



ANEXO – ESPECIFICAÇÕES TÉCNICAS

PROCESSO ADMINISTRATIVO Nº 09280.000134/2023-09

1. DEFINIÇÃO DO OBJETO DA CONTRATAÇÃO

Aquisição de comutadores centrais (switches core) e componentes para o Data Center do Ministério das Relações Exteriores (MRE), incluindo software de gerência, garantia de 60 (sessenta) meses, serviços agregados de instalação/migração e treinamento, para atender as necessidades do MRE, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

2. DESCRIÇÃO DA SOLUÇÃO DE TI

2.1. A solução se destina à implantação de switches core para a rede de Data Center do MRE, em topologia de rede “Spine and Leaf”, com tecnologia VXLAN (RFC7348) e suporte a SDN (Software Defined Network), conforme quantitativos a seguir:

Item	Produto	Quantidade	Métrica
1	Switch tipo 1 - Spine	2	Unidade
2	Switch tipo 2 – Leaf	8	Unidade
3	Switch tipo 3 – Distribuição	2	Unidade
4	Switch tipo 4 – Out of band	4	Unidade
5	Componentes tipo 1 – Conexões Spines/Leaves (20 metros)	18	Unidade
6	Componentes tipo 2 – Transceivers 10G	322	Unidade
8	Software de gerência de rede	1	Licença
9	Serviços de implantação, instalação e configuração	1	Serviço
10	Treinamento	30	Horas

3. ESPECIFICAÇÕES TÉCNICAS

3.1. Definição da solução:



3.1.1. A solução para provimento de arquitetura de rede de Data Center de duas camadas em topologia “Spine and Leaf”, composta pelos itens 1 e 2, deve conter:

- a) Conjunto de switches que realizarão as funções de “Spine” e “Leaf”.
- b) Camada de Plano de Controle (“underlay network”) com, no mínimo, as seguintes características:
 - I) Baseada em protocolo IP (camada 3 do modelo OSI);
 - II) Permitir a criação de uma topologia “full-mesh” sem loops e sem utilização do protocolo Spanning Tree;
 - III) Permitir balanceamento de tráfego baseado em ECMP (“Equal-Cost Multipath”) ou utilizar MP-BGP EVPN (Multiprotocol BGP Ethernet VPN);
 - IV) Compatível com o mecanismo de “Multi-Chassis Etherchannel (MEC)” ou “MultiChassis Link Aggregation (MLAG)” e/ou similares proprietário ou livre.
- c) Camada de Plano de Dados (“overlay network”), utilizando o protocolo Virtual eXtensible Local Area Network (VXLAN), RFC7348, com, no mínimo, as seguintes características:
 - I) Permitir configuração de VTEP (VXLAN Tunnel End Point) nos dispositivos físicos do Fabric (switches Leaf);
 - II) Permitir tráfego de camada 2 (intra-VXLAN) e camada 3 (inter-VXLAN);
 - III) Permitir função de “Layer 2 Gateway” ou “VTEP Gateway” para mapear VLANs para VXLANs e fazer encapsulamento e desencapsulamento de VXLAN;
 - IV) Configuração de ambiente Multi-Tenant, permitindo a criação de domínios lógicos segregados para atender diferentes aplicações.
- d) Suporte a Software Define Network (SDN) para permitir as funcionalidades de:
 - I) Ativação do plano de controle e do plano de dados de forma automatizada, permitindo, pelo menos, o suporte aos protocolos OpenFlow 1.3 ou superior, OpenConfig ou OVSDB;



II) Automação, configuração, gerenciamento e monitoração da saúde física dos equipamentos de forma centralizada, através de um controlador de rede, via GUI (“Graphical User Interface”);

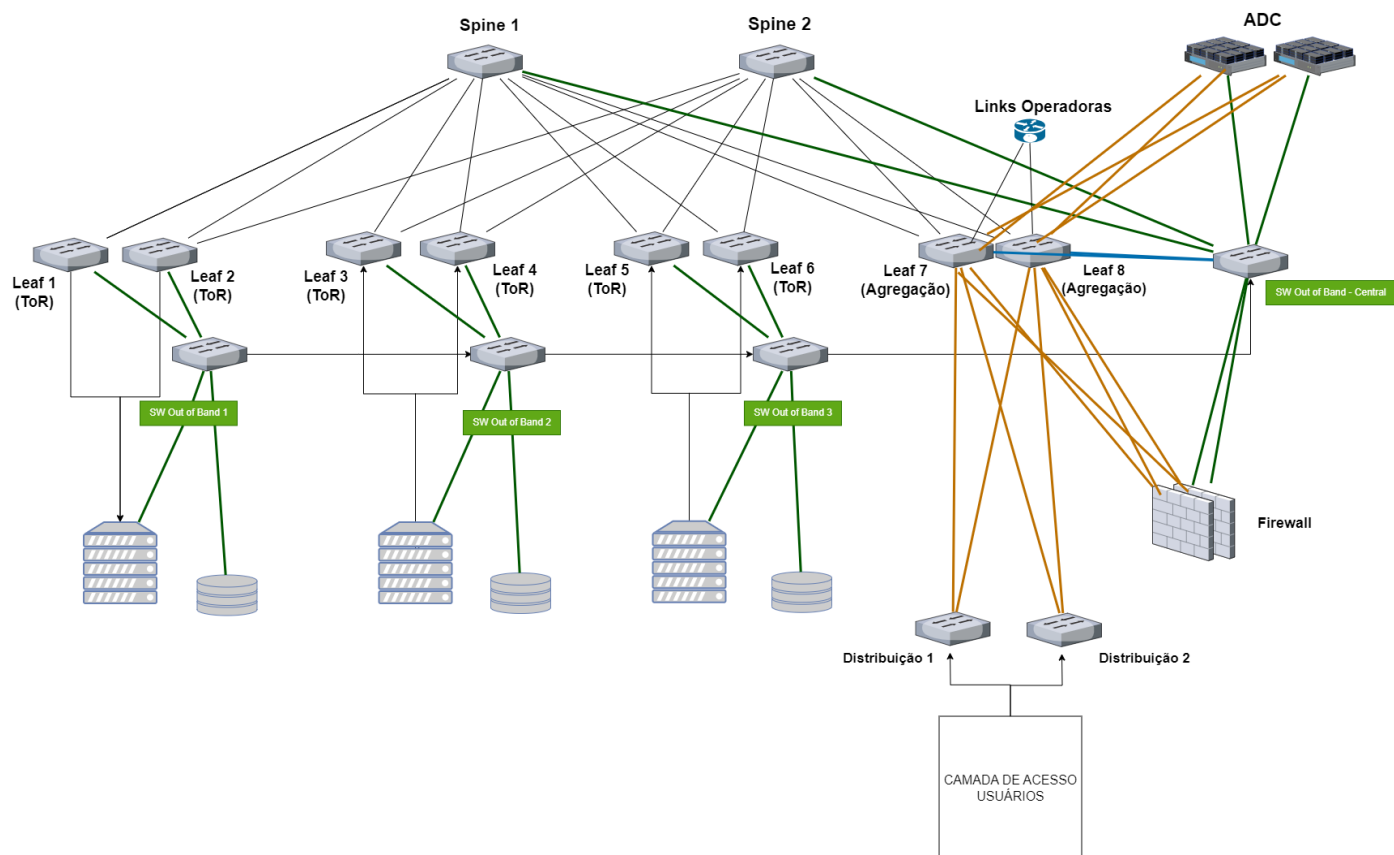
III) Configuração via API (“Application Programming Interface”) REST ou outra tecnologia compatível;

IV) Configuração via Python e Ansible.

- 3.1.2.** Os equipamentos devem possuir fontes de alimentação redundantes AC bivolt internas com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- 3.1.3.** As fontes dos equipamentos deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
- 3.1.4.** Os equipamentos devem ser capazes de sustentar a carga com todas as portas ativas, com apenas uma das fontes instalada.
- 3.1.5.** Os equipamentos devem permitir a troca da fonte redundante em pleno funcionamento, sem impacto na performance (“hot-swappable”).
- 3.1.6.** As fontes deverão vir acompanhadas com cabos de energia elétrica em conformidade com o padrão NBR14.136.
- 3.1.7.** Os equipamentos devem permitir operação normal em temperaturas de 0°C até 40°C.
- 3.1.8.** Os equipamentos devem ser instaláveis em rack padrão de 19” com fornecimento dos respectivos kit’s de fixação.
- 3.1.9.** Os equipamentos devem possuir sistema de ventilação redundante e que permitam substituição em caso de falha, sem necessidade de troca do switch.

3.2. Topologia de referência da solução:

- 3.2.1.** Com base na arquitetura atual do Data Center do MRE, o presente projeto visa a implantação de nova arquitetura em topologia “Spine and Leaf” conforme desenho a seguir:



3.3. Switch tipo 1 – Spine

3.3.1. As especificações a seguir devem ser aplicadas para cada switch do tipo 1 (Spine).

3.3.2. Hardware:

- 3.3.2.1.** Dispor de, no mínimo, 24 portas 40 Gigabit Ethernet, compatíveis com transceivers QSFP+/QSFP28 (não incluindo portas combo).
- 3.3.2.2.** A camada “Spine” deverá ser escalável, no mínimo, para 2 (dois) equipamentos.
- 3.3.2.3.** Possuir capacidade de associação das portas de mesma capacidade, no mínimo, em grupo de 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
- 3.3.2.4.** Dispor de fonte de alimentação redundante AC bivolt internas com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- 3.3.2.5.** As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
- 3.3.2.6.** Suportar balanceamento de carga entre as fontes de alimentação redundantes.



- 3.3.2.7.** As fontes devem ser dimensionadas para permitir o completo funcionamento do switch considerando a falha de metade das fontes ativas.
- 3.3.2.8.** Dispor de cabo de alimentação para a fonte com no mínimo 1,80m (um metro e oitenta centímetros) de comprimento.
- 3.3.2.9.** Ter dimensões compatíveis com montagem em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- 3.3.2.10.** Dispor de módulos de ventilação redundantes e “hot swappable”. O Data Center possui ar frio no corredor frontal.
- 3.3.2.11.** Dispor de porta de console para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
- 3.3.2.12.** Fornecer cabo de console compatível com a porta de console do equipamento. A extremidade do cabo que se conecta ao notebook deverá ser USB ou ser fornecido adaptador para USB.

3.3.3. Funcionalidades:

- 3.3.3.1.** Suportar a funcionalidade de “Spine”, na arquitetura “Spine and Leaf”.
- 3.3.3.2.** Dispor de configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas neste Termo de Referência.
- 3.3.3.3.** Possuir separação do plano de controle do plano de dados.
- 3.3.3.4.** Suportar capacidade de, no mínimo, 80 mil rotas IPv4 unicast.
- 3.3.3.5.** Possuir capacidade de pelo menos 128.000 endereços MAC na tabela de comutação.
- 3.3.3.6.** Suportar capacidade de encaminhamento de pacotes em camada 2 de no mínimo 3,2 Tbps.
- 3.3.3.7.** Suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com a solução.
- 3.3.3.8.** Dispor de sistema operacional modular e permitir a aplicação de patches no sistema operacional.
- 3.3.3.9.** Permitir a atualização de software sem perda de pacotes (ISSU – In Service Software Upgrades). Também serão aceitas soluções que implementem um cluster de 2 (dois) ou mais switches em uma arquitetura que permita a atualização de software sem perda de pacotes.



