MINISTÉRIO DAS CIDADES

Secretaria Executiva
Subsecretaria de Planejamento, Orçamento e Administração
Coordenação-Geral de Tecnologia da Informação

ANEXO I - ESPECIFICAÇÃO DA SOLUÇÃO

1. SWITCH DE CORE COM 48 PORTAS SFP

1.1. ESPECIFICAÇÕES GERAIS

1. Deve permitir instalação em rack de 19” padrão Telco EIA;
2. Deve possuir altura máxima 1 (um) rack unit (RU);
3. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;
4. Deve possuir fonte de alimentação redundante interna e hot-swappable;
5. Deve possuir capacidade de processamento igual ou superior a 670 (seiscentos e setenta) Mpps;
6. Deve possuir capacidade de switching igual ou superior a 900 (novecentos) Gbps;
7. Deve possuir 48 (quarenta e oito) portas SFP, sendo que no mínimo 12 (doze) dessas portas devem operando 1G/10GbE compatíveis com SFP/SFP+ e o restante das portas devem operar em 1GbE SFP;
8. Deve permitir empilhamento de até 10 (dez) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;
9. Deve possuir banda agregada de empilhamento mínima de 160 (cento e sessenta) Gbps ,podendo ser através de 2 (duas) portas de 40 (quarenta) Gbps operando em full-duplex. As portas de empilhamento deverão ser fornecidas nesse certame;
10. O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;
11. Deve suportar expansão futura de pelo mínimo 1 (uma) porta 100Gbps QSFP28 adicional as portas solicitadas nesse certame;
12. Deve suportar expansão futura de pelo no mínimo 2 (duas) portas 40Gbps QSFP+ adicionais as portas solicitadas nesse certame;
13. Deve suportar expansão futura de pelo menos 4 (quatro) portas 1/10Gbps SFP+ adicionais as portas solicitadas nesse certame;
14. Deve ser compatível com SFP 1000BASE-SX, 1000BASE-LX e 1000Base-T;
15. Deve ser compatível com SFP+ 10GBASE-SR,10GBASE-LR, 10GBASE-ER;
16. Deve ser compatível com QSFP+ 40GBASE-SR4, 40GBASE-LR4 e 40G-BiDi;
17. Deve ser compatível com QSFP28 100GBASE-SR4, 100GBASE-LR4 e 100GBASE-CWDM4;

18. Deve possuir pelo menos 8MB de buffer de pacotes;
19. Deve possuir, no mínimo, 4GB de memória DRAM e 4GB de memória NVRAM (flash);
20. Deve possuir ventilação front to back, isto é, o fluxo de ar deve seguir no sentido das portas de interface para as fontes de energia;
21. Deve suportar a inversão do fluxo de ar de ventilação para o modo “back to front” através de pelo menos um dos seguinte métodos: troca de ventiladores e fontes, atualização de firmware ou alteração do arquivo de configuração;
22. Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;
23. Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;
24. Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;
25. Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;
26. Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;
27. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;
28. Deve possuir botão de reset voltar a para configuração default de fábrica;
29. O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;
30. A proposta comercial deve descriminar o fabricante e o modelo do equipamento ofertado bem como seus respectivos “P/Ns”;
31. Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;
32. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet

1.2. **FUNÇÕES DE CAMADA 2**

1. Deve possuir capacidade de no mínimo 110.000 (cento e dez mil) endereços MAC;
2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad.
3. Deve permitir a configuração de pelo menos 250 (duzentos e cinquenta) grupos de LACP com pelo menos 16 (dezesseis) portas dentro de um mesmo grupo;
4. Deve permitir a configuração de grupos de portas agregadas (LAGs) com balanceamento simétrico, garantindo que o tráfego de um mesmo origem e destino passe pelo mesma porta de um LAG de forma bidirecional;
5. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;
6. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);
7. Deve ser compatível com o protocolo PVST+;
8. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

9. Deve implementar BPDU Guard e Root Guard;
10. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;
11. Deve permitir a criação VLANs privadas;
12. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;
13. Deve implementar selective QinQ;
14. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;
15. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;
16. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;
17. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown) ;
18. Deve permitir a configuração de endereços MAC de unicast multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;
19. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
20. Deve implemenetar MLD snooping v1 e v2;
21. Deve implementar MVRP (Multiple VLAN Registration Protocol);
22. Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;
23. Deve implementar protocolo de proteção de topologia em anel;

1.3. **FUNÇÕES DE CAMADA 3**

1. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;
2. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
3. Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;
4. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;
5. Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;
6. Deve implementar roteamento usando o protocolo BGP4 e BGP4+;
7. Deve implementar criação de túneis GRE;
8. Deve implementar VRF ou VRF-lite, com suporte a pelo menos 32 (trinta e duas) instâncias;
9. Deve implementar os protocolos VRRP e VRRPv3;
10. Deve implementar ECMP com no mínimo 8 (oito) caminhos;
11. Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;
12. Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.

13. Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs
14. Deve permitir a configuração de pelo menos 2.000 (duas mil) rotas estáticas IPv4;
15. Deve permitir a configuração de pelo menos 1.000 (mil) rotas estáticas IPv6;
16. Deverá suportar a capacidade pelo menos 97.000 (noventa e sete mil) entradas em sua tabela de roteamento IPv4;
17. Deverá suportar a capacidade de pelo menos 17.000 (dezessete mil) entradas em sua tabela de roteamento IPv6;
18. Deve possuir DHCP Server para IPv4 e IPv6;
19. Deve permitir a configuração de DHCP Relay;
20. Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;
21. Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para a escolher a rota default apropriada pelo host IPv6;

1.4. **SEGURANÇA**

1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;
2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;
3. Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuirem suplicantes 802.1X;
4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;
5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:
    1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;
    2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;
    3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;
6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;
8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;
9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;
10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;
11. Deve implementar ACLs de entrada e ACLs de saída para IPv4;
12. Deve implementar ACLs de entrada e ACLs de saída para IPv6;

13. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;
14. Deve permitir a criação de filtros de endereço MAC de origem e destino;
15. Deve possuir protocolos para proteção de ataques de Denial of Service;
16. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;
17. Deve possuir funcionalidade de proteção contra ataques do tipo “ARP Poisoning”;
18. Deve permitir a configuração de Dynamic ARP Inspection em pelo menos 500 vlans;
19. Deve implementar IP Source Guard;
20. Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;
21. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;
22. Deve implementar IPv6 RA guard e IPv6 ND inspection;
23. Deve implementar RADsec conforme RFC6614;
24. Deve implementar unicast Reverse Path Forwarding (uRPF) como ferramenta para evitar ataques do tipo source IP spoofing;

1.5. **GERENCIAMENTO**

1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;
7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritimos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
9. Deve implementar pelo menos 4 (quatro) grupos de RMON;
10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;
11. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
12. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha,

permitindo a continuidade do tráfego de dados durante o processo de atualização;

13. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;
14. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;
15. Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;
16. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
17. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.
18. Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;
19. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
20. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;
21. Deve possuir suporta a automação com Ansible;
22. Deve implementar RESTCONF;
23. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

1.6. QUALIDADE DE SERVIÇO

1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;
3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;
4. Deve implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
5. Deve permitir a configuração de Rate Limiting de entrada;
6. Deve permitir a configuração de Rate Shaping de saída;
7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

2. TIPO 01 - SWITCH DE ACESSO COM 24 PORTAS

2.1. ESPECIFICAÇÕES GERAIS

1. Deve permitir instalação em rack de 19” padrão Telco EIA;
2. Deve possuir altura máxima 1 (um) rack unit (RU);

3. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;
4. Deve possuir 24 (vinte e quatro) portas 10/100/1000 Mbps, usando conectores RJ-45;
5. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;
6. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP/SFP+, as quais não devem operar em modo "combo" com as portas 10/100/1000 BASE-T em par trançado;
7. Deve possuir capacidade de processamento igual ou superior a 98 (noventa e oito) Mpps;
8. Deve possuir capacidade de switching igual ou superior a 132 (cento e trinta e dois) Gbps;
9. Deve possuir, pelo menos, 2 MB de buffers de pacotes;
10. Deve possuir, pelo menos, 1 GB de memória DRAM;
11. Deve possuir, pelo menos, 2 GB de memória flash;
12. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);
13. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;
14. Deve ser do tipo fanless ou permitir operação com os ventiladores internos desligados;
15. Deve permitir empilhamento de até 8 (oito) unidades com outros equipamentos em topologia linear e em anel;
16. Deve permitir o empilhamento com switches da mesma série, sendo switches 24 portas, switches 48 portas, switches multi-gigabit e switches PoE+, e permitir gerenciar a pilha com um único endereço IP;
17. Deve suportar banda agregada de empilhamento de no mínimo 80Gbps fullduplex, podendo ser através de agregação de portas de 10G. Essas portas podem ser formadas pelas portas do item 2.1.6;
18. O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;
19. Deve possuir porta de gerenciamento "out-of-band" operando a 10/100/1000 Mbps;
20. Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;
21. Deve possuir slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;
22. Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;
23. Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;
24. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;
25. Deve possuir botão de reset para voltar a para configuração default de fábrica;
26. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);
27. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

2.2. **FUNÇÕES DE CAMADA 2**

1. Deve possuir capacidade de no mínimo 16.000 (dezesseis mil) endereços MAC;
2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad.
3. Deve permitir configuração de pelo menos 120 (cento e vinte) grupos de LACP copelo menos 8 (oito) portas dentro de um mesmo grupo;
4. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;
5. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);
6. Deve ser compatível com o protocolo PVST+;
7. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;
8. Deve implementar BPDU Guard e Root Guard;
9. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;
10. Deve permitir a criação VLANs privadas;
11. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;
12. Deve implementar selective QinQ;
13. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;
14. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet
15. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;
16. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);
17. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;
18. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
19. Deve implmenetar MLD snooping v1 e v2;
20. Deve implementar MVRP (Multiple VLAN Registration Protocol);
21. Deve implementar MVP (Multicast VLAN Registration);
22. Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste permitindo medir a continuidade da rede e o desempenho da porta ethernet;
23. Deve implementar protocolo de proteção de topologia em anel.

