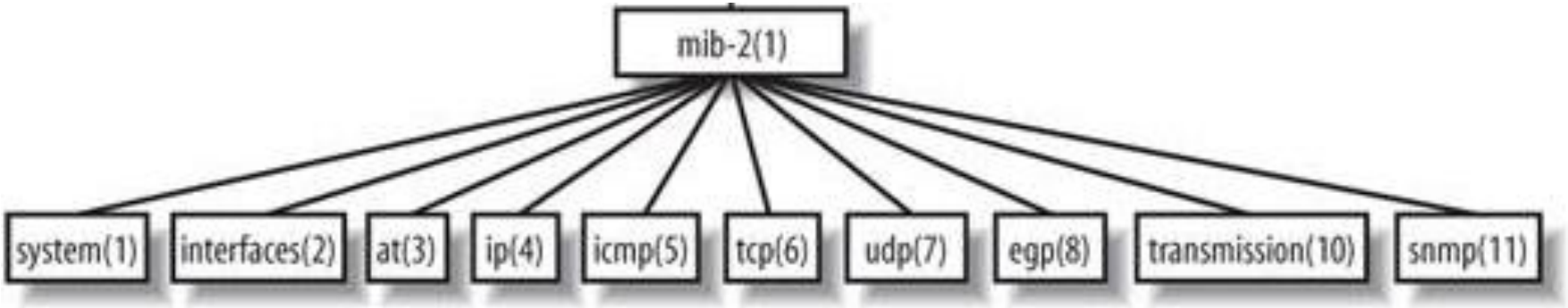
MIB - Management Information Base

- MIB-2(1)
  - sys/system (1)
    - Informações gerais sobre o nó
  - if/interface (2)
    - Informações sobre todas as interfaces instaladas no nó
  - at (3)
    - Address translation
    - Informações sobre a tabela ARP



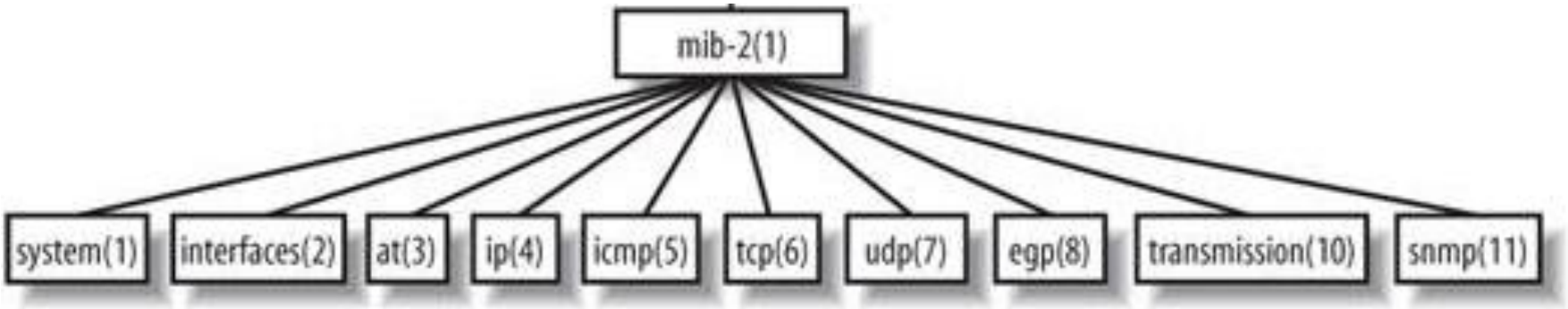
MIB - Management Information Base

- MIB-2(1)
  - ip (4)
    - Informações relativas ao protocolo IP
  - icmp (5)
    - Informações relativas ao protocolo ICMP
  - tcp (6)
    - Informações relativas ao protocolo TCP
  - udp (7)
    - Informações relativas ao protocolo UDP



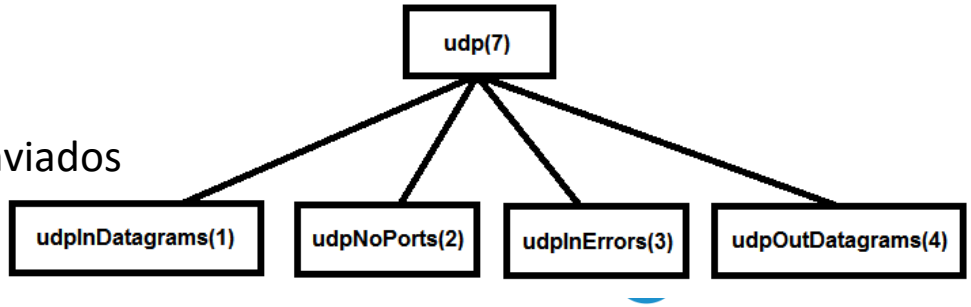
MIB - Management Information Base

- MIB-2(1)
  - egp (8)
    - Informações relativas ao protocolo Exterior Gateway Protocol
  - transmission (10)
    - Protocolo de transmissão (WAN)
  - snmp (11)
    - Informações relativas ao próprio SNMP



MIB - Management Information Base

- udp (7)
  - udpInDatagrams
    - 1.3.6.1.2.1.7.1
    - Número total de datagramas UDP recebidos
    - Counter32
  - udpNoPorts
    - 1.3.6.1.2.1.7.2
    - Número total de datagramas UDP recebidos endereçados para portas fechadas
    - Counter32
  - udpInErrors
    - 1.3.6.1.2.1.7.3
    - Número de datagramas UDP recebidos que não puderam ser entregues por outras razões distintas do erro de portas fechadas
    - Counter32
  - udpOutDatagrams
    - 1.3.6.1.2.1.7.4
    - Número total de datagramas enviados
    - Counter32



MIB - Management Information Base

- Classes de objetos gerenciados
  - Escalar
    - Objetos que definem uma única instância
    - Ex. sys(1)
  - Tabular
    - Objetos que definem multiplas intâncias relacionadas e agrupadas um uma tabela MIB
    - Ex. ip(4)

MIB - Management Information Base

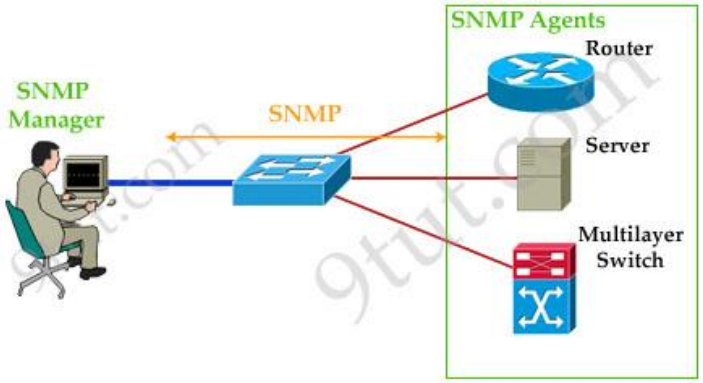
- Conceito de Estado
  - Estado do dispositivo gerenciado
    - Conjunto de valores dos objetos de um dispositivo gerenciado em determinado momento
  - Estado da rede
    - Conjunto de valores de todos os objetos de todos os dispositivos gerenciados de uma rede em um determinado momento

SNMP

- Arquitetura de Gerenciamento na Internet
  - SMI (Structure of Management Information)
    - Estrutura de informações de gerenciamento
    - Impõe regras para a construção da base de dados
  - MIB (Management Information Base)
    - Base de informações de gerenciamento
    - Contém as informações sobre objetos gerenciados
  - SNMP (Simple Network Management Protocol)
    - Protocolo de comunicação

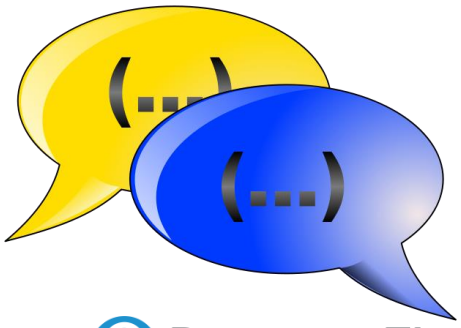
SNMP

- Protocolo de comunicação
  - Não gerencia a rede sozinho
- Sem conexão
  - UDP / 161 e 162
- Define o formato dos pacotes
  - Nomes dos objetos
  - Estados
- Pacotes de tamanho variável



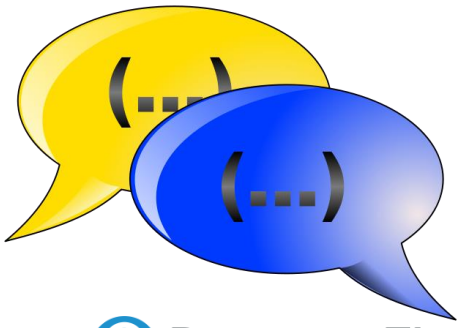
SNMP

- Mensagens SNMP / PDUs
  - GetRequest
    - Gerente -> Agente
    - Utilizado para leitura de uma variável ou conjunto de variáveis
  - GetNextRequest
    - Gerente -> Agente
    - Busca o próximo registro de uma tabela
  - GetBulkRequest
    - Gerente -> Agente
    - Permite a leitura de uma grande quantidade de dados
    - Incluído na versão SNMPv2



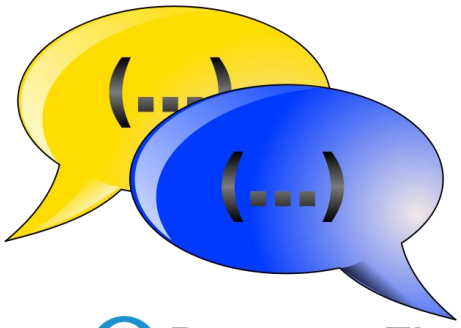
SNMP

- Mensagens SNMP / PDUs
  - SetRequest
    - Gerente -> Agente
    - Utilizado para armazenar uma valor em uma variável
  - Response
    - Gerente <- Agente
    - Contém os valores das variáveis solicitadas pelo gerente
    - Informa sucesso ou erro
  - Trap
    - Gerente <- Agente
    - Utilizado pelo agente para notificar um evento anormal
    - Não há confirmação



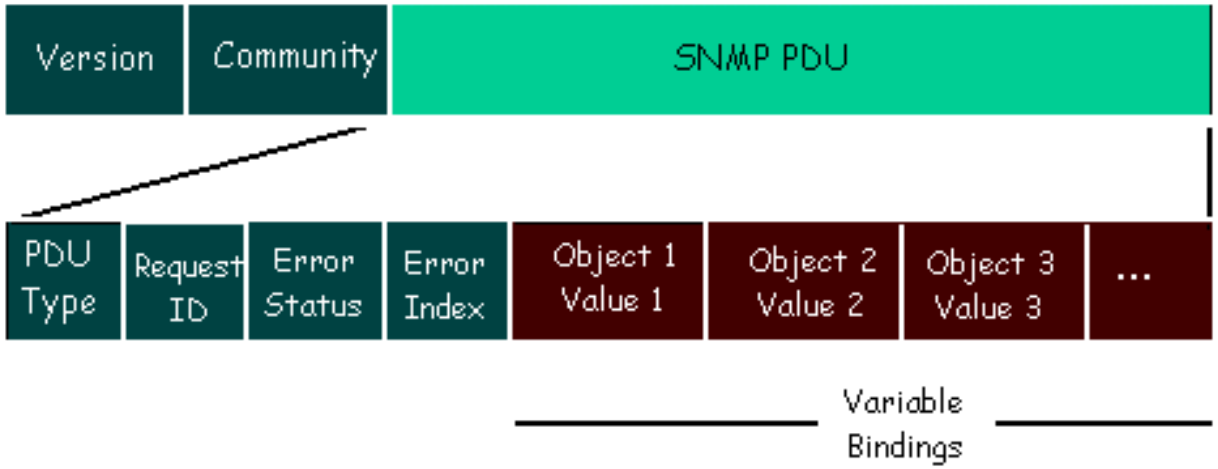
SNMP

- Mensagens SNMP / PDUs
  - InformRequest/Inform
    - Incluído na versão SNMPv2
    - Gerente <-> Gerente
      - Tem a finalidade de obter o valor de variáveis de agentes sob controle de outro gerente
      - Gerente remoto responde com um Response
    - Gerente <- Agente
      - Utilizado de maneira alternativa a um Trap
      - Garantia de recebimento
  - Report
    - Foi projetado para mensagens de erro entre gerentes
    - Ainda não usado



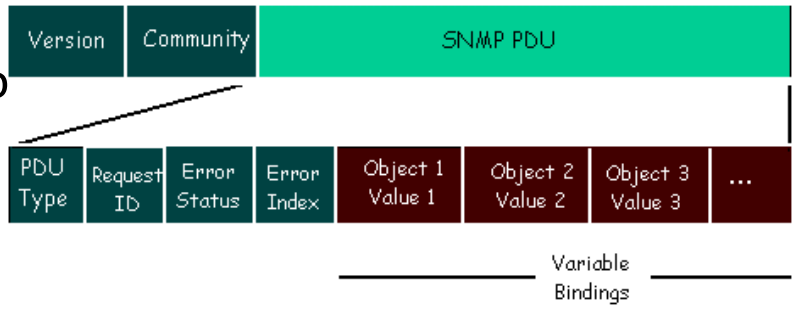
SNMP

- Cabeçalho SNMP
  - Version (Integer – 4 bytes)
    - Descreve a versão do SNMP empregada na mensagem
    - Começa em 0 (zero)
  - Community (Octet String – variável)
    - Identifica a comunidade utilizada na mensagem



SNMP

- Cabeçalho SNMP
  - PDU
    - PDU Type (Integer - 4 bytes)
      - Indica o tipo de PDU/Mensagem
    - Request ID (Integer - 4 bytes)
      - Utilizado para associar uma solicitação a uma reposta
    - Error Status (Integer - 4 bytes)
      - Exibe o código do erro
    - Error Index (Integer - 4 bytes)
      - Informa ao gerente qual objeto provocou o erro
    - Variable Bindings (Variável)
      - Informação a ser transmitida



Questões de Aprendizagem

SMI

MIB

SNMP

Acerca de sistemas operacionais e redes de comunicação, julgue os itens subsecutivos.

1. O SNMP, um protocolo de gerenciamento de redes de computadores que implementa comunicação mediante criptografia, permite a administração remota de um servidor Unix por meio da porta 22.

Acerca de sistemas operacionais e redes de comunicação, julgue os itens subsecutivos.

1. O SNMP, um protocolo de gerenciamento de redes de computadores que implementa comunicação mediante criptografia, permite a administração remota de um servidor Unix por meio da porta 22.

2.No contexto do protocolo SNMP é INCORRETO afirmar

A. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

B. ASN.1 é o padrão de codificação designado para as mensagens SNMP.

C. O conjunto de todos os objetos SNMP organiza-se dentro de uma base MIB.

D. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP.

E. O software de gerência de redes segue o modelo cliente-servidor convencional.

2.No contexto do protocolo SNMP é INCORRETO afirmar

A. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

B. ASN.1 é o padrão de codificação designado para as mensagens SNMP.

C. O conjunto de todos os objetos SNMP organiza-se dentro de uma base MIB.

D. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP.

E. O software de gerência de redes segue o modelo cliente-servidor convencional.

3.Julgue os seguintes itens referentes ao SNMP.

I O SNMP permite que estações de gerência enviem comandos para agentes nos dispositivos sendo gerenciados. Por meio desses comandos, uma estação de gerência pode acessar valores de objetos nos agentes.

II Um agente coleta informações acerca da unidade sendo gerenciada e as armazena em uma base de gerenciamento (MIB) para acesso futuro por uma unidade de gerência. Uma MIB é composta por variáveis que descrevem objetos gerenciados.

III Uma MIB armazena dados escalares e tabelas, mas não estruturas de dados complexas. As informações em uma MIB são organizadas de forma não hierárquica como coleções de objetos relacionados.

IV O SNMP possibilita que agentes enviem notificações assíncronas às estações de gerência quando ocorrem eventos relevantes. Por exemplo, um agente pode notificar uma falha na autenticação.

3.Julgue os seguintes itens referentes ao SNMP.

V O SNMP é orientado a mensagens e usa o TCP. Isso possibilita que o SNMP garanta a entrega das mensagens, inclusive das mensagens assíncronas que podem ser enviadas pelos agentes.

A quantidade de itens certos é igual a

A. 2.

B. 3.

C. 4.

D. 5.

3.Julgue os seguintes itens referentes ao SNMP.

V O SNMP é orientado a mensagens e usa o TCP. Isso possibilita que o SNMP garanta a entrega das mensagens, inclusive das mensagens assíncronas que podem ser enviadas pelos agentes.

A quantidade de itens certos é igual a

A. 2.

B. 3.

C. 4.

D. 5.

4.O SNMP (Simple Network Management Protocol) é um protocolo em nível de aplicação usado na gerência de redes TCP/IP. Realiza troca de informações entre os dispositivos de rede, possibilitando aos seus administradores gerenciar o desempenho da mesma, encontrar e resolver seus eventuais problemas. As requisições básicas GET e SET operam sobre um objeto individual, identificado por seu OID. Esse objeto é denominado

A. NID
B. MOD
C. NOB
D. MIB
E. MOB

4.O SNMP (Simple Network Management Protocol) é um protocolo em nível de aplicação usado na gerência de redes TCP/IP. Realiza troca de informações entre os dispositivos de rede, possibilitando aos seus administradores gerenciar o desempenho da mesma, encontrar e resolver seus eventuais problemas. As requisições básicas GET e SET operam sobre um objeto individual, identificado por seu OID. Esse objeto é denominado

A. NID
B. MOD
C. NOB
D. MIB
E. MOB

5.O SNMP - Simple Network Management Protocol, desde sua concepção, possui como característica a separação entre as informações trocadas e o protocolo usado para transportar essas informações. Com essa característica, as operações do protocolo não precisam ser definidas de acordo com comandos específicos usados para recuperar informações ou alterar as configurações de um dispositivo. O SNMPv1 define cinco tipos de PDU - Protocol Data Units, sendo eles: GetRequest, GetNextRequest, GetResponse, SetRequest e

A. UpdateRequest.
B. ProcessRequest.
C. Reject.
D. Trap.
E. Raise.

5.O SNMP - Simple Network Management Protocol, desde sua concepção, possui como característica a separação entre as informações trocadas e o protocolo usado para transportar essas informações. Com essa característica, as operações do protocolo não precisam ser definidas de acordo com comandos específicos usados para recuperar informações ou alterar as configurações de um dispositivo. O SNMPv1 define cinco tipos de PDU - Protocol Data Units, sendo eles: GetRequest, GetNextRequest, GetResponse, SetRequest e

A. UpdateRequest.
B. ProcessRequest.
C. Reject.

D. Trap.
E. Raise.

6.O protocolo SNMPv2 (Simple Network Management Protocol - versão 2) especifica um tipo de PDU (Protocol Data Unit) denominado de trap, cuja característica principal é apresentar notificação

A. assíncrona, enviada do agente para o elemento gerenciador, informando uma situação excepcional.

B. assíncrona, enviada do elemento gerenciador para o agente, requisitando o valor de objetos MIB.

C. programada, enviada do elemento gerenciador para o agente, requisitando o valor de objetos MIB.

D. programada, enviada do agente para o elemento gerenciador, indicando que todos os valores de objetos MIB estão corretos.