- 3.3.3.10.** Permitir, pelo menos, o acesso via CLI (“Command Line Interface”).
- 3.3.3.11.** Implementar SSH para acesso à interface de linha de comando.
- 3.3.3.12.** Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento.
- 3.3.3.13.** Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (SecureCopy) utilizando um cliente padrão ou SFTP (Secure FTP).
- 3.3.3.14.** Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- 3.3.3.15.** Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- 3.3.3.16.** Implementar o protocolo NTP (Network Time Protocol).
- 3.3.3.17.** Permitir o encaminhamento de “jumbo frames” (pacotes de 9216 bytes).
- 3.3.3.18.** Dispor de ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- 3.3.3.19.** Suportar protocolo de coleta de informações de fluxos que trafegam pelo equipamento contemplando as informações do sFlow v5.
- 3.3.3.20.** Permitir especificar o uso de uma funcionalidade somente para tráfego de entrada, somente para tráfego de saída (e também para ambos os sentidos simultaneamente) em uma dada interface.
- 3.3.3.21.** Permitir o espelhamento da totalidade do tráfego de uma porta ou de um grupo de portas para outra porta localizada no mesmo switch ou para outro dispositivo remoto. Deverá ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- 3.3.3.22.** Implementar roteamento estático.
- 3.3.3.23.** Implementar protocolo de roteamento dinâmico OSPF.
- 3.3.3.24.** Implementar protocolo de roteamento BGPv4 e MP-BGP (“Multiprotocol Extensions for BGP-4”).
- 3.3.3.25.** Implementar o padrão IEEE 802.3ad.



- 3.3.3.26.** Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).
- 3.3.3.27.** Devem ser fornecidas todas as licenças necessárias, do tipo perpétua(s), para implementar todas as funcionalidades e/ou protocolos descritos neste Termo de Referência.

3.3.4. Gerenciamento:

- 3.3.4.1.** Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- 3.3.4.2.** Implementar, pelo menos, os seguintes níveis de segurança para SNMP versão 3:
 - a)** Sem autenticação e sem privacidade (noAuthNoPriv);
 - b)** Com autenticação e sem privacidade (authNoPriv);
 - c)** Com autenticação e com privacidade (authPriv) utilizando algoritmos de criptografia AES.
- 3.3.4.3.** Ter suporte a MIB II.
- 3.3.4.4.** Permitir a implementação da MIB privativa que forneça informações relativas ao funcionamento do equipamento.
- 3.3.4.5.** Conter descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
- 3.3.4.6.** Permitir a obtenção da configuração do equipamento através do protocolo SNMP.
- 3.3.4.7.** Permitir a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
- 3.3.4.8.** Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
- 3.3.4.9.** Dispor de armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
- 3.3.4.10.** Permitir a criação ou restauração de versões de configuração e suporte a “rollback” ou “restore” da configuração para versões anteriores.



- 3.3.4.11.** Suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet e RADIUS, provendo identificação gerencial única ao equipamento de rede.
- 3.3.4.12.** Dispor de 1 (uma) porta 1000BaseT, com conector RJ-45, para gerência do equipamento. Esta porta será conectada na rede de gerência e o switch deverá permitir a configuração de endereço IP próprio para gerenciamento.

3.3.5. Funcionalidades de segurança:

- 3.3.5.1.** Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação, Autorização e Contabilização.
- 3.3.5.2.** Proteger a interface de comando do equipamento através de senha.
- 3.3.5.3.** Implementar o protocolo SSH para acesso à interface de linha de comando.
- 3.3.5.4.** Permitir a criação de listas de controle de acesso (ACL) baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- 3.3.5.5.** Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
- 3.3.5.6.** Implementar listas de controle de acesso (ACL - Access Control List) para IPv4 e IPv6.
- 3.3.5.7.** Implementar listas de controle de acesso (ACL), com definições de parâmetros de camada 2, 3 e 4.
- 3.3.5.8.** Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- 3.3.5.9.** Controlar e auditar quais comandos os usuários e grupos de usuários podem executar em determinados elementos de rede.
- 3.3.5.10.** Permitir o controle do volume de tráfego unicast ou unknown unicast, multicast e broadcast de uma interface, atribuindo porcentagens ou taxas permitidas para cada um dos tráfegos.

3.4. Switch tipo 2 – Leaf

- 3.4.1.** As especificações a seguir devem ser aplicadas para cada switch do tipo 2 (Leaf).



3.4.2. Hardware:

- 3.4.2.1.** Dispor de, no mínimo, 48 portas 10/25 Gigabit Ethernet non-blocking.
- 3.4.2.2.** Dispor de, no mínimo, 4 portas 40 Gigabit Ethernet QSFP+ non-blocking.
- 3.4.2.3.** Possuir capacidade de associação das portas 10/25 Gigabit Ethernet, no mínimo, em grupo de 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
- 3.4.2.4.** Possuir capacidade de associação das portas 40 Gigabit Ethernet, no mínimo, em grupo de 2 (duas) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
- 3.4.2.5.** Dispor de porta de console para acesso à interface de linha de comando. Poderá ser fornecida porta de console serial RJ-45 ou USB, para ligação direta.
- 3.4.2.6.** Fornecer cabo de console compatível com a porta de console do equipamento.
- 3.4.2.7.** A extremidade do cabo que se conecta ao notebook deverá ser USB ou ser fornecido adaptador para USB.
- 3.4.2.8.** Dispor de fonte de alimentação redundante AC bivolt internas com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- 3.4.2.9.** As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
- 3.4.2.10.** Suportar balanceamento de carga entre as fontes de alimentação redundantes.
- 3.4.2.11.** As fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte.
- 3.4.2.12.** Dispor de cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.
- 3.4.2.13.** Sustentar a carga de todo o equipamento com todas as portas ativas.
- 3.4.2.14.** Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- 3.4.2.15.** Possuir, no máximo, 2RU ("Rack Unit").

3.4.3. Funcionalidades:

- 3.4.3.1.** Suportar a funcionalidade de "Leaf", na arquitetura "Spine and Leaf".



- 3.4.3.2.** Permitir o acesso via GUI (“Graphical User Interface”) e CLI (“Command Line Interface”).
- 3.4.3.3.** Implementar SSH para acesso à interface de linha de comando.
- 3.4.3.4.** Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- 3.4.3.5.** Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- 3.4.3.6.** Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- 3.4.3.7.** Implementar o protocolo NTP (Network Time Protocol).
- 3.4.3.8.** Permitir o encaminhamento de “jumbo frames” (pacotes de 9216 bytes).
- 3.4.3.9.** Dispor de ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- 3.4.3.10.** Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo equipamento.
- 3.4.3.11.** Deverá permitir a implementação de 2 (duas) sessões de espelhamento de tráfego simultaneamente.
- 3.4.3.12.** Permitir a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
- 3.4.3.13.** Permitir implementação de VLANs por porta.
- 3.4.3.14.** Permitir implementação de VLANs compatíveis com o padrão IEEE 802.1q.
- 3.4.3.15.** Permitir implementação de mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q.
- 3.4.3.16.** Possuir capacidade de pelo menos 128.000 endereços MAC na tabela de comutação.
- 3.4.3.17.** Suportar capacidade de encaminhamento de pacotes em camada 2 de no mínimo 1,2 Tbps.
- 3.4.3.18.** Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- 3.4.3.19.** Implementar padrão IEEE 802.1q (Vlan Frame Tagging).



- 3.4.3.20.** Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- 3.4.3.21.** Implementar padrão IEEE 802.3ad.
- 3.4.3.22.** Implementar padrão IEEE 802.1AB (LLDP).
- 3.4.3.23.** Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).
- 3.4.3.24.** Implementar roteamento estático.
- 3.4.3.25.** Implementar protocolo de roteamento dinâmico OSPF.
- 3.4.3.26.** Implementar protocolo de roteamento BGPv4 e MP-BGP (Multiprotocol Extensions for BGP-4).
- 3.4.3.27.** Dispor de configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas neste Termo de Referência.
- 3.4.3.28.** Fornecer todas as licenças necessárias para implementar todas as funcionalidades e/ou protocolos descritos neste Termo de Referência.

3.4.4. Gerenciamento:

- 3.4.4.1.** Permitir implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- 3.4.4.2.** Permitir implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - a)** Sem autenticação e sem privacidade (noAuthNoPriv);
 - b)** Com autenticação e sem privacidade (authNoPriv);
 - c)** Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia DES.
- 3.4.4.3.** Ter suporte a MIB II.
- 3.4.4.4.** Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
- 3.4.4.5.** Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
- 3.4.4.6.** Permitir a obtenção da configuração do equipamento através do protocolo SNMP.



- 3.4.4.7.** Permitir a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
 - 3.4.4.8.** Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
 - 3.4.4.9.** Dispor de armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
 - 3.4.4.10.** Permitir a criação ou restauração de versões de configuração e suporte a “rollback” ou “restore” da configuração para versões anteriores.
 - 3.4.4.11.** Permitir a atualização de software sem perda de pacotes (ISSU – In Service Software Upgrades). Também serão aceitas soluções que implementem um cluster de 2 (dois) ou mais switches em uma arquitetura que permita a atualização de software sem perda de pacotes.
 - 3.4.4.12.** Dispor de 1 (uma) porta 1000BaseT, com conector RJ-45, para gerência do equipamento. Esta porta será conectada na rede de gerência e o Switch deverá permitir a configuração de endereço IP próprio para gerenciamento.
 - 3.4.4.13.** Suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet e RADIUS, provendo identificação gerencial única ao equipamento de rede.
- 3.4.5.** Funcionalidades de segurança:
- 3.4.5.1.** Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um Servidor de Autenticação/Autorização do tipo RADIUS.
 - 3.4.5.2.** Proteger a interface de comando do equipamento através de senha.
 - 3.4.5.3.** Implementar o protocolo SSH para acesso à interface de linha de comando.
 - 3.4.5.4.** Permitir a criação de listas de controle de acesso (ACL) baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
 - 3.4.5.5.** Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
 - 3.4.5.6.** Implementar listas de controle de acesso (ACL - Access Control List) para IPv4 e IPv6.



- 3.4.5.7.** Implementar listas de controle de acesso (ACL), com definições de parâmetros de camada 2, 3 e 4.
- 3.4.5.8.** Implementar listas de controle de acesso (ACL), em todas as interfaces e VLANs, para tráfegos ingress ou egress.
- 3.4.5.9.** Possuir controle de broadcast, multicast e unicast por porta, podendo limitar o tráfego em porcentagem de banda ou pacotes por segundo (PPS).
- 3.4.5.10.** Implementar mecanismos de AAA (Authentication, Authorization e Accounting).
- 3.4.5.11.** Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- 3.4.5.12.** Controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede.
- 3.4.5.13.** Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- 3.4.5.14.** Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP.
- 3.4.5.15.** Possuir análise do protocolo ARP (“Address Resolution Protocol”) com proteção nativa contra ataques do tipo “ARP Poisoning” ou soluções contra ataque ARP Spoofing.
- 3.4.5.16.** Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding”, conforme previsto no padrão IEEE 802.1w.

3.5. Switch tipo 3 – Distribuição

- 3.5.1.** As especificações a seguir devem ser aplicadas para cada switch do tipo 3 (Distribuição).
- 3.5.2.** Hardware:
 - 3.5.2.1.** Dispor de, no mínimo, 48 portas 10 Gigabit Ethernet non-blocking.
 - 3.5.2.2.** Dispor de, no mínimo, 4 portas 40 Gigabit Ethernet non-blocking.



- 3.5.2.3.** Possuir capacidade de associação das portas 10 Gigabit Ethernet, no mínimo, em grupo de 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
 - 3.5.2.4.** Possuir capacidade de associação das portas 40 Gigabit Ethernet, no mínimo, em grupo de 2 (duas) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
 - 3.5.2.5.** Permitir a criação de links de agregação entre interfaces dos equipamentos deste tipo. Essa funcionalidade também é conhecida como Multi-Chassis Link Aggregation, Multi-Chassis Etherchannel, Multi-Switch Link Aggregation (M-LAG) ou Virtual PortChannel.
 - 3.5.2.6.** Possuir porta de console para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
 - 3.5.2.7.** Fornecer cabo de console compatível com a porta de console do equipamento.
 - 3.5.2.8.** A extremidade do cabo que se conecta ao notebook deverá ser USB ou ser fornecido adaptador para USB.
 - 3.5.2.9.** Dispor de fonte de alimentação redundante AC bivolt internas com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
 - 3.5.2.10.** As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
 - 3.5.2.11.** Suportar balanceamento de carga entre as fontes de alimentação redundantes.
 - 3.5.2.12.** As fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte.
 - 3.5.2.13.** Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.
 - 3.5.2.14.** Ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas.
 - 3.5.2.15.** Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
 - 3.5.2.16.** Possuir, no máximo, 2RU ("Rack Unit").
- 3.5.3.** Funcionalidades:
- 3.5.3.1.** Permitir o acesso via CLI (command line interface).



- 3.5.3.2.** Implementar SSH para acesso à interface de linha de comando.
- 3.5.3.3.** Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- 3.5.3.4.** Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- 3.5.3.5.** Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- 3.5.3.6.** Implementar o protocolo NTP (Network Time Protocol).
- 3.5.3.7.** Permitir o encaminhamento de “jumbo frames” (pacotes de 9216 bytes).
- 3.5.3.8.** Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- 3.5.3.9.** Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo equipamento.
- 3.5.3.10.** Permitir a implementação de 2 (duas) sessões de espelhamento de tráfego simultaneamente.
- 3.5.3.11.** Implementar VLANs por porta.
- 3.5.3.12.** Implementar VLANs compatíveis com o padrão IEEE 802.1q.
- 3.5.3.13.** Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q.
- 3.5.3.14.** Ter capacidade de pelo menos 100.000 endereços MAC na tabela de comutação.
- 3.5.3.15.** Suportar capacidade de encaminhamento de pacotes em camada 2 de no mínimo 1 Tbps.
- 3.5.3.16.** Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- 3.5.3.17.** Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- 3.5.3.18.** Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- 3.5.3.19.** Implementar padrão IEEE 802.3ad.
- 3.5.3.20.** Implementar padrão IEEE 802.1AB (LLDP).



- 3.5.3.21.** Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).
- 3.5.3.22.** Implementar roteamento estático.
- 3.5.3.23.** Implementar protocolo de roteamento dinâmico OSPF.
- 3.5.3.24.** Implementar protocolo de roteamento BGPv4 e MP-BGP (“Multiprotocol Extensions for BGP-4”).
- 3.5.3.25.** Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas neste Termo de Referência.
- 3.5.3.26.** Fornecer todas as licenças necessárias para implementar todas as funcionalidades e/ou protocolos descritos neste Termo de Referência.

3.5.4. Gerenciamento:

- 3.5.4.1.** Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- 3.5.4.2.** Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - a)** Sem autenticação e sem privacidade (noAuthNoPriv);
 - b)** Com autenticação e sem privacidade (authNoPriv);
 - c)** Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia DES.
- 3.5.4.3.** Ter suporte a MIB II.
- 3.5.4.4.** Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
- 3.5.4.5.** Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
- 3.5.4.6.** Permitir a obtenção da configuração do equipamento através do protocolo SNMP.
- 3.5.4.7.** Permitir a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
- 3.5.4.8.** Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.



- 3.5.4.9.** Dispor de armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
- 3.5.4.10.** Permitir criação ou restauração de versões de configuração e suporte a “rollback” ou “restore” da configuração para versões anteriores.
- 3.5.4.11.** Possuir 1 (uma) porta 1000BaseT, com conector RJ-45, para gerência do equipamento. Esta porta será conectada na rede de gerência e o Switch deverá permitir a configuração de endereço IP próprio para gerenciamento.
- 3.5.4.12.** Suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet e RADIUS, provendo identificação gerencial única ao equipamento de rede.

3.5.5. Funcionalidades de segurança:

- 3.5.5.1.** Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um Servidor de Autenticação/Autorização do tipo RADIUS.
- 3.5.5.2.** Proteger a interface de comando do equipamento através de senha.
- 3.5.5.3.** Implementar o protocolo SSH para acesso à interface de linha de comando.
- 3.5.5.4.** Permitir a criação de listas de controle de acesso (ACL) baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- 3.5.5.5.** Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
- 3.5.5.6.** Implementar listas de controle de acesso (ACL - Access Control List) para IPv4 e IPv6.
- 3.5.5.7.** Implementar listas de controle de acesso (ACL), com definições de parâmetros de camada 2, 3 e 4.
- 3.5.5.8.** Implementar listas de controle de acesso (ACL), em todas as interfaces e VLANs, para tráfegos ingress ou egress.
- 3.5.5.9.** Possuir controle de broadcast, multicast e unicast por porta, podendo limitar o tráfego em porcentagem de banda ou pacotes por segundo (PPS).
- 3.5.5.10.** Implementar mecanismos de AAA (Authentication, Authorization e Accounting).



- 3.5.5.11.** Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- 3.5.5.12.** Controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede.
- 3.5.5.13.** Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- 3.5.5.14.** Dispor de método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP.
- 3.5.5.15.** Possuir análise do protocolo ARP (Address Resolution Protocol) com proteção nativa contra ataques do tipo “ARP Poisoning” ou soluções contra ataque ARP Spoofing.
- 3.5.5.16.** Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree”.
- 3.5.5.17.** Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding”, conforme previsto no padrão IEEE 802.1w.

3.6. Switch tipo 4 – Out of Band

- 3.6.1.** As especificações a seguir devem ser aplicadas para cada switch do tipo 4 (Out of Band).
- 3.6.2.** Hardware:
 - 3.6.2.1.** Dispor de, no mínimo, 48 portas UTP 1 Gigabit Ethernet non-blocking.
 - 3.6.2.2.** Dispor de, no mínimo, 4 portas SFP+ 10 Gigabit Ethernet non-blocking.
 - 3.6.2.3.** Possuir capacidade de associação das portas 1 Gigabit Ethernet, no mínimo, em grupo de 4 (quatro) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
 - 3.6.2.4.** Possuir capacidade de associação das portas 10 Gigabit Ethernet, no mínimo, em grupo de 2 (duas) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
 - 3.6.2.5.** Ter porta de console para acesso à interface de linha de comando. Poderá ser fornecida porta de console serial RJ-45 ou USB, para ligação direta.



- 3.6.2.6.** Fornecer cabo de console compatível com a porta de console do equipamento.
- 3.6.2.7.** Possuir fonte de alimentação redundante AC bivolt internas com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- 3.6.2.8.** As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
- 3.6.2.9.** Suportar balanceamento de carga entre as fontes de alimentação redundantes.
- 3.6.2.10.** As fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte.
- 3.6.2.11.** Dispor de cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.
- 3.6.2.12.** Ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas.
- 3.6.2.13.** Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- 3.6.2.14.** Possuir, no máximo, 1RU (Rack Unit).

3.6.3. Funcionalidades:

- 3.6.3.1.** Permitir o acesso via CLI (“Command Line Interface”).
- 3.6.3.2.** Implementar SSH para acesso à interface de linha de comando.
- 3.6.3.3.** Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- 3.6.3.4.** Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- 3.6.3.5.** Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- 3.6.3.6.** Implementar o protocolo NTP (“Network Time Protocol”).
- 3.6.3.7.** Permitir o encaminhamento de “jumbo frames” (pacotes de 9216 bytes).
- 3.6.3.8.** Dispor de ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.



- 3.6.3.9.** Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo equipamento.
- 3.6.3.10.** Implementar 2 (duas) sessões de espelhamento de tráfego simultaneamente.
- 3.6.3.11.** Implementar VLANs por porta.
- 3.6.3.12.** Implementar VLANs compatíveis com o padrão IEEE 802.1q.
- 3.6.3.13.** Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q.
- 3.6.3.14.** Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação.
- 3.6.3.15.** Suportar capacidade de encaminhamento de pacotes em camada 2 de no mínimo 960 Mbps.
- 3.6.3.16.** Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- 3.6.3.17.** Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- 3.6.3.18.** Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- 3.6.3.19.** Implementar padrão IEEE 802.3ad.
- 3.6.3.20.** Implementar padrão IEEE 802.1AB (LLDP).
- 3.6.3.21.** Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).
- 3.6.3.22.** Implementar roteamento estático.
- 3.6.3.23.** Implementar protocolo de roteamento dinâmico OSPF.
- 3.6.3.24.** Implementar protocolo de roteamento BGPv4 e MP-BGP (“Multiprotocol Extensions for BGP-4”).
- 3.6.3.25.** Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas neste Termo de Referência.
- 3.6.3.26.** Fornecer todas as licenças necessárias para implementar todas as funcionalidades e/ou protocolos descritos neste Termo de Referência.

3.6.4. Gerenciamento:



- 3.6.4.1.** Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
 - 3.6.4.2.** Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - a)** Sem autenticação e sem privacidade (noAuthNoPriv);
 - b)** Com autenticação e sem privacidade (authNoPriv);
 - c)** Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia DES.
 - 3.6.4.3.** Ter suporte a MIB II.
 - 3.6.4.4.** Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
 - 3.6.4.5.** Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
 - 3.6.4.6.** Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
 - 3.6.4.7.** Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
 - 3.6.4.8.** Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
 - 3.6.4.9.** Dispor de armazenamento interno das mensagens de log geradas pelo equipamento de, no mínimo, 2048 bytes.
 - 3.6.4.10.** Permitir a criação ou restauração de versões de configuração e suporte a “rollback” ou “restore” da configuração para versões anteriores.
 - 3.6.4.11.** Dispor de 1 (uma) porta 1000BaseT, com conector RJ-45, para gerência do equipamento. Esta porta será conectada na rede de gerência e o switch deverá permitir a configuração de endereço IP próprio para gerenciamento.
 - 3.6.4.12.** Suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet e RADIUS, provendo identificação gerencial única ao equipamento de rede.
- 3.6.5.** Funcionalidades de segurança:



- 3.6.5.1.** Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um Servidor de Autenticação/Autorização do tipo RADIUS.
- 3.6.5.2.** Proteger a interface de comando do equipamento através de senha.
- 3.6.5.3.** Implementar o protocolo SSH para acesso à interface de linha de comando.
- 3.6.5.4.** Permitir a criação de listas de controle de acesso (ACL) baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- 3.6.5.5.** Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
- 3.6.5.6.** Implementar listas de controle de acesso (ACL - Access Control List) para IPv4 e IPv6.
- 3.6.5.7.** Implementar listas de controle de acesso (ACL), com definições de parâmetros de camada 2, 3 e 4.
- 3.6.5.8.** Implementar listas de controle de acesso (ACL), em todas as interfaces e VLANs, para tráfegos “ingress” ou “egress”.
- 3.6.5.9.** Possuir controle de broadcast, multicast e unicast por porta, podendo limitar o tráfego em porcentagem de banda ou pacotes por segundo (PPS).
- 3.6.5.10.** Implementar mecanismos de AAA (Authentication, Authorization e Accounting).
- 3.6.5.11.** Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- 3.6.5.12.** Controlar e auditar quais comandos os usuários e grupos de usuários podem executar em determinados elementos de rede.
- 3.6.5.13.** Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- 3.6.5.14.** Dispor de método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo servidor de DHCP.
- 3.6.5.15.** Possuir análise do protocolo ARP (Address Resolution Protocol) com proteção nativa contra ataques do tipo “ARP Poisoning” ou soluções contra ataque ARP Spoofing.



3.6.5.16. Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree”.

3.6.5.17. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding”, conforme previsto no padrão IEEE 802.1w.

3.7. Componentes tipo 1 – Conexões Spines/Leaves

3.7.1. Cabo DAC (Direct Attach Cable) ou AOC (Active Optical Cable) com transceivers 40Gbps QSFP+ integrados em ambas as pontas.

3.7.2. Permitir a instalação em slots/portas tipo QSFP+.

3.7.3. Deve ser do tipo “hot-swappable”, permitindo sua conexão/desconexão com o equipamento em operação.

3.7.4. Deve possuir comprimento mínimo de 20 (vinte) metros.

3.7.5. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados nos itens switch tipo 1, switch tipo 2 e switch tipo 3 deste Termo de Referência.

3.8. Componentes tipo 2 – Transceivers 10G

3.8.1. Transceiver 10G Multimodo (LC) com o padrão 10GBase-SR, operando sobre fibras multimodo OM3/OM4 para distâncias de até 300m/400m, respectivamente.

3.8.2. Ser compatível com fibras de 850nm.

3.8.3. Permitir a instalação em slots/portas tipo SFP+.

3.8.4. Deve ser do tipo “hot-swappable”, permitindo sua conexão/desconexão com o equipamento em operação.

3.8.5. Dispor de conector do tipo LC duplex.

3.8.6. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados no item switch tipo 3 deste Termo de Referência.

3.9. Software de gerência de rede:



- 3.9.1.** O sistema de gerenciamento de equipamentos de rede do Data Center deverá ser fornecido em quantidade suficiente para atender a necessidade da solução.
- 3.9.2.** Deve ser fornecido com todos os hardwares e licenças necessários para a implementação de todas as funcionalidades descritas nas especificações técnicas deste documento.
- 3.9.3.** Os controladores deverão ser licenciados e capazes de operar, controlar e gerenciar o total de equipamentos do objeto desta contratação.
- 3.9.4.** Os controladores de rede poderão ser fornecidos através de um conjunto de dispositivos físicos e software ou apenas por software.
- 3.9.5.** Deverá ter solução de alta disponibilidade e recuperação de desastres em Data Centers distintos.
- 3.9.6.** Deverá realizar a ativação do plano de controle (“underlay network”) e do plano de dados (“overlay network”) nos switches pertencentes à arquitetura “Spine and Leaf” de forma automatizada.
- 3.9.7.** Deverá realizar automação, configuração, gerenciamento e monitoração da saúde física dos equipamentos, via GUI (“Graphical User Interface”).
- 3.9.8.** Deverá permitir a criação de versões de configuração dos equipamentos pertencentes à topologia “Spine and Leaf” e suporte a “rollback” da configuração para versões anteriores.
- 3.9.9.** Deverá expor como serviço, via API (“Application Programming Interface”) REST, todas as configurações de rede, tanto da camada “underlay” quanto da camada “overlay”, permitindo a configuração da infraestrutura de rede por orquestradores externos.
- 3.9.10.** Deverá ser capaz de implementar o protocolo SSH para acesso à interface de linha de comando, protegido por senha.
- 3.9.11.** Deverá ser capaz de implementar mecanismo de autenticação e autorização para acesso local ou remoto à solução, baseado em RADIUS ou grupos LDAP.
- 3.9.12.** Permitir, controlar e auditar quais comandos os usuários e grupos de usuários podem executar em determinados elementos de rede.



- 3.9.13.** Devem ser fornecidos em regime de alta disponibilidade através de clusters de gerenciamento redundantes.
- 3.9.14.** Deverá suportar níveis de usuários com permissões diferentes, contemplando pelo menos nível administrador, operador e visualização.
- 3.9.15.** Realizar a configuração dos protocolos e recursos necessários para a ativação das camadas UNDERLAY e OVERLAY nos switches pertencentes ao Fabric de rede do Data Center de forma automatizada, através de interface gráfica (GUI).
- 3.9.16.** Permitir configurar microssegmentação e políticas de segurança.
- 3.9.17.** Prover recursos de configuração de, no mínimo, as seguintes funcionalidades: NTP, DNS, DHCP, VRF, OSPF e BGP.
- 3.9.18.** Possuir integração via API com as seguintes soluções:
 - 3.9.18.1.** VMware vSphere;
 - 3.9.18.2.** VMware NSX-T.

3.10. Serviços de implantação, instalação e configuração

- 3.10.1.** Os serviços de instalação e configuração, necessários para a operacionalização dos switches na topologia “Spine and Leaf”, conforme especificado neste Termo de Referência, além da implantação e configuração do software de gerenciamento, devem ser executados pela Contratada.
- 3.10.2.** A implantação, instalação e configuração dos componentes deverá seguir o seguinte cronograma:
 - 3.10.2.1.** Etapa 1 – Preparo e iniciação do projeto: Etapa de definição do escopo, abrangência, validação dos requisitos técnicos e cronograma do projeto de instalação e configuração.
 - 3.10.2.2.** Etapa 2 – Plano e arquitetura da solução: Etapa de planejamento, desenho e concepção da solução.
 - 3.10.2.3.** Etapa 3 – Configuração e integração da solução: Etapa de instalação, configuração, integração e testes da solução instalada.
 - 3.10.2.4.** Etapa 5 – Migração: Etapa de planejamento e execução da migração de recursos da infraestrutura existente à nova solução.



3.10.2.5. Etapa 6 – Garantia especializada do fabricante: A contratada auxiliará a contratante no entendimento e suporte à operação da solução instalada em produção e deverá auxiliar o MRE no Gerenciamento de Incidentes junto ao suporte técnico do fabricante da solução.

3.10.3. A qualidade dos serviços deve ser assegurada por meio da disponibilização de equipe técnica qualificada com técnicos especialistas do fabricante da solução contratada.

3.11. Treinamento

3.11.1. O treinamento deve garantir que toda a informação gerada durante os processos de instalação e migração seja integral e formalmente apresentada à equipe da Contratante por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente.

3.11.2. É parte integrante do escopo do treinamento a disponibilização de toda a documentação técnica, incluindo manuais de instalação, configuração e de usuário, relativa a todos os componentes integrantes da solução.

3.11.3. A contratada deverá apresentar um Plano de Transferência de Conhecimento com 30 horas de treinamento, apresentando o conteúdo, carga horária diária, duração em dias e avaliações de aprendizagem. O treinamento poderá ser ministrado pela manhã ou manhã e tarde, a critério do MRE.

3.11.4. O treinamento deverá prever a capacitação para 6 alunos.

3.11.5. A transferência de conhecimento deverá ser realizada em Brasília-DF, preferencialmente nas dependências do MRE, por técnicos com certificação(ões) técnica(s) emitida(s) pelo fabricante dos equipamentos. Caso não seja possível a realização do treinamento nas dependências do MRE, a Contratada deverá prover toda a estrutura para o treinamento.

3.11.5.1. Em casos excepcionais a serem julgados pelo MRE, a transferência de conhecimento poderá ser realizada na modalidade de ensino a distância (EAD).

3.11.6. A Contratada deverá fornecer toda a infraestrutura necessária para a realização do treinamento.

3.11.7. Todo material didático disponibilizado no treinamento deverá ser fornecido pela Contratada e estarão inclusos no escopo da transferência de conhecimento.



3.11.8. Ao término da transferência de conhecimento, deverá ser realizada uma avaliação da atividade por parte da equipe do MRE, que atribuirá as seguintes classificações:

3.11.8.1. A – Mais que suficiente

3.11.8.2. B – Suficiente

3.11.8.3. C – Insuficiente

3.11.9. Caso 50% (cinquenta por cento) ou mais avalie a transferência de conhecimento como insuficiente, a Contratada deverá providenciar, sem ônus, outro período para a transferência de conhecimento.

3.11.10. Ao final de cada transferência de conhecimento, cada treinando deverá receber um certificado de participação.

3.11.11. A contratada arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades da transferência de conhecimento.

4. GARANTIA E SUPORTE

4.1. A garantia deverá abranger os itens 1, 2, 3, 4, 5, 6 e 8 (conforme item 2.1) do objeto deste Termo de Referência, garantindo o correto funcionamento pelo período de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo (TRD) da solução.

4.2. A contratada deverá prover canal para abertura de chamados, em regime 24x7, onde serão registrados pelo MRE as solicitações de garantia e manutenção.

4.3. A contratada deverá repassar ao MRE todas as senhas do sistema. Ficará a critério do MRE alterá-las segundo sua conveniência. A contratada deverá incluir no Manual de Operação os procedimentos para troca de todas as senhas de administração da solução e software de gerência de rede.

4.4. A contratada deverá agir preventivamente (p.ex.: manutenções proativas sobre problemas conhecidos) a fim de garantir o funcionamento do equipamento e mitigar riscos devido ao seu uso continuado.

4.5. A contratada deverá atuar em incidentes ou problemas identificados pela equipe técnica do MRE e que requeira intervenção técnica especializada do fabricante, de modo a restabelecer o pleno funcionamento dos equipamentos.

4.6. Os serviços de suporte técnico especializado deverão ser prestados pela empresa contratada, às próprias expensas, na forma on-site, em regime 24x7, incluindo a atualização de softwares



e bases de dados de conhecimento e sempre que for necessário ao bom funcionamento da solução adquirida.

- 4.7.** O suporte técnico especializado deverá ser executado por corpo técnico qualificado, sendo funcionários pertencentes ao quadro da contratada, e com certificação comprovada pelo fabricante da solução, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual. Os serviços não terão custos adicionais ao MRE e deverão ser prestados durante todo o período de garantia.
- 4.8.** O suporte técnico deverá ser prestado de forma presencial na sede do MRE ou em outro endereço, em Brasília-DF, indicado pela DISI. É vedado o suporte remoto.
- 4.9.** Todas as peças e componentes necessários ao perfeito funcionamento da solução, quando necessário, devem ser substituídos pela contratada sem custos adicionais ao MRE.
- 4.10.** Caso a intervenção técnica indique interrupção de algum dos serviços operados pelo(s) switch(es), o MRE poderá determinar que a contratada execute a manutenção fora do horário de expediente, inclusive em finais de semana, sem qualquer ônus adicional ao MRE.
- 4.11.** É vedada a desativação de hardware, software ou quaisquer recursos computacionais da contratante sem prévio conhecimento e autorização expressa. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais do MRE, a contratada deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado, sob pena de inexecução parcial do contrato. Em caso da necessidade de retirada do equipamento, o MRE poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional.
- 4.12.** Caso algum dos equipamentos apresentem defeito de fabricação ou necessite reparo que não possa ser realizado nas dependências do MRE, a contratada deverá substituir imediatamente o equipamento por um novo, por mesmo modelo ou superior em características técnicas, do mesmo fabricante, sem ônus para o MRE, e deverá deixá-lo instalado e em operação no ambiente.
- 4.13.** Havendo necessidade de substituição de hardware, a contratada deverá efetuar a substituição por mesmo modelo de peça ou superior em características técnicas, do mesmo fabricante, sem ônus para o MRE, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:
- a) Caso ocorram 4 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;



- b) Caso ocorram problemas recorrentes no mesmo hardware, seja na restauração ou na substituição de peças, assim considerada como recorrente a repetição de uma mesma falha em um intervalo inferior a 2 (dois) meses;
- c) O(s) equipamento(s) (hardware) empregado(s) em substituição ao(s) equipamento(s) defeituoso(s) deverá(ão) possuir prazo de garantia equivalente àquela prevista em contrato.

4.14. Ao término de cada evento de suporte técnico e manutenção deverá ser gerado e entregue à DISI, em até 5 (cinco) dias após o serviço, um Relatório de Atendimento Técnico (RAT) com as seguintes características:

- a) Tipo de serviço de suporte e manutenção realizado, bem como toda a verificação realizada;
- b) Registro com a identificação do equipamento (nome/modelo/série);
- c) Descrição clara do(s) problema(s) identificado(s), procedimentos adotados para a sua resolução e o tempo de resolução para o chamado.