

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

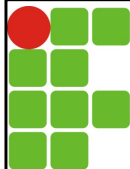


Gerência de Redes

Turma : 20171.5.01405.1V

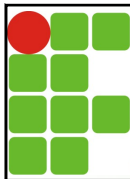
SNMPv1

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>



Agenda

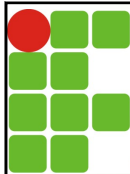
- Introdução
- Agentes
 - Comunidades
- Protocolo
 - Comunicação
 - Operações
 - Mensagens



Introdução

- O SNMP é considerado o "coração" do sistema de gerenciamento
 - SNMPv1 foi definido na RFC 1157 (05/1990)
 - <https://www.ietf.org/rfc/rfc1157.txt>
- A arquitetura do SNMP é composta por 4 elementos principais:
 - Estação de Gerenciamento (**Gerente**)
 - Agente de Gerenciamento (**Agente**)
 - Base de Informações Gerenciadas (**MIB**)
 - Protocolo de Gerenciamento (o **SNMP** em si)

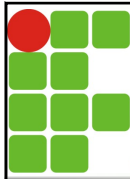
3



Introdução

- Agente de Gerenciamento (**Agente**)
 - **Comunidades**
- Protocolo de Gerenciamento (o **SNMP** em si)
 - **Comunicação, Operações e Mensagens**
- Estação de Gerenciamento (**Gerente**)
- Base de Informações Gerenciadas (**MIB**)

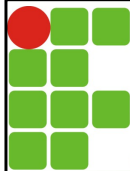
4



Introdução

- Principais **deficiências do SNMPv1**
 - Não é apropriado para o gerenciamento de redes grandes (polling performance)
 - Autenticação fraca
 - Modelo MIB limitado
 - Não suporta comunicação gerente-gerente

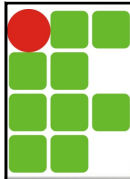
5



Agente – Comunidades

- O agente é responsável por controlar sua própria MIB local
 - É ele que define como se darão as leituras e alterações das informações contidas na mesma
 - Minimamente dois aspectos de segurança devem ser levados em conta:
 - **Autenticação**: o agente pode desejar limitar o acesso à MIB
 - **Política de Acesso**: o agente pode conceder diferentes privilégios de acesso aos gerentes

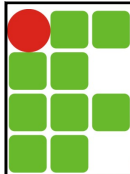
6



Agente – Comunidades

- O SNMPv1 possui uma **funcionalidade (primitiva e limitada) para fornecimento das necessidades de segurança** conceitualmente nomeada de **"comunidade SNMP"**
 - Uma comunidade **permite o relacionamento entre um agente e um ou mais gerentes**
 - Cada comunidade **deve possuir um nome único** de conhecimento do gerente

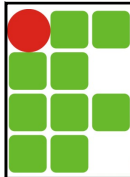
7



Agente – Comunidades

- **Autenticação**
 - **O mecanismo de autenticação do SNMP é trivial**
 - **Cada operação realizada por um gerente inclui o nome da comunidade**
 - Essa comunidade **funciona como uma senha**. Ela deve ser conhecida pelo gerente para que o mesmo possa **"acessar"** as informações do agente
 - Administradores devem possuir um cuidado especial na definição dos nomes das comunidades
 - Por padrão, os equipamentos usam **"public"** e **"private"**

8

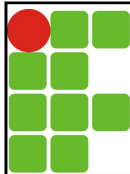


Agente – Comunidades

■ Política de Acesso

- Cada comunidade pode prover diferentes tipos de acesso à MIB em termos de:
 - **Visualização da MIB:** cada comunidade pode permitir a visualização de toda MIB ou de apenas uma sub-árvore da mesma
 - **Modo de Acesso:** cada comunidade pode permitir leitura e alteração (**read-write**), apenas leitura (**read-only**) ou envio de alertas (**trap**)
- A combinação da "Visualização da MIB" e do "Modo de Acesso" é conhecido como **SNMP community profile**
- Ainda é possível **restringir qual IP pode "acessar" uma determinada comunidade**

