

**APÊNDICE “A”**

**REQUISITOS TÉCNICOS MÍNIMOS DA SOLUÇÃO**

# ITEM 1 - APPLIANCE PARA A SOLUÇÃO CISCO ACI

* 1. **Arquitetura de Hadware:**
     1. Deverá ser fornecido em formato appliance virtual ou físico em hardware x86 dedicado para gerenciamento, configuração e monitoramento de switches físicos ou virtuais.
     2. Deverá ter CPU, Memória, Disco e Conectividade suficientes para suportar todas as funcionalidades requeridas neste apêndice.
     3. Todos os appliances (controladoras) devem ter conectividade redundante com interfaces de no mínimo 10Gbps.
     4. Deverá suportar regime de alta disponibilidade através de clusters de gerenciamento redundantes, com no mínimo 3 appliances fisicos ou virtuais independentes.
     5. Todos os appliances físicos fornecidos deverão ter fontes e ventiladores redundantes.
     6. A controladora deverá operar de forma independente do plano de dados da rede, não podendo ser um ponto de convergência do fluxo de dados da rede do Data Center.
     7. Todas as controladoras devem ser licenciadas afim de suportar todas as funcionalidades descritas neste documento. Data Center Fabricante cluster de controladores SDN deve implementar um protocolo de Fabricante Ethernet que possua as seguintes características:
        1. A solução deverá ser capaz de configurar, visualizar e gerenciar tanto os switches físicos quanto virtuais;
        2. Em caso de perda de comunicação entre os switches e o cluster de controladoras, a rede deverá continuar a operar normalmente sem interrupção de tráfego.
     8. Deverá permitir através de interface gráfica a visualização, configuração e monitoramento do underlay (switches fisicos, adaptadores, roteamento e VTEPs) e overlay (VNIDs, encapsulamentos, segmentação e tenants).
     9. Deverá utilizar VXLAN para encapsulamento de tráfego (overlay) e também ser compatível com ambiente tradicional (VLAN-based).
     10. A solução deve suportar a criação de múltiplos tenants de forma que um tenant não se comunique com o outro.
     11. A solução deve suportar a criação de um tenant compartilhado, de modo a ser consumido por todos os outros tenants.
     12. A plataforma deverá exibir de forma nativa todas as topologias de rede criadas, seja da rede física ou virtual.
     13. A controladora deverá implementar mecanismos de Zero Touch Provisioning baseado em protocolos abertos para descoberta automática de novos elementos do Fabricante.
     14. A controladora de rede deve exibir de forma nativa estatísticas de tráfego para elaboração de relatórios de performance da rede fisica e virtual por ao menos seis meses.
     15. A solução deve permitir a visualização de todos os endpoints(VMs, Bare Metal e containers) reconhecidos pela rede, assim como permitir a divisão dos mesmos em grupo de interesse.
     16. Deve implementar mecanismos dc detecção de loops sem a necessidade de Spanning Tree Protocol.
     17. Suportar, nos switches leaf, agrupamento de interfaces de acesso, por meio de protocolo LACP, para dar conectividade aos recursos (ex: servidores, firewall, LB).
     18. Suportar funcionalidade Multi -Chassis Link Aggregation ou similar, que permite o agrupamento de interfaces de acesso, por meio de protocolo LACP, com dois switches leaf.
     19. A solução deverá permitir gateway distribuído de forma que um endpoint não fiquem dependente de um único elemento para saída e possa ser movimentado dentro da rede.
     20. A solução deve prover redundância de gateway, tanto para os dispositivos, quanto para a borda da rede, através de protocolo HSRP ou similar.
     21. Deverá permitir integração com redes externas modelo OSI através de roteamento estático e dos protocolos de roteamento OSPF para IPv4 e IPv6 e BGP para 1Pv4 e IPv6.
     22. Implementar mecanismos, para BGP, que permite a escolha de determinadas rotas baseada em informações específicas (ex: community) e que permite, também, alterálas (ex: preference, next -hop, weight).
     23. Implementar funcionalidade de filtro de rotas BGP.
     24. A solução deve implementar a visualização de todas as rotas aprendidas (internamente e externamente) via GUI e REST API.
     25. Implementar Protocol Independent Multicast (PIM) Sparse Mode, Any Source Multicast (ASM) e Source -Specified Multicast (SSM).
     26. Permitir que rotas de uma VPN MPLS externa possam ser anunciadas para uma VRF interna ao Fabricante.
     27. Permitir que rotas internas ao Fabricante possam ser anunciadas para uma VPN MPLS externa.
     28. Deverá possuir mecanismo de controle de tráfego em volume excessivo de pacotes do tipo: broadcast, unknown unicast e multicast.
     29. Deverá permitir configuração de QoS e limitação de tráfego.
     30. Deverá implementar espelhamento de tráfego para análise.
     31. A solução deve exibir alertas para monitoramento da saúde de toda a rede do Data Center. Todos os alertas devem ser classificados de acordo com a severidade, assim como determinar quais aplicações e endpoints serão afetados.
     32. Implementar monitoramento de fluxo, de forma que seja possível visualizar o caminho do pacote de um endpoint a outro.
     33. A solução deverá possuir funcionalidades troubleshooting e correção de erros de configuração de forma nativa, sem a necessidade de elementos externos.
     34. A solução deverá implementar funcionalidade de troubleshooting fim -a-fim de forma gráfica, afim de mostrar todas as falhas, drops, contadores atômicos e políticas de segurança que possam impactar o tráfego entre endpoints físicos e/ou virtuais.
     35. Deverá apresentar de forma nativa, ferramenta de capacity planning, de forma a mostrar o consumo de recursos da rede.
     36. Implementar mecanismo de autenticação para acesso local ou remoto baseada em Autenticação, Autorização e Auditoria (AAA), assim como RBAC, via servidor de autenticação do tipo RADIUS ou TACACS+.
     37. Armazenar logs relativo as alterações realizadas na rede, como usuário, data e descritivo da alteração.
     38. A controladora deve permitir a visualização de todos os elementos da rede, permitindo backup e restore de todas as configurações.
     39. Permitir mecanismos de monitoração da saúde do Fabricante fim afim, permitindo a detecção de perda ou problemas de encaminhamento de pacotes.
     40. A interface gráfica deve permitir a visualização e alteração de configurações de forma simples por diferentes equipes de trabalho, de forma que cada equipe tenha seu próprio nível de acesso.
     41. A controladora deve implementar de forma nativa ferramentas para upgrade de software de todo o Fabricante (switches fisicos, virtuais e controladora).
     42. A solução deve suportar upgrade não disruptivo, contanto que os endpoints estejam conectados de maneira redundante (dual -homed).
     43. A solução deve permitir a configuração de rede para múltiplas VLANs por porta.
     44. A solução deve suportar exportação em formato NetFlow ou equivalente.
     45. Suportar 802.ip e Differentiated Services Code Point (DSCP). Integrações cluster de controladores SDN deve implementar as seguintes integrações de forma nativa (sem necessidade de soluções externas):
         1. Servidores Bare Metal;
         2. VMWare vSphere (versão 6.0 ou superior);
         3. Microsoft SCVMM (versão 2016 ou superior);
         4. Openstack (versão Newton ou superior);
         5. RedHat Openshift (versão 3.6 ou superior);
         6. Kubernetes (versão 1.7 ou superior).
     46. Deverá integrar com os seguintes componentes, provendo um ponto único de configuração e gerenciamento para a rede física e virtual:
         1. Servidores Bare Metal;
         2. VMWare vSphere (versão 6.0 ou superior);
