# Resolução

Nome: Rui Filipe Chaves Alunos nº: PG47637

1. **Explique como é que o facto de o SNMP ser um protocolo não confirmado pode influir na implementação dos gestores e dos agentes no modelo INMF.**

   R: O facto de o SNMP ser um protocolo não confirmado, tal como assincrono e assimetrico, significa que, tirando um única primitiva em que é necessário obter uma confirmação, tudo o resto não requere uma resposta a uma mensagem SNMP. Assim, o manager não sabe se os pedidos/respostas foram de facto recebidos pelo agentes e vice-versa.
   No que toca à implementação em si do SNMP nos dispositivos de rede, o facto de não ser confirmado, neste contexto pela IETF, implica que as implementações do protocolo possam variar entre fornecedores/fabricantes e versões do mesmo. Esta falta de conformidade faz com que a interoperabilidade entre dispositivos fique comprometida e influencie a implementação segundo o modelo INMF. Esta incompatibilidade, em certos casos, pode impossibilitar a troca de mensagens compreensíveis por ambos os intervenientes, levando possivelmente a erros na gestão e perda de informação.

2. **Já deve ter lido muitas vezes que “o modelo INMF está muito difundido, não só para gestão de equipamentos de rede, mas também para gestão de muitos outros tipos de equipamentos e sistemas distribuídos, ainda que a sua implementação possa apresentar desafios nalguns contextos aplicacionais particulares.” Nesse sentido, discuta o eventual uso do SNMP como protocolo de gestão e controlo de sistemas veiculares individuais, ou seja, na gestão e controlo dos sistemas de sensores e atuadores (sistemas de travagem, iluminação, controlo de velocidade, estacionamento automático, verificação de componentes mecânicos, etc.) que integram os veículos automóveis modernos, incluindo veículosautomóveis não tripulados.**
   R: Várias características do SNMP poderiam ser consideradas limitações no contexto da implementação do mesmo em redes veículares. Assumindo que a implementação deste protocolo está associado apenas à implementação num

veículo individual e não num contexto de gestão de vários, temos que ter considerações no que toca a segurança, rapidez da comunicação, entre outros. O facto, por exemplo, de ser um protocolo relativamente simples é uma vantagem. O facto de, geralmente, os objetos de mais alto nível serem implementados do lado do gestor é outra vantagem no sentido em que os sensores são dispositivos relativamente pequenos e com um objetivo bastante específico sem o poder de computação necessário para a implementação de um protocolo que não fosse simples e que não distribui-se o trabalho para uma entidade com mais recursos como o gestor. O facto de os veículos, principalmente os não tripulados, ter um conjunto elevado de sensores de controlo, poderia levar de certa forma a um *bottleneck* no gestor incapacitando-o de gerir esta grande quantidade de informação, problema geral da centralização da gestão. O facto de os pedidos serem feitos pelos gestores e sem haver confirmação de receção por ambas as partes (aparte de certas mensagens), implica que, assumindo um tipo de comunicação contínua e proativa (não requerendo um pedido por parte do gestor), característica dos sensores, possa vir a ser imcompatível com a especificação do protocolo (ou ocorra uma abundância de mensagens trap/notification por parte dos sensores/agentes). A comunicação é maioritariamente feita por UDP, o que pode simplificar a comunicação com os diversos sensores em si mas acarreta um problema de segurança e fiabilidade desnecessário num ambiente que é controlado e confinado, como um carro. O protocolo seria ideal para o caso da verificação de componentes mecânicos por isto acontecer em situações específicas e o gestor saber previamente todos os pedidos/testes que tem que realizar para saber o estado dos diversos componentes do veículo, podendo levar o seu tempo para fazer um teste completo (assumindo um contexto de não urgência que está associado a um veículo parado), mas podendo-se suportar no histórico de mensagens trap, por exemplo. A organização hierárquica das MIBs associado à implementação do SNMP é vantajogo por permitir aceder remotamente a informações e uma organização hierárquica entre dispositivos mas, por vezes, o facto de ser um protocolo muito centralizado também não é ideal.

3. **Porque é que acha que a segunda versão da arquitetura INMF/SNMP continua a ser mais usada que a terceira versão?**
   R: Isto poderá se dever ao facto de o SNMPv3 ser uma versão mais recente e mais focada na segurança e incompatível com anteriores implementações do SNMP. Na versão 3 foi feita uma revisão completa da especificação pelo que a

incompatibilidade (ou uma limitação da mesma na troca de mensagens) com versões anteriores limitou de certa forma a interoperabilidade com gestores que não foram ‘atualizados’. A atualização para a versão 3 implicava uma alteração significativa nos dispositivos e na infraestrutura. Esta é na minha opinião, a questão mais importante. A implementação da versão 3 implicava um foco na segurança e frequentemente esta é desconsiderada, ou em certos contextos de gestão simples, desnecessária, sendo valorizada a rapides. As falhas de segurança estavam muito associadas à fase de configuração e instalação (ao configurar um router por exemplo) pelo que após esta fase as questões de segurança não eram tão relevantes. A versão 3 foi apresentada apenas em 1999, um tempo considerável após a introdução das versões anteriores, pelo que isto pode ter tornado a adoção mais complicada, pretendendo-se, claro, a compatibilidade com versões anteriores.

4. **Para que servem as normas Management Base Information (MIB) da arquitetura INMF? Quais as vantagens e desvantagens da sua utilização no contexto da gestão de aplicações multimédia distribuídas?**
   R: As MIBs são boas abstrações do que é possível fazer com um determinado hardware e há um conjunto de regras a cumprir de forma a garantir a normalização das mesmas, de forma a torná-las em boas bases de dados de gestão. Sendo as MIBs uma abstração e tendo um objeto comum subjacente, a principal vantagem será a sua garantia de interoperabilidade entre diferentes equipamentos e sistemas, desde que haja à priori um bom padrão e uma MIB bem construída, apenas sendo necessário traduzir devidamente a instrução na máquina que se pretende gerir, e ajudando na reutilização e simplificando a configuração de dispositivos semelhantes. Outra vantagem associada às MIBs é a sua característica de organização hierárquica, análoga ao DNS. Tudo isto representam vantagens no contexto de aplicações multimédia distribuídas, pelo facto de estas serem possíveis devido à existência de uma rede enorme muito distribuida geográficamente, muitas vezes recorrendo até a redes CDN havendo assim uma heterogeneidade muito grande e grande quantidades de equipamentos e sendo necessário uma coordenação entre estes muito bem definida, padronizada, hierárquica e simples de replicar e monitorizar. Recorrendo às MIBs temos isto tudo, sendo possível aos gestores monitorizarem remotamente as informações dos equipamentos garantindo eficiência e obtendo dados de monitorização e desempenho, essenciais para o descobrimento de falhas tanto a nível da rede como dos equipamentos.
   As MIBs, no entanto, são objetos algo complexos e que necessitam de uma boa

adaptação à maquina em si, no sentido em que disponibilizar e traduzir uma primeira vez todas os recursos pode ser demoroso, tanto na implementação como na testagem. Outra desvantagem associada é a falta de segurança oferecida pelas MIBs para este contexto de necessidade de garantias de resiliência e controlo de acesso, podendo as mensagens de gestão da rede estarem vulneráveis a ataques dependendo apenas na segurança da infraestrutura e acesso aos dispositivos em si.