Banco do Nordeste

ANEXO II

QUANTITATIVOS E CARACTERÍSTICAS DOS EQUIPAMENTOS

1. FINALIDADE

As informações contidas neste Anexo descrevem os requisitos gerais, quantitativos e especificações técnicas de componentes e equipamentos necessários à implantação da solução tecnológica objeto do Edital. A solução deverá contemplar comutadores *(switches)* de acesso à rede local, de acordo com as quantidades e requisitos deste Anexo.

Os requisitos para fornecimento da solução especificados neste documento deverão ser rigorosamente atendidos. O não atendimento a qualquer das exigências, por completo ou em parte, desclassifica a proposta.

2. REQUISITOS COMUNS PARA O FORNECIMENTO DOS EQUIPAMENTOS COMUTADORES (SWITCHES)

2.1. Todos os componentes fornecidos no escopo da contratação em pauta deverão ser novos, isto é, sem utilização anterior.

2.2. Deverão ser fornecidos todos os acessórios para montagem apropriada em armário de fiação (rack) no padrão especificado neste Anexo.

2.3. Deverá observar, ainda, que quais acessórios não explícitos abaixo, tais como: memórias (de qualquer natureza), cabos elétricos, suportes e quaisquer outros componentes essenciais ao funcionamento deverão estar inclusos na solução ofertada, sendo todos os componentes da solução cobertos pelos termos da garantia e suporte durante toda a vigência contratual.

3. CARACTERÍSTICAS DOS COMUTADORES DE ACESSO À REDE LOCAL (SWITCHES)

Item 1 – Aquisição de Switches para agências

Para suprir todas as necessidades gerais por pontos de rede no BANCO, as configurações abaixo são para aquisição de equipamentos novos e com funcionalidades mais aderentes às novas necessidades de acesso. Descrevemos a seguir as principais características que deverão ser minimamente atendidas nos comutadores de acesso.

3.1. QUANTIDADE DE EQUIPAMENTOS

3.1.1. deverão ser fornecidos 366 (trezentos e sessenta e seis) equipamentos para este item.

3.2. NECESSIDADE DE AQUISIÇÃO NA CAMADA DE ACESSO À REDE LOCAL (SWITCHES)

3.2.1. devem possuir LED's indicativos do estado de funcionamento do equipamento;

3.2.2. devem possibilitar a obtenção de estatísticas de tráfego e falhas das portas para todas as portas;

3.2.3. devem estar equipados com recursos que permitam a reconfiguração dinâmica das diversas portas e módulos, inclusive permitindo a ativação e desativação de portas e

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

módulos sem causar reinício, instabilidade ou qualquer impacto que venha a comprometer o funcionamento do equipamento;

3.2.4. devem implementar ajuste de *clock* utilizando NTP (*Network Time Protocol*);

3.2.5. devem permitir a atualização de versões de código utilizando os protocolos *File Transfer Protocol* (FTP) ou *Trivial File Transfer Protocol* (TFTP);

3.2.6. devem permitir enviar logs para servidores remotos (*Syslog*);

3.2.7. devem implementar *traceroute* para o descobrimento do caminho seguido por um pacote dentro da rede;

3.2.8. todas as portas deverão ser autoconfiguráveis MDI/MDIX dispensando o uso de cabos *cross over* ou qualquer configuração para conexão a outro switch;

3.2.9. devem permitir que um conjunto de switches seja administrado por único endereço IP;

3.2.10. o número de switches trabalhando em conjunto deverá ser de no mínimo 8 (oito);

3.2.11. devem suportar protocolo para cópias seguras de arquivos de configuração do switch, seja *Secure Copy Protocol* (SCP) ou *Secure File Transfer Protocol* (SFTP);

3.2.12. devem estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (*Simple Network Management Protocol*), com suporte a RFC 1213 (MIB-II). Suporte ao SNMP v3;

3.2.13. deve suportar protocolo de gerenciamento e configuração através do protocolo NETCONF;

3.2.14. devem permitir a monitoração de desempenho de tráfego entre o switch e outro equipamento via MIB SNMP;

3.2.15. devem implementar mecanismos de monitoramento e análise local e remota de tráfego em portas de switches pertencentes a uma mesma VLAN, através de configuração de espelhamento de portas;

3.2.16. devem suportar o *Link Layer Discovery Protocol* (LLDP) e *LLDP for Media Endpoint Devices* (LLDP-MED): Padrão do IEEE para descobrimento de dispositivos em nível de enlace em redes Ethernet;

3.2.17. devem estar equipados com 1 (uma) porta de comunicação *out-of-band* para gerenciamento de configuração, podendo essa ser uma porta serial, ou isolar uma porta de comunicação do switch através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso;

3.2.18. devem estar equipados com recursos que permitam o gerenciamento através de *Command Line Interface* (CLI);

3.2.19. deverá estar equipado com recursos que permitam o gerenciamento através de web browser com suporte a SSL (*Secure Socket Layer*) versão 3 ou e SSH (*Secure Shell*) versão 2;

3.2.20. devem estar equipados com recursos que permitam o gerenciamento através de TELNET;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

3.2.21. devem implementar autenticação centralizada de controle de acesso dos equipamentos através de RADIUS ou TACACS+ (ou padrão compatível);

3.2.22. devem possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas, ocupando uma unidade (1U), sendo incluso o fornecimento dessas peças para prender no rack, conhecidas como "orelhas" por exemplo, ou trilhos, mantendo 1U;

3.2.23. a capacidade encaminhamento de pacotes na camada 2 (dois) ou camada 3 (três), quando aplicável (modelo de referência OSI), em milhões de pacotes por segundo (pacotes de 64 bytes) com a qual cada equipamento deverá estar equipado deve ser de no mínimo 42 (quarenta e dois);

3.2.24. a matriz de comutação (*Switch Fabric*) deverá ter capacidade de *throughput* mínima de 56 (cinquenta e seis) gigabits por segundo;

3.2.25. a quantidade de memória DRAM (ou SDRAM) que o equipamento deve possuir (em megabytes) deve ser de no mínimo 512 (quinhentos e doze);

3.2.26. a quantidade de memória Flash que o equipamento deve possuir (em megabytes) é de no mínimo 128 (cento e vinte e oito);

MÓDULOS / PLACAS DE INTERFACES REQUERIDOS

3.2.27. LAN: 10/100/1000 Mbps, interfaces RJ-45, para cabos UTP categoria 6 ou superior, full duplex, *GigaEthernet, autosense*, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT;

QUANTIDADE DE PORTAS INSTALADAS

3.2.28. quantidade mínima de portas com interfaces RJ-45, para cabos UTP categoria 6, 10/100/1000BaseTX, *full duplex*, *ethernet*, *autosense*, que deverão estar instaladas em cada comutador (switch), para conexão de estações de trabalho: 24 (vinte e quatro);

3.2.29. quantidade mínima de slots SFP, para cabos LC, Gigabit, que deverão estar instaladas em cada comutador (switch), para conexão de *uplink*: 4 (quatro). Deverão ser entregues 4 *transceivers* Gigabit SFP para fibras LC multimodo;

REQUISITOS DE SEGURANÇA

3.2.30. os equipamentos devem implementar o gerenciamento de configuração através da porta de gerenciamento com processo de autenticação e identificação positiva ou implementar o gerenciamento de configuração através da porta de gerenciamento *out-of-band* ou *xmodem* (console) com processo de autenticação e identificação positiva;

3.2.31. devem permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao switch via Telnet. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

3.2.32. devem implementar ACLs baseadas em Portas (Ethernet) Físicas do switch;

3.2.33. devem implementar ACLs baseadas em tempo;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

Banco do Nordeste

3.2.34. devem implementar autenticação de login/senha para a liberação de tráfego na porta através do protocolo IEEE 802.1x com as seguintes funcionalidades:

a) atribuição de VLAN conforme a autenticação do usuário;

b) reautenticação forçada de todas as portas;

c) reautenticação periódica e definição de período de inatividade após falha de autenticação;