         3. Openstack (versão Newton ou superior);
         4. RedHat Openshift (versão 3.6 ou superior);
         5. Kubernetes (versão 1.7 ou superior).
     47. Deverá exibir inventário de elementos Bare Metal:
         1. Interfaces Físicas (pNICs);
         2. Endereços IP;
         3. MAC Address.
     48. Deverá exibir inventário de elementos do hypervisor:
         1. Interfaces Físicas (pNICs);
         2. Interfaces Virtuais (vNICs);
         3. Nome das Máquinas Virtuais;
         4. Endereços IP;
         5. MAC Address.
     49. Deverá exibir inventário de elementos do ambiente containers:
         1. Interfaces Físicas (pNICs);
         2. Endereçamento IP;
         3. Namespaces;
         4. PODs;
         5. Serviços;
         6. Status dos Serviços;
         7. Portas Utilizados por serviço;
         8. Topologias de regras de segurança e comunicação do cluster.
     50. O software da controladora deverá estar totalmente licenciado de forma a permitir a implementação e utilização de todos os módulos e interfaces, com todas as funcionalidades solicitadas neste apêndice, sem depender de integração com outros softwares fornecidos por outros Fabricanteantes e sem ônus adicional.
     51. Interconexão de Data Centers (DCI).
     52. A solução deve suportar a funcionalidade de Interconexão de Data Centers com os seguintes requisitos:
         1. A solução deverá estender o domínio L2 utilizando VXLAN;
         2. A solução deverá implementar isolamento de domínio de falha de forma nativa, no qual um problema de rede em um Data Center não seja propagado para o outro;
         3. Permitir a flexibilidade e movimentação de workloads de um site para o outro, sem necessidade de alteração na rede ou nos dispositivos;
         4. A controladora deverá implementar o gerenciamento de ambos os sites em uma única interface;
         5. A controladora deverá exibir todos os MACs aprendindos em ambos os Data Centers em uma console única;
         6. A solução deverá suportar múltiplos domínios fisicos e virtuais em ambos os sites, além de gerenciar políticas de rede e segurança de forma unificada para ambos;
         7. Esta solução deverá implementar a micro -segmentação de máquinas fisicas e virtuais de forma unificada, ou seja, todas as políticas (incluindo filtros e atributos) feitas na controladora deverão estar presentes em ambos os Data Centers.
     53. Segurança e Serviços:
         1. A solução deverá possibilitar a ativação de regras de segurança em qualquer lugar do Fabricante, independentemente do switch ou rack;
         2. A solução deverá oferecer políticas de segurança entre aplicações, segregando a rede logicamente em contextos ou tenants distintos. Esta política de segurança deve oferecer ao administrador controle de permissão de tráfego entre aplicações.
     54. Deverá implementar a micro -segmentação entre dispositivos fisicos e virtuais, em qualquer parte do Fabricanteante. Utilizando elementos:
         1. Nome do dispositivo;
         2. Nomeda VM;
         3. Sistema Operacional;
         4. IP;
         5. MAC Address;
         6. DNS.
     55. Deverá implementar segmentação de tráfego granular entre VMs, servidores Bare Metal e Containers mesmo quando no mesmo grupo de interesse, possibilitando filtros de tráfego específico.
     56. Deverá implementar uma interface única para aplicar regras de firewall e políticas de segurança (enforcement).
     57. Programabilidade e Automação.
     58. O cluster de controladoras SDN deverá possuir as seguintes funcionalidades quanto a programabilidade de todo o Fabricante:
         1. Permitir integração com ferramentas de Orquestração de Data Center, de forma nativa ou via REST APIs;
         2. A solução deverá possibilitar o consumo de APIs e módulos nativos para automação (configuração de rede e serviços de Firewall) via Ansible e Terraform.
     59. Deverá possuir SDKs nativas, com a qual toda a solução possa ser configurada de forma automatizada.
     60. Solução de rede de acesso definida por software
     61. Esse descritivo técnico é composto por uma solução completa de uma arquitetura de rede de acesso baseada em premissas de Software Defined Network. Deverá ser fornecida incluindo todos os seus componentes, como:
     62. Equipamentos de acesso;
     63. Equipamentos de Borda (Conexão a Redes Externas ao Fabricante);
     64. Equipamentos para controle do Fabricante;
     65. Controladoras do tipo appliance (software e hardware).
     66. A rede para suportar a implantação desta solução deverá se uma solução baseada em um conceito de mercado denominado de "Fabricante", desta maneira permitindo a virtualização e segmentação, automação e análise para redes cabeada e sem fio.
     67. A segmentação deve permitir a aplicação de políticas de acesso com base em contexto do usuário ou grupo de usuários independente de qual equipamento dentro do Fabricante estiver provendo o acesso a esse usuário. A virtualização de rede deve reduzir drasticamente as etapas de implementação provendo automação e programabilidade alinhadas com funcionalidades de segurança integradas, capacidade de operação de rede simplificada através de algoritmo avançado que além de extrair as informações, prove sugestões de melhorias e resolução de problemas de maneira proativa e preditiva.
     68. Fabricante deve implementar a comunicação entre os dispositivos com topologia arbitrária, permitindo a utilização de redes virtualizadas através de rede fisica baseada em camada 3. A solução de rede sugerida baseia-se no conceito de Software Defined Network, contendo como premissas:
     69. Os planos de dados e de controle são desacoplados, de forma que os equipamentos de rede tenham a função de apenas encaminhar pacotes.
     70. Permitir a definição de premissas ou critérios de funcionamento para todos os seus elementos de forma programável e sem necessariamente intervenção de um operador.
     71. Decisões de encaminhamento baseado em fluxos (sequência de pacotes entre origem e destino) e não apenas endereços destino. Todo fluxo deve possuir a mesma política de encaminhamento nos dispositivos.
     72. Dada as premissas de um Fabricante SDN, a solução deverá ser construída em duas camadas definidas abaixo:
         1. REDE UNDERLAY: Camada onde se encontra toda a infraestrutura física, switches de rede, adaptadores, conectores, cabos, roteamento e túneis, permitindo conexões de Layer 2 ou Layer 3, em um mesmo site ou sites distintos;
         2. REDE OVERLAY: Camada que utiliza o controlador ou conjunto de controladoras para criação de redes virtuais, abstração e automação de toda a rede, sempre utilizando protocolos padronizados, não será aceita solução com protocolos proprietários.
     73. Componentes da solução:
         1. Gerenciamento: Projeta, provisiona, habilita políticas e garante serviços de rede, por meio do gerenciamento centralizado. Permitir a visibilidade dos serviços de rede end -to -end para ambientes de Campus e filiais tanto para rede cabeada com sem fio;
         2. Automação: Automatizar totalmente a infraestrutura de rede com base em uma política única para toda rede de acesso. Simplifica e dimensione as operações, automatizando a configuração, o provisionamento e a solução de problemas do dia-a-dia;
         3. Análises: Prevê proativamente problemas de desempenho, através da coleta e correlação de informações de dados de usuários, dispositivos e aplicações;
         4. Segurança: Detecte e mitigue ameaças com segmentação de rede de ponta a ponta e aplique políticas de segurança em toda a rede. Identifique e mitigue ameaças e vulnerabilidades no tráfego criptografado com análise de rede.

