5.3.70. Deve permitir ser gerenciado através de IPv6;
5.3.71. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
5.3.72. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
5.3.73. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
5.3.74. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
5.3.75. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
5.3.76. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
5.3.77. Deverá suportar ser configurado e monitorado através de REST API;
5.3.78. Deve possuir ferramenta para captura de pacotes que auxíliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;
5.3.79. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;
5.3.80. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
5.3.81. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
5.3.82. Deve suportar temperatura de operação de até 45º Celsius;
5.3.83. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
5.3.84. Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V;
5.3.85. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
5.4. Solução de Conectividade – Tipo 4 | ITEM 4
5.4.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
5.4.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
5.4.3. Adicionalmente, deve possuir 2 (dois) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
5.4.4. Adicionalmente, deve possuir 2 (dois) slots QSFP operando em 40GbE;
5.4.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
5.4.6. Deve possuir 1 (uma) interface USB;
5.4.7. Deve possuir capacidade de comutação de pelo menos 228 Gbps e ser capaz de encaminhar até 415 Mpps (milhões de pacotes por segundo);
5.4.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
5.4.9. Deve possuir tabela MAC com suporte a 90.000 endereços;
5.4.10. Deve operar com latência igual ou inferior à 2 us (microsegundo);
5.4.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
5.4.12. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;
5.4.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
5.4.14. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;
5.4.15. Deve suportar a comutação de Jumbo Frames;
5.4.16. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
5.4.17. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
5.4.18. Deve suportar pelo menos 16k de entradas na tabela de roteamento;
5.4.19. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
5.4.20. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, IS-IS, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;
5.4.21. Deve suportar protocolos de roteamento multicast
5.4.22. Deverá suportar Equal Cost Multipath Routing (ECMP)
5.4.23. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;
5.4.24. Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;
5.4.25. Deve implementar serviço de DHCP Server e DHCP Relay;
5.4.26. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;
5.4.27. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);
5.4.28. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;
5.4.29. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;
5.4.30. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
5.4.31. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
5.4.32. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
5.4.33. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
5.4.34. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
5.4.35. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
5.4.36. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
5.4.37. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
5.4.38. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
5.4.39. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;
5.4.40. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);
5.4.41. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
5.4.42. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
5.4.43. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;
5.4.44. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
5.4.45. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
5.4.46. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
5.4.47. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
5.4.48. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
5.4.49. Deve suportar MAC Authentication Bypass (MAB);
5.4.50. Deve implementar RADIUS CoA (Change of Authorization);
5.4.51. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
5.4.52. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
5.4.53. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
5.4.54. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
5.4.55. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
5.4.56. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
5.4.57. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
5.4.58. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC