

Cap. 02 – Modelo de Informação

2.1 – Padrões de Gerência de Redes

2.2 – Arquitetura da Solução SNMP

2.3 – Objetos, Instâncias e MIBs

2.4 – MIB-2

2.5 – Structure of Management Information (SMI v1)

2.6 – SMI V2

Referências Bibliográficas

- Jacques F. Sauvé - “Gerência de Redes de Computadores”, DSC, UFCG, 2002. Notas de Aula, ”<http://www.dsc.ufcg.edu.br/~jacques>”
- Alexandre Sztajnberg - “Conceitos Básicos sobre SNMP e CMIP”, COPPE-UFRJ, 1996, Relatório Técnico.
<http://www.gta.ufrj.br/alexsz/>
- James F. Kurose; Keith W. Ross - “Redes de Computadores e a Internet”, Addison-Wesley, 3a Edição, ISBN-10: 8588639181 ou ISBN-13: 9788588639188

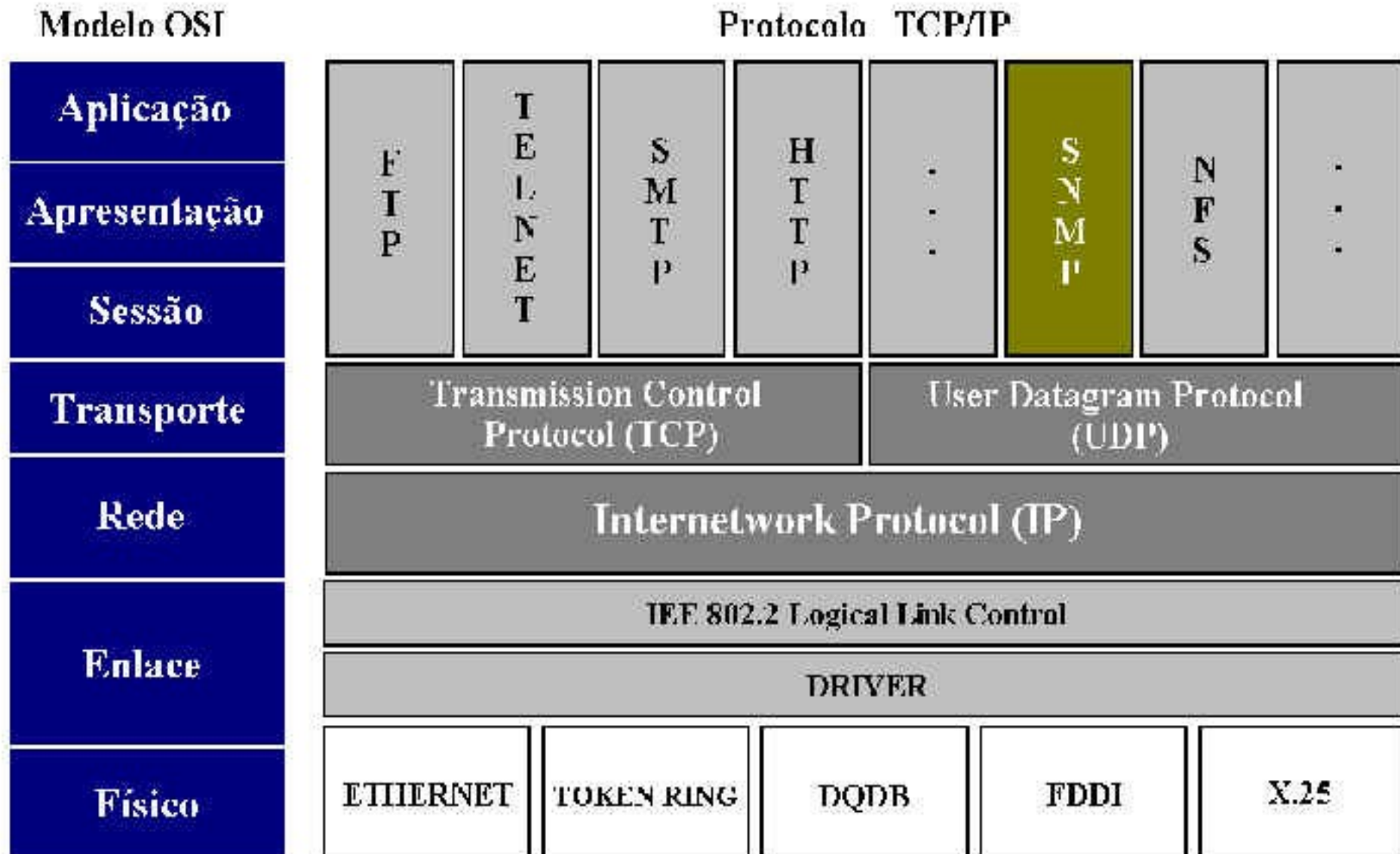
2.2 – Arquitetura da Solução SNMP

- Utiliza o Modelo “Fetch-Store” de variáveis de gerência mantida nos agentes de gerenciamento;
 - simples mas eficiente;
 - Ações especiais são efeitos colaterais de operações “store”, p.ex., “link up”, “link down”, etc.
- 03 versões SNMP v1, SNMP v2 e SNMPv3;

... 2.2 – Arquitetura da Solução SNMP

- SNMP v1 – primitivas básicas:
 - GET – obter o valor de uma variável;
 - GET-NEXT – permite caminhar nas variáveis;
 - para caminhar em tabelas de tamanho desconhecido;
 - quando não se sabe que variáveis são suportadas pelo agente.
 - SET – alterar o valor de uma variável
 - TRAP – informar eventos extraordinários do agente para o gerente;