# ITEM 2 - APPLIANCE PARA A SOLUÇÃO CISCO DNA CENTER

* 1. **Hardware:**
     1. Deverá ser fornecido em formato appliance virtual ou físico em hardware x86 dedicado para gerenciamento, configuração e monitoramento de switches fisicos ou virtuais.
     2. Deverá ter CPU, memória, disco e conectividade suficientes para suportar todas as funcionalidades requeridas neste apêndice.
     3. Todos os appliances (controladoras) devem ter conectividade redundante com interfaces de no mínimo 10Gbps.
     4. Deverá suportar regime de alta disponibilidade através de clusters de gerenciamento redundantes, com no mínimo 3 appliances fisicos.
     5. Todos os appliances fornecidos deverão ter fontes e ventiladores redundantes.
     6. A controladora deverá operar de forma independente do plano de dados da rede, não podendo ser um ponto de convergência do fluxo de dados da rede do Data Center.
     7. Todas as controladoras devem ser licenciadas afim de suportar todas as funcionalidades descritas neste documento.
  2. **Funcionalidades:**
     1. Permitir a descoberta de dispositivos na rede e automaticamente inclui-los na lista de dispositivos descobertos, deverá para otimização de descoberta, permitir filtros com sub -net de rede, endereço IP especifico e intervalo de endereços IP;
     2. Deverá possuir inventario dos dispositivos da rede, com no mínimo as seguintes informações:
        1. Nome do Dispositivo;
        2. Endereço IF;
        3. Status do Dispositivo (Conectado, Conectado e habilitado para receber;
        4. comandos, Conectado e não autenticado e não conectado);
        5. Endereço MAC;
        6. Versão de Software;
        7. Número Serial;
        8. Modelo do dispositivo (Part-number);
        9. Tempo que o dispositivo está ativo e operacional;
        10. Configuração do dispositivo, com exeção de Pontos de Acesso e Controladoras;
        11. WiFi.
  3. **Função do dispositivo na rede:**
     + 1. Desconhecida;
       2. Acesso;
       3. Core;
       4. Distribuição;
       5. Dispositivo para conexão da Rede Fabricante com as demais redes do cliente.
  4. **Localização Geográfica do dispositivo;**
     1. Status da última coleta de informações:
        1. Gerenciado - Dispositivo está totalmente gerenciado;
        2. Falha na coleta total das informações - Algumas informações não foram coletadas do dispositivo, deverá ser possível verificar quais informações não foram coletadas;
        3. Inacessível - Dispositivo não esta conectado e nenhuma informação foi coletada;
        4. Credenciais erradas - As credencias para acesso ao dispositivo foram alteradas após este ter sido adicionado;
        5. Em processo - Processo de coleta de informações já iniciado, mas ainda não finalizado.
     2. Deverá permitir atualização do sistema operacional dos dispositivos gerenciados, com no mínimo as seguintes funcionalidades:
        1. Armazenar em sua base de dados todas as imagens dos sistemas operacionais dos dispositivos gerenciados pela solução;
        2. Permitir atualização dos sistemas operacionais de dispositivos gerenciados;
        3. Permitir a definição de uma versão como sendo a mais adequada para uma família de produtos, e desta maneira simplificar a atualização dos dispositivas para a versão mais indicada.
     3. Deverá possuir mapa da topologia da rede com no mínimo as seguintes funcionalidades:
        1. Elaborar mapa da topologia da rede, automaticamente e baseado nas informações das regras definidas durante o processo de descoberta dos dispositivos ou através da atualização das informações dos dispositivos no inventario;
        2. Permitir a visualização da topologia selecionando esta visualização por Área, Site, Prédio ou andar;
        3. Permitir a visualização detalhada das informações dos dispositivos apresentados nos mapas;
        4. Permitir a visualização das informações dos links.
     4. Permitir a filtragem de dispositivos a serem visualizados pelas seguintes opções:
        1. Layer 2 (VLAN);
        2. Layer 3 (ISS, OSPF ou Rotas Estáticas);
        3. Dispositivos que suportam a capacidade de VFR;
        4. Permitir salvar as alterações efetuadas no layout da topologia;
        5. Permitir exportar uma visão completa da topologia para arquivo externo no formato PNG (Portable Network Graphics).
     5. Deverá possuir funcionalidade para graficamente projetar uma nova infraestrutura de rede hierárquica com no mínimo as seguintes características:
        1. Topologia fisica da rede;
        2. Parâmetros da Rede;
        3. Características dos Dispositivo;
        4. Localização geográfica;
        5. Sites;
        6. Áreas;
        7. Andares.
     6. Escalabilidade mínima:
        1. Total de mínimo 1.000 diapositivos, incluindo switchs, roteadores e controladoras wifi;
        2. Total de no mínimo 500 dispositivos no Fabricante;
        3. Total de no mínimo 4.000 pontos de acesso WiFi;
        4. Total de no mínimo 25.000 clientes (Wireless e cabeados);
        5. Total de no mínimo 10 Fabricantes independentes.
     7. Escalabilidade por Fabricante:
        1. Total de no mínimo 500 dispositivos;
        2. Total de no mínimo 15.000 clientes (Wireless e cabeados);
        3. Automação;
        4. Fabricante SDN.
     8. Permitir total automação dos processos de configuração tanto da Rede
     9. UNDERLAY com da Rede OVERLAY;
     10. Possuir integração com a plataformas de Controle de Acesso à Rede, e assim efetuar todas as configurações que sejam necessárias para implementação das políticas estabelecidas para acesso dos clientes aos recursos da Rede (Cabeda ou sem fio) a partir das definições estabelecidas nesta plataforma;
     11. Permitir a total automação de processo de configuração dos serviços de WiFi.
     12. Não Fabricante SDN:
         1. Permitir total automação dos processos de configuração dos dispositivos gerenciados pela plataforma;
     13. Análises:
     14. Deverá fornecer intuitivamente maneiras para solução de problemas relacionados a rede, aos clientes e as aplicações. Deverá possuir base de conhecimento interna e coletar dados da rede para isto.
     15. Deverá possuir no mínimo as seguintes funcionalidades:
     16. Apresentar através de cores representativas e diferenciadas o resumo da situação rede, com no mínimo os seguintes status:
         1. Problemas Críticos;
         2. Problemas que necessitam serem verificados;
         3. Nenhum problema;
         4. Não existem informações coletadas;
         5. Aprsentar a lista dos 10 maiores problemas;
         6. Permitir selecionar visibilidade por sites, lista ou através da topologia da rede;
         7. Permitir definir a visibilidade referente as ultimas 3 horas, ultimas 24 horas e últimos 7 dias.
     17. Visibilidade de Dispositivos e Clientes:
         1. Percentual histórico de cada dispositivo de usuário;
         2. Identificação proativa de qualquer problema que afete a experiência dos clientes;
         3. Gráfico que represente a situação da saúde de conectividade (Data Plane e Control Plane) dos dispositivos;
         4. Informações referentes a experiência do usuários no uso das aplicações;
         5. Permitir definir a visibilidade referente as ultimas 3 horas, ultimas 24 horas e últimos 7 dias;
     18. Permitir retornar ao momento que um problema tenha ocorrido na rede e conseguir verificas no mínimo as seguintes informações:
         1. Histórico dos eventos críticos ocorridos no período do problema;
         2. Todas as alterações ocorridas nos dispositivos dos clientes ou da rede no período do problema;
         3. Possuir base de conhecimento interna capaz de indicar rapidamente ações para remediar problemas e detalhar qual o seu impacto no serviço;
         4. Possibilitar agendamento de testes através de sensores definindo que aplicações e que tipo de teste será executado;
         5. Possibilitar que os dispositivos gerenciados enviem informações de telemetria diretamente a esta plataforma, sem a necessidade de coleta;
         6. Deve possibilitar a visualização do caminho feito por um pacote de dados TCP ou UDP entre dois dispositivos conectados à rede em uma visão de topologia, obtendo dados estatístico de performance dos elementos de rede no caminho, bem como identificando qualquer lista de controle de acesso (ACL) que bloqueie ou afete o fluxo de dados.
  5. **Segurança e Políticas:**
     1. Deverá possuir integração com a plataformas de Controle de Acesso à Rede, para garantir que a políticas de segurança e virtualização seja e assim efetuar todas as configurações que sejam necessárias para implementação da virtualização dos recursos das políticas para acesso dos clientes aos recursos da Rede (Cabeda ou sem fio).
     2. Deverá possuir no mínimo as seguintes funcionalidades:
        1. Deve permitir a criação e aplicação de políticas de controle de acesso à rede baseada em IP;
        2. Deve permitir a criação e aplicação de políticas de controle de acesso à rede baseada em grupos de usuários;
        3. Deve permitir a criação e aplicação de políticas de cópia de tráfego, com base em interfaces de origem e destino de um fluxo de dados e definição da interface que receberá a cópia do tráfego;
        4. Deve ser capaz de traduzir as políticas em configurações necessárias e aplicá-las automaticamente em diferentes tipos de equipamentos;
        5. Deve permitir a criação de redes virtuais para segmentação de rede;
        6. Deve permitir criar através de uma interface gráfica políticas de micro segmentação dentro das redes virtuais;
        7. A criação das redes virtuais deve disparar a configuração automática de SSIDs e VRFs;
        8. Deve permitir a criação e aplicação de políticas de aplicações, configurando QoS na rede;
        9. Deve permitir o bloqueio de tráfego em toda a rede de acordo com relatórios de ameaças detectadas em análise de tráfego criptografado.

