MATERIAL PERMANENTE					
ITEM	ESPECIFICAÇÕES	QTD/ UND	CÓDIGO	VALOR UNIT.	VALOR GLOBAL
04	**SWITCH GERENCIAVEIS 16 PORTAS** - Possuir, no mínimo, 16 portas Ethernet 10/100/simultaneamente ativas com autosensing de velocidade e com conectores RJ-45. - Deve possuir, no mínimo, 2 portas adicionais 1000Base-X para suporte a uplinks flexíveis. Em cada um das portas deverão ser suportados transceivers (GBICs ou SFPs), que permitam a utilização dos seguintes padrões: 1000Base-SX, 1000BaseLX/LH, 1000BaseZX,1000BaseT. - Todas as portas Ethernet 10/100/ devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática. -Possibilitar a configuração de status de portas por software, permitindo a definição de portas ativas/inativas. - Implementar VLANs por porta. - Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica. - Possui porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB. - Deverá ser fornecido cabo de console compatível com a porta de console do equipamento. -Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários. **-Possuir LEDs para a indicação do status das portas em atividade.** - Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps. Implementar os seguintes modos de operação para SNMPv3: ı Sem autenticação e sem privacidade (noAuthNoPriv); ı Com autenticação e sem privacidade (authNoPriv); - Com autenticação e com privacidade (authPriv). Deve ser suportado o algoritmo criptográfico AES. - Possuir suporte a MIB II, conforme RFC 1213. - Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento. - Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa. - Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP. - Possuir armazenamento interno das mensagens de log geradas pelo equipamento. - Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas. - Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas. - Deve suportar o protocolo LLDP e as extensões LLDP-MED. - Deve suportar a associação de endereços IP e MAC em uma porta específica. - Deve suportar notificação via SNMP caso algum endereço MAC não autorizado seja recebido. - Implementar Telnet para acesso à interface de linha de comando. - Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial. - Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS. - Permitir a gravação de log externo (syslog). - Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação,voltar à operação normalmente na mesma configuração anterior à queda de alimentação. - Possuir ferramentas para depuração e gerenciamento em primeiro nível, tal como log de eventos com redirecionamento para servidor Syslog. - Permitir o espelhamento de uma porta, de um grupo de portas para outra porta localizada no mesmo switch. - Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas. - Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: - somente tráfego de entrada - somente tráfego de saída - ambos os sentidos, simultaneamente. - Implementar mecanismo de autenticação para acesso local e remoto ao equipamento baseada em um Servidor AAA (Autenticação, Autorização e Accounting). - Implementar filtragem de pacotes (ACL - Access Control List). - Proteger a interface de comando do equipamento através de senha. - Suportar protocolo SSH V2 para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES. - Permitir a criação de listas de acesso baseadas em endereço IP ou funcionalidade equivalente para limitar o acesso ao switch via Telnet. - SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH. - Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino. - Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão. - Implementar mecanismos de Autenticação, Autorização e Accounting de comandos através de protocolo AAA com as seguintes características mínimas: - todas as tentativas de execução de comandos devem ser autorizadas individualmente (e registrados) no servidor AAA. - Deve se basear em transporte TCP para que se tenha garantia de entrega - Todos os pacotes entre switch e servidor AAA devem ser cifrados - Deve haver autenticação mútua entre o switch (cliente AAA) e o servidor AAA. - Todas as formas de acesso gerencial (telnet, SSH, HTTPS, HTTP e porta física de console) devem ser controladas através da solução AAA. - Possuir a funcionalidade de detecção de looping em suas portas, desabilitando a porta na ocorrência de um looping. - Possuir a funcionalidade de detecção de looping em suas portas, desabilitando a vlan específica causadora do looping (em caso de porta com vlan trunking); l-Possui a funcionalidade de controle de tráfego broadcast (Broadcast Storm Control) podendo configurar a quantidade de pacotes broadcast por segundo permitida na rede. Deve permitir a configuração de ações como descarte dos pacotes excedentes e shutdown. Deve ser possível também controlar, por porta, o volume de tráfego multicast e "unknown unicast". - Deve possuir a funcionalidade DHCP Snooping, em que é possível filtrar os pacotes de servidores DHCP não autorizados. - Implementar padrão IEEE 802.1d (Spanning Tree Protocol). -- Implementar padrão IEEE 802.1q (Vlan Frame Tagging). - Implementar padrão IEEE 802.1p (Class of Service) para cada porta. - Implementar padrão IEEE 802.3ad. - Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP). Modelo de Referência: Equivalente ou de melhor qualidade HP 4210 MARCA: SWITCH 1920 16G (JG923A)	50 UND	183213-1	1.329,00	66.450,00