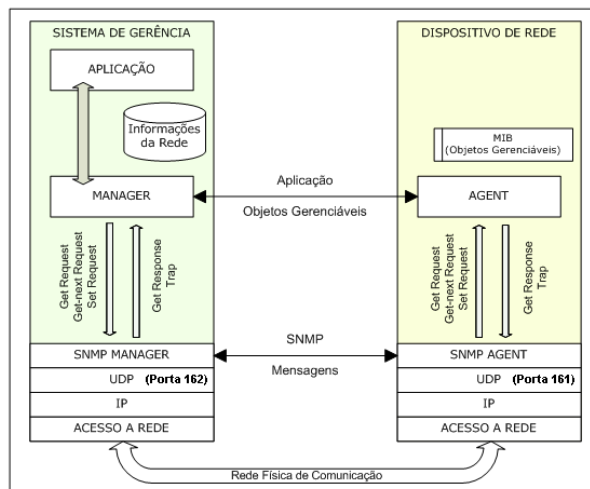
9

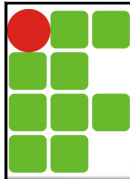


SNMP – Comunicação

■ Utiliza **UDP**

- Agente escuta na porta **161**
- Gerente escuta na porta **162** (TRAPS)

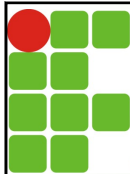




SNMP – Operações

- O SNMPv1 dá suporte a um conjunto de operações extremamente simples
 - Basicamente, permite somente ler ou alterar valores de objetos de uma MIB
- As operações são:
 - **GET** : Gerente lê o valor de **um** objeto da MIB de um agente
 - **SET** : Gerente altera o valor de **um** objeto na MIB de um agente
 - **TRAP** : Agente envia o valor de **um** objeto da MIB, mesmo que não solicitado, para um gerente

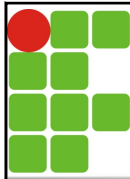
11



SNMP – Operações

- Operações **não** suportadas pelo protocolo SNMPv1
 - Alterar a estrutura da MIB de um agente
 - Adicionar ou remover objetos da MIB de um agente
 - Acessar uma tabela ou conjunto de objetos em uma única operação
 - ...
- A arquitetura extremamente simples do SNMP **simplifica bastante a sua implementação** (principalmente nos agentes)
 - Em contrapartida limita seu conjunto de funcionalidades

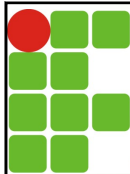
12



SNMP – Mensagens

- Cada mensagem do SNMP possui:
 - A **versão do protocolo**
 - O **nome da comunidade**
 - **Campos adicionais específicos de cada mensagem**
- Mensagens disponíveis no SNMPv1
 - GetRequest
 - GetNextRequest
 - GetResponse
 - SetRequest
 - Trap

13



SNMP – Mensagens

- Formato das mensagens SNMP

SNMP Message

Version	Community	SNMP PDU				
---------	-----------	----------	--	--	--	--

GetRequest, GetNextRequest PDU and SetRequest PDU

PDU type	Request id	0	0	Variablebindings		
----------	------------	---	---	------------------	--	--

GetResponse PDU

PDU type	Request id	error-status	error-index	Variablebindings		
----------	------------	--------------	-------------	------------------	--	--

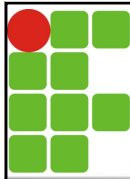
Trap PDU

PDU type	Enterprise	Agent-addr	Generic-Trap	Specific-trap	Time-stamp	Variablebindings
----------	------------	------------	--------------	---------------	------------	------------------

Variablebindings

name1	value1	name2	value2	...	name n	value n
-------	--------	-------	--------	-----	--------	---------

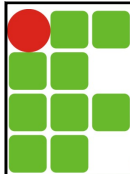
14



SNMP – Mensagens

- Campos das mensagens SNMP
 - **Version**: versão do protocolo SNMP
 - **Community**: nome da comunidade SNMP
 - **PDU type**: indicada qual tipo de mensagem está sendo transmitida
 - 0 (GetRequest), 1 (GetNextRequest), 2 (GetResponse), 3 (SetRequest), 4 (Trap)
 - **Request ID**: código utilizado para distinguir as diversas requisições enviadas pelos gerentes e casar com as respectivas respostas

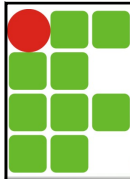
15



SNMP – Mensagens

- Campos das mensagens SNMP
 - **error-status**: usado para indicar uma exceção ocorrida no processamento da requisição
 - 0 (noError), 1 (tooBig), 2 (noSuchName), 3 (badValue), 4 (readOnly), 5 (genErr)
 - **error-index**: caso error-status seja diferente de 0, pode prover informações adicionais indicando qual objeto da lista causou a exceção
 - **Variablebindings**: lista de nomes de objetos e seus respectivos valores (nas requisições são nulos)

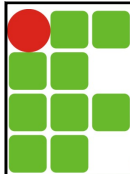
16



SNMP – Mensagens

- Variable Bindings (vinculação de variáveis)
 - Todas as mensagens SNMP possuem este campo
 - Contém um conjunto de referências à objetos junto com seus valores (nulos nas requisições)
 - Torna possível agrupar um conjunto de operações do mesmo tipo (get, set ou trap) em uma única mensagem SNMP
 - Uma requisição do valor de vários objetos
 - Uma resposta contendo todos os valores
 - Reduz substancialmente o volume de tráfego na rede

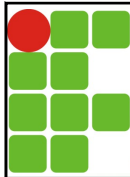
17



SNMP – Mensagens

- Campos das mensagens SNMP
 - **Enterprise**: tipo do agente que gerou o Trap (baseado no *sysObjectID*)
 - **Agent-addr**: endereço IP do agente que enviou o Trap
 - **Generic-trap**: tipos predefinidos (genéricos) de Trap
 - 0 (coldStart), 1 (warmStart), 2 (linkDown), 3 (linkUp), 4 (authenticationFailure), 5 (egpNeighborLoss), 6 (enterpriseSpecific)
 - **Specific-trap**: código mais específico do Trap (de acordo com o equipamento)
 - **Time-stamp**: contém o valor de sysUpTime do momento de geração do Trap

18



SNMP – Mensagens

■ GetRequest

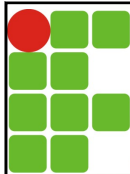
■ Enviada por um **gerente** para um **agente**

- O **request-id** deve possuir um valor que identifique unicamente a requisição
 - Possibilita também a detecção de PDUs duplicadas
- A lista de objetos requisitados deve estar presente no campo **variablebindings**

■ O agente responde a um GetRequest com um GetResponse com o mesmo request-id

- A **operação é atômica**: ou todos os valores dos objetos solicitados são retornados, ou nenhum deles

19



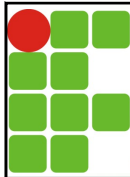
SNMP – Mensagens

■ GetRequest

■ Situações que podem gerar erros:

- Um objeto solicitado no campo **variablebindings** não existe na MIB do agente
 - Mensagem **GetReponse** terá campo **error-status = noSuchName**; e **error-index** indicará a posição do objeto no campo **variablebindings**
- Tamanho da mensagem **getResponse** muito grande
 - Mensagem **GetResponse** terá campo **error-status = tooBig**

20

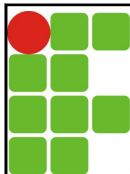


SNMP – Mensagens

■ GetNextRequest

- Permite recuperar um grupo de objetos-valores
- É praticamente idêntica a **GetRequest**
 - Formato, troca de mensagem, condições de erro, ...
- A única, e importante, diferença é que:
 - Na mensagem **GetRequest**, cada item existente no campo **variablebindings**, refere-se a **um objeto** cujo valor deve ser retornado pelo agente
 - Na mensagem **GetNextRequest**, para cada item existente no campo **variablebindings**, o agente deve retornar o valor do **próximo objeto** existente na árvore que representa sua MIB

21

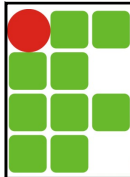


SNMP – Mensagens

■ GetNextRequest

- Esta diferença, aparentemente pequena, possui grandes implicações:
 - Possibilita ao gerente "**descobrir**" a estrutura da MIB de um agente
 - Provê um mecanismo eficiente para **percorrer tabelas** cujo tamanho ou formato não é conhecido
- Os algoritmos de descobrimento e percorrimento utilizam-se da forma numérica em que os OIDs são organizados
 - Eles vão incrementando o OID até receberem uma mensagem de erro