# ITEM 3 - SWITCH LEAF DE 40/100 GBPS

* 1. Os switches Tipo Leaf devem ser totalmente compatíveis com a atual topologia Spine/Leaf do datacenter da ANTT orquestrada pelo Cisco ACI.
  2. Não deverá haver Stacking entre os switches, garantindo encaminhamento line -rate.
  3. Deverá ser ofertado um modelo de switch específico para a rede de Data Center, conforme classificação do Fabricanteante, com características e capacidade de Software Defined Network.
  4. Possuir fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
  5. As fontes deverão permitir a sua conexão a circuitos elétricos distintos possuindo alimentação independente.
  6. Possuir ventiladores redundantes.
  7. Deverá suportar OpenFlow ou similar.
  8. Deverá possuir no mínimo 36 portas 1/10/25/40/50//100 Gbps atendendo ao padrão Ethernet QSFP28 sem bloqueio (line-rate), totalmente licenciadas.
  9. A mudança de velocidade das portas deverá ser feita de forma automática, de acordo com o transceiver instalado, e não por grupo de portas.
  10. Implementar, em hardware, o protocolo VXLAN, conforme padronizado na RFC 7348, permitindo a criação e a extensão de segmentos de redes virtuais através da camada de redes;
  11. Implementar funcionalidade Route Reflector para BGP.
  12. Deverá implementar Equal -Cost Multi Path (ECMP) para os múltiplos links de conexão entre os switches.
  13. Deverá possuir buffer de no mínimo 40MB.
  14. Possuir no mínimo 24GB de memória RAM.
  15. Suportar no mínimo 128GB para armazenamento (memória Flash ou SSD).
  16. Deverá possuir capacidade de comutação de no mínimo 7,2 (sete virgula dois) Tbps.
  17. Latência máxima não superior a 1 (um) microssegundos para comutação de pacotes de 64 bytes.
  18. Deverá possuir capacidade mínima de encaminhamento de 2,4 bpps (dois virgula quatro bilhões de pacotes por segundo).
  19. Possuir porta de gerenciamento Ethernet 10/100/1000BASE-T.
  20. Possuir ao menos uma porta 10G SFP+ para gerenciamento.
  21. Possuir no mínimo 1 (uma) porta USB permitindo upgrade de firmware através dessa porta;
  22. Deverá suportar MACSEC em line -rate, para segurança link a link.
  23. O switch deverá ser um equipamento homologado pela Agência Nacional de Telecomunicações (ANATEL).
  24. Deverá oferecer suporte a FPGA ou EPLD para upgrade de software.
  25. Deve implementar os protocolos de gerência de rede SNMPv2c e SNMPv3 gerando traps para servidor externo.
  26. Deve possuir capacidade para pelo menos 256.000 endereços MAC.
  27. Deve implementar pelo menos 3000 vlans.
  28. Suportar Jumbo frames de no mínimo 9018 Bytes.
  29. Deverá suportar, pelo menos, 800.000 (oitocentas mil) rotas IPV4 na tabela de roteamento.
  30. Deverá suportar, pelo menos,400.000 (quatrocentas mil) rotas IPV6 na tabela de roteamento.
  31. Deverá suportar, pelo menos, 2.000 Listas de Controle de Acesso.
  32. Deverá permitir autenticação para acesso local ou remoto ao equipamento usando base de usuários e permissões em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.
  33. Deve implementar protocolo de roteamento dinâmico OSPF conforme padronizado pelas RFCs 2328, 3101 ou 1587.
  34. Deve implementar protocolo de roteamento BGPv4 conforme padronizado pelas RFCs 4271, 1997 e 2385.
  35. Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol) ou similar.
  36. Deve implementar Policy-Based Routing (PBR).
  37. Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.
  38. Deve implementar roteamento multicast PIM-SM e PIM-SSM para IPV4.
  39. Deve implementar o protocolo IGMP nas versões v1 e v2.
  40. Deve implementar o mecanismo IGMP Snooping nas versões v1 e v2.
  41. Suporte aos mecanismos de QoS WRR ou WRED ou similar.
  42. Deve implementar o protocolo de roteamento OSPF for IPv6.
  43. Deve implementar o protocolo de roteamento BGP4 for IPv6.
  44. Deve suportar mecanismo de Dual Stack para uso de IPv4 e IPv6.
  45. Implementar protocolo BGP-EVPN conforme padronizado pela RFC 7432 ou atualizada.
  46. Deve possuir planos de dados e de controle processados de forma separada.
  47. Deve permitir configuração via Python, Ansible ou similar.

# ITEM 4 - SWITCH DE AGREGAÇÃO

* 1. Deve ser totalmente compatível com a atual solução de gerenciamento, automação e orquestração Cisco DNA Center, componente da rede daANTT. Essa compatibilidade dever permitir que o equipamento seja gerenciado e controlado pela solução citada.
  2. Deverá atuar na função de switch de Controle da Rede Fabric, Concentração dos Equipamentos de Acesso e Equipamentos de Borda (Conexão a Redes Externas ao Fabric):
     1. Deverá possuir a funcionalidade de agregação em um StackWise.
     2. Interfaces:
        1. Deve possuir, no mínimo, 24 (vinte e quatro) portas 1/10/25 Gigabit;
        2. Ethernet (SFP/SFP+/SFP28) sem bloqueio (non-blocking);
        3. Deve possuir, no mínimo, 4 (quatro) portas 40/100 Gigabit Ethernet (QSFP+/QSFP28) sem bloqueio (non-blocking);
        4. Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
        5. Deve possuir no mínimo 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management).
     3. Dimensões:
        1. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;
        2. Deve possuir no máximo 1 Rack Unit (RU).
     4. Visualização:
        1. Possuir LEDs para a indicação do status das portas;
        2. Possuir LEDs do tipo blue beacon para identificação do switch afim de facilitar sua a manutenção.
     5. Capacidade e Desempenho:
        1. Possuir matriz de comutação com capacidade de, pelo menos, 2 Tbps (Terabits por segundo);
        2. Possuir capacidade de processamento de, pelo menos, 1 Bpps (bilhões de pacotes por segundo);
        3. Possuir capacidade de, no mínimo, 82.000 endereços MAC;
        4. Suporte a Jumbo Frames de, no mínimo, 9198 bytes em todas as suas portas;
        5. Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.
     6. Fontes de Alimentação:
        1. Possuir fontes de alimentação redundantes simétricas internas ao equipamento, sendo que cada fonte deverá possuir potência suficiente para manter o equipamento em pleno funcionamento em sua capacidade máxima, ou seja, com todas as portas ocupadas;
        2. Possuir fontes de alimentação que operem de 90V a 260V com frequência de 50Hz a 60Hz;
        3. Os cabos de energia deverão ser fornecidos no padrão brasileiro (NBR 14.136);
        4. As fontes e as unidades de ventilação devem ser capazes de serem trocadas com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).
     7. Alta Disponibilidade:
        1. Suportar Non-Stop Forwarding e Stateful Switchover (NSF/SSO);
        2. Suportar upgrade de software em serviço (In Service Software Upgrade - ISSU).
     8. Deve prover total redundância com outros equipamentos da mesma marca e modelo, devendo atender uma das seguintes formas de alta disponibilidade:
     9. Formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente. Esta funcionalidade pode ser provida através de:
        1. Tecnologias de Stacking (físico ou virtual), garantindo que a pilha continue a funcionar na eventual falha de um dispositivo, sendo a pilha gerenciada como uma entidade única;
        2. Tecnologias do tipo Multi-LAG (Multi Link Aggregation) permitindo a redundância de link?s entre switches distintos;
        3. Em caso de empilhamento ou Multi-LAG, deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e/ou cabos/transceivers para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;
        4. Cada switch deve ser fornecido com fontes e ventiladores redundantes e hot-swappable;
        5. Possuir fontes de alimentação redundantes que operem no modo N+1 ou N+N de forma a garantir o pleno funcionamento do equipamento conforme configuração solicitada, em caso de falha de pelo menos uma das fontes de alimentação.
     10. Funcionalidades de Camada 2:
         1. Implementar até 4.000 VLAN IDs simultâneas conforme definições do padrão IEEE 802.1Q;
         2. Deve suportar VLANs dinâmicas. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;
         3. Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados;
         4. Deve implementar Private VLANs;
         5. Implementar a funcionalidade de "Link Aggregation" (LAGs) conforme padrão IEEE 802.3ad, com no mínimo 16 (dezesseis) portas por (sendo 8 ativas e 8 em standby);
         6. Deve implementar o padrão IEEE 802.1d ("Spanning Tree Protocol"), IEEE 802.1s ("Multiple Spanning Tree") e IEEE 802.1w ("Rapid Spanning Tree");
         7. Deve implementar no mínimo 64 (sessenta e quatro) múltiplas Instâncias de Spanning Tree;
         8. Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente de camada 2;
         9. 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;
         10. Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP), permitindo a descoberta dos elementos de rede vizinhos;
         11. Deve suportar exportação de fluxos (IPFIX ou Netflow) para análise do tráfego da rede;
         12. Deverá ter contadores de entrada e saída de pacotes por porta;
         13. Deverá suportar NTP.
     11. Funcionalidades de Camada 3:
         1. Possuir roteamento nível 3 entre VLANs;
         2. Suportar roteamento de pacotes IPv4 e IPv6;
         3. Suporte a, pelo menos, 64.000 (sessenta e quatro mil) rotas IPv4 dinâmicas;
         4. Suporte a, pelo menos, 32.000 (trinta e duas mil) rotas IPv6 dinâmicas;
         5. Implementar roteamento estático e dinâmico;
         6. Implementar protocolo de roteamento dinâmico OSPF v2 e v3;
         7. Implementar protocolo de roteamento dinâmico BGPv4;
         8. Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;
         9. Implementar o protocolo IGMP v2, v3;
         10. Implementar o protocolo VRRP (Virtual Router Redundancy Protocol);
         11. Implementar roteamento multicast PIM (Protocol Independent Multicast) em modo "sparse-mode", PIMv2 e PIM-SSM (Source- Specific Multicast);
         12. Implementar Policy Based Routing;
     12. Segurança:
         1. Implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4, IPv6 MAC e portas de origem e destino;
         2. Suportar autenticação via RADIUS e TACACS+;
         3. Suporte para identificar e mitigar ameaças e vulnerabilidades em tráfego criptografado;
         4. Possuir suporte a protocolo de autenticação para controle do acesso administrativo ao equipamento;
         5. Deverá permitir criação de ACL para VLANs (VACL?s);
         6. Deverá permitir criação de ACL para acesso de terminais (VTY) para TELNET e SSH;
         7. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
         8. Implementar filtragem de pacotes (ACL - Access Control List), com definições de parâmetros camada 2, 3 e 4;
         9. Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;
         10. Proteger a interface de comando do equipamento através de senha;
         11. Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
         12. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
         13. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
         14. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
         15. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.
         16. Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
         17. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
         18. Deve suportar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.
     13. Facilidades:
         1. Implementar Telnet e SSH para acesso à interface de linha de comando;
         2. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet;
         3. Ser configurável e gerenciável via GUI (graphical user interface ), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
         4. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;
         5. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);
         6. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
         7. Permitir que a sua configuração seja feita através de terminal assíncrono;
         8. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch;
         9. 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;
         10. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;
         11. 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 e ambos simultaneamente;
         12. Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento;
         13. Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas;
         14. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;
         15. Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas ("promíscuas"), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas ("promíscuas") de uma dada VLAN;
         16. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;
     14. Deverá suportar funcionalidade que permita responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
         1. ICMP echo;
         2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);
         3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);
         4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente;
         5. Suportar facilidades de programabilidade através de NETCONF/YANG;
         6. Suportar scripts de configuração em Python.
     15. Qualidade de Serviço (QoS):
         1. Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;
         2. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);
         3. Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
         4. Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force);
         5. Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing";
         6. Deve ser possível a especificação de banda por classe de serviço.
     16. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como:
         1. Transmissão do pacote sem modificação;
         2. Transmissão com remarcação do valor de DSCP.
     17. Descarte do pacote.
     18. Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP - Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa;
     19. Suportar diferenciação de QoS por VLAN;
     20. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);
     21. Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop);
     22. Implementar pelo menos oito filas por porta de saída (egress port).
     23. Gerenciamento:
     24. Gerenciável via SSHv2;
     25. Deve ser gerenciável via SNMP (v1, v2 e v3);
     26. Implementar o protocolo Syslog para funções de "logging" de eventos;
     27. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
     28. Possuir suporte a MIB II;
     29. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
     30. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
     31. Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
     32. Implementar nativamente 2 grupos RMON (Alarms e Events);
     33. Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;
     34. Suporte a IPv6 (Telnet, FTP, SNMP, SSH, NTP);
     35. Licença de Switch de Distribuição, para a solução de gerenciamento;
     36. Deve permitir atualização de software de forma automatizada;
     37. Deve ser possível verificar a versão de software e indicar atualização;
     38. Deve permitir que o equipamento seja orquestrado pelo Cisco DNA Center através de fabric;
     39. Deve suportar micro segmentação entre dispositivos conectados através dos switches de rede;
     40. Deve suportar a implementação do protocolo IPsec;
     41. Deve permitir visibilidade e controle de aplicativos por meio do reconhecimento de aplicativos baseado em rede de última geração;
     42. Deve permitir atribuir políticas a aplicativos com base na prioridade de QoS.

# ITEM 5 - SWITCH DE ACESSO 48 PORTAS

* 1. Deve suportar a inserção de módulo com, no mínimo, 4 portas 1/10 Gigabit;
  2. Ethernet padrão SFP e SFP+ para conexão de uplink;
  3. Possuir, no mínimo, 48 portas 1Gigabit Ethernet UTP;
  4. Todas as portas Ethernet; 10/100/1000 RJ-45 devem suportar negociação automática de velocidade e de modo de operação Half-Duplex e Full-Duplex);
  5. Deve disponibilizar simultaneamente, no mínimo, 15W por porta para alimentação através de POE de dispositivos clientes; caso seja necessário pode-se ofertar fonte interna redundante para atender ao requisito;
  6. Deve implementar funcionamento de porta, no mínimo, para os dispositivos cliente que suportem cada uma das seguintes combinações de parâmetros:
     1. 1000 Mbps e Full-Duplex;
     2. 100 Mbps e Full-Duplex;
     3. 100 Mbps e Half-Duplex;
     4. 10 Mbps e Full-Duplex;
     5. 10 Mbps e Half-Duplex;
  7. Para os uplinks suporte aos transeivers 10GBASE-X conforme opções:
     1. 10GBase-SR;
     2. 10GBase-ER.
  8. Todas as 48 portas devem operar simultaneamente em conjunto com as 4 portas de uplink.
  9. Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP;
  10. Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
  11. Implementar VLANs compatíveis com o padrão IEEE 802.1q.
  12. Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.
  13. Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá opcionalmente ser fornecida porta de console com interface USB.
  14. Possuir porta Ethernet 10/100 Base-T dedicada para gerenciamento out-of-band Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.
  15. Suportar fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz). No caso de funcionamento com duas fontes, estas deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
  16. Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch.
  17. No caso de funcionamento com duas fontes redundantes, deve suportar balanceamento de carga entre as mesmas. As fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte.
  18. Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade da troca do switch.
  19. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
  20. Possuir LEDs para a indicação do status das portas e atividade, além de duplex.
  21. Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275);
  22. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
  23. Sem autenticação e sem privacidade (noAuthNoPriv);
  24. Com autenticação e sem privacidade (authNoPriv);
  25. Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES 256-bit;
  26. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
  27. Possuir armazenamento interno das mensagens de log geradas pelo equipamento.
  28. Deve armazenar pelo menos as 500 últimas mensagens Possuir capacidade de exportar as mensangens de log geradas pelo equipamento Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps.
  29. Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events)
  30. Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED.
  31. Estar totalmente integrado em todas as suas funcionalidades com sistema de gerenciamento a ser ofertado, para o sistema proposto neste apêndice. Não serão aceitos equipamentos que recusem qualquer acesso e/ou não suporte a um recurso disponibilizado pelo “Sistema de Gerenciamento de Rede” proposto neste apêndice;
  32. Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX,
  33. NetStream ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.
  34. Deve implementar NETCONF (RFC 6241) e YANG;
  35. Implementar Telnet para acesso à interface de linha de comando.
  36. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
  37. Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
  38. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol).
  39. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
  40. Permitir que a sua configuração seja feita através de terminal assíncrono.
  41. 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.
  42. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
  43. 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 e ambos simultaneamente.
  44. Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.
  45. Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
  46. O espelhamento não pode interferir no funcionamento normal do equipamento.
  47. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
  48. Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
  49. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deverão ser suportadas no mínimo as seguintes operações de teste:
      1. ICMP echo;
      2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
      3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
  50. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
  51. Implementar o protocolo NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4. Deve ser suportada autenticação entre os peers.
  52. Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.
  53. Implementar roteamento estático.
  54. Implementar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453).
  55. Implementar protocolo de roteamento OSPF.
  56. Implementar o roteamento nível 3 entre VLANs.
  57. Implementar o protocolo VRRP (RFC 2338) ou HSRP de redundância de gateway.
  58. Implementar roteamento baseado em origem, com possíbilidade de definição do próximo salto camada 3, baseado em uma condição de origem.
  59. Implementar roteamento estático para IPv6.
  60. Implementar roteamento dinâmico RIPng para IPv6.
  61. Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação.
  62. Implementar , no mínimo, 4000 vlans s.
  63. Implementar, no mínimo, 1000 interfaces vlans simultaneamente, para roteamento nível 3 entre as vlans configuradas.
  64. Possuir capacidade de comutação de, no mínimo, 170 Gbps (Gigabits por segundo)
  65. Possuir uma taxa de encaminhamento de no mínimo 130 de Mpps (Milhões de pacotes por segundo;
  66. Deve possuir desempenho wirespeed e non-blocking;
  67. Deve possuir, no mínimo, 2 (dois) GBytes de DRAM/SDRAM;
  68. Deve possuir, no mínimo, 1 (um) GByte de memória flash;
  69. Deve possuir, no mínimo, 4 (quatro) MBytes de buffer;
  70. Suportar Jumbo frames de no mínimo 9198 Bytes.
  71. Possuir porta dedicada de empilhamento com capacidade de 160 Gbps (Gigapits por segundo). Este valor deve ser adicional a capacidade de comutação do switch. Deve ser fornecido um cabo de empilhamento por switch.
  72. Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 8 switches.
  73. Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.
  74. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.
  75. Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
  76. Proteger a interface de comando do equipamento através de senha.
  77. Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
  78. Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
  79. Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
  80. Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
  81. 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.
  82. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
  83. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
  84. Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elemento da rede, independente do método de gerenciamento.
  85. Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
  86. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
  87. Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo.
  88. Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
  89. Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.
  90. Deve suportar padrão IEEE 802.1AE para autenticação e encriptação de dados entre switches através de MACsec utilizando AES 128-bit. Essa funcionalidade pode ser ativada em todas as interfaces de rede;
  91. Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
  92. Implementar padrão IEEE 802.1q (Vlan Frame Tagging);
  93. Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
  94. Implementar padrão IEEE 802.3ad;
  95. Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
  96. Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);
  97. Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree, sem limite de quantidade de VLANs associada a cada instância;
  98. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS;
  99. Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control).
  100. Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
       1. A estação não tem cliente 802.1x (suplicante);
       2. As credenciais do usuário não estão corretas (falha de autenticação);
       3. Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan);
       4. Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL).
  101. Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
       1. Nome do usuário;
       2. Switch em que o computador do usuário está conectado;
       3. Porta do switch utilizada par acesso;
       4. Endereço MAC da máquina utilizada pelo usuário;
       5. Endereço IP do usuário; vi. Horários de início e término da conexão;
       6. Bytes transmitidos e recebidos durante a conexão.
  102. Deve reautenticar (reautenticação periódica) e ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar;
  103. Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x;
  104. Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;
  105. Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch;
  106. Deve suportar a autenticação 802.1x através do protocolos EAPOL;
  107. Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;
  108. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
  109. Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra;
  110. Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS;
  111. Deve implementar o mecanismo mudança de autorização dinamica, Radius “Change of Authorization”, conforme descrito na RFC 5176.
  112. Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376);
  113. Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1,v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
  114. Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse- mode” (RFC 2362) e “dense-mode”. Deve ser suportada, por interface, a operação simultânea nos modos “sparse-mode” e “dense mode”;
  115. Suportar no mínimo 1000 grupos multicast para IPv4.
  116. Implementar priorização de tráfego através do protocolo IEEE 802.1p.
  117. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
  118. Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
  119. Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" – nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force);
  120. Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”;
  121. Deve ser possível a especificação de banda por classe de serviço.
  122. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);
  123. Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop);
  124. Implementar pelo menos oito filas de prioridade por porta de saída (egress port).
  125. Implementar IPv6;
  126. Permitir a configuração de endereços IPv6 para gerenciamento;
  127. Permitir consultas de DNS com resolução de nomes em endereços IPv6;
  128. Implementar ICMPv6 com as seguintes funcionalidades:
       1. ICMP request;
       2. ICMP Reply;
       3. ICMP Neighbor Discovery Protocol (NDP),
       4. ICMP MTU Discovery;
       5. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

# ITEM 6 - GBIC 25GBPS

* 1. Atender ao padrão SFP28;
  2. Atender o padrão 25 Gigabit Ethernet IEEE802.3by, 850nm, MMF, até 300m;
  3. Deve possuir conector do tipo LC;
  4. Deve atender ao padrão 25GBASE-SR;
  5. Deve ser compatível com os switches ofertados;

# ITEM 7 - GBIC 40 GBPS

* 1. Atender ao padrão QSFP;
  2. Atender o padrão 40 Gigabit Ethernet IEEE802.3ba, 850nm, MMF, até 150m;
  3. Deve possuir conector do tipo LC ou MPO;
  4. Deve atender ao padrão 4OGBASE-SR4;
  5. Deve ser compatível com os switches ofertados;

# ITEM 8 – GIBIC 100 GBPS

* 1. Atender ao padrão QSFP28;
  2. Atender o padrão 40 Gigabit Ethernet IEEE802.3bm, 850nm, MMF, até 100m;
  3. Deve possuir conector do tipo MPO;
  4. Deve atender ao padrão 100GBASE-SR4;
  5. Deve ser compatível com os switches ofertados;

# ITEM 9 - CONTROLADORA DE REDE SEM FIO

* 1. A controladora de rede Wi-fi deve suportar até 2.000 pontos de acesso atendendo aos padrões padrões 802.11a, 802.11b/g, 802.11, 802.11n, 802.11ac e 802.11ax;
  2. Deve suportar a conexão de no mínimo 30.000 clientes;
  3. Deverá ser fornecida em appliance físico;
  4. Deverá possuir no mínimo 4 portas 10G padrão SFP+
  5. Deverá ser fornecida com licenças suficientes para controlar todos os pontos de acesso objeto desta aquisição;
  6. Deverá estar licenciado para todas as funcionalidades exigidas nesta especificação;
  7. Deverá ter throughput mínimo de 5 (cinco) Gbps;
  8. Implementar criptografia do tráfego de dados e controle, na comunicação entre APs e controladora;
  9. Deve possuir funcionalidade que permita a utilização dos APs em sites remotos, onde através de conexão pela internet este automaticamente estabeleça um túnel seguro até o controlador permitindo que os SSIDs corporativos sejam disponibilizados aos usuários. Deverá também permitir a criação de um SSID local, que efetue a conexão direta via internet, sem a utilização do túnel seguro. Caso esta funcionalidade necessite de licenças adicionais, estas deverão estar contempladas para totalidade da capacidade do controlador.
  10. Deverá suportar no mínimo os seguintes modos de operação dos Pontos de Acessos:
  11. Centralizado;
  12. Local switching;
  13. Fabricante orquestrado pelo Sistema de Gerenciamento Baseado em Inteligência artificial, conforme descrito ítem 3;
  14. A rede Wifi local não pode se tornar inoperante devido à ocorrência de qualquer uma das 03 (três) falhas isoladas ou simultâneas listadas a seguir:
  15. Falha no controlador Wifi;
  16. Falha no Sistema de Autenticação Centralizado;
  17. Falha no link de comunicação entre os pontos de acesso e o controlador (WAN ou LAN)
  18. Deverá também, na ocorrência de inoperância, de acordo com o item anterior, deve continuar operando e permitir:
  19. Que os usuários já autenticados na rede e associados aos pontos de acesso continuem a possuir acesso à rede. Deve permitir que os usuários efetuem roaming entre os pontos de acesso do mesmo site nesta situação;
  20. Que novos usuários se autentiquem de acordo com 802.1x e se associem à rede sem qualquer prejuízo de acesso aos mesmos;
  21. No caso de falha do Sistema de Autenticação, deverá permitir a criação de uma base de usuários interna ao ponto de acesso, para que os usuários sejam autenticados através de 802.1x;
  22. Deverá suportar sistema de alta disponibilidade (HA) de forma a permitir uma topologia redundante com escalabilidade. No caso de falha do Controlador WLAN, os Pontos de Acesso deverão se associar a um controlador WLAN secundário de forma automática. O controlador redundante poderá estar em uma rede diferente;
  23. Deve suportar a adição de fonte de energia redundante interna;
  24. Deverá ser fornecido 1 (um) par de controladores do tipo appliance físico, com as mesmas configurações, em topologia redundante e totalmente licenciada para esta funcionalidade
  25. Permitir que os eventos sejam gravados remotamente utilizando syslog;
  26. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
  27. Possui suporte a MIB II, conforme RFC 1213;
  28. Possibilitar a obtenção da configuração lógica e física do equipamento através do protocolo SNMP;
  29. Possibilitar a obtenção via SNMP de, no mínimo, informações de capacidade e desempenho da CPU, memória e portas;
  30. Deve ser capaz de controlar Pontos de Acesso nos padrões 802.11a/b/g/n/ac/ax simultaneamente;
  31. Deve atender aos padrões IEEE 802.11d e 802.11h;
  32. Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:
      1. EAP-Transport Layer Security (EAP-TLS);
      2. EAP-TTLS/MSCHAPv2;
      3. PEAPv0/EAP-MSCHAPv2;
      4. PEAPv1/EAP-GTC;
      5. EAP-FAST;
      6. EAP Subscriber Identity Module (EAP-SIM).
  33. Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
  34. Deve possuir, quando utilizando Pontos de Acessos específicos, capacidade para classificar e mitigar interferências não WiFi que impactem diretamente no funcionamento da rede em menos de 1 minuto;
  35. Deve implementar WPA 3, WPA – 2;
  36. Deve implementar o padrão IEEE 802.11i;
  37. Possibilitar roaming com integridade de sessão, dando suporte à aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
  38. Deve ser fornecida com recursos instalados, compatíveis com a controladora de rede de acesso objeto deste edital, para implementar mecanismo de autenticação através de portal Web (Captive Portal) para usuários visitantes;
  39. Deve ser fornecido com recursos instalados para implementar listas de controle de acesso (ACL) com suporte a contadores (ACL Counters), ou seja, para um determinado pacote deve ser possível verificar qual entrada da lista de controle de acesso foi utilizada;
  40. Implementar listas de controle de acesso (ACL) baseadas em protocolos e endereços MAC;
  41. Deve ser fornecida com recursos instalados para implementar o bloqueio da comunicação entre usuários em um mesmo SSID;
  42. Deve ser fornecido com recursos instalados para implementar mecanismo para detecção de Pontos de Acesso invasor (Rogue AP);
  43. Deve ser fornecida com recursos instalados para implementar mecanismo para detecção de clientes invasores (Rogue clients detection);
  44. Deve ser fornecida com recursos instalados para implementar mecanismo para detecção de Redes Ad-Hoc;
  45. Implementar suporte a assinaturas de ataques de RF e prevenção de intrusão para ajudar ao administrador a customizar arquivos de assinatura de ataques para rapidamente detectar ataques de RF mais comuns tais como: denial of service(DoS), Netstumbler e FakeAP;
  46. Implementar varredura de RF continua, programada ou sob demanda;
  47. Deve possuir recursos para implementar ajuste dinâmico de canais 802.11 para otimizar a cobertura de rede e mudar as condições RF baseado em performance;
  48. Deve permitir acesso à interface de gerenciamento para todas as funcionalidades que existem localmente no controlador WLAN, sendo, no mínimo, suporte as seguintes opções:
      1. Telnet,
      2. Secure Shell (SSH) Protocol;
      3. HTTP;
      4. Secure HTTP (HTTPS);
  49. Deve possuir recursos instalados para implementar detecção de interferência e reajuste dos parâmetros de RF evitando problemas de cobertura e performance;
  50. Deve possuir recursos instalados para implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar a performance durante elevada utilização da rede;
  51. Deve possuir recursos instalados para implementar mecanismos automáticos de gerenciamento de recursos de rádio, detectando áreas sem cobertura, indisponibilidades de pontos de acesso, e executando auto configuração, autocorreção e auto otimização;
  52. Deve possuir recursos instalados para implementar mecanismo que ajusta dinamicamente a saída de potência dos Pontos de Acesso individualmente para acomodar as condições de alterações da rede, garantindo a performance e escalabilidade;
  53. Deve possuir recursos instalados para implementar mecanismo que no evento de falha de um ponto de acesso, o controlador ajuste automaticamente potência dos pontos de acesso adjacentes para dar cobertura de área onde o ponto de acesso que falhou estava provendo o sinal;
  54. Ajustar, dinamicamente, o nível de potência e canal dos rádios dos APs, de modo a otimizar o tamanho da célula de RF, garantido a performance e escalabilidade;
  55. Permitir a seleção/uso de servidor Radius ou LDAP com base no SSID;
  56. Permitir o uso de VoWLAN e dados sobre um mesmo SSID;
  57. Deve suportar 802.11e com WMM, U-APSD e T-SPEC;
  58. Implementar associação dinâmica de usuários a VLAN, com base nos parâmetros da etapa de autenticação;
  59. Suportar, no mínimo, 4096 VLANs;
  60. Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN.
  61. Deve possuir mecanismo de otimização automática de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast.
  62. Deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes, por exemplo 300 Mbps, mesmo que está não seja "rate" mandatório.
  63. Implementar qualidade de serviço com a marcação de pacotes utilizando Diffeservice e suporte a 802.1p, para QoS;
  64. Deve permitir visibilidade e controle das aplicações, permitindo a priorização de aplicações críticas, redução na prioridade de aplicações menos críticas e o bloqueio de aplicações não permitidas já na camada de acesso. Deve ter a capacidade de identificar, no mínimo, 1000 (um mil) aplicações diferentes;
  65. Deve implementar técnica de inspeção de pacotes para controle de aplicações que não utilizam portas fixas ou que utilizam protocolo TCP porta 80 ou 443;
  66. Permitir, opcionalmente, a reserva automática de banda da rede WLAN para o controle de admissão de chamada de voz;
  67. Permitir configurar os APs como sensores de RF para fazer a monitoração do ambiente Wireless;
  68. Implemetar DHCP Relay;
  69. Permitir o uso de múltiplos SSIDs simultaneamente;
  70. Permitir definir o número máximo de clientes por SSIDs.
  71. Deverá ser acompanhada das licenças necessárias para funcionamento com o CISCO DNA Center
  72. Deverá suportar os pontos de acesso existentes na ANTT modelo.

# ITEM 10 - PONTOS DE ACESSO

* 1. Deve ser gerenciado e controlado pelo Sistema gerenciador de Ponto de Acesso sem Fio;
  2. Possuir, no mínimo, uma interface Ethernet padrão IEEE 802.3bz multigigabit que funcione nas velocidades 100M/1G/2.5G;
  3. Deve possuir, no mínimo, uma porta serial (console) para acesso console ao equipamento com conector RJ45.
  4. Deverá suportar fonte de alimentação elétrica local que opere em AC 100- 240V, bivolt, 50/60Hz ou ser alimentado exclusivamente por dispositivo PoE;
  5. Deve possuir suporte a energia fornecida pelo padrão PoE, PoE+ conforme especificados na norma IEEE 802.3at e 802.3af.
  6. Possuir funcionamento em modo gerenciado por controlador WLAN para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento do espectro de Rádio Frequência;
  7. Poderá estar remotamente conectado ao switch controlador WLAN, inclusive via roteamento da camada de rede OSI, através de rede pública ou privada;
  8. Se um controlador WLAN falhar, os APs relacionados deverão se associar automaticamente a um controlador WLAN alternativo, não permitindo que a rede sem fio se torne inoperante;
  9. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces Ethernet e serial (terminal assíncrono);
  10. Permitir a configuração e gerenciamento através de SSH e porta serial;
  11. Os APs instalados remotamente devem manter as conexões mesmo com desconexão da controladora;
  12. Ao ser conectado na rede, deve encontrar automaticamente uma controladora, e atualizar as configurações do ponto de acesso;
  13. Possuir LED’s indicativos do estado de operação, da atividade do rádio;
  14. Permitir habilitar e desabilitar a divulgação do SSID;
  15. Possuir diferentes tipos de combinações de encriptação/autenticação por SSID;
  16. Possuir cliente DHCP, para configuração automática de rede;
  17. Possuir WPA2 com algoritmo de criptografia AES, IEEE 802.11i;
  18. Possuir as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 24 e 6 Mbps IEEE 802.11n: no mínimo MCS23 (MCS0 até MCS23) para 2.4GHz e 5GHz 802.11n high-throughput (HT) support: HT 20/40 para 5GHz; 802.11ac support: VHT 20/40/80/160; 802.11ax support: HE 20/40/80/160; e 802. 11n/ac packet aggregation: A-MPDU, A-MSDU. Operar nas modulações 802.11n, 802.11ac wave 2 e 802.11ax;
  19. Possuir capacidade de selecionar automaticamente o canal de transmissão;
  20. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;
  21. Possuir potência máxima de transmissão de, no mínimo, 23 dBm para protocolos padrão IEEE 802.11a/b/g/n/ac/ax;
  22. Possuir sensibilidade de recepção de valor menor ou igual: a -100 dBm a 6 Mbps no padrão 802.11g; e a -100 dBm a 6Mbps no padrão 802.11a;
  23. Operar em temperaturas entre 0°C e 40º C;
  24. Equipamento de Ponto de Acesso para rede local sem fio atendendo aos padrões IEEE 802. 11a, IEEE 802. 11b, IEEE 802. 11g, 802. 11ac, 802. 11ac wave 2 e 802. 11ax com capacidade de configuração via software.
  25. Permitir simultaneamente usuários configurados nos padrões IEEE 802.11b/g/n, 802.11a/n/ac e 802.11ax com SU-MIMO ou MU-MIMO;
  26. Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac/ax e 802.11/b/g/n com ganho de, pelo menos, 4 dBi operando em 2.4GHz e 5 dBi operando em 5GHz, com padrão de irradiação omnidirecional multi-banda dipolar, integradas e com no mínimo 4 transmissores e 4 receptores;
  27. Permitir o bloqueio da configuração do AP via rede sem fio;
  28. Possuir criptografia do tráfego local;
  29. Deverá ser acompanhado das licenças necessárias para funcionamento com o CISCO DNA Center.

# ITEM 11 - SERVIÇOS GERENCIADOS – COMUNICAÇÃO E CONECTIVIDADE

* 1. Os recursos principais de atendimento ao objeto deverão ser centralizados na sede da ANTT, sendo que nas demais unidades o serviço fica limitado ao mínimo necessário para atendimento rotineiro. Com isto importantes recursos podem ser compartilhados, tais como: Central de Atendimento centralizado, sistema de controle de chamadas e atendimento de suporte único, ficando restrito às unidades o atendimento local sob demanda, mediante deslocamento dos recursos da sede.
  2. Após a análise dos padrões mais praticados pelos Órgãos e Entidades públicos, em conformidade com o disposto no Art. 11, alínea II, da IN 94/2022 da SGD/ME, o modelo adotado para a contratação de serviços de gerenciados de comunicação e conectividade será por remuneração por valor fixo mensal referentes aos serviços classificados como manutenção do tipo EVOLUTIVA e para os serviços classificados como manutenção CORRETIVA com forte relação aos níveis mínimos de serviço, conforme descritos no Catálogo de Serviço, vinculada exclusivamente ao atendimento de níveis mínimos de serviços estabelecidos. Todos os serviços deverão constar do Relatório Gerencial apresentado.
  3. Este modelo de contratação, no que tange equipe técnica, não se configura como de dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho.
  4. Sendo vedado ao órgão realizar a distribuição, controle, fiscalização ou supervisão dos recursos humanos da contratada, a exemplo de quantidade de perfis, base salarial, jornada, frequência ou outros critérios relacionados à alocação de mão de obra.
  5. A estimativa para o dimensionamento na composição da equipe e a alocação dos perfis profissionais considerou o histórico dos atendimentos efetuados e os registros de controle e acompanhamento dos chamados de serviço do contrato vigente.
  6. O atendimento deverá ser presencial nos horários previstos neste documento pelos perfis profissionais, em atenção às qualificações exigidas para desempenho das atribuições previstas para cada um dos serviços contratados;
  7. Fica a cargo da CONTRATADA a formulação de equipe respeitando os níveis de atuação determinados no Catálogo de Serviço constante nesse documento;
  8. O Quantitativo de Profissionais para referência está apresentado na tabela abaixo. Tal fato se justifica pela necessidade do serviço a ser prestado, bem como a manutenção do conhecimento explícito pela equipe que prestará o serviço.

|  |  |  |
| --- | --- | --- |
| **Descrição**  **Categoria** | **Perfil Profissional** | **Quantidade**  **Estimada** |
| Conectividade e Comunicação | Analista de redes e de comunicação de dados Júnior. | 1 |
| Analista de redes e de comunicação de dados Pleno. | 1 |
| Analista de redes e de comunicação de dados Sênior. | 1 |

* 1. Os profissionais da contratada deverão atuar de acordo com os níveis mínimos de SLA conforme descrito na tabela abaixo:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tipo de Manutenção** | **Horário de Atendimento** | **Tempo de Atendimento** | **Tempo de Resolução** | **SLA** |
| Evolutiva | 8:00h às 18:00h | 2 dias uteis | 10 dias uteis | 8x5 |
| Corretiva | 0:00h às 23:59h | 2 horas | 6 horas | 24x7 |

* 1. Considerando que não se trata de alocação de posto de trabalho, entende-se que a gestão dos profissionais compete à CONTRATADA, desde que não haja prejuízo ao cumprimento dos níveis mínimos de serviços.
  2. Relatório Gerencial;
  3. Todo serviço prestado pela equipe da CONTRATADA deverá constar do Relatório Gerencial apresentando-o ao CONTRATANTE, até o quinto dia útil do mês subsequente ao da prestação dos serviços, devendo constar dentre outras informações:
  4. Os indicadores e níveis de serviços alcançados em relação ao previsto no Apêndice “C”, Catálogo de Serviços.
  5. Relatório de análise e diagnóstico das causas (causa raiz) dos incidentes e problemas ocorridos;
  6. Manutenções evolutivas e corretivas realizadas;
  7. Erros operacionais;
  8. Sugestões de melhorias;
  9. Painel de volumetria de chamados (requisições de serviço, incidentes, problemas etc.) divididos por grupos solucionadores e responsáveis, demonstrando graficamente a evolução destas informações;
  10. Indicadores de aferição da qualidade de novos produtos e/ou serviços que venham a ser implantados no decorrer da vigência contratual.
      1. Serviços de categoria EVOLUTIVA:

|  |  |  |  |
| --- | --- | --- | --- |
| **Serviço** | **Descrição** | **Responsável Técnico** | **Valor do Serviço** |
| Operação Assistida | Acompanhamento do funcionamento de todo ambiente de conectividade de forma proativa garantindo desempenho e disponibilidade | Analista Junior |  |
| Configuração de Gerencia e Controle | Configuração de controle de fluxo sFlow ou Netflow | Analista Junior |  |
| Configuração Layer 3 | Monitoramento de fluxos resultados dos protocolos sFlow ou Netflow | Analista Junior |  |
| Monitoramento de fluxos resultados dos protocolos sFlow ou Netflow | Analista Junior |  |
| Criação de relatório de performance em rede automatizada | Analista Junior |  |
| Definição de alertas de erro em software de gerencia e controle | Analista Junior |  |
| Configuração dos alertas de erro em software de gerencia e controle | Analista Junior |  |
| Versão de Software | Analise junto a documentação do fabricante de erros conhecidos (bugs) em versão de software instalada | Analista Junior |  |
| Analise de versão de software recomendada pelo fabricante | Analista Junior |  |
| Analise junto a documentação do fabricante de erros conhecidos (bugs) em versão de software recomendada | Analista Junior |  |
| Analise de performance da rede | Site survey para analise de spectrum na rede wireless | Analista Pleno |  |
| Geração de relatórios para analise de performance da rede cabeada | Analista Pleno |  |
| Total do valor fixo para serviço de categoria EVOLUTIVA | | |  |

* + 1. Serviços de categoria CORRETIVA:

|  |  |  |  |
| --- | --- | --- | --- |
| **Serviço** | **Descrição** | **Responsável Técnico** | **Valor do Serviço** |
| Segmentação da rede | Criação ou exclusão de interface/vlan | Analista Pleno |  |
| Configuração de interfaces | Configuração de interfaces físicas com definição de banda, modo da interface entre outros | Analista Pleno |  |
| Agregação de link | Configuração de protocolo que permita a agregação de links para aumento de banda | Analista Pleno |  |
| Roteamento dinâmico | Configuração de protocolos de roteamento dinâmico para encaminhamentos de pacotes de forma automatizada | Analista Sênior |  |
| Configuração de redundância | Configuração de protocolos que permitam conectar links redundantes | Analista Pleno |  |
| Configuração de segurança | Configuração de protocolos que permitam adicionar segurança na comunicação dos dados | Analista Sênior |  |
| Mudança de topologia | Modificação de configuração visando mudança de topologia de acordo com a demanda | Analista Sênior |  |
| Configuração de usuários | Criação ou exclusão de usuários do tipo suporte ao equipamento | Analista Pleno |  |
| Ambiente de monitoração e controle | Configuração, atualização e melhorias no sistema de controle e monitoramento da rede | Analista Pleno |  |
| Configuração Layer 3 | Configuração de roteamento estático | Analista Sênior |  |
| Configuração de rotas BGP |  |
| Configuração de filtros BGP |  |
| Configuração de private vlan |  |
| Planejamento de vxlan |  |
| Configuração de vxlan |  |
| Definição de políticas através de ACL |  |
| Configuração de ACLs na camada de core |  |
| Configuração de ACL na camada de acesso |  |
| Discovery de ativos de rede |  |
| Definição grupos de acesso em rede automatizada |  |
| Configuração das políticas para grupos de acesso em rede automatizada |  |
| Configuração de agregação de links virtuais em switches LEAFS |  |
| Configuração de agregação de links virtuais em switches spine |  |
| Upgrade de imagens para sistema operacional dos switches LEAFS |  |
| Analise de logs na investigação de erros |  |
| Configuração Layer 2 | Upgrade de imagens para sistema operacional dos switches SPINE | Analista Pleno |  |
| Criação de SSIDs para rede wireless | Analista Pleno |  |
| Troubleshooting de problemas | Configuração de segurança de SSIDs para rede wireless | Analista Pleno |  |
| Configurações gerais de SSIDs para rede wireless | Analista Pleno |  |
| Configuração de características gerais de Aps | Analista Pleno |  |
| Configuração de WLANs | Configuração de características avançadas de Aps | Analista Pleno |  |
| Configuração de segurança de Aps | Analista Pleno |  |
| Configuração de perfil para Aps | Analista Pleno |  |
| Configuração de Ponto de Acesso | Criação e configuração de grupos de Aps | Analista Pleno |  |
| Criação de ACLs para acesso na rede wireless | Analista Pleno |  |
| Instalação de certificado digital | Analista Pleno |  |
| Configuração de servidor radius | Analista Pleno |  |
| Configuração de servidor TACACS+ | Analista Pleno |  |
| Configuração de Controladora Wireless | Criação de interface vlan | Analista Sênior |  |
| Configuração de interface vlan | Analista Sênior |  |
| Configuração de servidor DHCP | Analista Sênior |  |

# ---------------------------------------- FIM DO APÊNDICE “A” ----------------------------------------