3.2.35. devem permitir a configuração de portas confiáveis e não confiáveis de forma a manter uma tabela correlacionando informações como porta, VLAN, IP, MAC para cada interface não confiável. Os servidores DHCP, por exemplo, devem estar conectados a interfaces confiáveis, pois qualquer resposta a uma solicitação DHCP será descartada em interfaces não confiáveis. Tal funcionalidade garante maior segurança e controle das redes LAN;

3.2.36. devem implementar mecanismos de *Authentication*, *Authorization* e *Accounting* (AAA) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA;

3.2.37. todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

3.2.38. devem permitir controlar quais comandos os usuários e grupos de usuário podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados, assim como todas as tentativas de execução de comandos não autorizadas feitas por usuários que tiverem acesso ao equipamento gerenciado;

3.2.39. devem utilizar o protocolo TCP para prover maior confiabilidade ao tráfego dos envolvidos no controle administrativo;

3.2.40. devem permitir autenticação mútua entre o servidor AAA e o cliente AAA;

3.2.41. devem implementar mecanismos ao nível de porta de acesso que bloqueiem pacotes BPDUs inesperados;

3.2.42. devem possuir capacidade de limitação de endereços MAC por porta, acessíveis em uma dada interface de LAN do switch;

3.2.43. devem suportar a visualização de endereços MAC aprendidos pelo switch;

3.2.44. caso um MAC seja remanejado (fisicamente) para outra porta do switch, ou para outro switch na rede, o switch deverá de forma dinâmica entender a movimentação desse MAC não sendo necessário nenhum comando manual ou qualquer outro procedimento que não seja automático para que o switch aprenda o novo local do MAC;

3.2.45. devem implementar 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;

3.2.46. devem possibilitar controle de *broadcast* por porta através de comando específico. Não será permitido o controle de broadcast por porta através de ACL (Access Control List). O controle deve ser compatível com IPv4 e IPv6;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

3.2.47. devem possibilitar controle de *multicast* por porta através de comando específico. Não será permitido o controle de *multicast* por porta através de ACL (*Access Control List*). O controle deve ser compatível com IPv4 e IPv6;

PROTOCOLOS E PADRÕES REQUERIDOS

3.2.48. devem implementar, além dos padrões necessários para os requisitos desse edital, os seguintes protocolos e padrões:

3.2.48.1. IEEE 802.3, 10BaseT;

3.2.48.2. IEEE 802.3u, 100BaseTX;

3.2.48.3. IEEE 802.3ab, 1000BaseT;

3.2.48.4. IEEE802.3x, *Flow Control*;

3.2.48.5. IEEE 802.1q, VLAN *Tagging*;

3.2.48.6. IEEE 802.1d, S*panningTree*;

3.2.48.7. IEEE 802.1s, *Multiple Spanning Tree*;

3.2.48.8. IEEE 802.3ad, Link *Aggregation*;

3.2.48.9. IEEE 802.1x, *Port-Level Security*;

3.2.48.10. IEEE 802.1w, *Rapid Spanning Tree*;

3.2.49. devem implementar mecanismos de minimização do tempo de convergência de *Spanning-Tree* em caso de falha de enlace ou switch da rede local, e as seguintes funcionalidades: configuração da porta para o estado de *forwarding* automaticamente, manutenção da raiz do *Spanning-Tree* (*Root Guard*) e detecção de tráfego *Spanning-Tree* com opção de desabilitação da porta em caso de detecção positiva;

3.2.50. deve implementar proteção de BDPU por portas que de acordo com configuração irá permitir ou não o recebimento de BPDU na interface. Deverá ser possível configurar desativação automática da porta para proteção caso receba BDPU (recurso BPDU *Guard* ou equivalente), e deverá ser possível somente filtrar ou desconsiderar a BDPU (recurso BPDU *filter* ou equivalente). Para as portas desativadas por recebimento de BPDU, se configurada dessa forma, deverá ser possível o retorno automático das portas, ou seja, a reativação das interfaces, sem a necessidade de atuação manual;

3.2.51. devem implementar quadros ethernet de no mínimo 4000 bytes (*Jumbo Frames*) nas portas Gigabit Ethernet;

VLANs (Virtual LANs)

3.2.52. a quantidade mínima de VLAN's que deverão ser suportadas deve ser de 512 (quinhentas e doze);

3.2.53. devem implementar o protocolo de *trunking* IEEE 802.1q para que o tráfego de várias VLANs possa passar por um enlace. O switch deve implementar protocolo de negociação de *trunking*;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

QUALIDADE DE SERVIÇO

3.2.54. devem possuir 4 (quatro) filas em cada porta. Estas portas devem implementar os seguintes algoritmos de processamento de filas:

3.2.54.1. *Weighted Round Robin* (WRR) ou *Shaped Round Robin* (SRR) ou similar;

3.2.54.2. devem permitir a classificação de tráfego baseada em IEEE 802.1p;

MAC ADDRESS

3.2.55. a quantidade de MAC *address* que poderão ser utilizados simultaneamente deverá ser de no mínimo 8000 (oito mil);

AGREGAÇÃO DE PORTAS

3.2.56. devem implementar o aumento da largura de banda (nas ligações para comutador (switch) de núcleo e de acesso e para microcomputadores), através da agregação de múltiplas portas físicas funcionando como uma única porta lógica, conforme padrão IEEE 802.3ad. Este requisito valerá para todas as portas descritas no item "MÓDULOS / PLACAS DE INTERFACES SUPORTADOS";

3.2.57. o switch deve implementar o protocolo de negociação *Link Aggregation Control Protocol* (LACP);

MULTICAST

3.2.58. devem implementar funcionalidades de IP *multicast* via *Internet Group Management Protocol* (IGMP) *snooping* versões 1, 2 e 3 do IGMP;

3.2.59. deve suportar no mínimo 128 grupos IGMP;

DHCP

3.2.60. deverá implementar funcionalidades de *Dynamic Host Configuration Protocol* (DHCP) *snooping* e DHCP *Server*;

SISTEMA DE ALIMENTAÇÃO

3.2.61. a fonte alimentação deverá funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático;

3.2.62. deve possuir ventilação ativa através de um ou mais ventiladores para dissipação de calor. Deve possuir também ajuste inteligente de velocidade;

Item 2 – Aquisição de Switches Empilháveis para unidades de grande porte

Entende-se por unidade de grande porte, superintendências, centrais e/ou agência com mais de 100 usuários, além de contemplar mais de um rack de comunicação e com mais de 3 pavimentos.

Os números e funcionalidades abaixo informados fazem parte de um padrão de atendimento mínimo, podendo sofrer acréscimo em itens específicos abaixo para cada tipo de equipamento.

3.3. QUANTIDADE DE EQUIPAMENTOS

3.3.1. deverão ser fornecidos 30 (trinta) equipamentos para este item;

Banco do Nordeste

3.4. CARACTERÍSTICAS GERAIS REQUERIDAS DOS EQUIPAMENTOS

3.4.1. devem possuir LED's indicativos do estado de funcionamento do equipamento;

3.4.2. devem possibilitar a obtenção de estatísticas de tráfego e falhas das portas para todas as interfaces *in-band*.;

3.4.3. devem estar equipados com recursos que permitam a reconfiguração dinâmica das diversas portas e/ou módulos, inclusive permitindo a ativação e desativação de portas e/ou módulos sem causar reinício, instabilidade ou qualquer impacto que venha a comprometer o funcionamento do equipamento;

3.4.4. o equipamento deve ser montável em rack 19" devendo este vir acompanhado dos devidos acessórios para fixação no rack;

3.4.5. devem estar equipados com fonte de alimentação interna que trabalhe em 100V- 240V, 50/60 Hz, com detecção automática de tensão e frequência;

3.4.6. deve haver detecção automática MDI/MDIX em todas as portas de dados 10/100/1000BASE-T RJ-45;

3.4.7. todos os equipamentos deverão ser novos, ou seja, sem utilização anterior;

3.4.8. todos os equipamentos ativos de rede (switches) deverão ser do mesmo fabricante, incluindo software de gerenciamento;

3.4.9. o equipamento deve implementar ajuste de *clock* utilizando NTP (*Network Time Protocol*) com autenticação MD5 ou superior;

3.4.10. devem permitir a atualização de versões de código utilizando os protocolos de transferência de arquivo como por exemplo *File Transfer Protocol* (FTP) ou *Trivial File Transfer Protocol* (TFTP);

3.4.11. devem implementar protocolo para cópias seguras de arquivos de configuração do switch, seja *Secure Copy Protocol* (SCP) ou *Secure File Transfer Protocol* (SFTP);

3.4.12. devem implementar *ping* e *traceroute* para o descobrimento do caminho seguido por um pacote dentro da rede;

3.4.13. devem implementar SSH cliente;

3.4.14. todos os cabos e qualquer necessidade de hardware, software ou licença para o empilhamento deverão ser fornecidos pela contratada;

3.4.15. o endereçamento IP das pilhas, as VLANS para cada rack, bem como demais requisitos de configuração serão fornecidas pelo Banco durante implementação;

3.4.16. os switches de acesso deverão ser entregues com todas as licenças, conectores e *transceivers* necessários para o atendimento de todos os recursos, bem como qualquer outro componente lógico ou físico;

3.4.17. devem possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas, ocupando uma unidade (1U) cada switch;

3.4.18. as fontes deverão funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

Banco do Nordeste

3.4.19. devem implementar a configuração de uma VLAN de voz em cada porta para a separação do tráfego de telefonia IP;

3.4.20. devem implementar no mínimo 4000(quatro mil) VLANs ativas simultaneamente;

3.4.21. devem implementar protocolo MVRP (*Multiple VLAN Registration Protocol*) ou similar;

3.4.22. implementar quantidade mínima de 16.000 (dezesseis mil) MAC *address* que poderão ser utilizados simultaneamente;

PROTOCOLOS E PADRÕES REQUERIDOS

3.4.23. devem implementar, além dos padrões necessários para os requisitos desse edital, os seguintes protocolos e padrões:

3.4.23.1. IEEE 802.3u, 100BaseTX;

3.4.23.2. IEEE 802.3ab, 1000BaseT;

3.4.23.3. IEEE 802.3z, 1000BaseSX;

3.4.23.4. IEEE 802.1q, VLAN *Tagging*;

3.4.23.5. IEEE 802.1d, *SpanningTree*;

3.4.23.6. IEEE 802.1s, *Multiple Spanning Tree*, com suporte a no mínimo 04 instâncias simultâneas do protocolo *Spanning Tree*;

3.4.23.7. IEEE 802.3ad, *Link Aggregation*;

3.4.23.8. IEEE 802.1x, *Port-Level Security*;

3.4.23.9. IEEE 802.1w, *Rapid Spanning Tree*;

3.4.24. devem implementar mecanismos de minimização do tempo de convergência de *Spanning-Tree* em caso de falha de enlace ou switch da rede local, e as seguintes funcionalidades: configuração da porta para o estado de *forwarding* automaticamente, manutenção da raiz do *Spanning-Tree* (*Root Guard*) e detecção de tráfego *Spanning-Tree* com opção de desabilitação da porta em caso de detecção positiva;

3.4.25. devem implementar proteção de BDPU por portas que de acordo com configuração irá permitir ou não o recebimento de BPDU na interface. Deverá ser possível configurar desativação automática da porta para proteção caso receba BDPU (recurso BPDU *Guard* ou equivalente), e deverá ser possível somente filtrar ou desconsiderar a BDPU (recurso BPDU *filter* ou equivalente). Para as portas desativadas por recebimento de BPDU, se configurada dessa forma, deverá ser possível o retorno automático das portas, ou seja, a reativação das interfaces, sem a necessidade de atuação manual;

3.4.26. gerenciamento básico de IPv6, contemplando suporte a endereçamento *unicast*;

3.4.27. devem implementar quadros ethernet de no mínimo 9000 bytes (*Jumbo Frames*);

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

GERENCIAMENTO

3.4.28. devem estar equipados com 1 (uma) porta de comunicação *out-of-band* para gerenciamento de configuração, podendo essa ser uma porta serial, ou isolar uma porta de comunicação do switch através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso;

3.4.29. devem estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (*Simple Network Management Protocol*), sendo através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6. Serão aceitas RFCs em suas respectivas novas versões;

3.4.30. devem estar equipados com recursos que permitam o gerenciamento através de *Command Line Interface* (CLI) utilizando SSHv2;

3.4.31. deve suportar protocolo de gerenciamento NETCONF;

3.4.32. suportar *Sflow*, *Netflow* ou *Netstream*;

3.4.33. devem estar equipados com recursos que permitam o gerenciamento através de web browser com suporte a SSL (*Secure Socket Layer*), permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas. Este recurso poderá ser atendido através do software de gerenciamento fornecido;

3.4.34. devem permitir enviar logs para servidores remotos (*Syslog*), sendo pelo menos 2 (dois) servidores de destinos;

3.4.35. devem implementar espelhamento de porta e RSPAN (*Remote Mirroring*). No caso dos switches de acesso, deve permitir espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local;

3.4.36. devem implementar funcionalidades de gerenciamento relativas aos padrões de gerenciamento RMON (*Remote Network Monitor*) de acordo com a RFC 1757 ou 2819 com pelo menos 4 (quatro) grupos. Não serão aceitos *probes* externos ao equipamento. Para a solução *Spine/Leaf* poderão ser fornecidas funcionalidades semelhantes;

3.4.37. implementar o *Link Layer Discovery Protocol* (LLDP): Padrão do IEEE para descobrimento de dispositivos em nível de enlace em redes Ethernet;

AGREGAÇÃO DE PORTAS

3.4.38. devem implementar o aumento da largura de banda através da agregação de múltiplas portas físicas funcionando como uma única porta lógica, conforme padrão IEEE 802.3ad. Este requisito deverá ser válido para todas as portas descritas no subitem "**Quantidade de portas instaladas**" de cada item;

3.4.39. devem ser utilizados para agregação o protocolo de negociação *Link Aggregation Control Protocol* (LACP);

VLANS (VIRTUAL LANS)

3.4.40. implementar adição e distribuição, exclusão e renomeação automática de VLANs a partir de configuração realizada de forma centralizada, via software de gerência e diretamente no *fabric* quando for o caso;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

3.4.41. devem implementar o protocolo de *trunking* IEEE 802.1q para que o tráfego de várias VLANs possa passar por um enlace;

FUNCIONALIDADES DE SEGURANÇA

3.4.42. devem implementar autenticação centralizada de controle de acesso dos equipamentos através de RADIUS ou TACACS+ (ou padrão compatível);

3.4.43. devem implementar pelo menos dois níveis de permissão de usuário, sendo leitura (com comandos de visualização) e escrita (usuário administrador);

3.4.44. devem implementar o gerenciamento de configuração através da porta de gerenciamento (console) com processo de autenticação e identificação positiva;

3.4.45. devem implementar VLAN privada onde cada porta é protegida de outra sem que haja comunicação entre si. Serão aceitos protocolos semelhantes que executem este isolamento de portas;

3.4.46. devem implementar funcionalidades de IP *multicast* via *Internet Group Management Protocol* (IGMP) *snooping* versões 1 e 2 do IGMP;

3.4.47. devem suportar IGMPv1 (RFC 1112) e IGMP v2 (RFC 2236);

3.4.48. devem implementar funcionalidades de *Multicast Listener Discovery* (MLD) *Snooping* v1/v2;

3.4.49. devem implementar RFC 2710 (IPv6 Multicast Listener Discovery v1 (MLDv1)) e RFC 3810 (IPv6 Multicast Listener Discovery v2 (MLDv2)). Serão aceitas RFCs em suas respectivas novas versões;

3.4.50. devem implementar mecanismos de *Authentication, Authorization* e *Accounting* (AAA);

3.4.51. devem criptografar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

3.4.52. devem permitir controlar quais comandos os usuários e grupos de usuário podem executar nos equipamentos gerenciados;

3.4.53. deverá ser possível registrar no servidor tipo AAA ou via envio de *syslog* todos os comandos executados, assim como todas as tentativas de execução de comandos não autorizadas feitas por usuários que tiverem acesso ao equipamento gerenciado;

3.4.54. devem permitir autenticação mútua entre o servidor AAA e o cliente AAA;

3.4.55. devem implementar mecanismos ao nível de porta de acesso que bloqueiem pacotes BPDUs inesperados;

3.4.56. devem ser possível visualização de endereços MAC aprendidos pelo switch;

3.4.57. caso um MAC seja remanejado (fisicamente) para outra porta do switch, ou para outro switch na rede, o switch deverá de forma dinâmica entender a movimentação desse MAC não sendo necessário nenhum comando manual ou qualquer outro procedimento que não seja automático para que o switch aprenda o novo local do MAC;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

Banco do Nordeste

3.4.58. devem implementar a associação de um endereço MAC específico a uma dada porta do Switch, de modo que somente a estação/dispositivo que tenha tal endereço MAC possa usar a referida porta para conexão;

3.4.59. devem possibilitar controle de broadcast por porta através de comando específico. Não será permitido o controle de broadcast por porta através de ACL (*Access Control List*);

3.4.60. devem possibilitar controle de *multicast* por porta através de comando específico. Não será permitido o controle de *multicast* por porta através de ACL (*Access Control List*);

QUALITY OF SERVICE (QoS)

3.4.61. RFC 2474 *DiffServ Precedence*, RFC 2598 *DiffServ Expedited Forwarding* (EF), RFC 2597 *DiffServ Assured Forwarding* (AF), RFC 2475 *DiffServ Core and Edge Router Functions*;

3.4.62. devem implementar remarcação de prioridade de pacotes *Layer* 3, remarcando o campo *DiffServ* para grupos de tráfego classificados segundo portas TCP e UDP e endereço/subrede IP;

3.4.63. devem possuir 8 (oito) filas em cada interface;

3.4.64. devem implementar os algoritmos de gerenciamento de filas *Weighted Round Robin* (WRR) ou *Shaped Round Robin* (SRR);

MÓDULOS, PLACAS E INTERFACES QUE DEVEM SER SUPORTADOS:

3.4.65. interfaces RJ-45, para cabos UTP, full duplex, *GigaEthernet*, *autosense*, de acordo com os protocolos padrões Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT, IEEE802.3z 1000BASE-X;

QUANTIDADE DE PORTAS INSTALADAS

3.4.66. devem implementar quantidade mínima de 24 (vinte e quatro) portas com interfaces RJ-45, para cabos UTP, 10/100/1000BaseTX, *full duplex*, ethernet, *autosense*, que deverão estar instaladas em cada switch, para conexão de estações de trabalho;

3.4.67. quantidade mínima de slots SFP+, para cabos LC, 10 Gigabit, que deverão estar instaladas em cada comutador (switch), para conexão de *uplink*: 2 (dois). Deverão ser entregues 2 *transceivers* 10 Gigabit SFP+ para fibras LC multimodo;

3.4.68. as portas de empilhamento não devem ser contabilizadas no quantitativo de entregas de interfaces acima e deverão ser entregues com cabos e *transceivers* necessários para o empilhamento via interfaces redundantes;

EMPILHAMENTO (STACK)

3.4.69. os switches devem ser *Stackable*, ou seja, devem operar em conjunto representando somente 1(um) switch para fins de gerenciamento e encaminhamento de tráfego;

3.4.70. deverá implementar número mínimo de 8 (oito) switches trabalhando em conjunto;

3.4.71. cada switch deverá ser entregue com os recursos necessários para conexão de empilhamento, sejam *transceivers*, cabos dedicados, licenciamento ou qualquer

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

Banco do Nordeste

outra necessidade. Cada empilhamento será sempre realizado dentro do mesmo rack de acesso e as conexões de empilhamento deverão ser no mínimo de 50 (cinquenta) centímetros;

3.4.72. deverão ser fornecidos 12 (doze) cabos de *Stack* de pelo menos 3 (três) metros a fim de fechar a pilha, para conectar o último switch da pilha ao primeiro switch da pilha;

3.4.73. a velocidade disponível na conexão de empilhamento deverá ser no mínimo de 10Gbps full-duplex para cada link de empilhamento, sendo pelo menos 2 (dois) links necessários via fibra ou cabo/interface própria de empilhamento para garantir redundância;

3.4.74. o empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo o padrão 802.3ad;

3.4.75. o empilhamento deve implementar espelhamento de tráfego entre diferentes unidades da pilha;

Capacidade de processamento e memória:

3.4.76. deve implementar capacidade encaminhamento de pacotes na camada 2 (dois) ou camada 3 (três), quando aplicável (modelo de referência OSI), em milhões de pacotes por segundo (pacotes de 64 bytes) com a qual cada equipamento deverá estar equipado deve ser de no mínimo 96 (noventa e seis);

3.4.77. devem implementar capacidade agregada de *switching* mínima (*throughput*) de 128 (cento e vinte e oito) gigabits por segundo;

3.4.78. o switch deverá ser *non-blocking* em todas as interfaces *inband;*

3.4.79. devem implementar 512 (quinhentos e doze) Mb como quantidade mínima de memória DRAM (ou SDRAM) DDR3 ou superior;

3.4.80. devem implementar quantidade mínima de 2(dois) Gb de memória Flash ou capacidade para armazenar pelo menos 3 (três) imagens do sistema operacional do equipamento;

3.4.81. devem implementar no mínimo 200 (duzentas) rotas estáticas em camada 3, tanto para IPv4 como para IPv6;

3.4.82. devem implementar capacidade de armazenamento de 384 (trezentos e oitenta e quatro) entradas ARP;

3.4.83. devem implementar 192 (cento e noventa e duas) interfaces lógicas roteáveis;

3.4.84. deve implementar, no mínimo, os protocolos de roteamento OSPF, OSPFv3 e RIP.

RECURSOS DE SEGURANÇA

3.4.85. deverá implementar funcionalidades de *Dynamic Host Configuration Protocol* (DHCP) *snooping;*

3.4.86. a implementação do IEEE 802.1x deve incluir suporte a *Guest* VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA;

Este documento está classificado como INTERNO sob responsabilidade de MARCOS Paulo Cavalcante ROLIM F145351

3.4.87. deverá implementar autenticação de login/senha para a liberação de tráfego na porta através do protocolo IEEE 802.1x com no mínimo as seguintes funcionalidades:

3.4.87.1. atribuição de VLAN conforme a autenticação do usuário;

3.4.87.2. reautenticação forçada de todas as portas;

3.4.87.3. reautenticação periódica e definição de período de inatividade após falha de autenticação;

3.4.87.4. devem implementar *RFC 3579 RADIUS EAP support for 802.1x*;

3.4.87.5. devem possuir capacidade de limitação de quantidade de endereços MAC por porta e definir ações para cada tipo de violação.

Ambiente de Operações de TI

DAVSON Nogueira MAIA F159999
Gerente de Ambiente, em exercício

THYAGO Marcello Ribeiro F179181
Gerente Executivo, em exercício