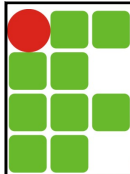
22



SNMP – Mensagens

- **GetResponse**
 - Enviado do **agente** para o **gerente**
 - Utilizado como resposta aos comandos **GetRequest**, **GetNextRequest** e **SetRequest**
 - Nas operações **Get** retorna os dados requisitados
 - Nas operações **Set** retorna se a modificação foi efetuada
 - Na execução do comando **GetNextRequest** é utilizado para indicar que existem mais variáveis a serem lidas

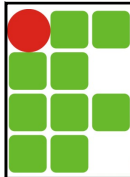
23



SNMP – Mensagens

- **SetRequest**
 - Enviada por um **gerente** para um **agente**
 - Possui o mesmo formato das mensagens **GetRequest** e **GetNextRequest**
 - É utilizada para **modificar o valor** de uma série de objetos gerenciados
 - Os identificadores e valores desses objetos estarão listados no campo **variablebindings**
 - Um agente responde ao **SetRequest** com uma mensagem **GetResponse** contendo o mesmo **request-id**
 - Somente objetos definidos na MIB como **read-write** ou **write-only** podem ser utilizados nesse comando

24

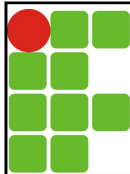


SNMP – Mensagens

■ SetRequest

- Como no **GetRequest**, a **operação é atômica**
- Se o agente alterou o valor de todos os objetos solicitados em **variablebindings**, ele irá responder com um **GetResponse** contendo estes valores
- Se o valor de algum objeto não pode ser alterado, então, nenhum valor é retornado em **variablebindings** nem alterado no agente
 - Códigos de erro (**error-status** e **error-index**) apropriados serão utilizados nestas respostas (**noSuchName**, **tooBig**, **badValue**, ...)

25

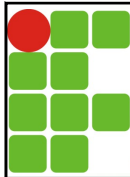


SNMP – Mensagens

■ Trap

- Enviada por um **agente** para um **gerente**
- Normalmente é configurado no agente o destino do Trap como o IP do gerente
- Em geral as Traps estão vinculadas a algum objeto da MIB que será utilizado para passar informações com a Trap
- Provê ao gerente **notificações assíncronas** de eventos significantes, dos seguintes tipos genéricos:
 - **ColdStart(0)**: Agente reinicializou devido a uma falha
 - **WarmStart(1)**: Agente reinicializou

26

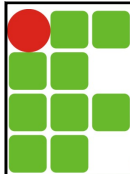


SNMP – Mensagens

■ Trap

- Provê ao gerente **notificações assíncronas** de eventos significantes, dos seguintes tipos genéricos:
 - **LinkDown(2)**: Informa a falha em algum link identificado no campo **variablebindings**
 - **LinkUp(3)**: Informa o retorno do funcionamento de algum link identificado no campo **variablebindings**
 - **AuthenticationFailure(4)**: Indica o recebimento de alguma mensagem que falhou na autenticação
 - **EgpNeighborLoss(5)**: Indica a queda de um peer do protocolo EGP
 - **EnterpriseSpecific(6)**: Utilizado para a notificação de eventos específicos. O campo **specific-trap** indicará o tipo de **Trap**

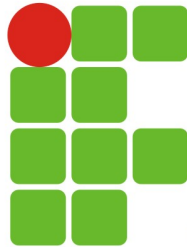
27



Referências

- MAURO, Douglas R., SHCMIDT, Kevin J. – **SNMP Essencial**. 1ª Ed., Editora Campus, 2001.
- KUROSE, J. F. e ROSS, K. - **Redes de Computadores e a Internet** - 5a Ed., Pearson, 2010.
- NETWORK WORKING GROUP. – **RFC 1157 (May 1990)**. disponível em: <https://www.ietf.org/rfc/rfc1157.txt>

28



**INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE**



Gerência de Redes

Turma : 20171.5.01405.1V

SNMPv1

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>