

PROJETO TÉCNICO

PREFEITURA MUNICIPAL DE CATALÃO

SISTEMA DE DISTRIBUIÇÃO DE FIBRA OPTICA URBANA

R01 - 06-07-2018

INTRODUÇÃO

Este projeto básico, tem como objetivo determinar as especificações e condições mínimas que visam orientar o fornecimento e a instalação de **SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO** que compõe o projeto de modernização tecnológica da Prefeitura Municipal de Catalão.

O objetivo deste projeto é aumentar os níveis de segurança, disponibilidade, integridade, desempenho e qualidade dos serviços de tecnologia disponibilizados pela Prefeitura em seus processos diários.

DESCRITIVO BÁSICO DO PROJETO

O projeto de modernização dos Sistemas de Tecnologia da Informação da Prefeitura Municipal de Catalão contempla o fornecimento de equipamentos e serviços que integram os sistemas de:

- *Data Center,*
- *Sistema de energia ininterrupta (UPS),*
- *Switchs,*
- *Cabeamento Óptico e cabeamento metálico,*
- *equipamentos de processamento e armazenamento de dados (Servidores e Storage).*

DATA CENTER

Deverá ser realizada a organização e instalação de sala de Data Center com fornecimento de Infraestrutura Física para lançamento de cabeamento lógico e elétrico, instalação e fornecimento de quadros de energia elétrica internos ao data center, a saber:

- instalação e fornecimento de equipamentos de fonte ininterrupta de energia elétrica (UPS);
- Instalação e fornecimento de Racks de Data Center;
- Instalação e fornecimento de Servidores de processamento e armazenamento de dados;
- Instalação e fornecimento de ativos de rede de dados;

BACK BONE OPTICO

O projeto contempla a Interligação dos órgãos, secretarias, escolas e hospitais através de enlace óptico monomodo, utilizando a tecnologia;

REDE SEM FIO

Disponibilização de Rede Sem Fio com acesso à Internet gratuito à população em praças e bosques da cidade;

O projeto de modernização tecnológica, visa aprimorar os sistemas de tecnologia da informação atualmente instalados e em operação, provendo equipamentos e infraestrutura adequadas à suportar as demandas atuais e futuras dos serviços de tecnologia disponibilizados, tais como: armazenamento e processamento de arquivos digitais, sistemas ERP, sistemas WEB, geoprocessamento e outros.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS E OBRIGATÓRIAS

ESPECIFICAÇÕES TÉCNICAS MINIMAS DO SISTEMA DE NOBREAKS

Todos os equipamentos e serviços fornecidos pela Licitante deverão necessariamente atender às exigências mínimas descritas no Termo de Referência - Projeto Técnico sendo comprovadas, obrigatoriamente, através de catálogos técnicos oficialmente divulgados pela fabricante.

Como meio de comprovação de atendimento às exigências técnicas exigidas no Termo de Referência - Projeto Técnico, a licitante deverá apresentar, na proposta comercial, marca e modelo, através do código do fabricante (Part Number) de todos os equipamentos de Tecnologia fornecidos. Todos os catálogos, manuais e especificações técnicas dos equipamentos/materiais deverão ser apresentados na íntegra para avaliação da comissão de licitação.

Nobreaks – Implantação ou Reestruturação de Data Center

Características de Entrada:

- Possuir potência 10 kVA / 8,0 kW;
- Fornecer tensão: bifásica 220V F+F+N;
- Frequência: 60 Hz + 5%;
- Possuir tipo de conexão: terminais do tipo “borne”;
- Características de Saída:
- Possuir tensão de saída: 220V / 110V – Saída Dupla /Bivolt. Com o fornecimento das tensões de 110V e 220V simultaneamente para alimentação de cargas especiais (sem auxílio de transformadores externos);
- Regulação estática, faixa aceitável: +/-1,0 % - sob carga plena tipo resistiva;
- Distorção Harmônica: THD < 3% - sob carga plena tipo resistiva;
- Tipo de conexão aceitável: através de terminais do tipo “borne”;
- Rendimento a Plena Carga: Maior ou igual a 90%;
- Suporte de sobre carga, operar dentro do indicado a seguir: até 120% suportar por 15 minutos, até 150% suportar por 15 Segundos, acima de 150%, deverá acionar o sistema de By-Pass mantendo isolamento galvânica;
- Possuir by pass automático em caso de falha ou sobrecarga no inversor;
- Possuir by bass manualmente através do teclado no painel do nobreak;
- Possuir saída Isolada da rede em qualquer condição de funcionamento do nobreak, seja em modo by-pass, seja em modo inversor;
- Tempo de transferência entre by-pass e inversor igual a Zero;

Características de Autonomia / Baterias

- Tempo de autonomia Total: 25 a 30 minutos sob meia carga. (Comprovados através de memorial de cálculo da bateria.). Não será aceito banco de baterias externo para atender a autonomia desejada;
- Tipo de Baterias: Seladas, VRLA, sem emissão de gases;
- As baterias devem ser alojadas internamente ao Nobreak, com entrada para módulos de baterias externas para aumentar o tempo de autonomia (em caso de expansão futura);
- Permitir ser ligado na ausência de rede elétrica;
- Possuir proteção contra descarga total das baterias;
- Recarga automática das baterias com tempo de recarga de no máximo 8 horas;

Características de Gerenciamento do Sistema:

- Possuir display LCD com leitura que permita o gerenciamento do sistema com interação através de teclado no painel;
- Comunicação Inteligente através de porta RS- 232C True Serial e RS-485;
- Possuir alarme audiovisual, e função de tecla silenciadora de alarme sonoro;
- Possuir software para gerenciamento de Energia disponível para os sistemas operacionais Windows e Linux;
- O software de gerenciamento deverá possuir função para fechamento automático de arquivos e do sistema operacional remotamente, de qualquer lugar conectado à internet;
- Visualização das condições de operação do nobreak e status da rede elétrica com gerenciamento da qualidade da energia elétrica através somente de comunicação inteligente com porta RS-232 e RS-485;

Instalação

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário a vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Conexão em Ponto de Energia Elétrica;
- Integração deste componente ao demais componentes da solução;
- Configuração de Softwares de Gerenciamento;
- Inclusão dos dados de configuração de todos os equipamentos na documentação depois de instalados.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO SISTEMA DE ATIVOS DE REDE E SERVIDORES DE DADOS

A aquisição dos equipamentos de tecnologia trata-se de uma solução composta entre hardwares, não somente a aquisição isolada de equipamentos, portanto, com o objetivo de preservar a garantia dos equipamentos, assim como a compatibilidade de funcionamento da solução, exige-se que os Switches Core, Switch TOR, Switchs 24P, Switchs 48P, Ativos de rede WLAN – CONTROLADORA, Ativos de rede WLAN – ACCESS POINT e Servidores sejam do mesmo fabricante. Desta forma todos os equipamentos e serviços fornecidos pela LICITANTE deverão necessariamente atender às exigências mínimas descritas no Termo de Referência - Projeto

Técnico sendo comprovadas, obrigatoriamente, através de catálogos técnicos oficialmente divulgados pela fabricante.

Como meio de comprovação de atendimento às exigências técnicas exigidas no Termo de Referência - Projeto Técnico, a licitante deverá apresentar, na proposta comercial, marca e modelo, através do código do fabricante (Part Number) de todos os equipamentos de Tecnologia fornecidos. Todos os catálogos, manuais e especificações técnicas dos equipamentos/materiais deverão ser apresentados na íntegra para avaliação da comissão de licitação.

Switch Core – Implantação ou Reestruturação de Datacenter

O switch deve ser do mesmo fabricante dos demais switches e servidores desse documento.

Portas:

- Possuir, no mínimo, 4 portas 10 Gigabit Ethernet padrão SFP+ para conexão de uplink;
- Devem ser fornecidos juntamente com o Switch, 04 (quatro) Transceivers 10 GB, padrão 10GBase-SR;
- Possuir, no mínimo, 48 portas Ethernet 10/100/1000 Base-T com autosensing de velocidade e com conectores RJ-45 para conexão de acesso. Todas as 48 portas devem operar simultaneamente em conjunto com as 4 portas de uplink, padrão SFP+;
- Todas as portas Ethernet 10/100/1000 Base-T devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);
- Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possuir throughput mínimo de 176 Gbps;
- Suportar mínimo de 32.000 endereços MAC;
- A taxa de encaminhamento deve ser de 130 Mpps ou superior;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta de terminal RS-232,USB, mini USB ou RJ 45;
- Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

Fonte de alimentação:

- Possuir fonte de alimentação redundante interna AC bivolt de no mínimo 1100W, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);
- As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;
- Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte;
- Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade da troca do switch.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Visualização:
- Possuir LEDs para a indicação do status das portas e atividade, além de duplex.

Gerenciamento:

- Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275):
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3;
- Sem autenticação e sem privacidade (noAuthNoPriv);
- Com autenticação e sem privacidade (authNoPriv);
- Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES 256-bit.
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento; Deve armazenar pelo menos as 500 últimas mensagens;
- Possuir capacidade de exportar as mensagens de log geradas pelo equipamento para um servidor syslog externo;
- Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps;
- Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events);
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;
- Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX, NetStream ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.

Facilidades:

- Implementar Telnet para acesso à interface de linha de comando;
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet;

- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol);
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
- Permitir que a sua configuração seja feita através de terminal assíncrono;
- 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;
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch;
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento;
- O espelhamento não pode interferir no funcionamento normal do equipamento;
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q;
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
 - ICMP echo;
 - TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);
 - UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);
 - O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

Protocolos:

- Implementar os protocolos NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4). Deve ser suportada autenticação entre os peers;
- Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.

Roteamento:

- Implementar roteamento estático;
- Suportar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453);
- Suportar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370);
- Suportar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385);

- Suportar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF;
- Implementar o roteamento nível 3 entre VLANs;
- Suportar o protocolo VRRP (RFC 2338) ou HSRP de redundância de gateway;
- Suportar a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas;
- Suporte a Policy Based Routing (PBR);
- Suportar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem;
- Suporte a mínimo de 20.000 rotas em IPv4.

Roteamento ipv6:

- Implementar roteamento estático para IPv6;
- Suportar roteamento dinâmico RIPng para IPv6;
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6;
- Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação;
- Implementar, no mínimo, 4000 VLANs simultaneamente;
- Implementar, no mínimo, 1000 interfaces VLANs simultaneamente, para roteamento nível 3 entre as VLANs configuradas;
- Suportar Jumbo frames de no mínimo 9198 Bytes.

Stacking:

- Possuir porta dedicada de empilhamento com capacidade de 400 Gbps (Gigapits por segundo).
- Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 4 switches;
- Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS;
- Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando;
- Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido;

- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;
- 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;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elemento de rede, independente do método de gerenciamento;
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;
- 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);
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo;
- 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;
- 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, essa filtragem deve ser por porta.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
- Implementar padrão IEEE 802.1q (VLAN Frame Tagging);
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- Implementar padrão IEEE 802.3ad;
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree, sem limite de quantidade de VLANs associada a cada instância;
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS;
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
- Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
 - A estação não tem cliente 802.1x (suplicante);

- As credenciais do usuário não estão corretas (falha de autenticação);
- Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de VLAN);
- Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL);
- Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
 - Nome do usuário;
 - Switch em que o computador do usuário está conectado;
 - Porta do switch utilizada para acesso;
 - Endereço MAC da máquina utilizada pelo usuário;
 - Endereço IP do usuário; vi. Horários de início e término da conexão;
 - Bytes transmitidos e recebidos durante a conexão;
- Deve reautenticar (reautenticação periódica) permitindo ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reconectar;
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch;
- Deve suportar a autenticação 802.1x através do protocolo EAPOL;
- Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
- Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma VLAN não interfira na outra;
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS;
- Deve implementar o mecanismo mudança de autorização dinâmica, Radius “Change of Authorization”, conforme descrito na RFC 5176;
- Multicast:
 - Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376);
 - Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
 - Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse-mode” (RFC 2362) e “dense-mode”. Deve ser suportada, por interface, a operação simultânea nos modos “sparse-mode” e “dense-mode”;
 - Suportar no mínimo 4000 grupos multicast para IPv4.

Qualidade de serviço (QoS):

- Implementar priorização de tráfego através do protocolo IEEE 802.1p;
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point"- nível 3), conforme definições do IETF (Internet Engineering Task Force);
- Suportar 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;
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa;
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop);
- Implementar pelo menos oito filas de prioridade por porta de saída (egress port);
- INTERNET PROTOCOL VERSÃO 6 (IPV6);
- Implementar IPv6;
- Permitir a configuração de endereços IPv6 para gerenciamento;
- Permitir consultas de DNS com resolução de nomes em endereços IPv6;
- "Implementar ICMPv6 com as seguintes funcionalidades:
 - ICMP request;
 - ICMP Reply;
 - ICMP Neighbor Discovery Protocol (NDP);
 - ICMP MTU Discovery";
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6;
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Configurações Básicas Rede: Nome do host, atribuição de IP, Configurações Gerais;
- Montagem do equipamento e seus acessórios;

- Conexão em Ponto de Energia Elétrica;
- Conexão em Ponto de Rede Estruturado Categoria 6 ou fibra óptica. Conexão em Gbics;
- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração de todos os equipamentos na documentação depois de instalados.
- Switch TOR – Implantação ou Reestruturação de Datacenter

Portas:

- Possuir, no mínimo, 2 portas 10 Gigabit Ethernet padrão SFP+ para conexão de uplink;
- Devem ser fornecidos juntamente com o Switch, 02 (dois) Transceivers 10 GB, padrão 10GBase-SR;
- Possuir, no mínimo, 24 portas Ethernet 10/100/1000 Base-T com autosensing de velocidade e com conectores RJ-45 para conexão de acesso. Todas as 24 portas devem operar simultaneamente em conjunto com as 2 portas de uplink, padrão SFP+;
- Todas as portas Ethernet 10/100/1000 Base-T devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);
- Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possuir throughput mínimo de 92 Gbps;
- Suportar mínimo de 32.000 endereços MAC;
- A taxa de encaminhamento deve ser de 68 Mpps ou superior;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta de terminal RS-232, USB, mini USB ou RJ 45;
- Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

Fonte de alimentação:

- Possuir fonte de alimentação redundante interna AC bivolt de no mínimo 1100W, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);
- As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;

- Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte;
- Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade da troca do switch.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Visualização:
- Possuir LEDs para a indicação do status das portas e atividade, além de duplex.
- Gerenciamento:
- Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275):
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3;
- Sem autenticação e sem privacidade (noAuthNoPriv);
- Com autenticação e sem privacidade (authNoPriv);
- Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES 256-bit.
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento; Deve armazenar pelo menos as 500 últimas mensagens;
- Possuir capacidade de exportar as mensagens de log geradas pelo equipamento para um servidor syslog externo;
- Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps;
- Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events);
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;
- Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX, NetStream ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.

Facilidades:

- Implementar Telnet para acesso à interface de linha de comando;
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet;
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol);

- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
- Permitir que a sua configuração seja feita através de terminal assíncrono;
- 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;
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch;
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento;
- O espelhamento não pode interferir no funcionamento normal do equipamento;
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q;
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
 - ICMP echo;
 - TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);
 - UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);
 - O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

Protocolos:

- Implementar os protocolos NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4). Deve ser suportada autenticação entre os peers;
- Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.

Roteamento:

- Implementar roteamento estático;
- Suportar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453);
- Suportar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370);
- Suportar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385);
- Suportar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF;
- Implementar o roteamento nível 3 entre VLANs;
- Suportar o protocolo VRRP (RFC 2338) ou HSRP de redundância de gateway;

- Suportar a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas;
- Suporte a Policy Based Routing (PBR);
- Suportar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem;
- Suporte a mínimo de 20.000 rotas em IPv4.

Roteamento ipv6:

- Implementar roteamento estático para IPv6;
- Suportar roteamento dinâmico RIPng para IPv6;
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6;
- Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação;
- Implementar, no mínimo, 4000 VLANs simultaneamente;
- Implementar, no mínimo, 1000 interfaces VLANs simultaneamente, para roteamento nível 3 entre as VLANs configuradas;
- Suportar Jumbo frames de no mínimo 9198 Bytes.

Stacking:

- Possuir porta dedicada de empilhamento com capacidade de 400 Gbps (Gigapits por segundo).
- Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 4 switches;
- Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS;
- Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando;
- Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido;
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;
- 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;

- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elemento de rede, independente do método de gerenciamento;
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;
- 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);
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo;
- 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;
- 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, essa filtragem deve ser por porta.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
- Implementar padrão IEEE 802.1q (VLAN Frame Tagging);
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- Implementar padrão IEEE 802.3ad;
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree, sem limite de quantidade de VLANs associada a cada instância;
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS;
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
- Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
- A estação não tem cliente 802.1x (suplicante);
- As credenciais do usuário não estão corretas (falha de autenticação);
- Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de VLAN);

- Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL);
- Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
 - Nome do usuário;
 - Switch em que o computador do usuário está conectado;
 - Porta do switch utilizada par acesso;
 - Endereço MAC da máquina utilizada pelo usuário;
 - Endereço IP do usuário; vi. Horários de início e término da conexão;
 - Bytes transmitidos e recebidos durante a conexão;
- Deve reautenticar (reautenticação periódica) permitindo ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reconectar;
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch;
- Deve suportar a autenticação 802.1x através do protocolo EAPOL;
- Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
- Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma VLAN não interfira na outra;
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS;
- Deve implementar o mecanismo mudança de autorização dinâmica, Radius “Change of Authorization”, conforme descrito na RFC 5176;

Multicast:

- Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376);
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
- Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse-mode” (RFC 2362) e “dense-mode”. Deve ser suportada, por interface, a operação simultânea nos modos “sparse-mode” e “dense-mode”;
- Suportar no mínimo 4000 grupos multicast para IPv4.

Qualidade de serviço (QOS):

- Implementar priorização de tráfego através do protocolo IEEE 802.1p;
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point"- nível 3), conforme definições do IETF (Internet Engineering Task Force);
- Suportar 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;
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa;
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop);
- Implementar pelo menos oito filas de prioridade por porta de saída (egress port);
- INTERNET PROTOCOL VERSÃO 6 (IPv6);
- Implementar IPv6;
- Permitir a configuração de endereços IPv6 para gerenciamento;
- Permitir consultas de DNS com resolução de nomes em endereços IPv6;
- "Implementar ICMPv6 com as seguintes funcionalidades:
 - ICMP request;
 - ICMP Reply;
 - ICMP Neighbor Discovery Protocol (NDP);
 - ICMP MTU Discovery";
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6;
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Configurações Básicas Rede: Nome do host, atribuição de IP, Configurações Gerais;
- Montagem do equipamento e seus acessórios;
- Conexão em Ponto de Energia Elétrica;
- Conexão em Ponto de Rede Estruturado Categoria 6 ou fibra óptica. Conexão em Gbics;

- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração de todos os equipamentos na documentação depois de instalados.
- Switchs 24P – Implantação ou Reestruturação de Datacenter

PORTAS:

- Possuir, no mínimo, 24 portas 10/100/1000, implementando o padrão 802.3af (15,4W PoE) e 802.3at (30W PoE+) em todas as 24 portas com, pelo menos, 370W disponíveis para PoE/PoE+;
- Deverá possuir para uplink, no mínimo, 4 (quatro) portas SFP GigabitEthernet, além das 24 portas UTP solicitadas anteriormente;
- Possuir capacidade de associação das portas de uplink em grupo de duas portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad;
- Deve ser fornecido, em conjunto com o Switch, 02 (dois) módulos GBIC 1000BASE-SX SFP;
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT),
- IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (n Control);
- Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q;
- Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.

Fonte de alimentação:

- Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);
- Suportar alimentação elétrica redundante interna ou externa capaz de suportar o equipamento com todas as funcionalidades solicitadas nesta especificação;
- A fonte de alimentação deverá possuir no mínimo 370W para alimentação PoE, além da energia necessária para funcionamento do switch. Não serão aceitos dispositivos externos para complementação de energia PoE no switch;

- Possuir cabo de alimentação para a fonte.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;
- Deve possuir no máximo 1 Rack Unit (RU).
- Visualização:
- Possuir LEDs para a indicação do status das portas, atividade, duplex e PoE.

Gerenciamento:

- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
- Sem autenticação e sem privacidade (noAuthNoPriv);
- Com autenticação e sem privacidade (authNoPriv);
- Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES;
- Possuir suporte a MIB II, conforme RFC 1213;
- Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;
- Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;
- Implementar MIB que forneça informações sobre utilização de energia para PoE;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 1024 bytes;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757;
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE;
- Suportar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 8 unidades, com velocidade de empilhamento de 40Gbps full-duplex (80Gbps total). Os módulos e cabos de empilhamento devem ser fornecidos.
- A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha além de permitir espelhamento de portas de qualquer porta para qualquer porta da pilha;

- O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede;
- Deverão ser fornecidos todos os elementos: interfaces, cabos e software para realizar o empilhamento físico deste item.

Facilidades:

- Implementar Telnet para acesso à interface de linha de comando;
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet;
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
- Permitir que a sua configuração seja feita através de terminal assíncrono;
- Permitir a gravação de log externo (syslog);
- 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;
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local;
- Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;
- Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas;
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q;
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN;
- Deve permitir a criação, remoção e distribuição através de portas configuradas como tronco IEEE 802.1Q;
- Deve suportar IPFIX ou Netflow para análise do tráfego da rede. Caso a análise seja feita por amostragem, deve ser suportada amostragem de 1 a cada 32 pacotes;

- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA);
- Devem ser suportadas no mínimo as seguintes operações de teste:
 - ICMP echo;
 - TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);
 - UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);
 - O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

Protocolos:

- Implementar o protocolo NTPv3 (Network Time Protocol, versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições da RFC 1305;
- Implementar DHCP Relay em múltiplas VLANs;
- Implementar roteamento estático IPv4 e IPv6;
- Implementar roteamento entre VLANs;
- Permitir a configuração de até 16 Interfaces nível 3 para roteamento.

Desempenho:

- Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação;
- Implementar, no mínimo, 1000 VLANs simultaneamente;
- Deve possuir capacidade de comutação full-duplex de no mínimo 100 Gbps;
- Deve possuir taxa de encaminhamento de no mínimo 70 Mpps;
- Suportar Jumbo frames de no mínimo 9018 Bytes.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS;
- Implementar filtragem de pacotes (ACL - Access Control List) IPv4 e IPv6;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando;
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Caso o número de endereços MAC configurado para a porta seja excedido, deve ser possível:
 - Bloquear o tráfego na porta;
 - Desabilitar a porta;
 - Enviar um trap SNMP;
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;
- Deve permitir pelo menos 500 entradas de filtros de listas de controle de acesso (ACL) em IPv4;

- Deve permitir pelo menos 500 entradas de filtros de listas de controle de acesso (ACL) em IPv6;
- 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;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- Permitir controlar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede, independente do método utilizado para acessar o switch;
- Possuir controle de broadcast, multicast e unicast por porta;
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;
- 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);
- 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;
- 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, essa filtragem deve ser por porta;
- Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN, com suporte a, no mínimo, 32 instâncias simultâneas;
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging);
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- Implementar padrão IEEE 802.3ad;
- Implementar padrão IEEE 802.3af;
- Implementar padrão IEEE 802.3at;
- Implementar padrão IEEE 802.3az;
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
- Implementar funcionalidade que design VLAN específica para o usuário, nos seguintes casos:
- A estação não tem cliente 802.1x (suplicante);

- As credenciais do usuário não estão corretas (falha de autenticação);
- Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan);
- Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL);
- Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
 - Nome do usuário;
 - Switch em que o computador do usuário está conectado;
 - Porta do switch utilizada para acesso;
 - Endereço MAC da máquina utilizada pelo usuário;
 - Endereço IP do usuário;
 - Horários de início e término da conexão;
 - Bytes transmitidos e recebidos durante a conexão;
- Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado
- a uma porta do switch habilitada para 802.1x;
- Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch;
- Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS em conjunto com o servidor RADIUS;
- Implementar serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
- Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra;
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS;
- Deve implementar o mecanismo mudança de autorização dinâmica, Radius “Change of Authorization”, conforme descrito na RFC 5176;
- Implementar padrão IEEE 802.1w (Rapid Spanning Tree Protocol), com suporte a, no mínimo, 32 instâncias simultâneas;
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 32 instâncias simultâneas do protocolo Spanning-Tree;

Multicast:

- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
- Suportar no mínimo 1.000 grupos multicast para IPv4;
- Implementar em todas as interfaces do switch o protocolo MLD (Multicast Listener Discovery) Snooping (v1 e v2) para IPv6;

Qualidade de serviço (QoS):

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point" - nível 3), conforme definições do IETF (Internet Engineering Task Force);
- Suportar 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 as seguintes ações:
- Transmissão do pacote sem modificação;
- Transmissão com remarcação do valor de DSCP;
- Descarte do pacote;
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa;
- Suportar diferenciação de QoS por VLAN;
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);
- Implementar pelo menos quatro filas de prioridade por porta de saída (egress port).
- Internet protocol versão 6 (ipv6):
- Implementar IPv6;
- Permitir a configuração de endereços IPv6 para gerenciamento;
- Permitir consultas de DNS com resolução de nomes em endereços IPv6;
- Implementar ICMPv6 com as seguintes funcionalidades:
 - ICMP request;
 - ICMP Reply;
 - ICMP Neighbor Discovery Protocol (NDP);
 - ICMP MTU Discovery;
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH e HTTP sobre IPv6;
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;
- A solução deve oferecer MTBF de 200.000 horas ou superior.

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Configurações Básicas Rede: Nome do host, atribuição de IP, Configurações Gerais;
- Montagem do equipamento e seus acessórios;
- Conexão em Ponto de Energia Elétrica;
- Conexão em Ponto de Rede Estruturado Categoria 6 ou fibra óptica. Conexão em Gbics;
- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração de todos os equipamentos na documentação depois de instalados.
- Switchs 48P – Implantação ou Reestruturação de Datacenter

Portas:

- Possuir, no mínimo, 48 portas 10/100/1000. Deverá possuir para uplink, no mínimo, 4 (quatro) portas SFP GigabitEthernet, além das 48 portas UTP solicitadas anteriormente;
- Possuir capacidade de associação das portas de uplink em grupo de duas portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad;
- Deve ser fornecido, em conjunto com o Switch, 02 (dois) módulos GBIC 1000BASE-SX SFP;
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (n Control);
- Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q;
- Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

Fonte de alimentação:

- Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);

- Suportar alimentação elétrica redundante interna ou externa capaz de suportar o equipamento com todas as funcionalidades solicitadas nesta especificação;
- Possuir cabo de alimentação para a fonte.

Visualização:

- Possuir LEDs para a indicação do status das portas e atividade;

Gerenciamento:

- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - Sem autenticação e sem privacidade (noAuthNoPriv);
 - Com autenticação e sem privacidade (authNoPriv);
 - Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES;
- Possuir suporte a MIB II, conforme RFC 1213;
- Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;
- Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 1024 bytes;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da
 - CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757;
- Suportar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizadas portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 8 unidades, com velocidade de empilhamento de 40Gbps full-duplex (80Gbps total). Os módulos e cabos de empilhamento deverão ser fornecidos;
- A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha além de permitir espelhamento de portas de qualquer porta para qualquer porta da pilha;
- O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede;
- Deverão ser fornecidos todos os elementos: interfaces, cabos e software para realizar o empilhamento físico deste item.

Facilidades:

- Implementar Telnet para acesso à interface de linha de comando;
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet;
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
- Permitir que a sua configuração seja feita através de terminal assíncrono;
- Permitir a gravação de log externo (syslog);
- 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.

Protocolos:

- Implementar o protocolo NTPv3 (Network Time Protocol, versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições da RFC 1305;
- Implementar DHCP Relay em múltiplas VLANs;
- Implementar roteamento estático IPv4 e IPv6;
- Implementar roteamento entre VLANs;
- Permitir a configuração de até 16 Interfaces nível 3 para roteamento.

Desempenho:

- Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação;
- Implementar, no mínimo, 1000 VLANs simultaneamente;
- Deve possuir capacidade de comutação full-duplex de no mínimo 216 Gbps;
- Deve possuir taxa de encaminhamento de no mínimo 100 Mpps;
- Suportar Jumbo frames de no mínimo 9018 Bytes.
- Segurança:
- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS;
- Implementar filtragem de pacotes (ACL - Access Control List) IPv4 e IPv6;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando;
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Caso o número de endereços MAC configurado para a porta seja excedido, deve ser possível:
- Bloquear o tráfego na porta;
- Desabilitar a porta;
- Enviar um trap SNMP;
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;
- Deve permitir pelo menos 500 entradas de filtros de listas de controle de acesso (ACL) em IPv4;
- Deve permitir pelo menos 500 entradas de filtros de listas de controle de acesso (ACL) em IPv6;
- 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;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- Permitir controlar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede, independente do método utilizado para acessar o switch;
- Possuir controle de broadcast, multicast e unicast por porta;
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;
- 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);
- 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.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN, com suporte a, no mínimo, 32 instâncias simultâneas;
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging);
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- Implementar padrão IEEE 802.3ad;
- Implementar padrão IEEE 802.3af;
- Implementar padrão IEEE 802.3at;
- Implementar padrão IEEE 802.3az;
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;

- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
- Implementar funcionalidade que design VLAN específica para o usuário, nos seguintes casos:
- A estação não tem cliente 802.1x (suplicante);
- As credenciais do usuário não estão corretas (falha de autenticação);
- Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de VLAN);
- Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL);
- Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
 - Nome do usuário;
 - Switch em que o computador do usuário está conectado;
 - Porta do switch utilizada para acesso;
 - Endereço MAC da máquina utilizada pelo usuário;
 - Endereço IP do usuário;
 - Horários de início e término da conexão;
 - Bytes transmitidos e recebidos durante a conexão;
- Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x;
- Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch;
- Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS em conjunto com o servidor RADIUS;
- Implementar serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
- Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma VLAN não interfira na outra;
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS;
- Deve implementar o mecanismo mudança de autorização dinâmica, Radius “Change of Authorization”, conforme descrito na RFC 5176;
- Implementar padrão IEEE 802.1w (Rapid Spanning Tree Protocol), com suporte a, no mínimo, 32 instâncias simultâneas;

- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 32 instâncias simultâneas do protocolo Spanning-Tree.

Multicast:

- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
- Suportar no mínimo 1.000 grupos multicast para IPv4;
- Implementar em todas as interfaces do switch o protocolo MLD (Multicast Listener Discovery) Snooping (v1 e v2) para IPv6.