2.3. **FUNÇÕES DE CAMADA 3**

1. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;
2. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
3. Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;

4. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;
5. Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;
6. Deve implementar os protocolos VRRP e VRRPv3;
7. Deve implementar ECMP com no mínimo 8 caminhos;
8. Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;
9. Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.
10. Deverá possuir no mínimo 350 (trezentos e cinquenta) interfaces virtuais para roteamento entre VLANs;
11. Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv4;
12. Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv6;
13. Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas na sua tabela de roteamento IPv4;
14. Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas em sua tabela de roteamento IPv6;
15. Deve possuir DHCP Server para IPv4 e IPv6;
16. Deve permitir a configuração de DHCP Relay;
17. Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;
18. Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para a escolher a rota default apropriada pelo host IPv6;

2.4. **SEGURANÇA**

1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;
2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;
3. Deve implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;
4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;
5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:
    1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;
    2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;
    3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;
6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;
8. Deve implementar “Change of Authorization” de acordo com a RFC 5176;

9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;
10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;
11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;
12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;
13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;
14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);
15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;
16. Deve permitir a criação de filtros de endereço MAC de origem e destino;
17. Deve possuir protocolos para proteção de ataques de Denial of Service;
18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;
19. Deve possuir funcionalidade de proteção contra ataques do tipo “ARP Poisoning”;
20. Deve implementar IP Source Guard em IPv4 e IPv6;
21. Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;
22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;
23. Deve implementar IPv6 RA guard e IPv6 ND inspection;
24. Deve implementar RADsec conforme RFC6614;

2.5. **GERENCIAMENTO**

1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;
7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES.
8. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

9. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
10. Deve implementar pelo menos 4 (quatro) grupos de RMON;
11. Deve permitir o monitoramento dos transceivers ópticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;
12. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;
13. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
14. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;
15. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;
16. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;
17. Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;
18. Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;
19. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
20. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.
21. Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;
22. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
23. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;
24. Deve possuir suporte a automação com Ansible;
25. Deve suportar RESTCONF ou RESTful API;

2.6. **QUALIDADE DE SERVIÇO**

1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;
3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;
4. Deve implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
5. Deve permitir a configuração de Rate Limiting de entrada;

6. Deve permitir a configuração de Rate Shaping de saída;
7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;
8. Deve suportar SDVoE (Software Defined Video over Ethernet);

3. TIPO 02 - SWITCH DE ACESSO COM 48 PORTAS

3.1. ESPECIFICAÇÕES GERAIS

1. Deve permitir instalação em rack de 19” padrão Telco EIA;
2. Deve possuir altura máxima 1 (um) rack unit (RU);
3. Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;
4. Deve possuir 48 (quarenta e oito) portas 10/100/1000 Mbps, usando conectores RJ-45;
5. As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;
6. Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP/SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;
7. Deve possuir capacidade de processamento igual ou superior a 130 (cento e trinta) Mpps;
8. Deve possuir capacidade de switching igual ou superior a 180 (cento e oitenta) Gbps;
9. Deve possuir, pelo menos, 4 MB de buffers de pacotes;
10. Deve possuir, pelo menos, 1 GB de memória DRAM;
11. Deve possuir, pelo menos, 2 GB de memória flash;
12. Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);
13. Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;
14. Deve ser do tipo fanless ou permitir operação com os ventiladores internos desligados;
15. Deve permitir empilhamento de até 8 (oito) unidades com outros equipamentos em topologia linear e em anel;
16. Deve permitir o empilhamento com switches da mesma série, sendo switches 24 portas, switches 48 portas, switches multi-gigabit e switches PoE+, e permitir gerenciar a pilha com um único endereço IP;
17. Deve suportar banda agregada de empilhamento de no mínimo 80Gbps full-duplex, podendo ser através de agregação de portas de 10G. Essas portas podem ser formadas pelas portas do item 3.1.6;
18. O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;
19. Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;
20. Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;
21. Deve possuir slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

22. Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;
23. Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;
24. Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;
25. Deve possuir botão de reset para voltar a para configuração default de fábrica;
26. Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);
27. Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242com documentos disponíveis publicamente no sítio público dessa agência na Internet;

3.2. **FUNÇÕES DE CAMADA 2**

1. Deve possuir capacidade de no mínimo 16.000 (dezesseis mil) endereços MAC;
2. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 120 (cento e vinte) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;
3. Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatromil) vlans ativas;
4. Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);
5. Deve ser compatível com o protocolo PVST+;
6. Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias deSpanning Tree;
7. Deve implementar BPDU Guard e Root Guard;
8. Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;
9. Deve permitir a criação VLANs privadas;
10. Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;
11. Deve implementar selective QinQ;
12. Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;
13. Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;
14. Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;
15. Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);
16. Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;
17. Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
18. Deve implementar MLD snooping v1 e v2;

19. Deve implementar MVRP (Multiple VLAN Registration Protocol);
20. Deve implementar MVP (Multicast VLAN Registration);
21. Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;
22. Deve implementar protocolo de proteção de topologia em anel.

3.3. **FUNÇÕES DE CAMADA 3**

1. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;
2. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
3. Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;
4. Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;
5. Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;
6. Deve implementar os protocolos VRRP e VRRPv3;
7. Deve implementar ECMP com no mínimo 8 caminhos;
8. Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;
9. Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.
10. Deverá possuir no mínimo 350 (trezentos e cinquenta) interfaces virtuais para roteamento entre VLANs
11. Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv4;
12. Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv6;
13. Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas na sua tabela deroteamento IPv4;
14. Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas em sua tabela de roteamento IPv6;
15. Deve possuir DHCP Server para IPv4 e IPv6;
16. Deve permitir a configuração de DHCP Relay;
17. Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;
18. Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para escolher a rota default apropriada pelo host IPv6;

3.4. **SEGURANÇA**

1. Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;
2. Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;
3. Deve implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;
4. Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois)

dispositivos (Ex.:Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

5. Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:
    1. 2 (dois) dispositivos que suportam o padrão IEEE 802.1x;
    2. 2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;
    3. 1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;
6. O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
7. O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;
8. Deve implementar "Change of Authorization" de acordo com a RFC 5176;
9. Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;
10. Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;
11. Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereçoIP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;
12. Deve implementar ACLs de entrada e ACLs de saída para IPv4;
13. Deve implementar ACLs de entrada e ACLs de saída para IPv6;
14. Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);
15. Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;
16. Deve permitir a criação de filtros de endereço MAC de origem e destino;
17. Deve possuir protocolos para proteção de ataques de Denial of Service;
18. Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;
19. Deve possuir funcionalidade de proteção contra ataques do tipo "ARP Poisoning";
20. Deve implementar IP Source Guard em IPv4 e IPv6;
21. Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;
22. Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;
23. Deve implementar IPv6 RA guard e IPv6 ND inspection;
24. Deve implementar RADsec conforme RFC6614;

3.5. **GERENCIAMENTO**

1. Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
2. Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com

autenticação e com privacidade;

3. Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
4. Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
5. Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
6. Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;
7. Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
8. Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
9. Deve implementar pelo menos 4 (quatro) grupos de RMON;
10. Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;
11. Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;
12. Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
13. Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;
14. Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;
15. Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;
16. Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;
17. Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
18. Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.
19. Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;
20. Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos.
21. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
22. Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;
23. Deve possuir suporte a automação com Ansible;
24. Deve suportar RESTCONF;

25. Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

3.6. QUALIDADE DE SERVIÇO

1. Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
2. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;
3. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;
4. Deve implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
5. Deve permitir a configuração de Rate Limiting de entrada;
6. Deve permitir a configuração de Rate Shaping de saída;
7. Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;
8. Deve suportar SDVoE (Software Defined Video over Ethernet);

4. PONTO DE ACESSO INDOOR

4.1. ESPECIFICAÇÕES GERAIS

1. Deverá ser do mesmo fabricante do CONTROLADOR DE REDE SEM FIO - WLAN para fins de compatibilidade.
2. Deverá possuir estrutura metálica que permita a utilização do equipamento em locais internos, com fixação em teto.
3. Não serão aceitos equipamentos com padrão de instalação física em parede, conhecidos como “wall plate”, uma vez que a instalação física deverá ocorrer no teto.
4. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.
5. Deve visar a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO, Target Wake Time (TWT), se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 no programa da WiFi Alliance na data do pregão.
6. Deve possuir a certificação IEC 61373 para uso em ambientes sujeitos à vibração e impactos.
7. Deve ser compatível com o padrão UL 2043, o qual regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.
8. Deve suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.
9. Deve possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

10. Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE IEEE 802.3at ou IEEE 802.3af. Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.
11. Deve suportar temperatura de operação entre 0°C a 50°C.
12. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.
13. Deverá possuir 2 (duas) interfaces ethernet 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local.
14. Deverá possuir, no mínimo, um rádio embarcado para IoT, o qual deve ser compatível com BLE e ZigBee.
15. Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.
16. Deverá possuir LEDs para a indicação do status da alimentação do ponto de acesso, rádios de 2.4 GHz e 5 GHz, operação em Mesh e gerenciamento via controladora.
17. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS, e Wi-Fi Mesh habilitadas, incluindo auto cura via Mesh.
18. Deve ser compatível com IPv4, IPv6 e dual-stack.

4.2. CARACTERÍSTICAS DOS RÁDIOS

1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.
2. Deverá implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a 300 Mbps, IEEE 802.11ac: 6.5 Mbps a 867 Mbps e IEEE 802.11ax: 4 Mbps a 1200 Mbps.
3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 1.5 dBi para 2.4GHz e 2.5 dBi para 5GHz.
4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 25 dBm na frequência de 5 GHz e 26 dBm na frequência de 2.4 GHz.
5. Deverá suportar canalização de 20 MHz, 40 MHz e 80 MHz.
6. Deverá possuir mecanismo de rádio com suporte a 4 (quatro) fluxos espaciais, sendo 2x2:2 em 5 GHz e 2.4 GHz para SU-MIMO e MU-MIMO.
7. Deve possuir sensibilidade mínima de recepção de -97dBm considerando MCS0 HE20 (802.11ax) em 5GHz e 2.4GHz.
8. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.
9. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.
10. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

4.3. SERVIÇOS, SEGURANÇA E GERENCIAMENTO

1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.
2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.
3. Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.
4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.
5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.
6. Deve suportar a configuração de limite de banda por usuário ou por SSID.
7. Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services).
8. Deve implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.
9. Deve suportar VLANs conforme o padrão IEEE 802.1Q.
10. Deve suportar atribuição dinâmica de VLAN por usuário.
11. Deve implementar balanceamento de usuários por ponto de acesso.
12. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.
13. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.
14. Deve suportar HotSpot 2.0, Captive Portal e WISPr.
15. Deverá implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK (Pre-Shared Key) única por dispositivo cliente em um mesmo SSID, IEEE 802.1X e IEEE 802.11i.
16. Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.
17. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.
18. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.
19. Deve permitir habilitar e desabilitar a divulgação do SSID.
20. Deverá implementar autenticação de usuários usando portal de captura.
21. Deverá suportar funções para análise de espectro.
22. Deve suportar conversão de tráfego multicast para unicast.

23. Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.
24. Deve permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.
25. Deve permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.
26. Deverá implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.
27. Deve permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

5. SISTEMA DE GERENCIAMENTO EM NUVEM

5.1. ESPECIFICAÇÕES GERAIS

1. A solução deverá ser baseada nas premissas de computação em nuvem ofertada como serviço pelo fabricante e ser compatível com a plataforma de gerenciamento, os pontos de acesso e os switches propostos nesse certame;
2. A solução deverá ser baseada em algoritmos de inteligência artificial e nos conceitos de *machine learning* (aprendizagem de máquina);
3. A solução deverá atuar em conjunto com as funcionalidades do controlador LAN/WLAN desde que seja do mesmo fabricante dos controladores, pontos de acesso e switches utilizados na solução. Os dados de telemetria enviados pelo controlador LAN/WLAN para a nuvem devem estar criptografados.
4. Deve permitir seu acesso e gerenciamento através de navegador web padrão (HTTPS);
5. Deve possuir interface gráfica para visualização das informações, dashboards e relatórios;
6. O Dashboard deve mostrar um resumo da integridade da rede, incluindo os principais incidentes e recomendações de reparo;
7. Deve classificar automaticamente os incidentes de rede por nível de severidade em pelo menos 4 níveis.
8. Deve fornecer contagem total dos incidentes que ocorreram na rede e categorizá-los de acordo com a severidade, sendo possível analisar os incidentes dos últimos 90 dias.
9. Deve ser possível exportar a lista de incidentes, pelo menos no formato CSV.
10. Para cada incidente, deverá apresentar análise contendo: severidade, descrição detalhada do incidente, data e horário de início do incidente, duração, equipamentos e/ou clientes impactados, causa raiz e recomendações de reparo.
11. Para incidentes relacionados à conexão, deve identificar pelo menos os seguintes problemas:
    1. Falhas elevadas de associação e autenticação 802.11;
    2. Falhas elevadas com servidores de DHCP;
    3. Falhas elevadas com EAP;
    4. Falhas elevadas com servidores RADIUS;

5. Elevado tempo para conexão de dispositivos e/ou usuários;

12. Para incidentes relacionados à desempenho, deve identificar pelo menos os seguintes problemas:
    1. Cobertura - Clientes com baixo nível de sinal (RSSI);
    2. Condições do canal abaixo do ideal;
    3. Alta utilização de CPU da controladora;
    4. Alta utilização de memória dos switches;
    5. Alta utilização do *Airtime* dos APs nas bandas de 2.4GHz, 5GHz e 6GHz, identificando se a alta utilização é devido à transmissão (TX), recepção (RX) ou interferências;
13. Para incidentes relacionados à infraestrutura, deve identificar pelo menos os seguintes problemas:
    1. Erro de sincronismo de horários;
    2. PoE – APs recebendo menos energia do que o necessário para o máximo desempenho;
    3. Incompatibilidade de velocidade da interface do AP com o switch;
    4. Incompatibilidade de VLAN ID entre AP e switch;
    5. Falhas e alta latência na comunicação entre AP e Controladora;
    6. Elevado número de reinicializações dos APs;
14. Através de análise de fatores dinâmicos e estáticos que influenciam o comportamento da rede, a solução deve fornecer recomendações de configurações que melhoram a experiência do usuário e aprimoram o desempenho da rede.
15. Cada recomendação deve apresentar descrição detalhada, contendo horário de criação, nível de prioridade, justificativa da recomendação e possíveis impactos de sua aplicação.
16. Deve possuir solução inteligente de gerenciamento de recursos de rádio (*RRM – Radio Resource Management*), a fim de reduzir ao máximo a interferência co-canal.
    1. A solução deve analisar continuamente as condições da rede e informar via recomendação sempre que houver uma oportunidade para melhorar o ambiente de RF. A recomendação de RRM deve considerar os parâmetros de canal, canalização e potência de rádio.
    2. Deve ser possível aceitar ou recusar a recomendação. Em caso de aceite, deve ser possível agendamento do horário de execução. A aplicação da recomendação dever ser executada diretamente pela solução de análise, sem necessitar que o administrador de rede tenha que fazer qualquer configuração na controladora WLAN.
    3. Para cada recomendação, antes de seu aceite, deve ser possível visualizar quais alterações de canal, canalização e potência de rádio serão executadas em cada AP.
17. Deve fornecer informações sobre a saúde da rede através de indicadores de desempenho, que permitam analisar o comportamento da rede em linha de tempo. A linha de tempo deve permitir filtrar as últimas 24 horas, última semana, últimos 30 dias e customização de período com os últimos 90 dias. Deve apresentar no mínimo os seguintes indicadores:
    1. Conexões realizadas com sucesso e conexões com falha;

2. Tempo para se conectar;
3. Porcentagem de autenticações 802.11 realizadas com sucesso;
4. Porcentagem de associações 802.11 realizadas com sucesso;
5. Porcentagem de tentativas EAP (4-way handshake) completadas com sucesso;
6. Porcentagem de tentativas de autenticação Radius realizadas com sucesso;
7. Porcentagem de tentativas de DHCP realizadas com sucesso;
8. Porcentagem de tentativas de Roaming realizadas com sucesso;
9. *Throughput* estimado de *downlink* para os clientes wi-fi;
10. Porcentagem dos usuários com nível de sinal (RSS) dentro de SLA definido. Por exemplo, mostrar a porcentagem de usuários com nível de sinal melhor do que -75dBm.

18. Deve monitorar e analisar alterações nos indicadores de desempenho da rede devido à alterações das configurações ou atualizações de firmware. Deve permitir a comparação dos indicadores antes e depois das alterações, e listar todas as alterações que foram realizadas na solução wi-fi entre esses dois períodos.
19. Deve proporcionar mecanismos de validação de serviço na rede, permitindo emular a conexão fim-à-fim de um cliente wi-fi em determinada WLAN. Devem ser analisados os parâmetros de EAP, Radius, Ping, DNS, Traceroute, DHCP, testes de velocidade e também validar a conexão via RF.
20. Os testes de validação de serviço, principalmente de validação de conexão via RF, podem ser realizados com os próprios Pontos de Acesso emulando clientes wi-fi ou com probes/sensores adicionais. No caso de utilização de probes/sensores extras, estes devem ser fornecidos junto com a solução de Análise e Visibilidade de Rede, e na quantidade de 1 sensor para cada 2 pontos de acesso.
21. Deve realizar testes para avaliar a qualidade de uma vídeo-chamada na rede wi-fi para pelo menos a plataforma Zoom;
22. Deve possuir mecanismos para investigação detalhada do processo de conexão para usuário individualmente, através do endereço MAC, IP ou nome do usuário. A solução deve permitir definir o período de tempo a ser investigado. Para o período definido, devem ser apresentadas as conexões com sucesso, causa de falhas, desconexões, roamings, qualidade do sinal e os incidentes relacionados com o usuário.
23. Deve gerar de relatórios dos seguintes tipos:
    1. Informações com status dos APs, modelos e versões de firmware;
    2. Informações com status dos switches, portas, modelos e versões de firmware;
    3. Informações das WLAN;
    4. Listagem de APs conectados, com histórico de usuários conectados e volume de tráfego por AP;
    5. Informação de utilização de *airtime* (rx, tx, interferências) nas bandas de 2.4GHz, 5GHz e 6GHz.
    6. Listagem das principais aplicações em uso por quantidade de usuários e por volume de tráfego.
    7. Listagem de clientes, sistema operacional e fabricante dos dispositivos;
24. Deve suportar a criação de relatórios customizados.
25. Deve possuir retenção de dados de pelo menos 90 dias para gerar relatórios;
26. Deve permitir que os relatórios sejam convertidos em arquivos pdf e csv;

27. A solução ofertada deve suportar a capacidade de monitorar simultaneamente, no mínimo, 2.000 (dois mil) pontos de acesso, 400 (quatrocentos) switches e 2 (dois) controladores de rede;

5.2. **LICENÇA OU SERVIÇO DE ASSINATURA**

1. Deve adicionar licença de uso para cada ativo (ponto de acesso ou switch) monitorado no item Solução de Análise e Visibilidade da Rede.
2. Deve permitir expansão de ativos monitorados em incrementos unitários, permitindo aquisição de licenças para o número exato de ativos monitorados.
3. Deve ter validade de no mínimo 5 anos, incluindo suporte do fabricante.

5.3. **ESPECIFICAÇÕES DE SEGURANÇA DE ACESSO**

1. Deverá ser do mesmo fabricante dos controladores WLAN e Pontos de Acesso, visando garantir a interoperabilidade entre as soluções.
2. Deve ser fornecido para instalação em ambiente virtualizado VMware 5.5 ou superior ou Hyper-V versão 2012 ou superior.
3. Deve vir licenciado para permitir o cadastramento de, no mínimo de 1000 (mil) usuários visitantes simultâneos, com capacidade de expansão futura para, no mínimo, 20000 (vinte mil) usuários.
4. A solução deve suportar clusterização no modo ativo/ativo ou ativo/passivo para prover resiliência e alta disponibilidade. Permitir a criação de páginas personalizadas para o captive portal, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos clientes.
5. Deve suportar autenticação de usuários através de redes sociais suportando, no mínimo, integração com Facebook, LinkedIn e Google.
6. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo visitante e em caso de autosserviço, especificando quais informações cadastrais dos visitantes são requisitadas.
7. Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login.
8. Deve implementar um portal web seguro (HTTPS) a ser apresentado automaticamente aos usuários temporários durante o início de sua conexão com a rede.
9. Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail ou impressão local.
10. O portal de autenticação deve ser suportado, no mínimo, pelos seguintes navegadores de Internet: Microsoft Internet Explorer, Mozila Firefox, Safari e Chrome, operando em PCs e dispositivos móveis.
11. Permitir a automatização do processo de conexão segura à rede sem fio através da instalação automática de certificado digital e configuração de perfil de rede sem fio em dispositivos móveis.
12. A solução deve provisionar automaticamente um certificado digital para o dispositivo cadastrado e configurar o dispositivo com o certificado gerado e com as configurações de rede sem fio para que o usuário utilize autenticação segura via 802.1X na rede corporativa.
13. A solução deve identificar automaticamente o tipo de dispositivo cadastrado e conectado à rede para provisionar o certificado digital e configurar o perfil da rede sem

fio conforme o sistema operacional utilizado e deverá suportar, no mínimo, os seguintes sistemas operacionais: Apple iOS, Windows, Mac OSx e Android.

14. A solução deve guiar/instruir o usuário durante o procedimento de instalação do certificado digital e configuração do perfil da rede sem fio através de página web ou através de aplicativo.
15. Após a finalização do processo de autosserviço e configuração do suplicante, a solução deve desconectar o dispositivo do usuário da rede visitante (captive portal) e conectá-lo automaticamente na rede corporativa com autenticação 802.1X em dispositivos que suportem tal ação.
16. A solução deve instalar os certificados digitais através de CA (Certification Authority) interna na ferramenta (certificado digital auto assinado) e também permitir a utilização de certificados digitais de CA externas (Root CA do Active Directory, por exemplo).
17. A solução deve suportar autenticação de usuários via integração direta com Microsoft Active Directory, LDAP, SAML 2.0 e base de usuários local.
18. Deve suportar autenticação PEAP com um servidor RADIUS embutido.
19. Possuir capacidade de autenticação dos usuários visitantes através de senhas pré cadastradas ou vouchers, para cada usuário ou grupo de usuários, no caso de utilização em eventos.
20. Permitir a configuração do número máximo de conexões simultâneas realizadas por uma mesma conta, possibilitando que um usuário possua mais de um dispositivo na rede com a mesma senha e que contas coletivas sejam utilizadas em eventos. Esta funcionalidade deve ser aplicada para usuários visitantes autenticados pelo captive portal.
21. Deve oferecer visibilidade e controle sobre dispositivos na rede com a possibilidade de revogar o acesso.
22. Realizar verificação de postura dos dispositivos quando os mesmos se associam pela primeira vez, incluindo checagem de antivírus, configurações de registro, patches, proxy, firewall, entre outros, com a possibilidade de remediação.
23. Deve permitir a criação de conjunto de chaves PSK privadas (PPSK, DPSK, MPSK ou similar), para serem associadas individualmente para cada usuário. Essas chaves devem ser criadas na própria solução, ou seja, sendo externas à controladora WLAN.
24. Deve suportar OCSP (Online Certificate Status Protocol) com revogação automática.
25. Deve suportar integração com OAuth 2.0 e SAML 2.0 para autenticação externa.
26. Deve prover REST APIs para permitir integração com soluções de terceiros.
27. Deve suportar Radius CoA (Change of Authorization) para o servidor RADIUS interno.
28. O servidor Radius interno deve suportar RadSec, e deve ser possível visualizar os logs de autenticação do Radius.
29. Disponibilizar servidor SMTP interno ou possibilitar a configuração de servidor SMTP externo para envio de e-mails.
30. Deve ser possível solicitar ao usuário visitante, no passo de autenticação, a inserção do e-mail da pessoa responsável por aprovar o seu acesso à rede, sendo que essa pessoa se encarregará por aprovar ou rejeitar a requisição uma vez que o sistema a notifique via e-mail.

6. CONTROLADOR DE REDE SEM FIO - WLAN

6.1. ESPECIFICAÇÕES GERAIS

1. Deverá ser do mesmo fabricante dos pontos de acesso fornecidos pela CONTRATADA, para fins de compatibilidade e gerenciamento;
2. O hardware e o software deverão ser do mesmo fabricante para garantir desempenho e confiabilidade da solução.
3. Deve possuir hardware dedicado com software de gerenciamento e administração já embarcado.
4. Não serão aceitas soluções baseadas nas premissas de computação virtual sem hardware dedicado, controladores baseados em computação em nuvem ou controladores agregados a outros equipamentos, tais como Firewalls ou Roteadores.
5. Deve possuir fonte de alimentação com seleção automática de tensão (100-240V AC).
6. Deve possuir porta de console para gerenciamento e configuração via linha de comando com conector RJ-45 ou RS-232 ou USB.
7. Deve possuir, no mínimo, 04 (quatro) portas do tipo 1000BASE-T com conectores RJ-45 e 04 (quatro) portas do tipo 10 GbE BASE-X compatíveis com transceivers SFP+.
8. Deve acompanhar 1 cabo do tipo DAC sfp+ para sfp+ de pelo menos 1 mt de comprimento.
9. Deve disponibilizar todos os acessórios necessários para fixação em rack padrão de 19 (dezenove) polegadas em 1RU de espaço.
10. Deve suportar temperatura de operação entre 0°C e 40°C.
11. Deve possuir sistema de ventilação interno redundante.
12. Deve ter disponível LEDs indicando o estado de operação do equipamento, do disco e das portas ethernet.
13. Deverá possuir a funcionalidade de operar como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores e expansível até 4 (quatro) controladores.
14. Deve vir acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, acessórios, cabo de energia elétrica, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução.
15. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax/be
16. Deverá ter a capacidade para gerenciar, no mínimo, 1.020 (mil e vinte) Pontos de Acesso simultâneos. S
17. Deve suportar, no mínimo, 24.000 (vinte e quatro mil) dispositivos simultâneos

6.2. **GERENCIAMENTO**

1. Deve prover o gerenciamento centralizado dos Pontos de Acesso
2. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Subredes pré-configuradas
3. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF) O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;
4. Deve possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP; Implementar MIB

privativa que forneça informações relativas ao funcionamento do equipamento. Permitir a visualização de alertas da rede em tempo real;

5. Implementar, no mínimo, dois níveis de acesso administrativo ao equipamento (apenas leitura e leitura/escrita) protegidos por senhas independentes.
6. Deve permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador. Permitir a configuração e gerenciamento através de navegador padrão (HTTPS);
7. Deve gerenciar de forma centralizada a autenticação de usuários. Deverá possuir base de dados de usuários interna com suporte a até 24 (vinte e quatro) mil usuários.
8. Deve permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS).
9. Deve permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;
10. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:
    1. 24 horas por dia, 7 dias na semana;
    2. Agendamento customizado permitindo escolher os dias da semana e horários;
    3. Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00;
11. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível;
12. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede;
13. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP;
14. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede wireless;
15. Monitorar o desempenho da rede wireless, permitindo a visualização de informações de cada ponto de acesso;
16. Implementar cluster de controladores WLAN no modo ativo/ativo, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability);
17. Deverá efetuar compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster;
18. Deverá em caso de falha realizar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede;
19. Deverá possuir a capacidade de geração de informações ou relatórios de no mínimo os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;
20. Deverá suportar a identificação de aplicações dos clientes conectados ao ponto de acesso com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações;
21. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;

22. Deverá possibilitar a importação de plantas baixas nos formatos .dwg ou .jpg ou .png, devendo permitir a visualização dos Pontos de Acesso instalados, com seu estado de funcionamento;
23. Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio;
24. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados;
25. A solução deve suportar a adição de um serviço de SMS externo, tal como Twilio.

6.3. **REDE**

1. Deverá implementar suporte aos protocolos IPv4 e IPv6;
2. Deverá suportar tagging de VLANs; Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x;
3. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação.
4. Deverá suportar, no mínimo, 2.000 (dois mil) SSIDs simultâneos no cluster.
5. Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fios devem continuar conectados com acesso à rede.
6. Deve permitir que novos usuários se associem à rede sem fios utilizando autenticação do tipo 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.
7. Deve ser possível evitar que dispositivos 802.11b se conectem a rede, visando melhorar o desempenho da rede sem fio. Deve suportar 802.11d e 802.11k.
8. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz e 5 GHz, bem como na interface LAN.

6.4. **SEGURANÇA**

1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);
2. Implementar, pelo menos, os seguintes padrões de segurança wireless:
    1. Wi-Fi Protected Access (WPA);
    2. Wi-Fi Protected Access 2 (WPA2);
    3. Temporal Key Integrity Protocol (TKIP);
    4. Advanced Encryption Standard (AES);
    5. Dynamic PSK;
    6. IEEE 802.1x;
    7. IEEE 802.11i;
    8. IEEE 802.11w.
3. Implementar, pelo menos, os seguintes controles/filtros:

1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;
2. Baseado em endereço IP;
3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;
4. Baseado em porta de origem e/ou destino;
5. Baseado em tipo ou sistema operacional do dispositivo;

4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:
    1. MAC Address;
    2. Autenticação Local;
    3. Captive Portal;
    4. Active Directory;
    5. RADIUS;
    6. IEEE 802.1x;
    7. LDAP.
5. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID
6. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.
7. A solução deverá suportar a criação de uma zona de visitantes, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso a rede wireless.
8. O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote).
9. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável.
10. Deve permitir que o portal interno para usuários visitantes (guest) seja customizável, bem como ser compatível com o idioma português.
11. Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede.
12. Deverá permitir enviar a senha de usuários visitantes (guests), por e-mail ou por SMS.
13. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa.
14. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subnet, sendo possível adicionar exceções com base em endereços MAC e IP.
15. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0
16. Implementar, mecanismos para detecção de pontos de acesso do tipo rogue com informações de, no mínimo:
    1. SSID-Spoofing – APs não pertencentes ao controlador propagando o mesmo SSID;
    2. MAC Spoofing – APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido;

3. Rogue APs – APs não pertencentes ao controlador;
4. Same Network – APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;

17. Deve implementar varredura de RF para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues);
18. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;
19. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;

6.5. **RECURSOS DE GERENCIAMENTO AUTOMÁTICO DE RÁDIO FREQUÊNCIA (RF)**

1. Na ocorrência de inoperância de um Ponto de Acesso, o controlador WLAN deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;
2. Deve ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
3. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar o desempenho. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso.
4. Deverá permitir que o serviço wireless seja desabilitado de determinado ponto de acesso.
5. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado.

6.6. **RECURSOS DE CONVERGÊNCIA E MULTIMÍDIA**

1. Deve suportar 802.11e.
2. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;
3. Deverá permitir a configuração de prioridade de um determinado SSID sobre os outros SSID's.
4. Deve acompanhar suporte do fabricante por 5 (cinco) anos.

7. **RACK E INSTALAÇÃO**

1. Padrão 19"
2. Deve possuir altura mínima de 42U's, profundidade mínima de 600mm e largura mínima de 600mm;
3. Deve ser fornecido com 2 ventiladores, kit rodizio e pés niveladores;
4. Deve possuir entrada e saída de cabos pelo teto ou pela base do rack;
5. Deve possuir longarinas ajustáveis em profundidade, confeccionado em aço com perfurações de ½ em ½ Us e demarcações das unidades de altura, permitindo a instalação de equipamentos de rede e bandejas padrão 19";
6. Deve possuir porta frontal em vidro, que permita a visualização dos equipamentos e infraestrutura instalada. Esta porta deve ser removível, reversível e possuir fechadura;

7. Deve possuir porta traseira lisa em aço com fechadura;
8. Capacidade de carga estática de 600kg;
9. Deve possuir tampas laterais removíveis com sistema de encaixe e desencaixe rápido, sem o uso de ferramentas e perfuração preparada para instalação de fechadura tipo cilindro;
10. Todas as portas e a estrutura interna devem possuir ponto de aterramento;
11. Deve ser fornecido na cor preta com espessura mínima de chapa 1.2mm;
12. O rack deve ser fornecido desmontado, possibilitando o fácil transporte e permitindo que a montagem seja feita em qualquer local.

[assinado eletronicamente]

EMERSON MORERIRA DE MORAIS

Coordenador de Infraestrutura da Informação

Documento assinado eletronicamente por **Emerson Moreira de Morais**, **Coordenador de Infraestrutura da Informação**, em 14/02/2025, às 14:30, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site https://sei.mi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **5630320** e o código CRC **FCEF545B**.

Criado por bruno.freire, versão 2 por bruno.freire em 13/02/2025 13:31:47.