

**DEFINIÇÕES E RESPOSTAS AS SUGESTÕES APRESENTADAS PELO REPRESENTANTE DA ACTAR, VIA E-MAIL, DATADO DE 21/03/2011, RELATIVAS À CONSULTA PÚBLICA, REALIZADA NO DIA 16/03/2010, VISANDO DISCUSSÃO DAS ESPECIFICAÇÕES TÉCNICAS PARA O SWITCH CORE A SER ADQUIRIDO, MEDIANTE CONTRATO.**

**SUGESTÃO 1:**      **Item 2.16** – Implementar Vlan por porta e Vlan por MAC. [Juniper] Solicitar a remoção deste item.

**RESPOSTA:**      A redação do item será ajustada, para que seja exigida, no mínimo, a criação de VLAN por portas, que atende às necessidades da SEF.

**SUGESTÃO 2:**      **item 2.17** – Implementar 802.1v : Classificação por protocolo e porta. [Juniper] Solicitar a remoção deste item.

**RESPOSTA:**      O item será excluído, uma vez que o protocolo 802.1Q já incorpora as funcionalidades do IEEE 802.1v.

**SUGESTÃO 3:**      **item 2.19** – Implementar 802.1ad. [Juniper] Solicitar a remoção deste item ou a troca por 802.3ad (LACP).

**RESPOSTA:**      O item será excluído.

**SUGESTÃO 4:**      **item- 2.31** – Somente RFC 4760 (Multiprotocol extension). [Juniper] EX Suporta Multiprotocol extension for BGPv4 nas RFC's 2283, 2545 e 2858. Solicitar alteração deste item.

**RESPOSTA:**      O Item será alterado para exigir que o BGPv4 seja implementado de acordo com as seguintes RFCs: RFC 4760 ou RFC 2283 e RFC 2858 Multiprotocol Extensions for BGP4.

**SUGESTÃO 5:-**      **item 2.39** – Implementar IS-IS para as seguintes RFCs.[Juniper] RFC 1195 ok (suportado). EX suporta Dynamic hostname exchange mechanism for IS-IS na RFC 5301. Solicitar alteração deste item. EX suporta Domain-wide prefix distribution with two-level IS-IS na RFC 5302. Solicitar alteração deste item.

**RESPOSTA:**      O item será alterado para exigir que sejam implementadas as seguintes RFCs: RFC 2763 ou RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS RFC 2966 ou RFC 5302 Domain-wide Prefix Distribution with Two-Level IS-IS

**SUGESTÃO 6:**      **item 4.7** – Implementar atualização de imagem de software e configurações através de servidor TFTP. [Juniper] Solicitar alteração deste item para implementação mencionada seja realizada através de um servidor FTP ou serviço FTP.

**RESPOSTA:**      Será ampliado para TFTP ou FTP ou SCP.

**SUGESTÃO 7:**      **item 4.10** – Implementar Port mirroring, permitindo espalhar até 16 portas ou Vlans. [Juniper] Solicitar alteração para 7 grupos de análise.

**REPOSTA:**      Será alterada a especificação prevendo *port mirroring* para até 7 *mirrorings* (grupos de análise).

**SUGESTÃO 8:-** **item 4.12** – Implementar gerenciamento através de SNMPv1, v2c e v3 RFC (1157), (1901,1908) e (3410 e 3415). [Juniper] Item ok (suportado). Algumas destas RFC foram substituídas pro RFC mais recentes:  
\* RFC 1157: SNMPv1  
• RFC 1905, RFC 1907: SNMP v2c, SMIv2 and Revised MIB-II  
• RFC 2570–2575: SNMPv3, user-based security, encryption, and authentication  
• RFC 2576: Coexistence between SNMP Version 1, Version 2, and Version 3  
• RFC 1212, RFC 1213, RFC 1215: MIB-II, Ethernet-like MIB and traps  
• RFC 2578: SNMP Structure of Management Information MIB  
• RFC 2579: SNMP Textual Conventions for SMIv2

**RESPOSTA:** A redação do item será alterada de modo a abranger as RFCs alternativas, da seguinte maneira: Implementar gerenciamento através de SNMPv1, v2c e v3 (RFCs 3411 a 3415 ou RFCs 2570 a 2575). Cumpre salientar que, ao exigir-se o atendimento das RFCs 3411 a 3415, estão englobadas as RFCs 3411, 3412, 3413, 3414 e 3415. Da mesma maneira, ao exigir-se o atendimento das RFCs 2570 a 2575, estão englobadas as RFCs 2570, 2571, 2572, 2573, 2574 e 2575.

**SUGESTÃO 9:** **item 4.32** – Implementar proteção e robustez contra ataques mencionados e catalogados pela CERT. [Juniper] – Parcialmente suportado através de implementação de filtros de pacotes a nível de plano de controle. Solicitar alteração deste item.

**RESPOSTA:** O item foi avaliado internamente pela STI. Será exigida declaração do licitante vencedor de que irá implementar proteção contra os ataques, o que será verificado no aceite técnico.

**SUGESTÃO 10:** **item 4.33** – Implementar limitação de números de endereço MAC's apreendidos por uma porta, para uma determinada VLAN. [Juniper] – Parcialmente suportado por porta e não por Vlan. Solicitar alteração deste item.

**RESPOSTA:** A redação do item foi alterada para: Implementar limitação de número de endereços MAC apreendidos por uma porta, uma vez que o mecanismo de restrição por portas atende às necessidades da SEF.

**SUGESTÃO 11:** **item 4.41** – Implementar a funcionalidade que permita a exclusão de ACL's em um determinado horário do dia (time-based ACL). [Juniper] Solicitar a remoção deste item.

**RESPOSTA:** Item removido tendo em vista que é possível implementar esse tipo funcionalidade externamente ao switch, mediante solução de *scheduling* já disponível na SEF.

**SUGESTÃO 12:** **item 4.42** – Implementar políticas por usuário, permitindo que as configurações de ACL. Qos sejam aplicadas na porta utilizada para a conexão a rede, após autenticação. [Juniper] Solicitar a remoção deste item ou reescrita conforme consulta pública.

**RESPOSTA:** O Item será removido, uma vez que já está sendo exigida implementação do protocolo IEEE 802.1x, que atende às necessidades de controle de acesso da SEF.

**SUGESTÃO 13:** **item 4.43** – [Juniper] Solicitar a remoção deste item ou reescrita conforme consulta pública.

**RESPOSTA:** O item foi avaliado internamente pela STI e a especificação será alterada a fim de exigir contadores internos que possibilitem o envio de alertas e o disparo de ações baseados em limiares a serem definidos. Será exigida declaração do licitante vencedor de que irá implementar ações baseadas em limiares a serem definidos.