Qualidade de serviço (QoS):

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point" - nível 3), conforme definições do IETF (Internet Engineering Task Force);
- Suportar 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 as seguintes ações:
- Transmissão do pacote sem modificação;
- Transmissão com remarcação do valor de DSCP;
- Descarte do pacote;
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa;
- Suportar diferenciação de QoS por VLAN;
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);
- Implementar pelo menos quatro filas de prioridade por porta de saída (egress port);
- INTERNET PROTOCOL VERSÃO 6 (IPV6);
- Implementar IPv6;
- Permitir a configuração de endereços IPv6 para gerenciamento;
- Permitir consultas de DNS com resolução de nomes em endereços IPv6;
- Implementar ICMPv6 com as seguintes funcionalidades:
 - ICMP request;
 - ICMP Reply;
 - ICMP Neighbor Discovery Protocol (NDP);

- ICMP MTU Discovery;
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH e HTTP sobre IPv6;
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;
- A solução deve oferecer MTBF de 200.000 horas ou superior.
- Dimensões:
- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;
- Deve possuir no máximo 1 Rack Unit (RU).

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Configurações Básicas Rede: Nome do host, atribuição de IP, Configurações Gerais;
- Montagem do equipamento e seus acessórios;
- Conexão em Ponto de Energia Elétrica;
- Conexão em Ponto de Rede Estruturado Categoria 6 ou fibra óptica. Conexão em Gbics;
- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração de todos os equipamentos na documentação depois de instalados.

Ativos de rede WLAN - CONTROLADORA

A controladora WLAN deverá ser um appliance dedicado ao gerenciamento da solução de redes sem fio, os equipamentos que compõe a solução de rede sem fio deverão ser do mesmo fabricante (Controladoras e Pontos de Acesso), compondo uma solução única para assegurar a compatibilidade funcional de todos os recursos e facilitar o gerenciamento;

O appliance deve possuir recursos instalados para implementar o gerenciamento da solução de rede sem fio proposta, como balanceamento de carga, mecanismos automáticos de gerenciamento de recursos, detecção de áreas sem cobertura, indisponibilidades de pontos de acesso, autoconfiguração, autocorreção e auto otimização, visibilidade e controle das aplicações;

Especificação de Hardware:

Os equipamentos que compõe a solução de Data Center deverão ser do mesmo fabricante (Switches Core e Switches TOR), compondo uma solução única para assegurar a compatibilidade funcional de todos os recursos e facilitar o gerenciamento;

Especificação:

- Possuir no mínimo 01 (um) processador de no mínimo 06 núcleos, arquitetura x64, sendo:

- Performance de referência Intel E5 2600 versão 3 ou superior;
- Frequência base mínima de 2.20GHz ou superior;
- Mínimo de 20MB de memória cache;
- 16 GB (dezesseis) de memória e com possibilidade de expansão para 768 GB (setecentos e sessenta e oito gigabytes);
- 01 (um) disco rígido de 4TB (quatro terabytes), 7,2k rpm (sete mil e duzentas rotações por minuto), “hot pluggable/hot swap”, padrão SAS, configuráveis para RAID 0, 1, 5 em seu controlador;
- No mínimo 04 slots internos para discos rígidos;
- No mínimo 2 portas USB 3.0;
- Possuir placa de vídeo integrada;
- Deverá possuir BIOS desenvolvida pelo mesmo fabricante do equipamento;
- 04 (quatro) portas de rede GigaBitEthernet;
- Suportar o uso de 2 discos flash em formato SD internamente com capacidade mínima de 32GB;
- Ventiladores redundantes, suportando o servidor em completa operacionalidade em caso de falha de um deles;
- Solução por hardware e/ou software de gerenciamento remoto, independente do sistema operacional e do estado do computador, com as seguintes características:
 - Controle remoto liga/desliga do servidor;
 - Console remota;
 - Servidor http e https;
 - Servidor SSH ou Telnet+SSL;
 - Criptografia SSL de 128 bits na comunicação;
 - Suporte a SNMP para consulta e traps;
 - Capacidade de atualização da BIOS a partir de estação remota;
 - Capacidade para registrar eventos e emitir alertas, em caso de falha de ventiladores ou fontes, temperaturas e tensões fora de limites e erros de memória;

Alimentação elétrica:

- Possuir fontes redundantes, hot-pluggable redundância 1+1;
- A alimentação será disponibilizada em dois circuitos, sendo que o equipamento deverá manter a operacionalidade, em caso de falha de qualquer um deles;
- Tensão de operação entre 100 a 240VCA, 60Hz circuito monofásico;
- Sistema Operacional Baseado na plataforma Unix.

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Configurações Básicas do Servidor: Nome, atribuição de IP, Configurações de Armazenamento, Máquinas virtuais, Configurações Gerais;

- Montagem do equipamento e seus acessórios um rack de 19”;
- Conexão em Ponto de Energia Elétrica ou Power Injector (quando se fizer necessário);
- Conexão em Ponto de Rede Estruturado Categoria 6;
- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto;
- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606.

Ativos de rede WLAN – ACCESS POINT

Requisitos do item:

- Fornecimento de Ponto de Acesso Wi-Fi, novo e sem uso anterior.
- Deve ser homologado pela ANATEL;
- Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g/n, 802.11n draft 2.0 e 802.11ac ou superior;
- Deve ser capaz de operar simultaneamente nos padrões 802.11a/n/ac e 802.11b/g/n, através de rádios independentes (Dual Radio AP);
- Deve ser um equipamento ponto de acesso Wi-Fi para rede local sem fio de uso externo, com antenas aparentes, que atenda os padrões IEEE 802.11b/g/n na faixa de 2.4GHz e 802.11a/n/ac na faixa de 5GHz simultaneamente com configuração via software. O equipamento deve ter capacidade de análise espectral;
- Possuir funcionamento em modo autônomo sem a necessidade de controlador. Neste modo, permitir configuração e funcionamento do ponto de acesso sem a necessidade do controlador;
- Possuir funcionamento em modo gerenciado por Controlador Wi-Fi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF;
- Deverá estar logicamente conectado a um Controlador Wi-Fi, inclusive via roteamento da camada de rede OSI, através de rede pública ou privada;
- Deve implementar cliente DHCP, para configuração automática de rede;
- Possuir mecanismo de funcionamento para trabalhar com Controladores Wi-Fi em redundância (principal e redundante);
- Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) Wi-Fi – operação em modo de “chaveamento de tráfego local”;
- Operando no modo de “chaveamento de tráfego local”, o controlador Wi-Fi e os pontos de acesso devem:
- O modo de operação de chaveamento de tráfego local deve prever que se a comunicação entre o ponto de acesso Wi-Fi e o(s) Controlador(es) Wi-Fi seja interrompida por qualquer motivo, como por exemplo falha no link WAN, LAN ou no(s) próprio(s) Controlador(es) Wi-Fi, o ponto de acesso Wi-Fi deve continuar operando e permitindo que os usuários já autenticados na rede e associados aos pontos de

acesso continuem a possuir acesso à rede. Deve permitir que os usuários efetuem roaming rápido entre os pontos de acesso do mesmo site nesta situação;

- Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) Wi-Fi seja interrompida por qualquer motivo, como por exemplo falha no link Wi-Fi ou no(s) próprio(s) Controlador(es) Wi-Fi, o ponto de acesso Wi-Fi em modo de chaveamento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que novos usuários se autenticuem de acordo com 802.1x e se associem à rede sem qualquer prejuízo de acesso aos mesmos;
- Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) Wi-Fi seja interrompida por qualquer motivo, como por exemplo falha no link Wi-Fi ou no(s) próprio(s) Controlador(es) Wi-Fi, o ponto de acesso Wi-Fi em modo de chaveamento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que os usuários efetuem roaming sem qualquer prejuízo de acesso aos mesmos;
- Deve permitir a operação de usuários configurados nos padrões IEEE 802.11b/g/n e 802.11a/n/ac simultaneamente;
- Atender os seguintes requisitos em 802.11n (faixas de 2.4GHz e 5GHz) e 802.11ac (faixas de 5GHz): 3x4 multiple-input multiple-output (MIMO);
- Operar em Canais de 20MHz para 2,4GHz e possibilitar channel bonding, canal de 40 MHz para 5GHz e canais de 80MHz para 5GHz;
- Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
- Possuir capacidade de selecionar automaticamente o canal de transmissão;
- Permitir habilitar e desabilitar a divulgação do SSID;
- Possuir padrão WMM (Wi-Fi Multimedia) da Wi-Fi Alliance para priorização de tráfego;
- Não deve haver licença restringindo o número de usuários por ponto de acesso. O Ponto de Acesso deve permitir, no mínimo, 200 usuários por rádio;
- Deve possuir no mínimo 02 rádios (dual radio) operando simultaneamente em frequências distintas;
- Possuir, no mínimo, uma interface IEEE 802.3 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX, com conectores RJ-45;
- Possuir no mínimo 01 LED indicativo do estado de operação;
- Possibilitar a alimentação via padrão PoE+ (IEEE 802.3at) utilizando apenas uma porta do switch onde estiver conectado;
- Possuir estrutura suporte para instalação em poste ou parede;
- 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);
- Implementar WEP (Wired Equivalent Privacy), chaves de 40 bits e 128 bits;

- Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check-MIC);
- Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES, 128 bits);
- Deve permitir a conexão de usuários em IPv4, IPv6;
- Deve ter a capacidade de mudar de canal caso seja detectada alguma interferência prejudicial;
- Os equipamentos que compõe o Termo de Referência - Projeto Técnico deverão ser do mesmo fabricante, compondo uma solução única de rede para assegurar a compatibilidade funcional de todos os recursos e facilitar o gerenciamento.

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Configurações Básicas do Servidor: Nome, atribuição de IP, Configurações de Armazenamento, Máquinas virtuais, Configurações Gerais;
- Montagem do equipamento e seus acessórios em poste ou parede;
- Conexão em Ponto de Energia Elétrica ou Power Injector (quando se fizer necessário);
- Conexão em Ponto de Rede Estruturado Categoria 6;
- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto;
- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606.

Servidores – Implantação ou reestruturação de datacenter

Os equipamentos que compõe a solução de Data Center deverão ser do mesmo fabricante (Switches Core e Switches TOR), compondo uma solução única para assegurar a compatibilidade funcional de todos os recursos e facilitar o gerenciamento.

Especificação:

- Possuir no mínimo 02 (dois) processadores de 10 núcleos, arquitetura x64, sendo:
- Performance de referência Intel E5 2600 versão 3 ou superior;
- Frequência base mínima de 2.40GHz ou superior;
- Mínimo de 25MB de memória cache;
- 64 GB (Sessenta e quatro gigabytes) de memória e com possibilidade de expansão para 768 GB (setecentos e sessenta e oito gigabytes);
- 02 (dois) discos rígidos de 4TB (quatro terabytes), 7,2k rpm (sete mil e duzentas rotações por minuto), “hot pluggable/hot swap”, padrão SAS, configuráveis para RAID 0, 1, 5 em seu controlador;
- No mínimo 12 slots internos para discos rígidos;
- No mínimo 2 portas USB 3.0;

- Possuir placa de vídeo integrada;
- Deverá possuir BIOS desenvolvida pelo mesmo fabricante do equipamento;
- 04 (quatro) portas de rede GigaBitEthernet;
- Deve possuir 01 (um) disco SSD específico para boot com capacidade de 120 GB;
- Ventiladores redundantes, suportando o servidor em completa operacionalidade em caso de falha de um deles;
- Solução por hardware e/ou software de gerenciamento remoto, independente do sistema operacional e do estado do computador, com as seguintes características:
 - Controle remoto liga/desliga do servidor;
 - Console remota;
 - Servidor http e https;
 - Servidor SSH ou Telnet+SSL;
 - Criptografia SSL de 128 bits na comunicação;
 - Suporte a SNMP para consulta e traps;
 - Capacidade de atualização da BIOS a partir de estação remota;
 - Capacidade para registrar eventos e emitir alertas, em caso de falha de ventiladores ou fontes, temperaturas e tensões fora de limites e erros de memória;

Alimentação elétrica:

- Possuir fontes redundantes, hot-pluggable redundância 1+1;
- A alimentação será disponibilizada em dois circuitos, sendo que o equipamento deverá manter a operacionalidade, em caso de falha de qualquer um deles;
- Tensão de operação entre 100 a 240VCA, 60Hz circuito monofásico;

O equipamento e demais componentes deverão ser compatíveis com os seguintes sistemas operacionais:

- Sistema Operacional “Red Hat Enterprise/Advanced Linux 6” ou superior para sistema “x86_64” em nível “Certified”. A comprovação será realizada através do site oficial da Red Hat <http://hardware.redhat.com/>;
- Sistema Operacional “Microsoft Windows Server versão 2008 R2 x64” ou superior em nível “Certified”. A comprovação será realizada através do site oficial da Microsoft <http://www.windowsservercatalog.com/>;
- Sistema Operacional Linux ou superior;
- Deve ser fornecido com sistema operacional na plataforma Unix.
- Fornecer todos os discos necessários para reinstalação do sistema, drivers e software de gerência ou imagem através do site do fabricante.

Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;

- Configurações Básicas do Servidor: Nome, atribuição de IP, Configurações de Armazenamento, Máquinas virtuais, Configurações Gerais;
- Montagem do equipamento e seus acessórios;
- Conexão em Ponto de Energia Elétrica ou Power Injector (quando se fizer necessário);
- Conexão em Ponto de Rede Estruturado Categoria 6;
- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto;
- Integração deste componente ao demais componentes da solução;
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração de todos os equipamentos na documentação depois de instalados.

Fibras Ópticas – Integração de órgãos da Administração Pública ou Rede de conectividade

Este item refere-se ao fornecimento e instalação de Rede Óptica Metropolitana para interligação dos órgãos públicos, unidades de saúde, escolas, praças e diferentes pontos de prestação de serviços à população.

A unidade de medição e pagamento deste item será o metro linear instalado e ativado. Deverá estar incluso no valor do metro todos os equipamentos (Optical Line Terminal (OLT) e Optical Network Unit (ONU), materiais ópticos, cabos ópticos, infraestrutura e serviços necessários para a instalação dos pontos de conexão listados no termo de referência e projeto técnico;

A solução óptica implantada deverá respeitar as características mínimas obrigatórias descritas no termo de referência e no projeto técnico e deverá obrigatoriamente ser implantada a tecnologia de Redes Gigabit Passive Optical Network – GPON, conforme projeto técnico;

Considera-se fibra ativada o assinante (ponto de conexão) conectado à rede óptica da Prefeitura Municipal, certificado e funcionando. Serviços executados: lançamento, ancoragem, fusões, instalação de caixas de emenda, distribuidores ópticos, cordões, extensões, splitters ópticos, certificação do enlace e configuração dos ativos OLT e ONU;

Todos os materiais ópticos para perfeito funcionamento da solução deverão ser fornecidos e inclusos no orçamento: cordões ópticos, extensões ópticas, distribuidores internos ópticos, caixas de emenda, splitters, rosetas ópticas, conectores e demais itens imprescindíveis ao funcionamento da solução. O material óptico ser do mesmo fabricante das fibras ópticas descritas no Termo de Referência - Projeto Técnico;

Todos os materiais necessários à sustentação, ancoragem e suporte do cabo óptico como: fitas de aço inox, suportes, isoladores, parafusos, braçadeiras BAP, conjunto de ancoragem, grampos de suspensão e quaisquer outros materiais que se faça necessários.

O custo do metro linear instalado deve contemplar todos os equipamentos (OLT, ONU), materiais e serviços citados no item.

A tabela abaixo descreve os pontos de conexão assinantes, que deverão receber conexão de fibras ópticas, conforme projeto técnico. Cada ponto deverá receber (um) ponto de fibra óptica e estar equipada com uma ONU.

RELAÇÃO DOS PONTOS DE CONEXÃO DE FIBRAS ÓPTICAS - ASSINANTES		
Nº	Obra	Endereço
1	Abrigo Dos Idosos	Rua Dom Pedro II, Teotonio Vilela
2	Ação social	Avenida 20 de agosto, Centro
3	Biblioteca Digital	Avenida Farid Miguel Safatle
4	CAPS (Centro de Atenção Psicossocial)	Vila Mutirão
5	CAPS AD (Centro de Atenção Psicossocial Álcool e Drogas)	Avenida 20 de agosto, Centro
6	Casa Da Criança	Rua Tenente João de Cerqueira Netto, Loteamento Jardim Primavera
7	Casa da Cultura	Avenida 20 de Agosto , Centro
8	CCPA (Centro de Convivência do Pequeno Aprendiz)	Rua Tenente João de Cerqueira Netto, Loteamento Jardim Primavera
9	Centro De Reabilitação	Avenida 20 de Agosto, Centro
10	Centro Integrado da Mulher	Rua Major Paulino, Nossa Senhora de Fátima
11	CION (Centro Integrado Ondonto Médico)	Rua Major Paulin, Nossa Senhora de Fátima
12	CMEI (Centro Municipal de Educação Infantil) - Anibal Rosa	Avenida Jose Marcelino, Castelo Branco
13	CMEI (Centro Municipal de Educação Infantil) - Cleonice	Rua 21, Número 9, Setor Universitário
14	CMEI (Centro Municipal de Educação Infantil) - Copacabana	
15	CMEI (Centro Municipal de Educação Infantil) - Ruth Silva	Rua 403, Pontal Norte

16	CRAS (Centro de Referência de Assistência Social)	Rua Ademar Ferrugem, Centro
17	CREAS (Centro de Referência Especializado de Assistência Social)	Rua Porto Nacional
18	Creche Alba Mathias	Avenida Espírito Santo Setor Aeroporto
19	Creche Francisco Clementino	Rua Antonio Souza, Ipanema
20	Creche Irma Yolanda	Rua Tenente João de Cerqueira Netto, Loteamento Jardim Primavera
21	Creche Jardim Europa	Rua 611, Jardim Europa
22	Creche Joao Margon, B	Rua 2, Flamboyant
23	Creche Lázaro Marra	Rua 308, Jardim Catalão
24	Creche Maria Amelia 1	Maria Amelia 1
25	Creche Municipal Ana Maria Guimaraes	Rua São Salvador, Vila Erondina
26	Creche Municipal Nilza Aires	Rua Sergipe, Vila Mutirão
27	Escola Caic São Francisco de Assis	Rua Tenente João de Cerqueira Netto, Loteamento Jardim Primavera
28	Escola Frei João Franciso	Rua A, Bairro Santa Helena 2
29	Escola Israel Macedo	Rua 502, 333 - S Santa Cruz, Catalão - GO
30	Escola José Sebba	Rua 143, Parque das Mangueiras
31	Escola Municipal – Wilson Da Paixão	Rua São Salvador, Vila Erondina
32	Escola Nilda Margon Vaz	Avenida Jose Marcelino, Castelo Branco
33	Escola Patotinha	Rua Guatemala, Bairro das Americas
34	Escola Pontal Norte	Pedro Netto Paranhos
35	ETA (Estação de tratamento de Água)	Av. São Salvador, 1-227 - Mãe de Deus, Catalão
36	Futura Sede Prefeitura	Avenida Doutor Lamartine Pinto de Avelar, