REQUISITOS TÉCNICOS

OBJETO

Aquisição de equipamentos para rede lógica e rede sem fio institucional, em atendimento ao PDTI UFSM 2012-2013, objetivo cinco, metas 16 e 18.

JUSTIFICATIVA

Implementar a infraestrutura de rede sem fio institucional da Universidade, e modernizar e ampliar a rele lógica para atender às demandas de TI da instituição, tais como: conectividade, acesso à internet, mobilidade e aulas em campo. Em atendimento ao PDTI UFSM 2012-2013, objetivo 5, metas 16 e 18.

ESPECIFICAÇÕES TÉCNICAS DETALHADAS

ITEM 01 - Controlador Tipo 1 para 500 Access Points

São equipamentos com interfaces Ethernet que se conectam à rede LAN e que controlam de maneira centralizada os pontos de acesso (Access Points ou APs) instalados e ligados às redes LAN e WAN da UFSM.

O equipamento ofertado deve ser entregue com capacidade para gerenciamento de, no mínimo, cem (100) APs simultaneamente, com capacidade de ampliação, por meio de expansão, para pelo menos quinhentos (500) APs.

O Controlador deve executar o controle, configuração e gerência dos APs indoor ou outdoor, bem como otimizar o desempenho e a cobertura da radiofrequência (RF) oferecida pela solução.

O Controlador deve apresentar as seguintes características:

- Suporte a alta disponibilidade, com utilização de equipamentos redundantes ou configuração em cluster, de forma a manter o serviço e todos os APs ativos caso um dos controladores falhe por qualquer motivo;
- Possibilitar a implantação de um esquema de redundância tipo 1+1 ou N+1, ou seja, independente do número de controladores necessário para atender a especificação um controlador deve ser suficiente para prover a redundância em caso de falha;
- Deve possuir, no mínimo, 08 interfaces 1000BASE-X, aceitando transceivers tipo SFP padrão SX, LX e T. Deve acompanhar três transceivers 1000BASE-T, conector RJ45, suportando padrão Gigabit Ethernet para cabos UTP;
- Deve permitir o tráfego IP, multicast e ipv6 através do Controlador (LAYER 2 OSI). O Controlador poderá estar diretamente e/ou remotamente conectado aos APs por ele gerenciados, inclusive via roteamento em LAYER 3 do modelo OSI;
- Deve realizar o gerenciamento das capacidades específicas de RF incluindo:
    - Ajuste dinâmico de canais IEEE 802.11 para otimizar a cobertura de rede e mudar as condições RF baseado em desempenho;
    - Detecção de interferência e reajuste dos parâmetros de RF evitando problemas de cobertura e desempenho;

- Permitir balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar o desempenho durante elevada utilização da rede;
- Controle dinâmico de potência, ajustando dinamicamente a saída de potência dos pontos de acesso individualmente para acomodar as condições de alterações da rede;
- Ajustar dinamicamente o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo desempenho e escalabilidade;
- Em eventos de falha de um AP, o controlador deve automaticamente ajustar a potência dos pontos de acesso adjacentes para dar cobertura de área onde o AP que falhou estava provendo o sinal;
- Gerenciamento automatizado de RF e potência, ou seja, os elementos da solução (Controlador + APs) devem definir, sem intervenção manual, os parâmetros de potência de transmissão e ajuste de canal de frequência, evitando interferências e sobreposição de canais;

- Deve ser capaz de operar em modo de "tráfego centralizado" (mesh) e de "chaveamento de tráfego local" (no-mesh), simultaneamente, nos padrões 802.11a/b/g/n.
  - No modo de operação de "tráfego centralizado" (mesh), o tráfego de dados gerado pelos usuários associados aos APs deve passar através do controlador ("ativo" ou "redundante"). O tráfego de controle dos APs deve ser enviado para o controlador.
  - Operando no modo de "chaveamento de tráfego local" (não-mesh), o controlador deve:
    - No caso de falha na comunicação lógica entre os APs da localidade com o controlador, ou com o Sistema de Autenticação Centralizado dos usuários, ou em caso de falha no link WAN (ou LAN) que realize a conexão lógica dos APs com o controlador, os usuários já associados aos pontos de acesso da localidade devem continuar a ter acesso à rede local. Deve ser possível fazer com que novos usuários se autentiquem se associem de forma alternativa à rede local sem qualquer prejuízo de acesso local. Os usuários também devem continuar realizando roaming entre os APs locais.
  - A rede sem fio local não pode se tornar inoperante devido à ocorrência de qualquer uma das três falhas isoladas ou simultâneas: falha no controlador, falha no Sistema de Autenticação Centralizado ou falha nos links de comunicação entre os pontos de acesso e o controlador (WAN ou LAN).
  - Caso a solução proposta não atenda os itens anteriores, a CONTRATADA deverá fornecer uma solução alternativa de redundância e autenticação para pontos de acesso operando com "chaveamento de tráfego local" para, pelo menos, cada uma das localidades que serão atendidas. A solução alternativa deverá ter capacidade de controlar, no mínimo e simultaneamente, 25 (vinte e cinco) pontos de acesso do mesmo fabricante operando com "chaveamento de tráfego local" e seus custos deverão ser inseridos neste item.

- Se o controlador falhar, os APs relacionados deverão poder se associar a um Controlador secundário de forma automática;

- O controlador deve ser fornecido com todos os recursos e licenças necessárias para implementar mecanismos de detecção, localização e contenção de:
    - Clientes invasores do tipo “Rogue Client”;
    - Pontos de Acesso não autorizados (rogues):
        - A detecção deve ser feita de forma contínua, integrada e automática, classificando-os como conhecido, malicioso ou não classificado;
        - Deve ser permitido ajustar um nível de sinal mínimo (RSSI) para que o ponto de acesso vizinho (rogue) seja detectado como ponto de acesso não autorizado;
    - Ataques “Denial of Service (DoS)” dos seguintes tipos, no mínimo:
        - “Association flood or storm”;
        - “Authentication flood or storm”;
        - “EAPOL Start”;
        - “EAPOL Logoff”;
        - “Deauthentication flood or storm”;
        - “Disassociation flood or storm”;
    - Ataques “Security Penetration Attacks” no mínimo dos seguintes tipos:
        - Detecção de “NetStumbler”;
        - Detecção de “Wellenreiter”;
        - Detecção de “Fake APs”;
- O controlador deve ser fornecido com todos os recursos e licenças necessárias para detectar, identificar, classificar, quantificar e mitigar interferências no meio de rádio frequência que não são wi-fi, tais como bluetooth, jammers, câmeras wireless, fornos microondas, telefones sem fio, APs em canais invertidos, entre outros, que impactem diretamente no funcionamento da rede em menos de 10 minutos.
- Deve implementar mecanismos de controle de associação de banda, de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do AP, quando os mesmos se associam à rede sem fio;
- 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;
- Deve possuir mecanismo de otimização automática de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast. Este mecanismo deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes mesmo que está não seja o “rate” mandatório;
- Deve implementar os padrões IEEE 802.11h e IEEE 802.11i e wireless mesh;
- Deve implementar o mapeamento de Diffserv/DSCP ou 802.1p em QoS nos protocolos de Wireless 802.11e e WMM;

- Deve prover suporte a mobilidade dos usuários em redes nas camadas 2 e 3 do modelo OSI, com suporte a IGMP Snooping, SNTP ou NTP, DHCP Relay;
- Deve possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real tais como: VoIP, Web Casting, videoconferência (VC) e etc.;
- Deve implementar os protocolos IEEE 802.1q (VLAN) e IEEE 802.11e;
- Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento;
- Deve permitir administração e gerência através de navegador padrão (HTTP/HTTPS), SSH, Telnet e interface console;
- O controlador WiFi deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes, temporários ou clientes corporativos;
- Deve garantir 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;
- Deve permitir a gravação de eventos em log interno e externo (Syslog);
- Deve implementar, no mínimo, SNMP v2c, incluindo a geração de traps;
- Deve possuir, no mínimo, suporte a MIB II, conforme RFC 1213;
- Deve possuir, no mínimo, indicadores luminosos (LED) para a indicação do status das interfaces e atividade;
- Deve ser fornecido em gabinete padrão e com todos os acessórios necessários para montagem em RACK de 19 (dezenove) polegadas e altura máxima de 2U (unidade de altura de RACK);
- Deve permitir configuração de política de segurança para grupos de usuários de acordo com seu perfil;
- Deve implementar, através do sistema de gerência única, a localização de usuário de forma integrada, com a possibilidade de utilizar filtros baseado em endereços MAC ou IP;
- Deve implementar o protocolo IEEE 802.1x, com pelo menos os seguintes métodos EAP: PEAP-Microsoft© Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2), EAP-Transport Layer Security (EAP-TLS);
- Deve implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
- Deve implementar tunelamento do tráfego entre o Controlador e os respectivos APs gerenciados;
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- O controlador deve poder operar com os padrões IEEE 802.11a/b/g/n;
- Deve implementar gerenciamento de políticas de segurança de usuários ou grupos de usuários wireless, incluindo:
    - Segurança acima da camada 3 do modelo OSI – Autenticação WEB (Portal);
    - Listas de controle de acesso (ACLs) – restrições de IP, tipos de protocolos e portas;

    - Autenticação, Autorização e Accounting (AAA) em servidor RADIUS. Permitindo gerenciamento de direitos e políticas de segurança de sessão por usuário;
    - Gerenciar chaves de criptografia WPA v1 e v2 dos Access Points;
    - Gerenciar chaves de criptografia WEP (40 e 128 bits), TKIP e AES dos APs;
    - Gerenciar chaves de criptografia WPA2 dos APs;
- Deve permitir a atualização automática ou manual de firmware dos APs;
- Deve implementar, no mínimo, 16 (dezesseis) domínios de mobilidade, para o mesmo padrão wireless 802.11, permitindo configurações distintas de autenticação, QoS, criptografia, SSID e VLAN para cada domínio. Deve ser possível especificar em quais APs/Grupo de APs cada domínio será aplicado;
- Cada Controlador deve suportar, no mínimo, seis mil (6.000) usuários wireless simultâneos;
- Deve permitir realizar a autenticação baseada em WEB, liberando acesso de acordo com o perfil do usuário e fornecendo informações para a tarifação e controle de acesso;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com seleção automática em 60Hz;
- Deve permitir a instalação de fonte de alimentação interna redundante.
- Deve ser fornecido com todas as licenças necessárias para permitir a criptografia das informações, assim como a proteção dos dados dos usuários móveis e remotos;
- Deve controlar APs de uso interno “indoor” e de uso externo “outdoor” em wireless mesh. Devem acompanhar licenças para habilitar tais funcionalidades para a quantidade total de pontos de acesso suportados pela controladora;
- Deve permitir o gerenciamento de APs 802.11a/b/g/n, em qualquer quantidade, até o limite de suporte de pontos de acesso do equipamento.
- Deve permitir a adição de APs que implementem análise de espectro, em hardware dedicado a esta finalidade, sem impacto no tráfego de rede dos clientes. A solução como um todo deve permitir o gerenciamento mais apurado no cenário RF, auxiliando assim na mitigação de interferências, possibilitando ações que devam ser tomadas para troubleshooting.
- Quando necessário, o controlador deve possuir, em conjunto com APs específicos para tal, modo de operação de analisador de espectro, acessível remotamente, para análise e captura de dados brutos da condição do espectro.
- Deve operar com APs remotos, mesmo acessado por NAT, através de túnel criptografado (VPN ou semelhante). Desta forma, é possível definir o IP público do controlador e fazer com que pontos de acesso remotos conectem-se automaticamente ao controlador através da Internet. Em caso de falha na comunicação entre controladora e ponto de acesso, o ponto de acesso deve continuar sua operação de transferência de dados aos clientes já conectados e aceitação de novos usuários sem ônus para a rede wireless local.

ITEM 02 - Controlador Tipo 2 para 50 Access Points

São equipamentos com interfaces Ethernet que se conectam à rede LAN e que controlam de maneira centralizada os pontos de acesso (Access Points ou APs) instalados e ligados às redes LAN e WAN da UFSM.

O equipamento ofertado deve ser entregue com capacidade para gerenciamento de, no mínimo, cinco (5) APs simultaneamente, com capacidade de ampliação, por meio de expansão, para pelo menos cinquenta (50) APs.

O Controlador deve executar o controle, configuração e gerência dos APs indoor ou outdoor, bem como otimizar o desempenho e a cobertura da radiofrequência (RF) oferecida pela solução.

O Controlador deve apresentar as seguintes características:

- Suporte a alta disponibilidade, com utilização de equipamentos redundantes ou configuração em cluster, de forma a manter o serviço e todos os APs ativos caso um dos controladores falhe por qualquer motivo;
- Possibilitar a implantação de um esquema de redundância tipo 1+1 ou N+1, ou seja, independente do número de controladores necessário para atender a especificação um controlador deve ser suficiente para prover a redundância em caso de falha;
- Deve possuir, no mínimo, 04 interfaces 1000BASE-T, conector RJ45, suportando padrão Gigabit Ethernet para cabos UTP;
- Deve permitir o tráfego IP, multicast e ipv6 através do Controlador (LAYER 2 OSI). O Controlador poderá estar diretamente e/ou remotamente conectado aos APs por ele gerenciados, inclusive via roteamento em LAYER 3 do modelo OSI;
- Deve realizar o gerenciamento das capacidades específicas de RF incluindo:
    - Ajuste dinâmico de canais IEEE 802.11 para otimizar a cobertura de rede e mudar as condições RF baseado em desempenho;
    - Detecção de interferência e reajuste dos parâmetros de RF evitando problemas de cobertura e desempenho;
    - Permitir balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar o desempenho durante elevada utilização da rede;
    - Controle dinâmico de potência, ajustando dinamicamente a saída de potência dos pontos de acesso individualmente para acomodar as condições de alterações da rede;
    - Ajustar dinamicamente o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo desempenho e escalabilidade;
    - Em eventos de falha de um AP, o controlador deve automaticamente ajustar a potência dos pontos de acesso adjacentes para dar cobertura de área onde o AP que falhou estava provendo o sinal;
    - Gerenciamento automatizado de RF e potência, ou seja, os elementos da solução (Controlador + APs) devem definir, sem intervenção manual, os parâmetros de potência de transmissão e ajuste de canal de frequência, evitando interferências e sobreposição de canais;
- Deve ser capaz de operar em modo de “tráfego centralizado” (mesh) e de “chaveamento de tráfego local” (no-mesh), simultaneamente, nos padrões 802.11a/b/g/n.
    - No modo de operação de “tráfego centralizado” (mesh), o tráfego de dados gerado pelos usuários associados aos APs deve passar através do controlador (“ativo” ou “redundante”). O tráfego de controle dos APs deve ser enviado para o controlador.

- Operando no modo de “chaveamento de tráfego local” (não-mesh), o controlador deve:
  - No caso de falha na comunicação lógica entre os APs da localidade com o controlador, ou com o Sistema de Autenticação Centralizado dos usuários, ou em caso de falha no link WAN (ou LAN) que realize a conexão lógica dos APs com o controlador, os usuários já associados aos pontos de acesso da localidade devem continuar a ter acesso à rede local. Deve ser possível fazer com que novos usuários se autentiquem se associem de forma alternativa à rede local sem qualquer prejuízo de acesso local. Os usuários também devem continuar realizando roaming entre os APs locais.
- A rede sem fio local não pode se tornar inoperante devido à ocorrência de qualquer uma das três falhas isoladas ou simultâneas: falha no controlador, falha no Sistema de Autenticação Centralizado ou falha nos links de comunicação entre os pontos de acesso e o controlador (WAN ou LAN).
- Caso a solução proposta não atenda os itens anteriores, a CONTRATADA deverá fornecer uma solução alternativa de redundância e autenticação para pontos de acesso operando com “chaveamento de tráfego local” para, pelo menos, cada uma das localidades que serão atendidas. A solução alternativa deverá ter capacidade de controlar, no mínimo e simultaneamente, 25 (vinte e cinco) pontos de acesso do mesmo fabricante operando com “chaveamento de tráfego local” e seus custos deverão ser inseridos neste item.

- Se o controlador falhar, os APs relacionados deverão poder se associar a um Controlador secundário de forma automática;
- O controlador deve ser fornecido com todos os recursos e licenças necessárias para implementar mecanismos de detecção, localização e contenção de:
  - Clientes invasores do tipo “Rogue Client”;
  - Pontos de Acesso não autorizados (rogues):
    - A detecção deve ser feita de forma contínua, integrada e automática, classificando-os como conhecido, malicioso ou não classificado;
    - Deve ser permitido ajustar um nível de sinal mínimo (RSSI) para que o ponto de acesso vizinho (rogue) seja detectado como ponto de acesso não autorizado;
  - Ataques “Denial of Service (DoS)” dos seguintes tipos, no mínimo:
    - “Association flood or storm”;
    - “Authentication flood or storm”;
    - “EAPOL Start”;
    - “EAPOL Logoff”;
    - “Deauthentication flood or storm”;
    - “Disassociation flood or storm”;
  - Ataques “Security Penetration Attacks” no mínimo dos seguintes tipos:
    - Detecção de “NetStumbler”;

    - Detecção de “Wellenreiter”;
    - Detecção de “Fake APs”;
- O controlador deve ser fornecido com todos os recursos e licenças necessárias para detectar, identificar, classificar, quantificar e mitigar interferências no meio de rádio frequência que não são wi-fi, tais como bluetooth, jammers, câmeras wireless, fornos microondas, telefones sem fio, APs em canais invertidos, entre outros, que impactem diretamente no funcionamento da rede em menos de 10 minutos.
- Deve implementar mecanismos de controle de associação de banda, de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do AP, quando os mesmos se associam à rede sem fio;
- 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;
- Deve possuir mecanismo de otimização automática de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast. Este mecanismo deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes mesmo que está não seja o “rate” mandatório;
- Deve implementar os padrões IEEE 802.11h e IEEE 802.11i e wireless mesh;
- Deve implementar o mapeamento de Diffserv/DSCP ou 802.1p em QoS nos protocolos de Wireless 802.11e e WMM;
- Deve prover suporte a mobilidade dos usuários em redes nas camadas 2 e 3 do modelo OSI, com suporte a IGMP Snooping, SNTP ou NTP, DHCP Relay;
- Deve possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real tais como: VoIP, Web Casting, videoconferência (VC) e etc.;
- Deve implementar os protocolos IEEE 802.1q (VLAN) e IEEE 802.11e;
- Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento;
- Deve permitir administração e gerência através de navegador padrão (HTTP/HTTPS), SSH, Telnet e interface console;
- O controlador WiFi deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes, temporários ou clientes corporativos;
- Deve garantir 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;
- Deve permitir a gravação de eventos em log interno e externo (Syslog);
- Deve implementar, no mínimo, SNMP v2c, incluindo a geração de traps;
- Deve possuir, no mínimo, suporte a MIB II, conforme RFC 1213;
- Deve possuir, no mínimo, indicadores luminosos (LED) para a indicação do status das interfaces e atividade;

- Deve ser fornecido em gabinete padrão e com todos os acessórios necessários para montagem em RACK de 19 (dezenove) polegadas e altura máxima de 2U (unidade de altura de RACK);
- Deve permitir configuração de política de segurança para grupos de usuários de acordo com seu perfil;
- Deve implementar, através do sistema de gerência única, a localização de usuário de forma integrada, com a possibilidade de utilizar filtros baseado em endereços MAC ou IP;
- Deve implementar o protocolo IEEE 802.1x, com pelo menos os seguintes métodos EAP: PEAP-Microsoft© Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2), EAP-Transport Layer Security (EAP-TLS);
- Deve implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
- Deve implementar tunelamento do tráfego entre o Controlador e os respectivos APs gerenciados;
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- O controlador deve poder operar com os padrões IEEE 802.11a/b/g/n;
- Deve implementar gerenciamento de políticas de segurança de usuários ou grupos de usuários wireless, incluindo:
    - Segurança acima da camada 3 do modelo OSI – Autenticação WEB (Portal);
    - Listas de controle de acesso (ACLs) – restrições de IP, tipos de protocolos e portas;
    - Autenticação, Autorização e Accounting (AAA) em servidor RADIUS. Permitindo gerenciamento de direitos e políticas de segurança de sessão por usuário;
    - Gerenciar chaves de criptografia WPA v1 e v2 dos Access Points;
    - Gerenciar chaves de criptografia WEP (40 e 128 bits), TKIP e AES dos APs;
    - Gerenciar chaves de criptografia WPA2 dos APs;
- Deve permitir a atualização automática ou manual de firmware dos APs;
- Deve implementar, no mínimo, 16 (dezesseis) domínios de mobilidade, para o mesmo padrão wireless 802.11, permitindo configurações distintas de autenticação, QoS, criptografia, SSID e VLAN para cada domínio. Deve ser possível especificar em quais APs/Grupo de APs cada domínio será aplicado;
- Cada Controlador deve suportar, no mínimo, quinhentos (500) usuários wireless simultâneos;
- Deve permitir realizar a autenticação baseada em WEB, liberando acesso de acordo com o perfil do usuário e fornecendo informações para a tarifação e controle de acesso;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com seleção automática em 60Hz;
- Deve permitir a instalação de fonte de alimentação interna redundante.

- Deve ser fornecido com todas as licenças necessárias para permitir a criptografia das informações, assim como a proteção dos dados dos usuários móveis e remotos;
- Deve controlar APs de uso interno “indoor” e de uso externo “outdoor” em wireless mesh. Devem acompanhar licenças para habilitar tais funcionalidades para a quantidade total de pontos de acesso suportados pela controladora;
- Deve permitir o gerenciamento de APs 802.11a/b/g/n, em qualquer quantidade, até o limite de suporte de pontos de acesso do equipamento.
- Deve permitir a adição de APs que implementem análise de espectro, em hardware dedicado a esta finalidade, sem impacto no tráfego de rede dos clientes. A solução como um todo deve permitir o gerenciamento mais apurado no cenário RF, auxiliando assim na mitigação de interferências, possibilitando ações que devam ser tomadas para troubleshooting.
- Quando necessário, o controlador deve possuir, em conjunto com APs específicos para tal, modo de operação de analisador de espectro, acessível remotamente, para análise e captura de dados brutos da condição do espectro.
- Deve operar com APs remotos, mesmo acessado por NAT, através de túnel criptografado (VPN ou semelhante). Desta forma, é possível definir o IP público do controlador e fazer com que pontos de acesso remotos conectem-se automaticamente ao controlador através da Internet. Em caso de falha na comunicação entre controladora e ponto de acesso, o ponto de acesso deve continuar sua operação de transferência de dados aos clientes já conectados e aceitação de novos usuários sem ônus para a rede wireless local.

ITEM 03 – Licença para expansão de 100 APs para controlador tipo 1

Pacote de expansão da quantidade de APs gerenciados no controlador tipo 1, até 500 APs, conforme os itens abaixo:

- Deve prover a expansão da quantidade de APs gerenciados no controlador tipo 1 em incrementos de cem (100) unidades;
- Deve adicionar o suporte para cem (100) APs ao número total de APs já suportados, respeitando o limite suportado pelo equipamento;
- A expansão deve manter para os APs adicionados todas as funcionalidades que o controlador possui para os APs previamente licenciados, para o pleno funcionamento da solução.

ITEM 04 – Licença para expansão de 25 APs para controlador tipo 2

Licença para expansão da quantidade de APs gerenciados n controlador tipo 2, até 50 APs, conforme os itens abaixo:

- Deve prover a expansão da quantidade de APs gerenciados no controlador tipo 2 em incrementos de vinte e cinco (25) unidades, através de hardware específico e/ou licença de software;;
- Deve adicionar o suporte para vinte e cinco (25) APs ao número total de APs já suportados, respeitando o limite suportado pelo equipamento;
- Deve manter para os APs adicionados todas as funcionalidades que o controlador possui para os APs previamente licenciados, para o pleno funcionamento da solução.

ITEM 05 – Sistema de gerência de rede

Sistema de gerenciamento de dispositivos LAN e WLAN, do mesmo fabricante e totalmente compatível com os equipamentos ofertados com, no mínimo, as seguintes características:

- Deve gerenciar os dispositivos de rede (switches);
- Deve possuir capacidade de gerenciamento hierárquico com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento;
- Deve implementar alta disponibilidade, ativo/standby, trabalhando com no mínimo dois servidores físicos/Virtuais. As licenças necessárias para implementar esse recurso devem estar incluídas;
- Deve suportar o gerenciamento inicial de, no mínimo, cem (100) dispositivos, sejam controladores, APs, switches ou roteadores, chegando a um total de pelo menos dez mil (10.000) dispositivos;
- Deve possuir ferramentas integradas para prever os requerimentos de RF para projeto da rede WLAN, incluindo qual o melhor local para os pontos de acesso na planta do prédio/andar, configuração e estimativa de desempenho e cobertura;
- Deve permitir ao administrador importar a planta dos andares e assinalar as características de RF dos pontos de acesso aumentando a precisão do projeto;
- Deve permitir a importação de arquivo baseado em mapas públicos gratuitos (Google Maps e Microsoft Bing) para melhor localização dos ativos espalhados em grandes áreas;
- Deve possibilitar o desenho de plantas baixas no próprio software para projeto de redes wireless;
- Deve possibilitar a importação de plantas baixas nos seguintes formatos DWG, DXF, GIF e JPEG;
- Deve realizar cálculo e definição automática da quantidade necessária e do posicionamento dos APs para que a cobertura nos padrões 802.11a, 802.11b e 802.11g desejada seja atingida, levando em consideração a banda média por usuário pretendida e a geografia do prédio (planta);
- Deve possuir ferramentas integradas para prever os requerimentos de RF para projeto da rede WiFi, incluindo qual o melhor local para os pontos de acesso na planta do prédio/andar, configuração e estimar o desempenho e a cobertura;
- Deve gerar planta de cobertura prevista e planta de cobertura real (pós-ativação) com indicação gráfica da potência média para cada local da planta baixa;
- Deve permitir o rastreamento em tempo real dos dispositivos móveis conectados na infraestrutura da rede WiFi;
- Deve implementar função de descoberta automática dos dispositivos individuais da infraestrutura wireless;
- Deve permitir visualização do mapa lógico da rede, com a representação gráfica dos equipamentos e sinalização por cor de seu estado operacional;
- Deve apresentar alertas da rede em tempo real, com indicação de severidade por cor, para APs e controladores WiFi operando em modo mesh e ponto local (não-mesh), de forma simultânea;
- Deve permitir a visualização de eventuais áreas sem cobertura de RF (coverage holes), bem como permitir ao administrador visualizar o layout da rede WLAN e monitorar o desempenho desta rede - incluindo mapa detalhado que exibe a cobertura de RF sobre os mapas com layout real dos andares;

- Deve monitorar o desempenho da rede wireless, consolidando informações de rede tais como: níveis de ruído, relação sinal-ruído, interferência, potência de sinal, topologia da rede, permitindo ao administrador isolar e resolver problemas nos vários níveis da rede;
- Deve prover alarmes e estatísticas de utilização para fácil e rápido monitoramento e troubleshooting;
- Deve permitir a atualização de software dos pontos de acesso de modo centralizado via interface web;
- Deve descobrir automaticamente os dispositivos individuais na infraestrutura de rede cabeada e wireless, eliminando a necessidade de configuração e manutenção, e provendo informação para fins de planejamento da capacidade e troubleshooting;
- Deve possuir funcionalidade para geração de relatórios que relacionam atividade da rede e informações de sistema, incluindo estatísticas dos usuários/clientes, utilização de rádio frequência, contadores 802.11, histórico da configuração de gerenciamento de RF;
- Deve vir com relatórios pré-configurados para fácil utilização da ferramenta;
- Deve possuir suporte para gerenciamento de falhas via SNMP (Simple Network Management Protocol) nas versões 2c e 3 para gerenciamento seguro entre a plataforma de gerenciamento e os controladores;
- Deve permitir o redirecionamento de eventos para um console de gerência central;
- Deve apresentar interface de gerência com acesso através de qualquer browser via HTTP ou HTTPS, permitindo o acesso à plataforma de gerência a qualquer momento de qualquer local;
- Deve implementar a detecção, localização e contenção de Rogue AP's e AD-HOC Networks;
- Deve implementar 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;
- Deve ser possível a geração de alarmes se um ataque for detectado;
- Deve apresentar relatórios contendo ameaças de segurança recorrentes antes que estes causem danos à infraestrutura LAN e WLAN;
- Deve fornecer suporte à criação e aplicação de políticas que permitam ao administrador gerir/criar: VLAN, RF, qualidade de serviço (QoS) e políticas de segurança, SSIDs múltiplos e únicos com parâmetros individuais de segurança;
- Deve permitir troubleshooting de clientes com dificuldade de se conectarem a rede wireless;
- Deve permitir a montagem de mapa da rede (topologia), de forma automática ou manual;
- Pode ser fornecido em forma de appliance, software ou máquina virtual;
- Todo o software necessários para a implantação de qualquer funcionalidade exigida deverão fazer parte do fornecimento, além de outros dispositivos eventualmente necessários ao seu pleno funcionamento em alta-disponibilidade.
- O sistema deve estar localizado para língua portuguesa do Brasil, com opção de utilização da língua inglesa (inglês).
- A CONTRATADA deverá fornecer uma solução que atenda a todos os requisitos anteriores, com capacidade igual ao mínimo exigido nestas especificações, sendo que todos os custos da solução devem ser contabilizados neste item.

ITEM 06 – Licença para expansão do sistema de gerência de redes para 100 dispositivos

Expansão do sistema de gerenciamento de dispositivos LAN e WLAN, do mesmo fabricante e totalmente compatível com os equipamentos com, no mínimo, as seguintes características:

- Deve adicionar ao sistema de gerência de redes de mais cem (100) dispositivos simultaneamente, sejam controladores, APs, switches ou roteadores;
- Pode ser entregue em papel ou cópia digital, desde que seja gerada uma chave de identificação única (tipo Serial Key) garantindo a integridade da expansão;
- Esta expansão deve ser somada à capacidade do sistema existente. Exemplo: se o sistema possuir capacidade de gerência de 100 dispositivos, a adição de uma unidade da expansão totalizará 200 licenças de dispositivos gerenciados;
- Deve manter para os dispositivos adicionados todas as funcionalidades que o sistema possui para os dispositivos previamente licenciados, para o pleno funcionamento da solução.

ITEM 07 – Sistema de monitoramento de mobilidade wireless

Sistema de monitoramento de mobilidade de clientes wireless, do mesmo fabricante e totalmente compatível com os equipamentos ofertados com, no mínimo, as seguintes características:

- Deve permitir a localização de pelo menos seis mil (6.000) clientes wireless simultaneamente;
- Deve permitir a visualização das áreas de cobertura, assim como a concentração dos usuários;
- Deve ser compatível com os APs e controladores especificados nesse edital;
- Deve ser compatível com tags RFIDs;
- Deve implementar SNMP v1, v2c e v3;
- Deve possuir API aberta baseada em XML para permitir o desenvolvimento de aplicações;
- Deve abstrair as aplicações da rede subjacente para fornecer a prestação unificada de serviços através de uma variedade de redes de mobilidade, incluindo Wi-Fi, WiMAX, Celular e Ethernet;
- Deve centralizar os serviços a partir do controlador sem fios, o que simplifica o gerenciamento e escalabilidade, e oferecer inteligência de rede para o desenvolvimento de aplicações para a mobilidade através de uma API aberta;
- Deve implementar solução de Wireless IPS (Intrusion Prevention System) que deve empregar análise de rede e técnicas baseadas em assinatura para oferecer proteção contra os pontos de acesso e clientes não autorizados, reconhecimento de rede, monitoração, tentativas de quebra de autenticação e criptografia, ataques man-in-the-middle, ataques de negação de serviço sem fio e ataques 0-day desconhecido;
- Deve oferecer prevenção proativa de ameaças de forma automatizada;
- Deve ter capacidade de localizar e efetuar rastreamento de, pelo menos seis mil (6.000) usuários/interferências simultaneamente;
- Ao exibir uma interferência “não wifi”, deve circular o raio de interferência na planta, permitindo a visualização da área atingida, bem como a facilidade de análise de canais atingidos;

- Possuir a capacidade de tracking de usuários, mostrando o histórico de conexões/posicionamento deste usuário na planta;
- Possuir API do tipo SOAP/XML para integração com plataformas de aplicação que podem usar suas informações contidas na infraestrutura wireless, por exemplo localização;
- Deve implementar assinaturas de ataques de rádio frequência e prevenção de intrusão para auxiliar o administrador a detectar rapidamente os ataques de RF do tipo “Denial of Service (DoS)”, “NetStumbler”, “Wellenreiter” e “Fake AP”;
- Deve ser fornecido com todos os itens necessários para operacionalização do sistema, tais como: softwares, licenças, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e completa operação do equipamento;
- A proponente deverá integrar o sistema de mobilidade perfeitamente às condições da rede local disponibilizada pela UFSM.
- A CONTRATADA deverá fornecer uma solução que atenda a todos os requisitos anteriores, com capacidade igual ao mínimo exigido nestas especificações, sendo que todos os custos da solução devem ser contabilizados neste item.

ITEM 08 – Access Point Indoor Tipo 1 802.11b/g/n para controlador

Ponto de Acesso para instalação em ambiente interno, que atenda, no mínimo, às seguintes características:

- A solução deverá ser composta de equipamentos do tipo Thin Access Point, ou seja, APs que permitam acesso à rede Ethernet via Wireless, que possuam todas as suas configurações centralizadas em um controlador;
- Deve permitir a operação em forma reversa, ou seja, tipo Fat Access Point, onde é possível a operação sem a presença do controlador wireless. Tal funcionalidade deve ser ativada através de software/firmware e sem custos para este órgão durante o período de garantia;
- Deve permitir a operação de usuários configurados nos padrões IEEE 802.11b/g/n simultaneamente;
- Deve possuir hardware e enclosure projetados com estrutura robusta, lacrada, sem espaços para problemas com poeira e/ou umidade, com facilidades para fixação em parede ou teto, capaz de operar em ambiente de salas de aula, corredores e escritórios.
- Deve acompanhar todos os acessórios para fixação em teto e parede;
- Deve operar em temperaturas de 0 a 40º C;
- Deve atender aos padrões 802.11b e 802.11g e 802.11n draft 2.0 ou superior;
- Deve possuir certificação da Wi-Fi Alliance para 802.11b/g e 802.11n draft 2.0 ou superior;
- Deve ser homologado pela ANATEL para utilização no Brasil;
- Deverá suportar as seguintes arquiteturas:
    - Distribuída: onde o Access Point opera de modo autônomo/inteligente;
    - Centralizada: onde o Access Point opera de modo lightweight e conta com controladores para gerenciamento das configurações, políticas de segurança, QoS e monitoramento de RF, utilizando para isto um protocolo de gerenciamento de RF especifico;

- Deve possuir, no mínimo, três (3) antenas omnidirecionais integradas para frequência de 2.4 GHz. O ganho das antenas deverá ser de, no mínimo, 4dBi em 2.4GHz;
- Deve possuir potência de transmissão máxima não inferior a 18dBm em todos os modos de operação (802.11b/g/n);
- Deve possuir sensibilidade mínima de -86 dBm operando em IEEE 802.11n;
- Deve implementar as seguintes taxas de transmissão e com fallback automático: IEEE 802.11b: 11; 5,5; 2 e 1 Mbps; IEEE 802.11g: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11n: MSC0- MSC15 (6.5 Mbps – 300 Mbps);
- Deve possuir, no mínimo, uma interface de uplink, autosensing, conforme o padrão IEEE 802.3ab, 10/100/1000BASE-T;
- Deve possuir capacidade de selecionar automaticamente o canal de transmissão, sem necessidade de reinicialização do AP;
- Deve fazer a atualização automática de firmware ao ser conectado no Controlador WLAN;
- Deve possuir LED que indique, no mínimo, o estado de operação;
- Deve possuir, pelo menos, uma porta de console exclusiva para gerenciamento via linha de comando (CLI – comand line interface) com conector RJ-45, conector padrão RS-232 ou USB;
- Deve implementar funcionamento em modo gerenciado por controlador, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF (Rádio Frequência);
- Deve implementar padrão Wireless Multimedia QoS (WMM) da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
- Deve possuir mecanismo de otimização automática de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast. Este mecanismo deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes mesmo que está não seja o “rate” mandatório;
- Deve implementar cliente DHCP, para configuração automática de rede;
- Deve ser fornecido com kit de instalação que permita fixação do equipamento em teto e parede;
- Deve possuir suporte a controladores WLAN redundantes, no caso de falha do controlador WLAN primário, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador secundário;
- Deve suportar, pelo menos, dezesseis (16) SSIDs;
- Deve permitir habilitar e desabilitar a divulgação do SSID;
- Deve possuir, no mínimo, MIMO (Multiple-Input Multiple-Output) 2x3 em 802.11n, operando em canais de 20MHz;
- Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-Transport Layer Security (EAP-TLS); EAP-TTLS/MSCHAPv2; PEAPv0/EAP-MSCHAPv2; PEAPv1/EAP-GTC; EAP Subscriber Identity Module (EAP-SIM);
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;

- Deve implementar WEP (Wired Equivalent Privacy), chaves estáticas e dinâmicas (40 bits e 128 bits);
- Deve suportar WPA com algoritmo de criptografia TKIP;
- Deve implementar WPA-2 (Wi-Fi Protected Access) com algoritmo de criptografia AES assistida em hardware, conforme o padrão IEEE 802.11i;
- Deve ser fornecido acompanhado de todos os acessórios e licenças necessários para a completa operação do equipamento, tais como: softwares, documentação técnica e manual que contenham informações suficientes para possibilitar a instalação, configuração e startup do equipamento;
- Deve ser capaz de realizar o switching local do tráfego gerado entre os clientes a ele associados, sem a necessidade de conectividade com o controlador para o tráfego dos clientes de cada ponto de acesso. Caso haja falha de comunicação com o controlador, os clientes associados devem continuar tendo acesso à rede, sem a necessidade de reautenticação;
- Deve possuir sistema antifurto tipo Kensington Security Lock ou similar;
- Deve implementar varredura de RF para identificação de Pontos de Acesso não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN; O sistema de monitoramento e controle de RF deve possuir mecanismos de detecção/bloqueio de intrusos no ambiente wireless;
- Deve permitir o bloqueio de comunicação entre clientes wireless diretamente (comunicação ad-hoc não é permitida);
- Deve possuir alimentação via PoE, padrão 802.3af;
- Deve possuir kit de instalação incluso no fornecimento. O equipamento instalado não deve exceder as dimensões 23cm x 23cm x 5,5cm (C x L x A) para adequar-se aos nichos existentes na UFSM;
- O equipamento deve ser totalmente compatível com os controladores ofertados.
- A proponente deverá integrar os equipamentos perfeitamente às condições da rede local disponibilizada pela UFSM.

ITEM 09 – Access Point Indoor Tipo 2 802.11a/b/g/n para controlador

Ponto de Acesso para instalação em ambiente interno, que atenda, no mínimo, às seguintes características:

- A solução deverá ser composta de equipamentos do tipo Thin Access Point, ou seja, APs que permitam acesso à rede Ethernet via Wireless, que possuam todas as suas configurações centralizadas em um controlador;
- Deve permitir a operação em forma reversa, ou seja, tipo Fat Access Point, onde é possível a operação sem a presença do controlador wireless. Tal funcionalidade deve ser ativada através de software/firmware e sem custos para este órgão durante o período de garantia;
- Deve possuir hardware e enclosure projetados com estrutura robusta, lacrada, sem espaços para problemas com poeira e/ou umidade, com facilidades para fixação em parede ou teto, capaz de operar em ambiente de salas de aula, corredores e escritórios.
- Deve acompanhar todos os acessórios para fixação em teto e parede;
- Deve operar em temperaturas de 0 a 40º C;

- Deve atender aos padrões 802.11a e 802.11b e 802.11g e 802.11n draft 2.0 ou superior;
- Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g e 802.11n draft 2.0 ou superior;
- Deve ser homologado pela ANATEL para utilização no Brasil;
- Deverá suportar as seguintes arquiteturas:
    - Distribuída: onde o Access Point opera de modo autônomo/inteligente;
    - Centralizada: onde o Access Point opera de modo lightweight e conta com controladores para gerenciamento das configurações, políticas de segurança, QoS e monitoramento de RF, utilizando para isto um protocolo de gerenciamento de RF especifico;
- Deve possuir, no mínimo, três (3) antenas omnidirecionais integradas para frequência de 2.4GHz e três (3) antenas omnidirecionais integradas para frequência de 5GHz. O ganho das antenas deverá ser de, no mínimo, 4dBi em 2.4GHz e 3dBi 5GHz.
- Deve possuir potência de transmissão máxima não inferior a 18dBm em todos os modos de operação (802.11a/b/g/n);
- Deve possuir sensibilidade mínima de -86 dBm operando em IEEE 802.11n;
- Deve implementar as seguintes taxas de transmissão e com fallback automático: IEEE 802.11a: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11b: 11; 5,5; 2 e 1 Mbps; IEEE 802.11g: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11n: MCS0-MCS15 (6.5 Mbps – 300 Mbps);
- Deve possuir, no mínimo, uma interface de uplink, autosensing, conforme o padrão IEEE 802.3ab, 10/100/1000BASE-T;
- Deve possuir capacidade de selecionar automaticamente o canal de transmissão, sem necessidade de reinicialização do AP;
- Deve fazer a atualização automática de firmware ao ser conectado no Controlador WLAN;
- Deve possuir LED que indique, no mínimo, o estado de operação;
- Deve possuir, pelo menos, uma porta de console exclusiva para gerenciamento via linha de comando (CLI – comand line interface) com conector RJ-45, conector padrão RS-232 ou USB;
- Deve implementar funcionamento em modo gerenciado por controlador, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF (Rádio Frequência);
- Deve implementar padrão Wireless Multimedia QoS (WMM) da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
- Deve implementar cliente DHCP, para configuração automática de rede;
- Deve ser fornecido com kit de instalação que permita fixação do equipamento em teto e parede;
- Deve possuir suporte a controladores WLAN redundantes, no caso de falha do controlador WLAN primário, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador secundário;
- Deve suportar, pelo menos, oito (8) SSIDs;

- Deve permitir habilitar e desabilitar a divulgação do SSID;
- Deve possuir, no mínimo, MIMO (Multiple-Input Multiple-Output) 2x3 em 802.11n (2.4GHz e 5GHz), operando em canais de 20MHz e 40MHz;
- Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-Transport Layer Security (EAP-TLS); EAP-TTLS/MSCHAPv2; PEAPv0/EAP-MSCHAPv2; PEAPv1/EAP-GTC; EAP Subscriber Identity Module (EAP-SIM);
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- Deve implementar WEP (Wired Equivalent Privacy), chaves estáticas e dinâmicas (40 bits e 128 bits);
- Deve suportar WPA com algoritmo de criptografia TKIP;
- Deve implementar WPA-2 (Wi-Fi Protected Access) com algoritmo de criptografia AES assistida em hardware, conforme o padrão IEEE 802.11i;
- Deve ser fornecido acompanhado de todos os acessórios e licenças necessários para a completa operação do equipamento, tais como: softwares, documentação técnica e manual que contenham informações suficientes para possibilitar a instalação, configuração e startup do equipamento;
- Deve ser capaz de realizar o switching local do tráfego gerado entre os clientes a ele associados, sem a necessidade de conectividade com o controlador para o tráfego dos clientes de cada ponto de acesso. Caso haja falha de comunicação com o controlador, os clientes associados devem continuar tendo acesso à rede, sem a necessidade de reautenticação;
- Deve possuir sistema antifurto tipo Kensington Security Lock ou similar;
- Deve implementar varredura de RF para identificação de Pontos de Acesso não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN; O sistema de monitoramento e controle de RF deve possuir mecanismos de detecção/bloqueio de intrusos no ambiente wireless;
- Deve permitir o bloqueio de comunicação entre clientes wireless diretamente (comunicação ad-hoc não é permitida);
- Deve possuir alimentação via PoE, padrão 802.3af;
- Deve possuir kit de instalação incluso no fornecimento. O equipamento instalado não deve exceder as dimensões 23cm x 23cm x 5,5cm (C x L x A) para adequar-se aos nichos existentes na UFSM;
- O equipamento deve ser totalmente compatível com os controladores ofertados.
- A proponente deverá integrar os equipamentos perfeitamente às condições da rede local disponibilizada pela UFSM.

ITEM 10 – Access Point Indoor Tipo 3 802.11a/b/g/n com analisador de espectro para controlador

Ponto de Acesso para instalação em ambiente interno, que atenda, no mínimo, às seguintes características:

- A solução deverá ser composta de equipamentos do tipo Thin Access Point, ou seja, APs que permitam acesso à rede Ethernet via Wireless, que possuam todas as suas configurações centralizadas em um controlador;

- Deve ter capacidade de análise espectral para identificação de interferências wi-fi e não wi-fi implementada em hardware;
- Deve ser um AP para rede local sem fio de uso interno, sem antenas aparentes, que atenda os padrões IEEE 802.11a/b/g/n nas faixas de 2.4GHz e 5GHz simultaneamente, com configuração via software.
- Deve possuir funcionamento em modo gerenciado por Controlador WiFi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF;
- Deve possuir hardware e enclosure projetados com estrutura robusta, lacrada, sem espaços para problemas com poeira e/ou umidade, com facilidades para fixação em parede ou teto, capaz de operar em ambiente de salas de aula, corredores e escritórios.
- Deve acompanhar todos os acessórios para fixação em teto e parede;
- Deve operar em temperaturas de 0 a 40º C;
- Deve atender aos padrões 802.11a e 802.11b e 802.11g e 802.11n draft 2.0 ou superior;
- Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g e 802.11n draft 2.0 ou superior;
- Deve ser homologado pela ANATEL para utilização no Brasil;
- Dever suportar a arquitetura centralizada: onde o Access Point opera de modo lightweight e conta com controladores para gerenciamento das configurações, políticas de segurança, QoS e monitoramento de RF, utilizando para isto um protocolo de gerenciamento de RF especifico;
- Deve possuir, no mínimo, três (3) antenas omnidirecionais integradas para frequência de 2.4GHz e três (3) antenas omnidirecionais integradas para frequência de 5GHz.
- Deve possuir potência de transmissão máxima não inferior a 18dBm em todos os modos de operação (802.11a/b/g/n);
- Deve possuir sensibilidade de recepção de valor menor ou igual a: -93dBm em 802.11a a 6Mbps; -92dBm em 802.11b a 5.5Mbps; -92dBm em 802.11g a 6Mbps; -92dBm em 802.11n (HT20) a MC0 em 2.4GHz; -91dBm em 802.11n (HT40) a MC0 em 2.4GHz;
- Deve implementar as seguintes taxas de transmissão e com fallback automático: IEEE 802.11a: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11b: 11; 5,5; 2 e 1 Mbps; IEEE 802.11g: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11n: MCS0-MCS15 (6.5 Mbps – 300 Mbps);
- Deve possuir capacidade de selecionar automaticamente o canal de transmissão;
- Deve implementar o protocolo de enlace CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão;
- Deve operar nas modulações DSSS e OFDM;
- O equipamento deve realizar a monitoração em tempo real das frequências de Rádio Frequência (análise espectral) em busca de interferências WiFi e simultaneamente atender os usuários da rede WiFi;
- As funções de monitoração real-time em Rádio Frequência (análise espectral) devem ser realizadas via hardware, com chipset (ASIC) dedicado para esta função localizado dentro do ponto de acesso;

- Deve detectar e gerar alarmes de interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar, classificar e gerar alarmes de interferências não-WiFi, tais como Bluetooth, telefones sem fio, câmeras de video sem fio, Microondas e outros;
- Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente;
- Deve operar nos seguintes modos: “Modo Local”, “Modo Monitor” e “Modo Analisador de Espectro”:
    - Operando em “Modo Local” o ponto de acesso deve fornecer informações ao Controlador WiFi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi. Deve fazer tanto a transmissão de dados WiFi quanto a análise de espectro simultaneamente;
    - Operando em “Modo Monitor” deve fornecer informações ao Controlador WiFi referente à qualidade do espectro de RF para todos os canais monitorados identificando equipamentos interferentes na rede WiFi e rogue APs em conjunto com a aplicação de segurança da solução;
    - Operando em “Modo Analisador de Espectro” deve operar de forma exclusiva apenas para monitorar o espectro de RF de forma a fornecer informações para um software analisador de espectro ou para o software de gerenciamento WiFi;
- Caso não seja possível a realização da monitoração espectral e o atendimento simultâneo dos usuários da rede WiFi em um único ponto de acesso (modo de operação “Local”) sem prejuízo de desempenho wifi, a CONTRATADA deverá fornecer 02 (dois) pontos de acesso WiFi deste tipo para atender o requerimento técnico. Um ponto de acesso será utilizado para realizar a monitoração espectral e outro ponto de acesso será utilizado para atender os usuários. O custo do Ponto de Acesso adicional deve ser incluído no item “Access Point Indoor Tipo 3”;
- Deve ser fornecido com fonte de alimentação com ajuste automático de tensão 110/220 volts e freqüência de 60 Hz;
- Deve possuir, no mínimo, uma interface de uplink, autosensing, conforme o padrão IEEE 802.3ab, 10/100/1000BASE-T;
- Deve possuir capacidade de selecionar automaticamente o canal de transmissão, sem necessidade de reinicialização do AP;
- Deve fazer a atualização automática de firmware ao ser conectado no Controlador WLAN;
- Deve possuir LED que indique, no mínimo, o estado de operação;
- Deve possuir, pelo menos, uma porta de console exclusiva para gerenciamento via linha de comando (CLI – comand line interface) com conector RJ-45, conector padrão RS-232 ou USB;
- Deve implementar funcionamento em modo gerenciado por controlador, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF (Rádio Frequência);
- Deve implementar padrão Wireless Multimedia QoS (WMM) da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

- Deve implementar cliente DHCP, para configuração automática de rede;
- Deve ser fornecido com kit de instalação que permita fixação do equipamento em teto e parede;
- Deve possuir suporte a controladores WLAN redundantes, no caso de falha do controlador WLAN primário, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador secundário;
- Deve suportar, pelo menos, dezesseis (16) SSIDs;
- Deve permitir habilitar e desabilitar a divulgação do SSID;
- Deve possuir, no mínimo, MIMO (Multiple-Input Multiple-Output) 2x3 em 802.11n (2.4GHz e 5GHz), operando em canais de 20MHz e 40MHz;
- Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-Transport Layer Security (EAP-TLS); EAP-TTLS/MSCHAPv2; PEAPv0/EAP-MSCHAPv2; PEAPv1/EAP-GTC; EAP Subscriber Identity Module (EAP-SIM);
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- Deve implementar WEP (Wired Equivalent Privacy), chaves estáticas e dinâmicas (40 bits e 128 bits);
- Deve suportar WPA com algoritmo de criptografia TKIP;
- Deve implementar WPA-2 (Wi-Fi Protected Access) com algoritmo de criptografia AES assistida em hardware, conforme o padrão IEEE 802.11i;
- Deve ser fornecido acompanhado de todos os acessórios e licenças necessários para a completa operação do equipamento, tais como: softwares, documentação técnica e manual que contenham informações suficientes para possibilitar a instalação, configuração e startup do equipamento;
- Deve ser capaz de realizar o switching local do tráfego gerado entre os clientes a ele associados, sem a necessidade de conectividade com o controlador para o tráfego dos clientes de cada ponto de acesso. Caso haja falha de comunicação com o controlador, os clientes associados devem continuar tendo acesso à rede, sem a necessidade de reautenticação;
- Deve possuir sistema antifurto tipo Kensington Security Lock ou similar;
- Deve implementar varredura de RF para identificação de Pontos de Acesso não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN; O sistema de monitoramento e controle de RF deve possuir mecanismos de detecção/bloqueio de intrusos no ambiente wireless;
- Deve permitir o bloqueio de comunicação entre clientes wireless diretamente (comunicação ad-hoc não é permitida);
- Deve possuir alimentação via PoE, padrão 802.3af;
- Deve possuir kit de instalação incluso no fornecimento. O equipamento instalado não deve exceder as dimensões 23cm x 23cm x 5,5cm (C x L x A) para adequar-se aos nichos existentes na UFSM;
- O equipamento deve ser totalmente compatível com os controladores ofertados.
- A proponente deverá integrar os equipamentos perfeitamente às condições da rede local disponibilizada pela UFSM.

ITEM 11 – Access Point Outdoor Tipo 4 802.11a/b/g/n para controlador

Ponto de Acesso para instalação em ambiente externo, que atenda, no mínimo, às seguintes características:

- A solução deverá ser composta de equipamentos do tipo Thin Access Point, ou seja, APs que permitam acesso à rede Ethernet via Wireless, que possuam todas as suas configurações centralizadas em um controlador;
- Deve permitir a operação em forma reversa, ou seja, tipo Fat Access Point, onde é possível a operação sem a presença do controlador wireless. Tal funcionalidade deve ser ativada através de software/firmware e sem custos para este órgão durante o período de garantia;
- Deve possuir hardware e enclosure com estrutura robusta, lacrada, sem espaços para problemas com poeira e/ou umidade, com facilidades para fixação em parede ou teto, capaz de operar em ambiente externo.
- Deve acompanhar todos os acessórios para fixação em teto e parede;
- Deve operar em temperaturas de 0 a 40º C;
- Deve atender aos padrões 802.11a e 802.11b e 802.11g e 802.11n draft 2.0 ou superior;
- Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g e 802.11n draft 2.0 ou superior;
- Deve ser homologado pela ANATEL para utilização no Brasil;
- Dever suportar a arquitetura centralizada: onde o Access Point opera de modo lightweight e conta com controladores para gerenciamento das configurações, políticas de segurança, QoS e monitoramento de RF, utilizando para isto um protocolo de gerenciamento de RF especifico;
- Deve possuir 6 antenas externas ao equipamento, sendo três para operação em 2.4GHz com ganho mínimo de 2.2 dBi e três para operação em 5GHz com ganho mínimo de 3.5 dBi e irradiação omnidirecional, as antenas e o AP devem ter conexão RP-TNC.
- Deve possuir potência de transmissão máxima não inferior a 18dBm em todos os modos de operação (802.11a/b/g/n);
- Deve implementar as seguintes taxas de transmissão e com fallback automático: IEEE 802.11a: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11b: 11; 5,5; 2 e 1 Mbps; IEEE 802.11g: 54; 48; 36; 24; 18; 12; 9 e 6 Mbps; IEEE 802.11n: MCS0-MCS15 (6.5 Mbps – 300 Mbps);
- Deve possuir, no mínimo, uma interface de uplink, autosensing, conforme o padrão IEEE 802.3ab, 10/100/1000BASE-T;
- Deve possuir capacidade de selecionar automaticamente o canal de transmissão, sem necessidade de reinicialização do AP;
- Deve fazer a atualização automática de firmware ao ser conectado no Controlador WLAN;
- Deve possuir, pelo menos, uma porta de console exclusiva para gerenciamento via linha de comando (CLI – comand line interface) com conector RJ-45, conector padrão RS-232 ou USB;
- Deve implementar funcionamento em modo gerenciado por controlador, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF (Rádio Frequência);

- Deve implementar padrão Wireless Multimedia QoS (WMM) da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
- Deve implementar cliente DHCP, para configuração automática de rede;
- Deve ser fornecido com kit de instalação que permita fixação do equipamento em teto e parede;
- Deve possuir suporte a controladores WLAN redundantes, no caso de falha do controlador WLAN primário, os Pontos de Acesso relacionados deverão se associar automaticamente a um controlador secundário;
- Deve suportar, pelo menos, dezesseis (16) SSIDs;
- Deve permitir habilitar e desabilitar a divulgação do SSID;
- Deve possuir, no mínimo, MIMO (Multiple-Input Multiple-Output) 2x3 em 802.11n (2.4GHz e 5GHz), operando em canais de 20MHz e 40MHz;
- Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-Transport Layer Security (EAP-TLS); EAP-TTLS/MSCHAPv2; PEAPv0/EAP-MSCHAPv2; PEAPv1/EAP-GTC; EAP Subscriber Identity Module (EAP-SIM);
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- Deve implementar WEP (Wired Equivalent Privacy), chaves estáticas e dinâmicas (40 bits e 128 bits);
- Deve suportar WPA com algoritmo de criptografia TKIP;
- Deve implementar WPA-2 (Wi-Fi Protected Access) com algoritmo de criptografia AES assistida em hardware, conforme o padrão IEEE 802.11i;
- Deve ser fornecido acompanhado de todos os acessórios e licenças necessários para a completa operação do equipamento, tais como: softwares, documentação técnica e manual que contenham informações suficientes para possibilitar a instalação, configuração e startup do equipamento;
- Deve ser capaz de realizar o switching local do tráfego gerado entre os clientes a ele associados, sem a necessidade de conectividade com o controlador para o tráfego dos clientes de cada ponto de acesso. Caso haja falha de comunicação com o controlador, os clientes associados devem continuar tendo acesso à rede, sem a necessidade de reautenticação;
- Deve possuir sistema antifurto tipo Kensington Security Lock ou similar;
- Deve implementar varredura de RF para identificação de Pontos de Acesso não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN; O sistema de monitoramento e controle de RF deve possuir mecanismos de detecção/bloqueio de intrusos no ambiente wireless;
- Deve permitir o bloqueio de comunicação entre clientes wireless diretamente (comunicação ad-hoc não é permitida);
- Deve possuir alimentação via PoE, padrão 802.3af;
- O equipamento deve ser instalado em caixa hermética, capaz de proteger o equipamento de água, chuva, vento e poeira. As antenas serão instaladas externas às caixas, favorecendo a comunicação com os demais equipamentos. Para isso, deve ser fornecido uma caixa hermética de plástico, padrão de mercado, com grau de proteção maior que IP55, em tom de cor claro, com

dimensões máximas de 50x50x30cm (L x A x P). Deve possuir kit de instalação incluso no fornecimento;

- O equipamento deve ser totalmente compatível com os controladores ofertados.
- A proponente deverá integrar os equipamentos perfeitamente às condições da rede local disponibilizada pela UFSM.

ITEM 12 - Access Point Outdoor Tipo 5 802.11a/b/g/n com analisador de espectro para controlador

Ponto de Acesso para instalação em ambiente externo, que atenda, no mínimo, às seguintes características:

- Deve possibilitar a instalação de antenas externas, que atenda os padrões IEEE 802.11a/b/g/n na faixa de 2,4GHz e 5GHz, simultaneamente com configuração via software;
- Deve operar em modo "mesh", com tráfego centralizado no controlador e possuir capacidade de análise espectral em Rádio Frequência;
- Deve funcionar em modo gerenciado por um Controlador para configuração de seus parâmetros, gerenciamento das políticas de segurança, e QOS e parâmetros de RF;
- Deverá operar logicamente conectado a um Controlador, inclusive via roteamento de camada 3 do modelo OSI, seja através de rede de comunicação pública ou rede de comunicação privada;
- Em caso de falha do controlador ao qual o ponto de acesso está associado, o ponto de acesso deverá se associar automaticamente a um controlador redundante, não permitindo que a rede sem fio se torne inoperante por este motivo;
- O ponto de acesso deve ter capacidade de operar de forma que realize o encaminhamento do tráfego dos usuários através do(s) Controlador(es);
- Deve suportar usuários wireless configurados nos padrões IEEE 802.11a/b/g/n simultaneamente;
- Deve operar, no mínimo, com temperaturas de -30 a +55°C (graus Celsius);
- Deve suportar, no mínimo, umidade do ar de 5% a 95% sem condensação;
- Deve operar em condições ambientais externas respeitando, no mínimo, a norma IEC 60529 nível IP-65 (International Protection Rating);
- Deve sobreviver a rajadas de ventos de até 265 Km/h ou 165 MPH;
- Deve possuir no mínimo 2x2 multiple-input multiple-output (MIMO) em 802.11n (faixas de 2,4GHz e 5GHz);
- Deve operar em canais de 20 e 40 MHz em 802.11n;
- Deve possuir, pelo menos, as seguintes taxas de transmissão e com fallback automático para 802.11a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
- Deve possuir pelo menos as seguintes taxas de transmissão e com fallback automático para 802.11n: MSC0 - MSC15 (6.5Mbps - 300Mbps);
- Deve ser capaz de selecionar automaticamente o canal de transmissão;
- Deve implementar o protocolo de enlace CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão;
- Deve suportar pelo menos modulação OFDM;

- Deve permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;
- Deve possuir funcionalidade de permitir ou bloquear a divulgação do SSID;
- Deve possuir padrão WMM (Wi-Fi Multimedia) da Wi-Fi Alliance para priorização de tráfego;
- Deve implementar tecnologia MRC - With maximum ratio combining (MRC) technology;
- Deve possuir, no mínimo, 02 (dois) rádios (dual-radio) operando simultaneamente em frequências distintas;
- O ponto de acesso deve possuir no mínimo 03 (três) conexões dual-band (2,4GHz e 5GHz) para instalação de pelo menos 03 (três) antenas externas. As antenas devem operar, no mínimo, nas faixas de frequência entre 2,400 e 2,480 MHz e entre 5.725 e 5.850 MHz, simultaneamente, na mesma antena. Estas antenas devem ser do tipo para instalação em ambientes externos e do mesmo fabricante do ponto de acesso;
- Devem ser fornecidas 03 (três antenas), que serão conectadas diretamente ao rádio, sem cabo externo;
- As antenas devem prover ganho de, no mínimo, 4.0 dBi na faixa de freqüência de 2,4GHz e de 7.0 dBi na faixa de freqüência de 5GHz, simultâneamente. As antenas devem operar com padrão de irradiação omnidirecional, provendo cobertura em 360º (trezentos e sessenta graus);
- Todas as antenas devem operar com padrão de irradiação omnidirecional, provendo cobertura em 360º (trezentos e sessenta graus). As antenas devem ser do tipo para instalação em ambientes externos e do mesmo fabricante do ponto de acesso;
- Deve possuir sensibilidade de recepção de valor menor ou igual:
    - -92dBm em 802.11a a 6Mbps;
    - -92dBm em 802.11b a 5.5Mbps;
    - -92dBm em 802.11g a 6Mbps;
    - -92dBm em 802.11n (HT20) a MC0 em 2,4GHz;
    - -89dBm em 802.11n (HT40) a MC0 em 5GHz.
- Deve possuir, no mínimo, 01 (uma) interface padrão IEEE 802.3ab 10/100/1000BaseT, auto-sensing, auto MDI/MDIX, com conectores RJ-45, OU 01 (uma) interface GigabitEthernet em fibra óptica monomodo padrão IEEE 802.3z 1000BaseLX 1310nm para conexão à rede local;
- O ponto de acesso deve possuir estrutura que permita fixação em poste e mastros. Todos os acessórios para que possa ser feita a fixação deverão ser fornecidos com o equipamento;
- Deve permitir a atualização remota ou local do sistema operacional e arquivos de configurações utilizados nos equipamentos, via interfaces ethernet ou serial;
- Deve possuir no mínimo 01 LED indicativo do estado de operação;
- O equipamento deve vir acompanhado de manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

- Deve ser acompanhado de todos os acessórios necessários para operacionalização, tais como: licenças de softwares, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização;
- Deve possuir varredura de RF nas bandas 802.11a, 802.11b, 802.11g e 802.11n para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WiFi, sem impacto no seu desempenho;
- Deve implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP:
    - EAP-PEAP;
    - EAP-TLS;
    - EAP-TTLS;
- Deve implementar criptografia do tráfego local;
- Deve implementar 802.11i;
- Deve possuir Wi-Fi Protected Access: WPA2 e WPA;
- Deve detectar e gerar alarmes de interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar, classificar e gerar alarmes de interferências não-WiFi, tais como bluetooth, telefones sem fio, câmeras de vídeo sem fio e outros;
- Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente;
- Todos os rádios do equipamento devem processar os dados WiFi dos usuários enquanto a análise de espectro é realizada pelo ponto de acesso de forma simultânea, sem prejuízo de performance;
- O ponto de acesso deve fornecer informações em tempo real ao controlador WiFi ao qual está associado referentes à qualidade do espectro de RF para o canal de operação atual e para todos os canais de operação nas faixas de 2,4GHz e 5GHz, ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi;
- Caso o ponto de acesso ofertado não possua capacidade para realizar simultâneamente a monitoração de espectro e o atendimento dos usuários da rede WiFi por todos os rádios do equipamento, sem prejuízo de desempenho, a proponente deverá ofertar 02 (dois) pontos de acesso WiFi para atender o requerimento técnico:
- O primeiro ponto de acesso será utilizado para realizar a monitoração de espectro de Rádio Frequência;
- Os custos dos dois pontos de acesso deverão ser inseridos no item “Access Point Outdoor Tipo 5”;
- O ponto de acesso WiFi deverá ser alimentado diretamente por ponto de energia elétrica de 100-240VAC e 60Hz. Caso seja fornecido com fonte de alimentação externa ou power injector externo, os mesmos devem respeitar:
    - Deve operar, no mínimo, com temperaturas de -20 a +55℃ (graus Celsius);
    - Deve suportar, no mínimo, umidade do ar de 5% a 95% sem condensação;
- O equipamento deve ser homologado pela ANATEL para utilização no Brasil.

ITEM 13 - Power Injector para Access Point Indoor

Necessita-se que este modelo de injetor atenda, no mínimo, às seguintes características:

- Deve ser compatível com todos os Access Point Indoor para controlador que compõem esse lote.
- Deve trabalhar com voltagem de entrada entre 100V AC e 240 V AC, com seleção automática e voltagem de saída compatível com padrão PoE dos Access Point indoor, em frequência de 50 ou 60 Hz.
- Deve possuir fonte de alimentação interna.
- Deve possuir duas interfaces 10/100/1000BASE-T.
- Deve utilizar apenas uma porta Ethernet do Switch de Acesso e do Access Point.
- Deve fornecer energia suficiente para alimentação do Access Point e habilitação de todas as funcionalidades em sua capacidade máxima.

ITEM 14 - Switch 24 Portas 10/100 BASE-T

Comutador de rede que atenda, no mínimo, às seguintes características:

- Deve possuir no mínimo vinte e quatro (24) portas 10/100Mbps com conectores RJ-45.
- Deve suportar pelo menos duas (02) portas de uplink flexíveis padrão Gigabit Ethernet, devendo suportar as interfaces 10/100/1000 com conector RJ45, 1000BaseT, 1000BaseSX e 1000BaseLX/LH.
- Todas as portas solicitadas devem ser utilizadas simultaneamente. Caso o equipamento utilize interfaces do tipo combo, deverão ser fornecidas interfaces adicionais para atender este termo sem prejuízo das portas solicitadas.
- Deve possuir uma matriz de comutação com pelo menos 15 Gbps.
- Deve possuir capacidade de processamento de pelo menos 6.0 milhões de pps.
- Deve possuir LEDs, por porta, que indiquem a integridade e atividade do link, a velocidade de conexão e também o modo de operação (half/full duplex).
- Deve suportar o encaminhamento de “mini jumbo frames” em todas as portas do switch (frames de 1530 bytes).
- Deve suportar o encaminhamento de “jumbo frames” nas portas Gigabit Ethernet do switch frames de 9018 bytes).
- Deve possuir capacidade para no mínimo 8000 endereços MAC.
- As interfaces devem obedecer às normas técnicas IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE 802.3ab (1000Base-T), IEEE 802.3z (1000Base-X).
- Deve suportar o modo de comutação "store and forward".
- Deve possuir no mínimo 32 megabytes de memória Flash.
- Deve possuir no mínimo 64 megabytes de memória DRAM.
- Deve suportar a instalação de fonte de energia redundante.
- Deve ser instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos kit’s de fixação.
- Deve implementar LAN Virtual (VLAN) conforme padrão IEEE 802.1Q.
- Deve permitir a criação de no mínimo 128 VLANs ativas baseadas em portas.
- Deve permitir a criação de no mínimo 128 instâncias do protocolo Spannig Tree.
- Deve implementar Wake on LAN.
- Deve permitir espelhar todo o tráfego do Switch para uma VLAN específica, permitindo que outro switch da rede conectado a esta VLAN receber o tráfego espelhado.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas “isoladas” e portas “promíscuas”, onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.

- Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deve Implementar "VLAN Trunking" padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet, devendo ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
- Deve implementar a funcionalidade de "Port Trunking" conforme padrão IEEE 802.3ad.
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Fast Ethernet (em "full duplex").
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Gigabit Ethernet (em "full duplex").
- Deve permitir a criação de pelo menos 06 grupos de portas agregadas.
- Deve ser possível agrupar logicamente pelo menos 12 switches deste mesmo modelo e família, formando um "cluster" lógico e gerenciá-los graficamente através de um único endereço IP.
- Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada. Deve ser possível espelhar o tráfego originado em um switch do "cluster" lógico para uma porta de destino localizada em um switch diferente do "cluster".
- Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d.
- Deve implementar o padrão IEEE 802.1s ("Multiple Spanning Tree") para pelo menos 32 instâncias.
- Deve implementar o padrão IEEE 802.1w ("Rapid Spanning Tree").
- Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Deve implementar Voice VLAN.
- Deve permitir criar filtros de pacotes que atuem nas interfaces do equipamento somente em determinadas horas do dia mediante agendamento.
- Deve implementar pelo menos quatro filas de saída por porta.
- Deve implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.
- Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem/destino.
- Deve implementar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Deve implementar filtro de pacotes via ACL incluindo camada 4.
- Deve implementar autenticação via WEB de usuários criados localmente.
- Deve implementar serviço de portal Web para autenticação do usuário para acesso à rede.
- Deve implementar Dynamic ARP Inspection.
- Deve possuir mecanismo de supressão e controle de Multicast e Unicast.
- 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.

- Deve suportar autenticação e autorização via RADIUS.
- Deve implementar controle de acesso por porta (IEEE 802.1x). Deve ser suportada a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN "Guest" caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional.
- Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Deve 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).
- Deve possuir uma interface de gerenciamento baseada em WEB (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão.
- Deve ser gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.
- Deve ser gerenciável via SSH versão 2 (SSHv2), suportando, no mínimo, o algoritmo de criptografia 3DES.
- Deve Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem.
- Deve ser gerenciável via SNMP (v1, v2 e v3) e RMON.
- Deve implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.
- Deve implementar LLDP.
- Deve implementar Local Proxy ARP.
- Deve implementar SCP.
- Deve implementar IGMP Querier.
- Deve implementar mecanismo "Weighted Tail Drop" em todas as interfaces.
- Deve implementar mecanimos de "Strict Priority" em todas as interfaces.
- Deve implementar TACACS+.
- Deve implementar filtros de quadros e/ou pacotes através de ACL.
- Deve implementar mecanismo de classificação de quadros e/ou pacotes via ACL.
- Deve permitir, baseado na classificação aplicada, priorizar todos os quadros e/ou pacotes classificados
- Deve implementar o protocolo Syslog para funções de "logging" de eventos.
- Deve permitir de upgrade de software através do protocolo TFTP.
- Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.
- Deve implementar "accounting" das conexões IEEE 802.1x. Devem ficar registradas pelo menos as seguintes informações da conexão : nome do usuário e grupo a que pertence, switch em que o computador do usuário está conectado, porta do switch usada para acesso, endereço MAC da máquina usada pelo usuário, horários de início e término da conexão, bytes transmitidos e recebidos.
- Deve 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente teste se conectar à porta.
- Deve ser possível estabelecer o número máximo de endereços MAC que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Deve permitir a criação de listas de acesso baseadas em endereços 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.

- Deve possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.
- Deve promover 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.
- Deve Implementar IGMP Snooping (v1, v2 e v3).

Item 15 - Switch 24 Portas 10/100 BASE-T PoE

Comutador de rede que atenda, no mínimo, às seguintes características:

- Deve possuir no mínimo 24 (vinte e quatro) portas 10/100Mbps com conectores RJ-45, implementando Power Over Ethernet (IEEE 802.3af).
- Deve permitir que todas as portas 10/100Mbps operem com alimentação PoE simultaneamente.
- Deve suportar pelo menos 02 (duas) portas de uplink flexíveis padrão Gigabit Ethernet, devendo suportar as interfaces 10/100/1000 com conector RJ45, 1000BaseT, 1000BaseSX e 1000BaseLX/LH.
- Todas as portas solicitadas devem ser utilizadas simultaneamente. Caso o equipamento utilize interfaces do tipo combo, deverão ser fornecidas interfaces adicionais para atender este termo sem prejuízo das portas solicitadas.
- Deve possuir uma matriz de comutação com pelo menos 15 Gbps.
- Deve possuir capacidade de processamento de pelo menos 6.0 milhões de pps.
- Deve possuir LEDs, por porta, que indiquem a integridade e atividade do link, a velocidade de conexão e também o modo de operação (half/full duplex).
- Deve suportar o encaminhamento de “mini jumbo frames” em todas as portas do switch (frames de 1530 bytes).
- Deve suportar o encaminhamento de “jumbo frames” nas portas Gigabit Ethernet do switch frames de 9018 bytes).
- Deve possuir capacidade para no mínimo 8000 endereços MAC.
- As interfaces devem obedecer às normas técnicas IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE 802.3ab (1000Base-T), IEEE 802.3z (1000Base-X).
- Deve suportar o modo de comutação "store and forward".
- Deve possuir no mínimo 32 megabytes de memória Flash.
- Deve possuir no mínimo 64 megabytes de memória DRAM.
- Deve suportar a instalação de fonte de energia redundante.
- Deve ser instalável em rack padrão de 19”, sendo que deverão ser fornecidos os espectivos Kit’s de fixação.
- Deve implementar LAN Virtual (VLAN) conforme padrão IEEE 802.1Q.
- Deve permitir a criação de no mínimo 128 VLANs ativas baseadas em portas.
- Deve permitir a criação de no mínimo 128 instâncias do protocolo Spannig Tree.
- Deve implementar Wake on LAN.
- Deve permitir espelhar todo o tráfego do Switch para uma VLAN específica, permitindo que outro switch da rede conectado a esta VLAN receber o tráfego espelhado.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas “isoladas” e portas “promíscuas”, onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.
- Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deve Implementar “VLAN Trunking” padrão IEEE 802.1Q nas portas Fast

Ethernet e Gigabit Ethernet, devendo ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.

- Deve implementar a funcionalidade de "Port Trunking" conforme padrão IEEE 802.3ad.
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Fast Ethernet (em "full duplex").
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Gigabit Ethernet (em "full duplex").
- Deve permitir a criação de pelo menos 06 grupos de portas agregadas.
- Deve ser possível agrupar logicamente pelo menos 12 switches deste mesmo modelo e família, formando um "cluster" lógico e gerenciá-los graficamente através de um único endereço IP.
- Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada. Deve ser possível espelhar o tráfego originado em um switch do "cluster" lógico para uma porta de destino localizada em um switch diferente do "cluster".
- Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d.
- Deve implementar o padrão IEEE 802.1s ("Multiple Spanning Tree") para pelo menos 32 instâncias.
- Deve implementar o padrão IEEE 802.1w ("Rapid Spanning Tree").
- Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Deve implementar Voice VLAN.
- Deve permitir criar filtros de pacotes que atuem nas interfaces do equipamento somente em determinadas horas do dia mediante agendamento.
- Deve implementar pelo menos quatro filas de saída por porta.
- Deve implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.
- Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem/destino.
- Deve implementar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Deve implementar filtro de pacotes via ACL incluindo camada 4.
- Deve implementar autenticação via WEB de usuários criados localmente.
- Deve implementar serviço de portal Web para autenticação do usuário para acesso à rede.
- Deve implementar Dynamic ARP Inspection.
- Deve possuir mecanismo de supressão e controle de Multicast e Unicast.
- 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.
- Deve suportar autenticação e autorização via RADIUS.
- Deve implementar controle de acesso por porta (IEEE 802.1x). Deve ser suportada a atribuição de VLANs após a identificação do usuário, atribuição do

usuário a uma VLAN “Guest” caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional.

- Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Deve 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).
- Deve possuir uma interface de gerenciamento baseada em WEB (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão.
- Deve ser gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.
- Deve ser gerenciável via SSH versão 2 (SSHv2), suportando, no mínimo, o algoritmo de criptografia 3DES.
- Deve Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem.
- Deve ser gerenciável via SNMP (v1, v2 e v3) e RMON.
- Deve implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.
- Deve implementar LLDP.
- Deve implementar Local Proxy ARP.
- Deve implementar SCP.
- Deve implementar IGMP Querier.
- Deve implementar mecanismo "Weighted Tail Drop" em todas as interfaces.
- Deve implementar mecanimos de "Strict Priority" em todas as interfaces.
- Deve implementar TACACS+.
- Deve implementar filtros de quadros e/ou pacotes através de ACL.
- Deve implementar mecanismo de classificação de quadros e/ou pacotes via ACL.
- Deve permitir, baseado na classificação aplicada, priorizar todos os quadros e/ou pacotes classificados
- Deve implementar o protocolo Syslog para funções de “logging” de eventos.
- Deve permitir de upgrade de software através do protocolo TFTP.
- Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.
- Deve implementar “accounting” das conexões IEEE 802.1x. Devem ficar registradas pelo menos as seguintes informações da conexão : nome do usuário e grupo a que pertence, switch em que o computador do usuário está conectado, porta do switch usada para acesso, endereço MAC da máquina usada pelo usuário, horários de início e término da conexão, bytes transmitidos e recebidos.
- Deve 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente teste se conectar à porta.
- Deve ser possível estabelecer o número máximo de endereços MAC que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Deve permitir a criação de listas de acesso baseadas em endereços 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.
- Deve possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de

broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.
- Deve promover 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.
- Deve Implementar IGMP Snooping (v1, v2 e v3).

Item 16 - Switch 24 Portas 10/100/1000 BASE-T

Comutador de rede que atenda, no mínimo, às seguintes características:

- Deve possuir pelo menos 24 (vinte e quatro) portas 10/100/1000 BASE-T auto-sensing para conexão via cabo UTP e conector RJ-45.
- Deve suportar pelo menos 04 (quatro) portas de uplink flexíveis padrão Gigabit Ethernet, devendo suportar as interfaces 10/100/1000 com conector RJ45, 1000BaseT, 1000BaseSX e 1000BaseLX/LH.
- Todas as portas solicitadas devem ser utilizadas simultaneamente. Caso o equipamento utilize interfaces do tipo combo, deverão ser fornecidas interfaces adicionais para atender este termo sem prejuízo das portas solicitadas.
- Deve possuir uma matriz de comutação com pelo menos 30 Gbps.
- Deve possuir capacidade de processamento de pelo menos 37.0 milhões de pps.
- Deve possuir LEDs, por porta, que indiquem a integridade e atividade do link, a velocidade de conexão e também o modo de operação (half/full duplex).
- Deve suportar o encaminhamento de “mini jumbo frames” em todas as portas do switch (frames de 1530 bytes).
- Deve suportar o encaminhamento de “jumbo frames” nas portas Gigabit Ethernet do switch frames de 9018 bytes).
- Deve possuir capacidade para no mínimo 12000 endereços MAC.
- As interfaces devem obedecer às normas técnicas IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE 802.3ab (1000Base-T), IEEE 802.3z (1000Base-X).
- Deve suportar o modo de comutação "store and forward".
- Deve possuir no mínimo 32 megabytes de memória Flash.
- Deve possuir no mínimo 64 megabytes de memória DRAM.
- Deve suportar a instalação de fonte de energia redundante.
- Deve ser Instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos kit’s de fixação.
- Deve implementar LAN Virtual (VLAN) conforme padrão IEEE 802.1Q.
- Deve permitir a criação de no mínimo 128 VLANs ativas baseadas em portas.
- Deve permitir a criação de no mínimo 128 instâncias do protocolo Spannig Tree.
- Deve implementar Wake on LAN.
- Deve permitir espelhar todo o tráfego do Switch para uma VLAN específica, permitindo que outro switch da rede conectado a esta VLAN receber o tráfego espelhado.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas “isoladas” e portas “promíscuas”, onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.
- Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deve Implementar “VLAN Trunking” padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet, devendo ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
- Deve implementar a funcionalidade de “Port Trunking” conforme padrão IEEE 802.3ad.

- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Fast Ethernet (em “full duplex”).
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Gigabit Ethernet (em “full duplex”).
- Deve permitir a criação de pelo menos 12 grupos de portas agregadas.
- Deve ser possível agrupar logicamente pelo menos 12 switches deste mesmo modelo e família, formando um “cluster” lógico e gerenciá-los graficamente através de um único endereço IP.
- Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada. Deve ser possível espelhar o tráfego originado em um switch do “cluster” lógico para uma porta de destino localizada em um switch diferente do “cluster”.
- Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d.
- Deve implementar o padrão IEEE 802.1s (“Multiple Spanning Tree”) para pelo menos 32 instâncias.
- Deve implementar o padrão IEEE 802.1w (“Rapid Spanning Tree”).
- Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
- Deve implementar Voice VLAN.
- Deve permitir criar filtros de pacotes que atuem nas interfaces do equipamento somente em determinadas horas do dia mediante agendamento.
- Deve implementar pelo menos quatro filas de saída por porta.
- Deve implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF.
- Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem/destino.
- Deve implementar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
- Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Deve implementar filtro de pacotes via ACL incluindo camada 4.
- Deve implementar autenticação via WEB de usuários criados localmente.
- Deve implementar serviço de portal Web para autenticação do usuário para acesso à rede.
- Deve implementar Dynamic ARP Inspection.
- Deve possuir mecanismo de supressão e controle de Multicast e Unicast.
- 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.
- Deve suportar autenticação e autorização via RADIUS.
- Deve implementar controle de acesso por porta (IEEE 802.1x). Deve ser suportada a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN “Guest” caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional.
- Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC

de origem e destino.

- Deve 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).
- Deve possuir uma interface de gerenciamento baseada em WEB (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão.
- Deve ser gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.
- Deve ser gerenciável via SSH versão 2 (SSHv2), suportando, no mínimo, o algoritmo de criptografia 3DES.
- Deve Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem.
- Deve ser gerenciável via SNMP (v1, v2 e v3) e RMON.
- Deve implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.
- Deve implementar LLDP.
- Deve implementar Local Proxy ARP.
- Deve implementar SCP.
- Deve implementar IGMP Querier.
- Deve implementar mecanismo "Weighted Tail Drop" em todas as interfaces.
- Deve implementar mecanismos de "Strict Priority" em todas as interfaces.
- Deve implementar TACACS+.
- Deve implementar filtros de quadros e/ou pacotes através de ACL.
- Deve implementar mecanismo de classificação de quadros e/ou pacotes via ACL.
- Deve permitir, baseado na classificação aplicada, priorizar todos os quadros e/ou pacotes classificados
- Deve implementar o protocolo Syslog para funções de “logging” de eventos.
- Deve permitir de upgrade de software através do protocolo TFTP.
- Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.
- Deve implementar “accounting” das conexões IEEE 802.1x. Devem ficar registradas pelo menos as seguintes informações da conexão : nome do usuário e grupo a que pertence, switch em que o computador do usuário está conectado, porta do switch usada para acesso, endereço MAC da máquina usada pelo usuário, horários de início e término da conexão, bytes transmitidos e recebidos.
- Deve 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente teste se conectar à porta.
- Deve ser possível estabelecer o número máximo de endereços MAC que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Deve permitir a criação de listas de acesso baseadas em endereços 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.
- Deve possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.
- Deve promover 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.
- Deve Implementar IGMP Snooping (v1, v2 e v3).
- Possuir suporte ao protocolo IGMP(v1,v2 e v3).
- Implementar roteamento de camada 3 entre VLANs.
- Implementar roteamento estático e roteamento dinâmico via RIPv1 (RFC 1058) e RIPv2 (RFC 2453).

Item 17 - Switch 24 Portas 10/100/1000 BASE-T PoE

Comutador de rede que atenda, no mínimo, às seguintes características:

- Deve possuir pelo menos 24 (vinte e quatro) portas 10/100/1000 BASE-T auto-sensing para conexão via cabo UTP e conector RJ-45.
- Deve prover alimentação PoE em todas as portas, conforme o padrão IEEE 802.3at, fornecendo 370W de potencia exclusiva PoE, para todas as portas simultaneamente, com até 30W em cada porta.
- Deve ser fornecido com 4 (quatro) portas SFP padrão mini-GBIC, aceitando módulos 1000 Base SX e 1000 Base LX. Não admite-se que estas portas sejam do tipo COMBO com as portas Gigabit anteriores.
- Deve possuir 28 portas ativas simultaneamente.
- Deve possuir taxa de encaminhamento de pacotes de pelo menos 41.7 mpps.
- Deve possuir porta de console para total gerenciamento local, com conector RS-232 ou RJ-45.
- Deve permitir configuração/administração remota através de SSH e SNMPv3.
- Deve possuir funcionalidade que permita o autodescobrimento do equipamento conectado na porta do switch. Após este descobrimento, o switch deve aplicar sem intervenção humana as regras na porta (VLAN, ACL, velocidade) conforme o tipo de equipamento conectado.
- O equipamento deve permitir sua configuração automática com base em outro equipamento da rede, sem intervenção humana, permitindo a rápida substituição do equipamento. Ao ser ligado, o equipamento deve buscar esta configuração com base em parâmetros de DHCP previamente definidos.
- Deve permitir a criação de pelo menos 3 níveis de administração e configuração do switch.
- Deve permitir a criação de pelo menos 8 rotas estáticas, operando em camada 3, permitindo a operação como um pequeno backbone.
- Deve permitir o espelhamento do tráfego de uma porta (port mirroring) para outra porta do mesmo switch ou de um switch remoto dentro da rede.
- Deve possuir jumbo frame de 9000 bytes.
- Deve possuir IGMP snooping para IPv4 e IPv6.
- Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, e deve permitir a criação de no mínimo 128 VLANs com IDs entre 1 e 4094.
- Deve possuir autenticação IEEE 802.1x com as seguintes extensões: assinalamento de VLAN por usuário e Guest VLAN para usuários não autenticados. Para usuários sem cliente IEEE 802.1x instalado, deve possuir um portal Web para autenticação.
- Deve possuir autenticação IEEE 802.1x de múltiplos usuários por porta, para o caso de links com switches não gerenciáveis. Apenas o tráfego dos usuários que se autenticarem será permitido.
- Deve permitir configurar quantos endereços MAC podem ser aprendidos em uma porta (port security), e permitir configurar qual ação será tomada quando esta regra for quebrada, alertar ou desativar a porta.
- Deve ser compatível com solução de NAC do mesmo fabricante do equipamento proposto.
- Deve permitir autenticação através de endereço MAC da estação.

- Deve identificar automaticamente portas em que telefones IP estejam conectados e associá-las automaticamente a VLAN de voz.
- Deve possuir autenticação IEEE 802.1X.
- Deve possuir Spanning Tree padrão IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU, suportando pelo menos 32 instancias de STP.
- Deve permitir spanning tree por VLAN ou similar.
- Deve implementar a funcionalidade de portas protegidas ou similar, onde uma determinada porta não recebe o tráfego gerado por outras portas protegidas (unicast, multicast, broadcast).
- Deve possuir o protocolo “Network Timing Protocol” (NTP) autenticado para a sincronização do relógio com outros dispositivos.
- Deve permitir a configuração de DHCP Relay.
- Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1AB para descobrimento de uplinks.
- Deve permitir o envio de mensagens geradas pelo sistema em servidor externo (syslog).
- Deve permitir funcionalidade que bloqueie a quantidade de endereços MAC aprendidos numa determinada porta.
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V / 60Hz, consumindo não mais que 40W por equipamento em sua capacidade máxima de operação. Deve ser incluído cabo no padrão brasileiro ou conector 2P+T.
- Gabinete padrão para montagem em rack de 19". Deve acompanhar todos os acessórios para instalação.

Item 18 - Switch 48 Portas 10/100 BASE-T

Comutador de rede que atenda, no mínimo, às seguintes características:

- Deve possuir no mínimo 48 (quarenta e oito) portas 10/100Mbps com conectores RJ-45.
- Deve suportar pelo menos 02 (duas) portas de uplink flexíveis padrão Gigabit Ethernet, devendo suportar as interfaces 10/100/1000 com conector RJ45, 1000BaseT, 1000BaseSX e 1000BaseLX/LH.
- Todas as portas solicitadas devem ser utilizadas simultaneamente. Caso o equipamento utilize interfaces do tipo combo, deverão ser fornecidas interfaces adicionais para atender este termo sem prejuízo das portas solicitadas.
- Deve possuir uma matriz de comutação com pelo menos 40 Gbps.
- Deve possuir capacidade de processamento de pelo menos 9.0 milhões de pps.
- Deve possuir LEDs, por porta, que indiquem a integridade e atividade do link, a velocidade de conexão e também o modo de operação (half/full duplex).
- Deve suportar o encaminhamento de “mini jumbo frames” em todas as portas do switch (frames de 1530 bytes).
- Deve suportar o encaminhamento de “jumbo frames” nas portas Gigabit Ethernet do switch frames de 9018 bytes).
- Deve possuir capacidade para no mínimo 8000 endereços MAC.
- As interfaces devem obedecer às normas técnicas IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE 802.3ab (1000Base-T), IEEE 802.3z (1000Base-X).
- Deve suportar o modo de comutação "store and forward".
- Deve possuir no mínimo 32 megabytes de memória Flash.
- Deve possuir no mínimo 64 megabytes de memória DRAM.
- Deve suportar a instalação de fonte de energia redundante.
- Deve ser Instalável em bastidor padrão de 19”, sendo que deverão ser fornecidos os respectivos kit’s de fixação.

- Deve implementar LAN Virtual (VLAN) conforme padrão IEEE 802.1Q.
- Deve permitir a criação de no mínimo 128 VLANs ativas baseadas em portas.
- Deve permitir a criação de no mínimo 128 instâncias do protocolo Spannig Tree.
- Deve implementar Wake on LAN.
- Deve permitir espelhar todo o tráfego do Switch para uma VLAN específica, permitindo que outro switch da rede conectado a esta VLAN receber o tráfego espelhado.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas "isoladas" e portas "promíscuas", onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.
- Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deve Implementar "VLAN Trunking" padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet, devendo ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
- Deve implementar a funcionalidade de "Port Trunking" conforme padrão IEEE 802.3ad.
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Fast Ethernet (em "full duplex").
- Deve ser possível criar grupos de portas contendo pelo menos 02 portas Gigabit Ethernet (em "full duplex").
- Deve permitir a criação de pelo menos 06 grupos de portas agregadas.
- Deve ser possível agrupar logicamente pelo menos 12 switches deste mesmo modelo e família, formando um "cluster" lógico e gerenciá-los graficamente através de um único endereço IP.
- Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada. Deve ser possível espelhar o tráfego originado em um switch do "cluster" lógico para uma porta de destino localizada em um switch diferente do "cluster".
- Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d.
- Deve implementar o padrão IEEE 802.1s ("Multiple Spanning Tree") para pelo menos 32 instâncias.
- Deve implementar o padrão IEEE 802.1w ("Rapid Spanning Tree").
- Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Deve implementar Voice VLAN.
- Deve permitir criar filtros de pacotes que atuem nas interfaces do equipamento somente em determinadas horas do dia mediante agendamento.
- Deve implementar pelo menos quatro filas de saída por porta.
- Deve implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).
- Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.
- Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem/destino.
- Deve implementar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do

valor de DSCP, descarte do pacote.

- Deve implementar filtro de pacotes via ACL incluindo camada 4.
- Deve implementar autenticação via WEB de usuários criados localmente.
- Deve implementar serviço de portal Web para autenticação do usuário para acesso à rede.
- Deve implementar Dynamic ARP Inspection.
- Deve possuir mecanismo de supressão e controle de Multicast e Unicast.
- 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.
- Deve suportar autenticação e autorização via RADIUS.
- Deve implementar controle de acesso por porta (IEEE 802.1x). Deve ser suportada a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN “Guest” caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional.
- Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Deve 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).
- Deve possuir uma interface de gerenciamento baseada em WEB (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão.
- Deve ser gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.
- Deve ser gerenciável via SSH versão 2 (SSHv2), suportando, no mínimo, o algoritmo de criptografia 3DES.
- Deve Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem.
- Deve ser gerenciável via SNMP (v1, v2 e v3) e RMON.
- Deve implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.
- Deve implementar LLDP.
- Deve implementar Local Proxy ARP.
- Deve implementar SCP.
- Deve implementar IGMP Querier.
- Deve implementar mecanismo "Weighted Tail Drop" em todas as interfaces.
- Deve implementar mecanimos de "Strict Priority" em todas as interfaces.
- Deve implementar TACACS+.
- Deve implementar filtros de quadros e/ou pacotes através de ACL.
- Deve implementar mecanismo de classificação de quadros e/ou pacotes via ACL.
- Deve permitir, baseado na classififcação aplicada, priorizar todos os quadros e/ou pacotes classificados
- Deve implementar o protocolo Syslog para funções de “logging” de eventos.
- Deve permitir de upgrade de software através do protocolo TFTP.
- Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.
- Deve implementar “accounting” das conexões IEEE 802.1x. Devem ficar registradas pelo menos as seguintes informações da conexão : nome do usuário e grupo a que pertence, switch em que o computador do usuário está conectado,

porta do switch usada para acesso, endereço MAC da máquina usada pelo usuário, horários de início e término da conexão, bytes transmitidos e recebidos.

- Deve 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente teste se conectar à porta.
- Deve ser possível estabelecer o número máximo de endereços MAC que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Deve permitir a criação de listas de acesso baseadas em endereços 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.
- Deve possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.
- Deve promover 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.
- Deve Implementar IGMP Snooping (v1, v2 e v3).

Condições gerais

FORNECIMENTO DOS EQUIPAMENTOS

Todos os itens deverão ser fornecidos em suas embalagens originais, novos e sem uso anterior.

GARANTIA

A Garantia deve ser de no mínimo 3 (três) anos em regime 8x5 com reposição de peças no próximo dia útil, incluindo atendimento telefônico 24x7 através de ligação 0800 em português para abertura de chamados técnicos.

Deve ser garantido o fornecimento de atualização de software/firmware do equipamento pelo período de garantia sem custos para a UFSM.

Nos prazos de garantia mencionados acima, no caso de defeito do equipamento, a empresa fornecedora deverá disponibilizar à UFSM, no prazo máximo de 01 (um) dia útil, contado do recebimento de notificação formal da Unidade Solicitante da UFSM, um equipamento reserva, completamente funcional, de propriedade da empresa fornecedora, o qual ficará em operação até que a mesma restitua o equipamento defeituoso devidamente consertado ou o substitua por um novo da mesma marca e modelo. O equipamento reserva deverá ser da mesma marca e modelo do equipamento defeituoso a ser substituído.

Caso o equipamento reserva disponibilizado seja novo, sem uso, a UFSM poderá, se julgar conveniente, optar por substituir o equipamento defeituoso pelo equipamento reserva ao invés de aguardar um equipamento para reposição. A referida opção será informada formalmente pela UFSM à empresa fornecedora.

Todos os custos de disponibilização de equipamento reserva, conserto/substituição do equipamento defeituoso e demais aspectos da garantia, são de responsabilidade da empresa fornecedora.

Os equipamentos entregues em desconformidade com as quantidades solicitadas, qualidade e especificações constantes deste documento, do edital e da proposta, deverão, sem ônus para a UFSM, ser substituídos no prazo máximo de 07 (sete) dias corridos contados do recebimento de notificação formal da Unidade Solicitante da UFSM.

INSTALAÇÃO E CONFIGURAÇÃO

Após a entrega dos equipamentos, a contratada deverá configurar a solução no prazo máximo de 30 dias, ficando a instalação física a cargo da UFSM.

A empresa vencedora deverá apresentar sugestão de instalação da solução, com todos os parâmetros a serem configurados, após discussão em reuniões com a equipe técnica da UFSM.

Os serviços devem ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Antes da execução dos serviços, cabe a este órgão a solicitação de informações com relação à experiência e qualificação do técnico que fará os serviços, cabendo a este órgão, a aceitação ou a solicitação de troca de profissional.

Ao final da instalação, deverá ser realizado um repasse de conhecimento “hands-on”, apresentando as configurações realizadas nos equipamentos, com duração não inferior a 16 horas. O repasse de conhecimento deverá incluir treinamento básico para até 4 pessoas, nas dependências da UFSM, que disponibilizará o local adequado para a transferência do conhecimento e acesso aos equipamentos de produção.