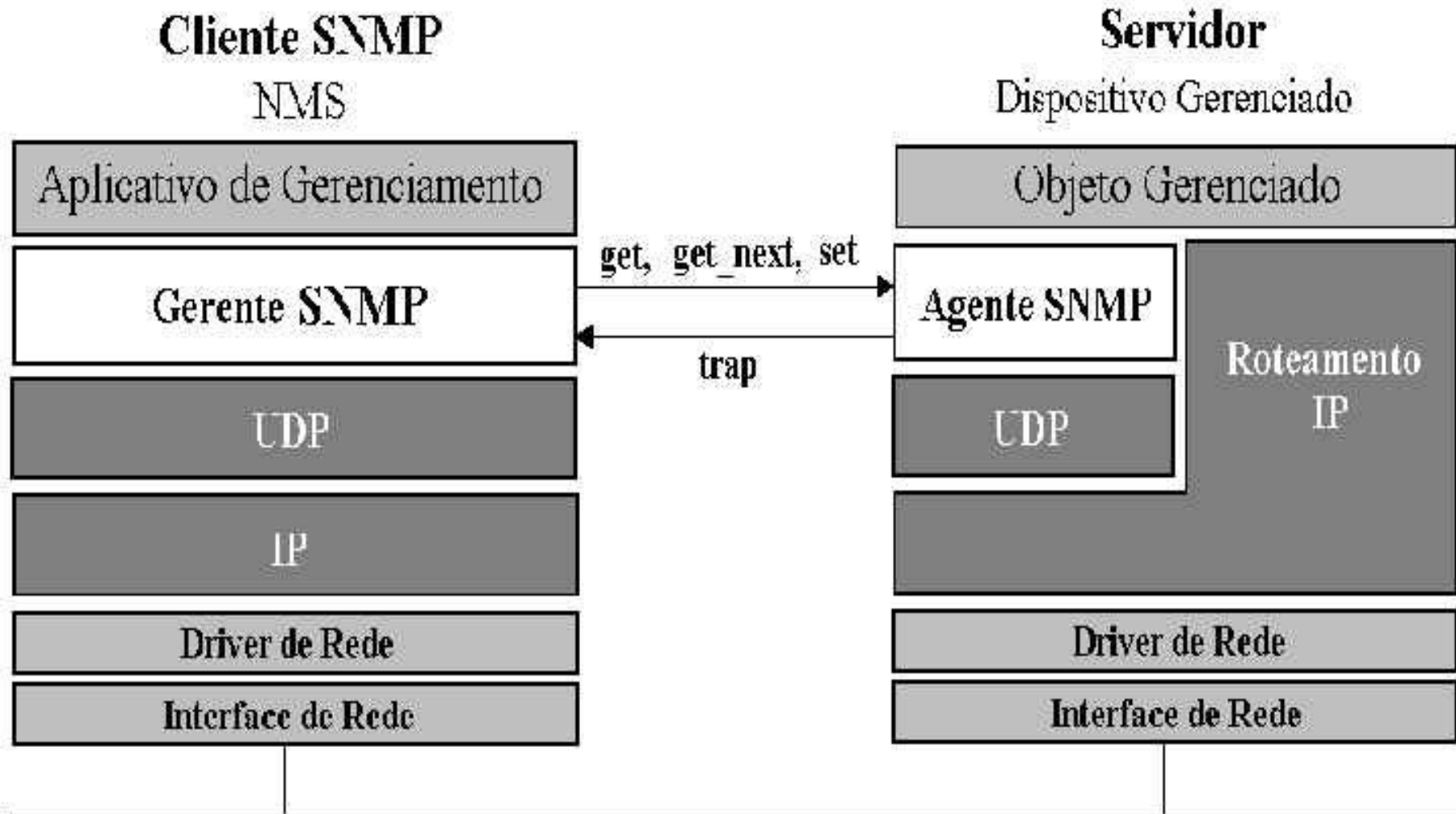
... 2.2 – Arquitetura da Solução SNMP



... 2.2 – Arquitetura da Solução SNMP

- Modelo: “*Trap-Directed Polling*” ou “*Trap-Based Polling*”
 - software de gerência de redes **não** segue o modelo **cliente-servidor** convencional pois para as operações:
 - GET e SET a estação de gerenciamento se comporta como cliente e o dispositivo de rede a ser analisado como servidor;
 - TRAP ocorre o oposto, pois no envio de alarmes é o dispositivo gerenciado que toma iniciativa da comunicação;
 - Assim, os sistemas de gerência evitam os termos “cliente-servidor” e optam por "gerente" para a aplicação na estação de gerenciamento e "agente" para a aplicação que roda no dispositivo de rede.

... 2.2 – Arquitetura da Solução SNMP



... 2.2 – Arquitetura da Solução SNMP

- SNMP “Communities”:
 - “community” no SNMP são grupos de dispositivos e estações de gerenciamento que rodam SNMP;
 - “community name” é utilizado para identificar um grupo e auxilia na definição para onde as informações são enviadas;
 - ... um dispositivo ou agente pode pertencer a mais de uma comunidade SNMP, no entanto, o mesmo não responderá por requisições de estações de gerenciamento que não pertençam ao menos a uma de suas comunidades:
 - 02 são as comunidades padrões:
 - Write = private ou Read = public

... 2.2 – Arquitetura da Solução SNMP

- Segurança no SNMP: ... na Internet pode ser alcançada através de um “firewall”, enquanto que na Comunidade SNMP há uma “trap” que oferece algum nível de segurança.
 - Send Authentication Trap – quando um dispositivo recebe uma autenticação que falha, uma “trap” é enviada para a estação de gerenciamento.
- Outros parâmetros de configuração que afetam a segurança:
 - Accepted Community Names – somente requisições de computadores na lista das “community names”;
 - Accept SNMP Packets from Any Host – padrão, embora a configuração em “hosts” específicos aumente a segurança;
 - Only Accept SNMP Packets from These Hosts – somente requisições de “hosts” da lista de endereços IP é aceita (p.ex., IP, IPX, “host name”).

... 2.2 – Arquitetura da Solução SNMP

- Segurança SNMP
 - razão para gerência incompleta de Redes SNMP:
 - SET é pouco usado para controlar dispositivos nos “hosts”;
 - Fabricantes (muitos) não implementam a função SET.
- Agente pode implementar várias comunidades:
 - cada comunidade dá acesso a uma “MIB View” definida localmente;
 - cada comunidade pode ter certos direitos de acesso (definidos localmente)
 - READ COMMUNITY
 - WRITE COMMUNITY