E. programada, enviada do elemento gerenciador para o agente, requisitando a interrupção do envio de mensagens.

6.O protocolo SNMPv2 (Simple Network Management Protocol - versão 2) especifica um tipo de PDU (Protocol Data Unit) denominado de trap, cuja característica principal é apresentar notificação

A. assíncrona, enviada do agente para o elemento gerenciador, informando uma situação excepcional.

B. assíncrona, enviada do elemento gerenciador para o agente, requisitando o valor de objetos MIB.

C. programada, enviada do elemento gerenciador para o agente, requisitando o valor de objetos MIB.

D. programada, enviada do agente para o elemento gerenciador, indicando que todos os valores de objetos MIB estão corretos.

E. programada, enviada do elemento gerenciador para o agente, requisitando a interrupção do envio de mensagens.

7.No gerenciamento SNMP

A. o protocolo é definido no nível de rede e é utilizado para obter informações de servidores SNMP.

B. cada máquina gerenciada pelo SNMP deve possuir um agente que é o responsável pela atualização das informações na base MIB e pelo armazenamento no servidor que hospeda o gerente.

C. os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte TCP.

D. os agentes se espalham em uma rede baseada na pilha de protocolos TCP/IP.

E. o gerente é o responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos para atuação dos agentes.

7.No gerenciamento SNMP

A. o protocolo é definido no nível de rede e é utilizado para obter informações de servidores SNMP.

B. cada máquina gerenciada pelo SNMP deve possuir um agente que é o responsável pela atualização das informações na base MIB e pelo armazenamento no servidor que hospeda o gerente.

C. os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte TCP.

D. os agentes se espalham em uma rede baseada na pilha de protocolos TCP/IP.

E. o gerente é o responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos para atuação dos agentes.

8.No modelo de gerenciamento SNMP, atua como uma coleção de pontos de acesso no agente para a estação de gerenciamento

A. a base de informações de gerenciamento.

B. o protocolo de gerenciamento da rede.

C. o backbone da rede.

D. o roteador.

E. o switch.

8.No modelo de gerenciamento SNMP, atua como uma coleção de pontos de acesso no agente para a estação de gerenciamento

A. a base de informações de gerenciamento.

B. o protocolo de gerenciamento da rede.

C. o backbone da rede.

D. o roteador.

E. o switch.

9.No protocolo SNMP, a operação GET-NEXT

A. é usada para informar a ocorrência de eventos, permitindo aos servidores SNMP enviarem informações aos clientes sempre que houver alterações nos objetos.

B. é usada por um cliente para alterar um ou mais atributos de um objeto gerenciado.

C. determina um cliente para obter o valor de um ou mais atributos de um objeto gerenciado.

D. é utilizada com a finalidade de ativação, execução e desativação do sistema.

E. especifica o objeto a acessar, para obter seus atributos e descobrir qual o próximo objeto na sequência léxica.

9.No protocolo SNMP, a operação GET-NEXT

A. é usada para informar a ocorrência de eventos, permitindo aos servidores SNMP enviarem informações aos clientes sempre que houver alterações nos objetos.

B. é usada por um cliente para alterar um ou mais atributos de um objeto gerenciado.

C. determina um cliente para obter o valor de um ou mais atributos de um objeto gerenciado.

D. é utilizada com a finalidade de ativação, execução e desativação do sistema.


E. especifica o objeto a acessar, para obter seus atributos e descobrir qual o próximo objeto na sequência léxica.

10.O tipo de dado da estrutura de informações de gerenciamento ou SMI (Structure of Management Information) do padrão Internet TCP/IP de gerenciamento, que define uma cadeia de bytes no formato ASN.1 (Abstract Syntax Notation One) para a representação de dados binários ou texto de até 65.535 bytes, é o

A. INTEGER

B. OCTET STRING

C. Counter32

D. Counter64

E. TimeTicks

10.O tipo de dado da estrutura de informações de gerenciamento ou SMI (Structure of Management Information) do padrão Internet TCP/IP de gerenciamento, que define uma cadeia de bytes no formato ASN.1 (Abstract Syntax Notation One) para a representação de dados binários ou texto de até 65.535 bytes, é o

A. INTEGER

B. OCTET STRING

C. Counter32

D. Counter64

E. TimeTicks

11.A MIB II usa uma arquitetura de árvore, definida na ISO ASN.1, para organizar todas as suas informações, sendo que, cada parte da informação da árvore é um nó rotulado. Nessa árvore, o MIB II pode ser localizado, percorrendo, sucessivamente, os nós

A. joint-iso-ccitt(2) _ org(3) _ dod(6) _ Internet(1) _ mgmt(2) _ mibII(2)

B. ccitt(0) _ org(3) _ dod(6) _ Internet(1) _ mgmt(2) _ mibII(2)

C. iso(1) _ org(3) _ dod(6) _ Internet(1) _ mgmt(2) _ mibII(1)

D. ccitt(0) _ iso(1) _ joint-iso-ccitt(2) _org(3) _ mgmt(4) _ mibII(5)

E. iso(1) _ org(3) _ dod(6) _ Internet(1) _ directory(1) _ mibII(1)

11.A MIB II usa uma arquitetura de árvore, definida na ISO ASN.1, para organizar todas as suas informações, sendo que, cada parte da informação da árvore é um nó rotulado. Nessa árvore, o MIB II pode ser localizado, percorrendo, sucessivamente, os nós

A. joint-iso-ccitt(2) _ org(3) _ dod(6) _ Internet(1) _ mgmt(2) _ mibII(2)

B. ccitt(0) _ org(3) _ dod(6) _ Internet(1) _ mgmt(2) _ mibII(2)

C. iso(1) _ org(3) _ dod(6) _ Internet(1) _ mgmt(2) _ mibII(1)

D. ccitt(0) _ iso(1) _ joint-iso-ccitt(2) _org(3) _ mgmt(4) _ mibII(5)

E. iso(1) _ org(3) _ dod(6) _ Internet(1) _ directory(1) _ mibII(1)

12.Em termos da estrutura de gerenciamento de redes, o componente que possibilita um gerente investigar os estados dos dispositivos gerenciados é

A. a base de informação de gerência ou MIB.

B. o objeto gerenciado.

C. o agente de gerenciamento de rede.

D. o protocolo de gerenciamento de rede.

E. a estrutura de informação de gerenciamento ou SMI

12.Em termos da estrutura de gerenciamento de redes, o componente que possibilita um gerente investigar os estados dos dispositivos gerenciados é

A. a base de informação de gerência ou MIB.

B. o objeto gerenciado.

C. o agente de gerenciamento de rede.

D. o protocolo de gerenciamento de rede.

E. a estrutura de informação de gerenciamento ou SMI

GABARITO

1. E
2. E
3. B
4. D
5. D
6. A
7. D
8. A
9. E
10. B
11. C
12. D

Gerenciamento de Redes

SNMP - Versões

CMIP

SNMPv1

- Segurança precária
  - Comunidade
    - Mecanismo para estabelecimento de confiança entre agentes e gerentes
    - Nomes de comunidade são essencialmente senhas
      - Transitam em texto claro
    - 3 Tipos de comunidade
      - Somente leitura (read-only)
      - Leitura e escrita (read-write)
      - Trap
- Comandos transportam poucos dados
  - GReq, GNR, SR, Resp, Trap
- Traps sem reconhecimento
  - Pouco confiável

SNMPv2

- Variações da versão
  - SNMPv2p (party-based)
    - Versão originalmente proposta
    - Novas PDUs
    - Novos tipos de dados
    - Implementação de segurança
  - SNMPv2u (user-based)
    - Esquema de segurança baseado em usuários
    - Mais simples que o party-based
    - Mais seguro que a segurança baseada em comunidade
  - SNMPv2* (star)
    - Não foi padronizado em RFC
    - Combina conceitos de segurança da party-based com user-based
  - SNMPv2c (community-based)
    - Padrão de fato
    - Utiliza melhorias da versão party-based
    - Mantém a segurança do SNMPv1 (comunidade)

SNMPv2

- Novidades
  - Melhoria na eficiência e na performance
    - GetBulkRequest
  - Confirmação de notificação eventual
    - Inform Request/Inform
  - Comunicação entre gerentes
    - Inform Request/Inform
  - Novo tipo de dados
    - Counter64
  - Novos códigos de erros
  - Facilidade na manipulação de linhas da MIB
  - Melhorias na definição de linguagem de dados
- Problemas
  - SNMPv1 não interopera com SNMPv2
  - Segurança baseada em comunidade

SNMPv3

- Segurança reforçada
  - Autenticação
    - Aposenta o conceito de comunidade
  - Privacidade
    - Criptografia
  - Controle de Acesso
    - Visões distintas para diferentes usuários
- Padroniza as soluções de segurança propostas nas derivações do SNMPv2
  - SNMPv2u, SNMPv2*

SNMPv3

- USM (User Security Model)
  - Modelo de segurança baseado em usuários
  - Provê autenticação e privacidade
  - Seguro contra
    - Modificação da Informação
    - Repetição de Mensagens
    - Descoberta
  - Não evita
    - Negação de Serviço (DoS)
    - Análise de Tráfego

SNMPv3

- VACM (View Access Control Model)
  - Modelo de segurança baseado em visões
  - Provê controle de acesso
  - Adota políticas de Grupo
  - Conceito de Contexto
- Padrões criptográficos
  - MD5, SHA-1
  - DES (CBC)
  - 3DES
  - AES

SNMPv3

- Entidades
  - Conjunto de módulos que interagem entre si para prover serviços SNMP
  - Módulos
    - Funcionalidades do SNMP
    - Independentes entre si
  - Pode atuar como agente, gerente ou ambos
  - Permite a definição de diferentes versões para cada módulo
- Utiliza mensagens/PDUs do SNMPv2
  - Não há mudanças nos tipos de dados e objetos MIB (SMIv2 e MIBv2)
- Compatível com as versões anteriores

CMIP

- Common Management Information Protocol
  - Protocolo de gerenciamento de rede baseado no modelo OSI
  - Padronizado pela ITU (X.700) e ISO
  - Boa segurança
    - Autenticação
    - Controle de acesso
    - Logs de segurança

CMIP

- CMIP vs SNMP
  - Orientado a conexão
  - Possui mais funcionalidades que o SNMP
    - Conjunto mais completo de operações
  - Mais complexo
    - Utiliza mais recursos de hardware do que o SNMP
  - Maioria dos dispositivos suporta SNMP, mas não o CMIP
  - É mais confiável que o SNMP

Questões de Aprendizagem

SNMP - Versões

Acerca dos protocolos TCP/IP e SNMP, julgue os seguintes itens.

1. A versão 3 do protocolo SNMP (simple network management protocol), que permite enviar pacotes de forma criptografada, foi desenvolvida para melhorar a segurança.

Acerca dos protocolos TCP/IP e SNMP, julgue os seguintes itens.

1. A versão 3 do protocolo SNMP (simple network management protocol), que permite enviar pacotes de forma criptografada, foi desenvolvida para melhorar a segurança.

OSI/ISO e TCP/IP são modelos de redes de computadores que contemplam serviços e protocolos para comunicação em geral. A esse respeito, julgue os itens a seguir.

2. No SNMPv1, a interação entre agente e gerente pode ser iniciada por qualquer uma das partes, e a segurança das mensagens que chegam nos agentes pode incluir o uso de senha não criptografada.

OSI/ISO e TCP/IP são modelos de redes de computadores que contemplam serviços e protocolos para comunicação em geral. A esse respeito, julgue os itens a seguir.

2. No SNMPv1, a interação entre agente e gerente pode ser iniciada por qualquer uma das partes, e a segurança das mensagens que chegam nos agentes pode incluir o uso de senha não criptografada.

3.Analise as seguintes afirmativas sobre gerenciamento de redes.

I. O protocolo SNMP é um protocolo da camada de aplicação utilizado para a gerência de redes TCP/IP que permite a troca de informações entre os dispositivos de rede e a estação de gerência.

II. A versão 3 do protocolo SNMP (SNMPv3) adiciona recursos de segurança com relação a privacidade, autenticação e controle de acesso.

III. O agente SNMPv2 utiliza a porta 161/udp para o envio de mensagens do agente a estação de gerência, já a autenticação é feita pela porta 162/udp e consiste no envio de uma string de comunidade em texto não criptografado.

Assinale a alternativa CORRETA:

A. A afirmativa III está errada e as afirmativas I, II estão corretas.

B. A afirmativa II está errada e as afirmativas I, III estão corretas.

C. A afirmativa I está errada e as afirmativas II, III estão corretas.

D. As afirmativas I, II e III estão corretas.

3.Analise as seguintes afirmativas sobre redes sem fio.

I. O protocolo SNMP é um protocolo da camada de aplicação utilizado para a gerência de redes TCP/IP que permite a troca de informações entre os dispositivos de rede e a estação de gerência.

II. A versão 3 do protocolo SNMP (SNMPv3) adiciona recursos de segurança com relação a privacidade, autenticação e controle de acesso.

III. O agente SNMPv2 utiliza a porta 161/udp para o envio de mensagens do agente a estação de gerência, já a autenticação é feita pela porta 162/udp e consiste no envio de uma string de comunidade em texto não criptografado.

Assinale a alternativa CORRETA:

A. A afirmativa III está errada e as afirmativas I, II estão corretas.

B. A afirmativa II está errada e as afirmativas I, III estão corretas.

C. A afirmativa I está errada e as afirmativas II, III estão corretas.

D. As afirmativas I, II e III estão corretas.

A respeito de gerenciamento de redes de comunicação com SNMP, julgue os próximos itens

4.Tanto o SNMP v1 quanto o SNMP v2 cifram a comunidade de escrita para coibir a captura de dados em texto claro.

5.Entradas ARP são comuns em switches e, por padrão, o SNMP identificação de entradas ARP que possam ter sido forjadas.

6.Uma vez definida uma comunidade de leitura, tanto na versão 1 quanto na versão 2 do SNMP, a estação de gerência, a partir dessa comunidade, poderá enviar comandos SNMP do tipo get <objeto> para verificar o que está definido no objeto em questão.

A respeito de gerenciamento de redes de comunicação com SNMP, julgue os próximos itens

4.Tanto o SNMP v1 quanto o SNMP v2 cifram a comunidade de escrita para coibir a captura de dados em texto claro.

5.Entradas ARP são comuns em switches e, por padrão, o SNMP identificação de entradas ARP que possam ter sido forjadas.

6.Uma vez definida uma comunidade de leitura, tanto na versão 1 quanto na versão 2 do SNMP, a estação de gerência, a partir dessa comunidade, poderá enviar comandos SNMP do tipo get <objeto> para verificar o que está definido no objeto em questão.

A respeito de gerenciamento de redes de comunicação com SNMP, julgue os próximos itens

7.O SNMP v3 utiliza comandos ethernet para habilitar e desabilitar portas UDP.

8.Por meio de comando SNMP do tipo set <objeto>, uma estação de gerência de rede é capaz de alterar um valor, desde que passe a comunidade que tenha permissão de escrita.

A respeito de gerenciamento de redes de comunicação com SNMP, julgue os próximos itens

7.O SNMP v3 utiliza comandos ethernet para habilitar e desabilitar portas UDP.

8.Por meio de comando SNMP do tipo set <objeto>, uma estação de gerência de rede é capaz de alterar um valor, desde que passe a comunidade que tenha permissão de escrita.

9.Considere:

I. Autenticação.

II. Privacidade.

III. Controle de acesso.

Quanto aos serviços, o protocolo SNMPv3 fornece o que se afirma em

A. I, apenas.

B. II, apenas.

C. I e II, apenas.

D. I e III, apenas.

E. I, II e III.

9.Considere:

I. Autenticação.

II. Privacidade.

III. Controle de acesso.

Quanto aos serviços, o protocolo SNMPv3 fornece o que se afirma em

A. I, apenas.

B. II, apenas.

C. I e II, apenas.

D. I e III, apenas.

E. I, II e III.

O gerenciamento de serviços de rede requer uma série de procedimentos, configurações, protocolos e especificações. Com relação às características de gerenciamento de redes, julgue os itens subsequentes

10.Autenticação, privacidade e controle de acesso são características das versões 2 e 3 do SNMP, mas não da versão 1.

11.O protocolo SNMPv1 requer o uso de uma senha para leitura e outra para leitura e escrita. Esta senha, que trafega cifrada por SSL, permite navegar pelas MIBs dos dispositivos.

O gerenciamento de serviços de rede requer uma série de procedimentos, configurações, protocolos e especificações. Com relação às características de gerenciamento de redes, julgue os itens subsequentes

10.Autenticação, privacidade e controle de acesso são características das versões 2 e 3 do SNMP, mas não da versão 1.

11.O protocolo SNMPv1 requer o uso de uma senha para leitura e outra para leitura e escrita. Esta senha, que trafega cifrada por SSL, permite navegar pelas MIBs dos dispositivos.

12.Analise as seguintes afirmações relativas aos recursos de segurança providos pelo protocolo SNMPv3:

I. O controle de acesso às informações de gerenciamento de redes é baseado em visões.

II. É usado o algoritmo DES no modo de endereçamento de blocos de cifras.

III. Há proteção contra ataques de reprodução, com base em um contador no receptor.

Indique a opção correta.

A. Apenas as afirmações I e II são verdadeiras.

B. Apenas as afirmações I e III são verdadeiras.

C. Apenas as afirmações II e III são verdadeiras.

D. As afirmações I, II e III são verdadeiras.

E. Nenhuma das afirmações é verdadeira.

12.Analise as seguintes afirmações relativas aos recursos de segurança providos pelo protocolo SNMPv3:

I. O controle de acesso às informações de gerenciamento de redes é baseado em visões.

II. É usado o algoritmo DES no modo de endereçamento de blocos de cifras.

III. Há proteção contra ataques de reprodução, com base em um contador no receptor.

Indique a opção correta.

A. Apenas as afirmações I e II são verdadeiras.
B. Apenas as afirmações I e III são verdadeiras.
C. Apenas as afirmações II e III são verdadeiras.
D. As afirmações I, II e III são verdadeiras.
E. Nenhuma das afirmações é verdadeira.

Com relação à administração e gerência de redes, julgue os itens a seguir.

13.Entre as vantagens do modelo de gerência SNMP em relação ao CMIP, cita-se o uso do protocolo TCP/IP, em vez da pilha de protocolos OSI, dada a simplicidade do modelo, além do fato de ser implementado na maioria dos dispositivos de rede, como hubs, bridges e routers.

14.Caso ocorra, no SNMPv3, incidência na rede, as notificações Trap e Inform podem ser utilizadas por um agente para a comunicação ao gerente sobre o evento ocorrido. A diferença fundamental entre elas é a necessidade de confirmação de recebimento pelo receptor quando se utiliza a notificação Inform.

15.O SNMPv3 elimina o conceito de gerenciadores e agentes e, por esse motivo, não oferece suporte às operações definidas no SNMPv1 e SNMPv2c.

Com relação à administração e gerência de redes, julgue os itens a seguir.

13.Entre as vantagens do modelo de gerência SNMP em relação ao CMIP, cita-se o uso do protocolo TCP/IP, em vez da pilha de protocolos OSI, dada a simplicidade do modelo, além do fato de ser implementado na maioria dos dispositivos de rede, como hubs, bridges e routers.

14.Caso ocorra, no SNMPv3, incidência na rede, as notificações Trap e Inform podem ser utilizadas por um agente para a comunicação ao gerente sobre o evento ocorrido. A diferença fundamental entre elas é a necessidade de confirmação de recebimento pelo receptor quando se utiliza a notificação Inform.

15.O SNMPv3 elimina o conceito de gerenciadores e agentes e, por esse motivo, não oferece suporte às operações definidas no SNMPv1 e SNMPv2c.

Com relação à arquitetura TCP/IP, julgue os itens subsequentes

16.O protocolo SNMP inclui mecanismos de segurança para a cifração e verificação de integridade das mensagens.

17.A SMI define a linguagem ASN.1 para especificar módulos, objetos e notificações, que são os objetos gerenciados que residem na MIB.

Com relação à arquitetura TCP/IP, julgue os itens subsequentes

16.O protocolo SNMP inclui mecanismos de segurança para a cifração e verificação de integridade das mensagens.

17.A SMI define a linguagem ASN.1 para especificar módulos, objetos e notificações, que são os objetos gerenciados que residem na MIB.

GABARITO

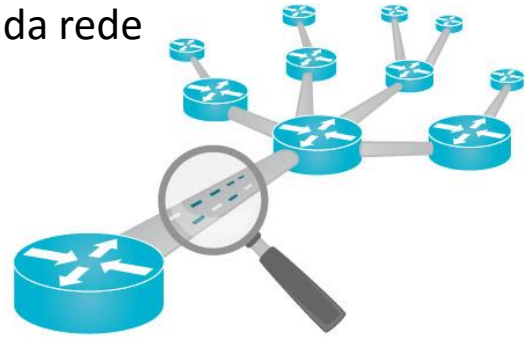
1. C
2. C
3. A
4. E
5. E
6. C
7. E
8. C
9. E
10. E
11. E
12. B
13. C
14. E
15. E
16. E
17. E

Gerenciamento de Redes

RMON

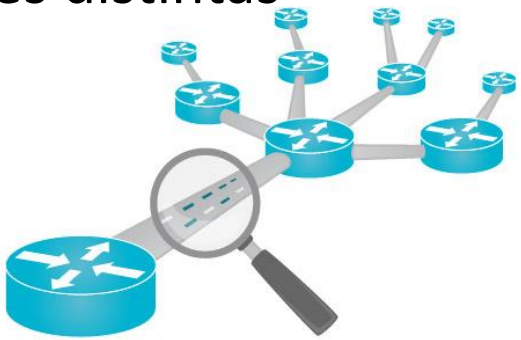
RMON

- Remote Network Monitoring MIB
  - Extensão da MIBv2
    - 1.3.6.1.2.1.16
  - Baseado no monitoramento remoto de fluxo
    - MIB nativa – Características do dispositivo
    - RMON - Padrões de tráfego
  - Probes (sondas)
    - Dispositivos de monitoramento
      - Coletam dados sobre o tráfego da rede
      - Analisam e interpretam os dados
      - Devolvem ao gerente informações sobre os fluxos da rede
    - Reduzem o tráfego na rede e o processamento do gerente
      - Evita o polling
    - Necessitam de mais recursos computacionais



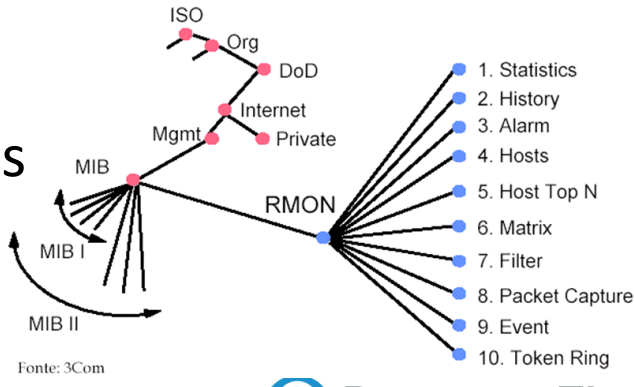
RMON

- Versões
  - RMON1
    - Foco no Ethernet e Token Ring
    - Camada física e enlace
    - Só enxerga a rede local
  - RMON2
    - Foco no monitoramento remoto de redes distintas
    - Camada de rede e aplicação



RMON

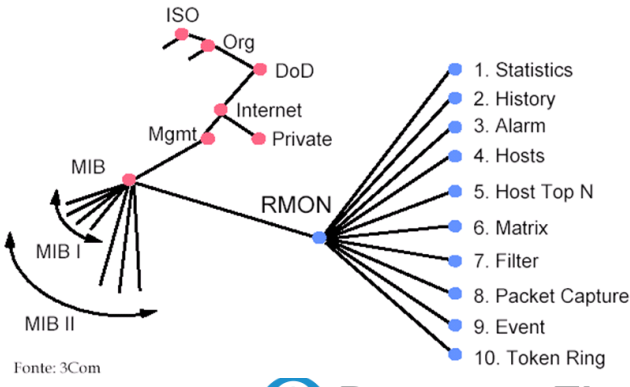
- RMON1
  - statistics (1)
    - Estatísticas da LAN em tempo real
    - Ex.
      - Pacotes/Bytes trafegados
      - Número de colisões
      - Pacotes com erro de CRC
  - history (2)
    - Histórico de estatísticas selecionadas
    - N últimas estatísticas



Fonte: 3Com

RMON

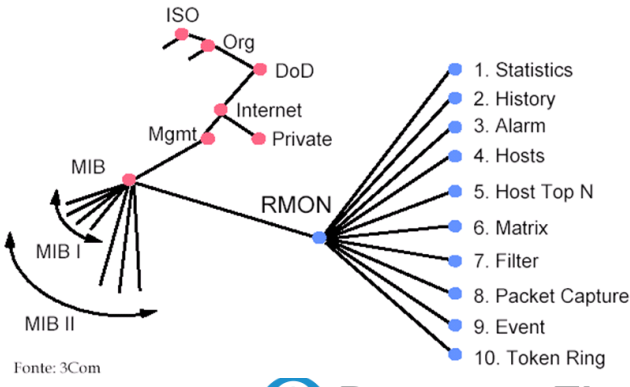
- RMON1
  - alarm(3)
    - Estabelece limites de operação para variáveis de MIB
    - Se excederem os limites, um evento é gerado
  - host (4)
    - Estatísticas de LAN de um host específico
  - hostTopN (5)
    - Registro dos N nós mais ativos sobre um dado período de tempo



Fonte: 3Com

RMON

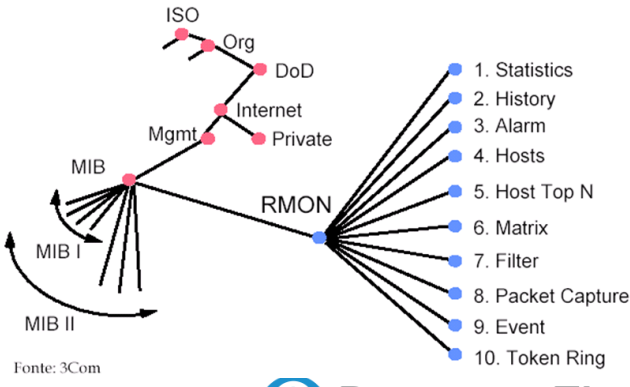
- RMON1
  - matrix (6)
    - Associa estatísticas de tráfego entre pares de nós da rede
  - filter (7)
    - Define padrões de pacotes de dados para captura/registro
  - capture (8)
    - Contém parâmetros de captura
    - Ex. Tamanho do buffer



Fonte: 3Com

RMON

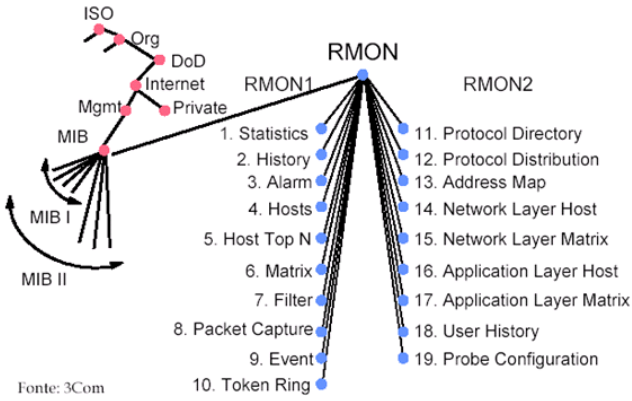
- RMON1
  - event (9)
    - Controla a geração e notificação de eventos
    - Ex.
      - Log interno
      - Trap
      - Log-and-Trap
  - tokenRing (10)
    - Extensões específicas do token ring



Fonte: 3Com

RMON

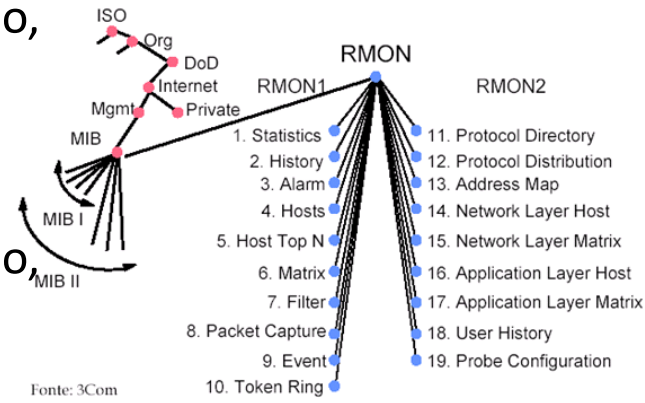
- RMON2
  - protocolDir (11)
    - Protocol Directory
    - Lista de protocolos que a probe pode monitorar
  - protocolDist (12)
    - Protocol Distribution
    - Estatísticas de tráfego para cada protocolo suportado
  - addressMap (13)
    - Address Map
    - Mapeia endereços de IP em endereços MAC



Fonte: 3Com

RMON

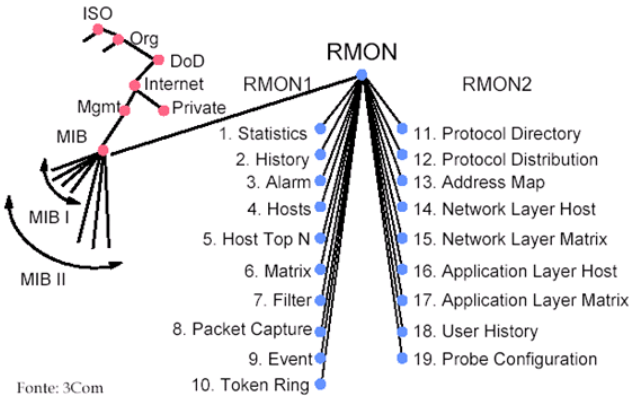
- RMON2
  - nlHost (14)
    - Network-Layer Host
    - Estatísticas de tráfego de camada 3, por host
  - nlMatrix (15)
    - Network-Layer Matrix
    - Estatísticas de tráfego de camada 3 entre um par de hosts
  - alHost (16)
    - Application-Layer Host
    - Estatísticas de tráfego da camada de aplicação, por host
  - alMatrix (17)
    - Application-Layer Matrix
    - Estatísticas de tráfego da camada de aplicação, por par de hosts



Fonte: 3Com

RMON

- RMON2
  - usrHistory (18)
    - User History
    - Histórico de coleta por usuário
  - probeConfig (19)
    - Probe Configuration
    - Configuração remota de probes
    - Interoperabilidade
  - rmonConformance (20)
    - RMON Conformance
    - Requisitos para conformidade com RMON2 MIB



Fonte: 3Com

Gerenciamento de Redes

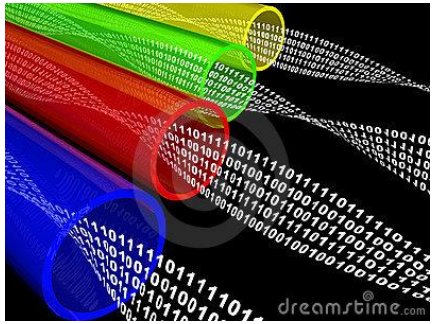
NetFlow

NetFlow

- Criado pela Cisco
- Coletar, interpretar e analisar dados de tráfego em redes IP
- Auxilia na detecção de problemas e anomalias
- Melhor aplicação da QoS
- Foi substituído pelo IPFIX
  - Internet Protocol Flow Information eXport
  - RFC 5101 e 5102
- Implementações em CLI e GUI

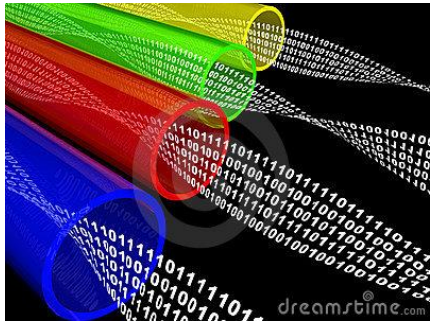
NetFlow

- Fluxo
  - Sequência unidirecional de pacotes que transitam um dispositivo gerenciado
  - Organizar o tráfego com base nas suas características
  - Identificação de um fluxo
    - Interface (ingresso)
    - IP de origem
    - IP de destino
    - Campo protocol – IP
    - Porta de origem
    - Porta de destino
    - ToS - IP



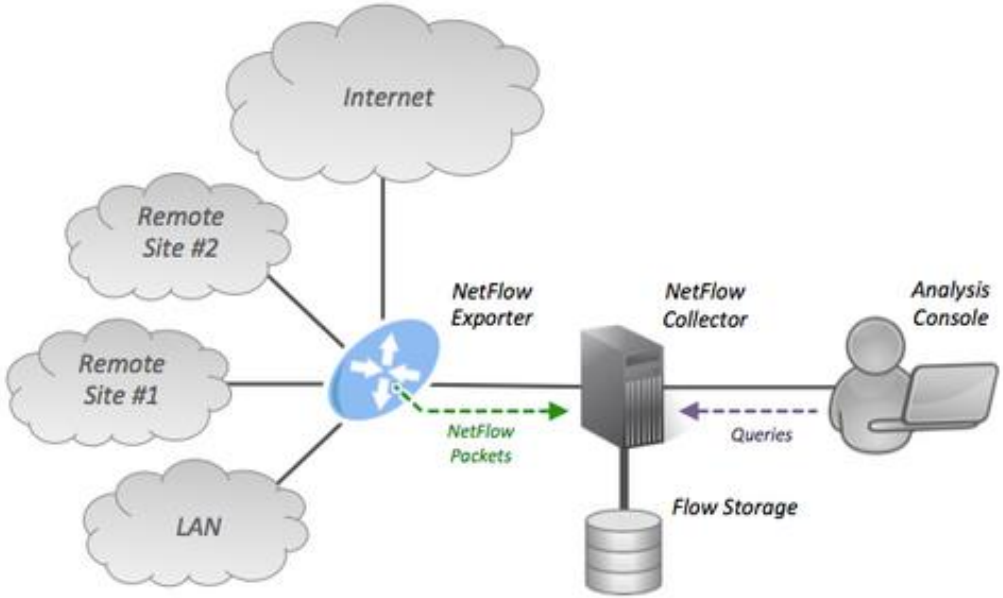
NetFlow

- Interface
  - Meio de entrada ou saída de dados de um dispositivo
  - Nativamente, o NetFlow captura pacotes recebidos por uma interface de ingresso
  - A caputra nas interfaces de entrada devem ser habilitadas individualmente
    - Desabilitado por padrão
    - Não há comando para habilitar todas as interfaces



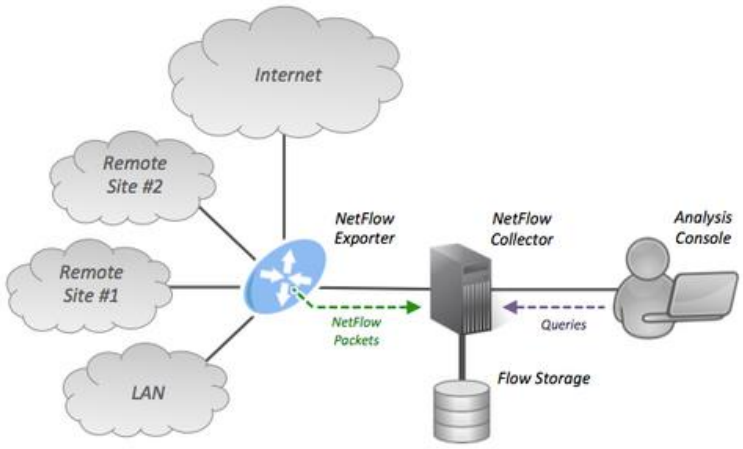
NetFlow

- 3 Componentes Essenciais
  - Cache de Fluxo (NetFlow Exporter)
  - Coletor de Fluxo (NetFlow Collector)
  - Analisador de Dados (Analysis Application)



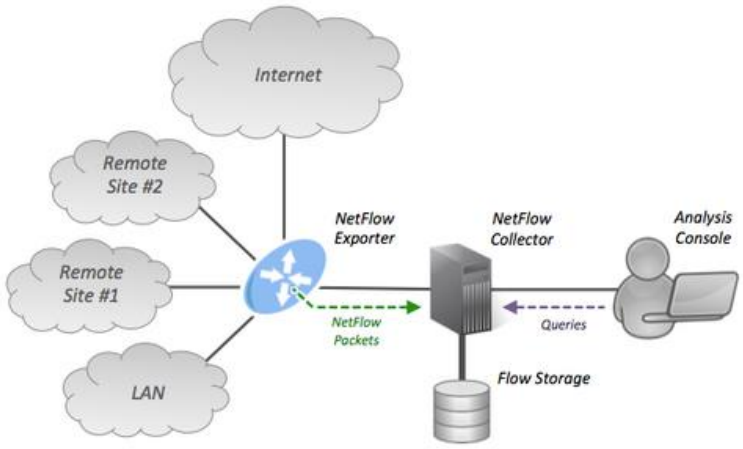
NetFlow

- Cache de Fluxo (NetFlow Exporter)
  - Instalado no dispositivo gerenciado
  - Agraga pacotes em fluxos
  - Exporta registros de fluxo a um ou mais coletores de fluxo
  - Exportados via UDP
    - Porta padrão 2055
    - Portas configuráveis



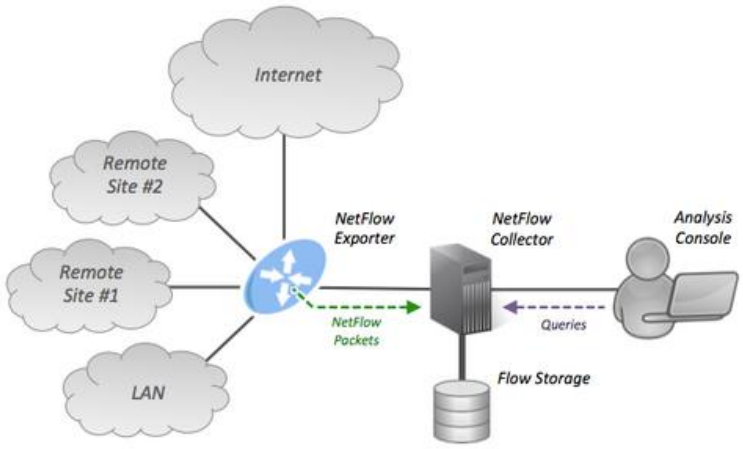
NetFlow

- Cache de Fluxo (NetFlow Exporter)
  - Funcionamento
    - Identificação
      - No momento da entrada do pacote, verifica se o fluxo está presente na tabela de cache
      - Se sim -> Encaminha o pacote diretamente a interface de destino
      - Se não -> Realiza um lookup nas tabelas de roteamento e nas tabelas de access-list
        - » Se sim -> cadastra o fluxo
        - » Se não -> descarta o pacote



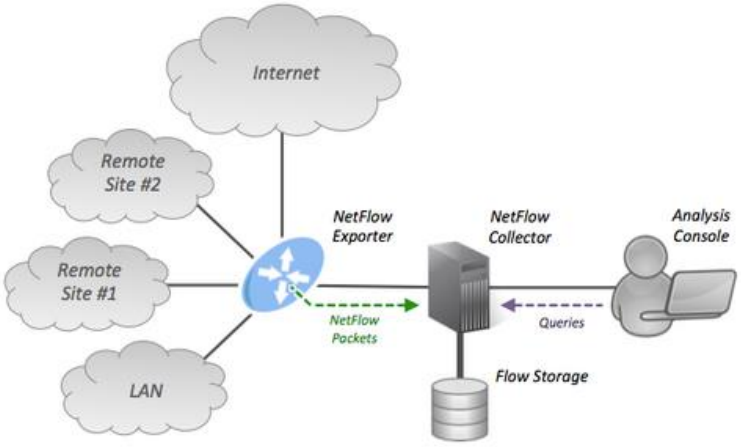
NetFlow

- Cache de Fluxo (NetFlow Exporter)
  - Funcionamento
    - Exportação
      - Exporta os dados de fluxo via UDP para o Coletor de Fluxo
      - Por tempo
        - » Se ocioso por mais de 15 segundos
        - » Se a duração do fluxo excede 30 minutos
      - Por flags
        - » Conexão TCP encerrada
          - FIN ou RST
      - Não necessita de polling
      - Apaga fluxos exportados



NetFlow

- Coletor de Fluxo (NetFlow Collector)
  - Recebe, organiza e interpreta os fluxos exportados
  - Combina os dados para geração de relatórios sobre o tráfego da rede
- Analisador de Dados (Analysis application)
  - Analisa as informações de fluxo sobre um determinado contexto
    - Detecção de problemas e anomalias



NetFlow

- Principais Vantagens
  - Acelera o encaminhamento por conta da tabela de cache de fluxos
    - Reduz consultas às tabelas de roteamento e à access-list
  - Não necessita de analisadores nos dispositivos gerenciados
    - Apenas agrupam e exportam os dados
    - Diminui a carga de processamento
  - Auxilia na melhor aplicação da QoS
  - Provê informações para a segurança da rede
    - Detecção de anomalias
  - Facilita
    - a análise de novas aplicações e novas políticas
    - a detecção de “top talkers”
    - a identificação de gargalos e a solução de problemas de desempenho

Gerenciamento de Redes

Ferramentas

Ferramentas

- Finalidades básicas
  - Verificar o desempenho na carga do tráfego de dados
  - Permite a detecção e previsão de falhas
  - Resolução proativa de problemas
  - Centralização do monitoramento
  - Suporte ao SNMP

MRTG

- Multi Router Traffic Grapher
- Código aberto distribuído sob a licença GPL
- Escrito em PERL
- Versões para Windows, Linux e Netware
- Faz leituras via SNMP ou comandos via scripts externos
  - Suporte ao SNMPv2c
  - Coleta dados a cada 5 minutos por padrão
- Permite monitorar informações específicas de serviços e equipamentos
- Gera páginas HTML com gráficos de dados
  - Diário
  - Semanal
  - Mensal
  - Anual
- Alerta via e-mail caso o valor do gráfico atinja um valor pré-estabelecido

Nagios

- Licença GNU/GPL
- Monitora equipamentos de rede e recursos de hosts
- Monitora serviços de rede
  - Protocolos da camada de aplicação
- Faz uso de túneis criptográficos SSH ou SSL
- Desenvolvimento simplificado de plugins
  - Atendendo a necessidades específicas
- Checagem de disponibilidade
  - Online/offline
- Checagem paralelizada

Nagios

- Notificação de eventos via e-mail, SMS ou outro meio customizado via por plugin
  - Problema/Falha
  - Limiar pré-cadastrado
  - Solução de um problema
- Armazenamento dos dados em arquivos texto em vez de bases de dados
- Rotação de logs automática
- Interface Web para visualização do status da rede
  - Não gera gráficos de utilização ou desempenho

Cacti

- Licença GNU/GPL
- Ferramenta para visualização de dados numéricos em forma de gráficos
  - Não coleta dados sozinho
  - Os dados são repassados para a ferramenta por meio de scripts ou programas encarregados de obter os dados
- Criação de hierarquias gráficas através da exibição em árvore
- Gerenciamento de usuários
- Suporte nativo ao SNMP
- Número ilimitado de itens no gráfico
- Geralmente utilizado em conjunto com o Nagios

Zabbix

- Licença GNU/GPL
- Herda características do Nagios e Cacti
- Suporte a inúmeros SGBDs
- Alto desempenho e alta escalabilidade
- Suporte para monitoramento via SNMP
- Monitoramento de estatísticas de SO
  - Agente Zabbix
  - Unix e Windows

ZABBIX

Zabbix

- Monitoramento básico de serviços
  - Agent-less monitoring
- Auto-discovery
- Gerenciamento de usuários
  - Autenticação segura
  - Permissão em nível de usuários, grupos ou Ips
- Notificação de e-mail em eventos pré-definidos
- Logs de auditoria

ZABBIX

Questões de Aprendizagem

RMON

NetFlow

Ferramentas

Com relação aos sistemas de gerenciamento de rede, julgue os próximos itens.

1. O MRTG (the multi router traffic grapher) é uma ferramenta open source que permite visualizar o tráfego da rede. O MRTG implementa o protocolo SNMP (simple network management protocol) para obter informações dos equipamentos de rede. Entretanto, o MRTG ainda não permite o acesso a contadores de 64 bits da versão 2 do SNMP.

2. O Nagios é um programa open source de monitoramento de redes que verifica constantemente a disponibilidade do serviço. O Nagios permite, entre outras coisas, monitorar os serviços de rede, tais como SMTP, POP3 e HTTP, e pode ser configurado para reportar, por meio de e-mail ou até mesmo celular (SMS), sobre o problema ocorrido.

Com relação aos sistemas de gerenciamento de rede, julgue os próximos itens.

1. O MRTG (the multi router traffic grapher) é uma ferramenta open source que permite visualizar o tráfego da rede. O MRTG implementa o protocolo SNMP (simple network management protocol) para obter informações dos equipamentos de rede. Entretanto, o MRTG ainda não permite o acesso a contadores de 64 bits da versão 2 do SNMP.

2. O Nagios é um programa open source de monitoramento de redes que verifica constantemente a disponibilidade do serviço. O Nagios permite, entre outras coisas, monitorar os serviços de rede, tais como SMTP, POP3 e HTTP, e pode ser configurado para reportar, por meio de e-mail ou até mesmo celular (SMS), sobre o problema ocorrido.

A respeito dos sistemas de gerenciamento de redes, julgue os próximos itens.

3. SNMP (Simple Network Management Protocol), versão 3, é um protocolo de gerência de redes da camada de aplicação que usa as portas 161 e 162 do UDP para transmitir as informações. Caso ocorra uma incidência na rede, a operação Write é utilizada por um agente para a comunicação ao gerente sobre o evento.

4. O padrão RMON (Remote Network Monitoring), um protocolo de gerenciamento proativo de redes que funciona sobre a pilha TCP/IP, apresenta como vantagem, em comparação com o SNMP, a implementação de criptografia mediante o algoritmo DES (Data Encryption Standard) e a autenticação utilizando-se MD5 ou SHA (Secure Hash Algorithm).

5. O protocolo de gerenciamento de rede NetFlow pode ser utilizado pelo administrador de rede para monitorar a banda, o que permitirá descobrir o IP e a porta de camada de transporte que estão sendo utilizados.

A respeito dos sistemas de gerenciamento de redes, julgue os próximos itens.

3. SNMP (Simple Network Management Protocol), versão 3, é um protocolo de gerência de redes da camada de aplicação que usa as portas 161 e 162 do UDP para transmitir as informações. Caso ocorra uma incidência na rede, a operação Write é utilizada por um agente para a comunicação ao gerente sobre o evento.

4. O padrão RMON (Remote Network Monitoring), um protocolo de gerenciamento proativo de redes que funciona sobre a pilha TCP/IP, apresenta como vantagem, em comparação com o SNMP, a implementação de criptografia mediante o algoritmo DES (Data Encryption Standard) e a autenticação utilizando-se MD5 ou SHA (Secure Hash Algorithm).

5. O protocolo de gerenciamento de rede NetFlow pode ser utilizado pelo administrador de rede para monitorar a banda, o que permitirá descobrir o IP e a porta de camada de transporte que estão sendo utilizados.

6. No contexto das plataformas abertas e fechadas, em gerência de monitoramento de redes, é correto afirmar que a ferramenta

A. MRTG pode monitorar qualquer coisa a partir do fornecimento de dados pelo host, por meio dos diversos protocolos de rede.

B. Nagios pode monitorar a carga do processador e uso de disco, como também efetuar monitoração remota suportada por meio de túneis criptografados SSH ou SSL.

C. Sniffer é implementada exclusivamente por software para interceptar e registrar o tráfego de dados em uma rede de computadores.

D. MRTG monitora apenas tráfego de rede.

E. Nagios não suporta monitoração remota por meio de túneis criptografados.

6. No contexto das plataformas abertas e fechadas, em gerência de monitoramento de redes, é correto afirmar que a ferramenta

A. MRTG pode monitorar qualquer coisa a partir do fornecimento de dados pelo host, por meio dos diversos protocolos de rede.

B. Nagios pode monitorar a carga do processador e uso de disco, como também efetuar monitoração remota suportada por meio de túneis criptografados SSH ou SSL.

C. Sniffer é implementada exclusivamente por software para interceptar e registrar o tráfego de dados em uma rede de computadores.

D. MRTG monitora apenas tráfego de rede.

E. Nagios não suporta monitoração remota por meio de túneis criptografados.

7. No ambiente de gerenciamento Internet, a RMON - Remote Network Monitoring é composta por nove grupos, entre os quais, "um que classifica as informações obtidas por outro grupo, gerando, por exemplo, os nodos que mais transmitiram pacotes" e outro que "mantém informações das interfaces do agente, por exemplo, o número de colisões".

Esses dois grupos denominam-se, respectivamente,

A. History e Host.

B. History e Capture.

C. HostTopN e Statistics.

D. Statistics e Event.

E. Event e Host.

7. No ambiente de gerenciamento Internet, a RMON - Remote Network Monitoring é composta por nove grupos, entre os quais, "um que classifica as informações obtidas por outro grupo, gerando, por exemplo, os nodos que mais transmitiram pacotes" e outro que "mantém informações das interfaces do agente, por exemplo, o número de colisões".

Esses dois grupos denominam-se, respectivamente,

A. History e Host.

B. History e Capture.

C. HostTopN e Statistics.

D. Statistics e Event.

E. Event e Host.

Acerca de software livre, especialmente quanto a ferramentas para monitoramento e diagnóstico de ambientes computacionais, julgue os itens subsequentes.

8. A ferramenta de monitoramento de rede Cacti recolhe e exibe informações sobre o estado de uma rede de computadores, especificamente sobre o estado de elementos de rede e da largura de banda utilizada. Todavia, ela não monitora informações sobre o uso de CPU e disco dos elementos.

9. O MRTG é um pacote escrito em PERL que somente realiza o monitoramento dos equipamentos que têm suporte ao protocolo SNMP.

10. A ferramenta Nagios permite o monitoramento remoto de rede suportado por meio de túneis criptografados SSH ou SSL.

Acerca de software livre, especialmente quanto a ferramentas para monitoramento e diagnóstico de ambientes computacionais, julgue os itens subsequentes.

8. A ferramenta de monitoramento de rede Cacti recolhe e exibe informações sobre o estado de uma rede de computadores, especificamente sobre o estado de elementos de rede e da largura de banda utilizada. Todavia, ela não monitora informações sobre o uso de CPU e disco dos elementos.

9. O MRTG é um pacote escrito em PERL que somente realiza o monitoramento dos equipamentos que têm suporte ao protocolo SNMP.

10. A ferramenta Nagios permite o monitoramento remoto de rede suportado por meio de túneis criptografados SSH ou SSL.

11. Com relação ao Monitoramento e Gerenciamento de Redes de Comunicação de Dados é correto afirmar:

A. No SNMP, grande parte da capacidade de processamento de armazenamento de dados reside no sistema gerenciado, restando para o sistema de gerenciamento um subconjunto complementar dessas funções.

B. RMON tem como objetivo definir padrões de monitoração e interfaces para a comunicação entre agentes e gerentes SNMP, o que lhe confere a capacidade de gerenciamento remoto do SNMP.

C. SNMPv2 é a versão que se propõe a solucionar problemas de segurança do SNMP, tais como autenticação, criptografia e controle de acesso.

11. Com relação ao Monitoramento e Gerenciamento de Redes de Comunicação de Dados é correto afirmar:

D. Em termos de gerenciamento de redes, tanto o SNMP quanto o CMIP são protocolos não orientados à conexão e executados sobre a pilha de protocolos OSI.

E. No RMON1 opera no nível da camada de rede e camadas superiores, coletando informações estatísticas e monitorando o tráfego gerado por diferentes tipos de aplicação.

11. Com relação ao Monitoramento e Gerenciamento de Redes de Comunicação de Dados é correto afirmar:

A. No SNMP, grande parte da capacidade de processamento de armazenamento de dados reside no sistema gerenciado, restando para o sistema de gerenciamento um subconjunto complementar dessas funções.

B. RMON tem como objetivo definir padrões de monitoração e interfaces para a comunicação entre agentes e gerentes SNMP, o que lhe confere a capacidade de gerenciamento remoto do SNMP.

C. SNMPv2 é a versão que se propõe a solucionar problemas de segurança do SNMP, tais como autenticação, criptografia e controle de acesso.

GABARITO

1. E
2. C
3. E
4. E
5. C
6. B
7. C
8. E
9. C
10. C
11. B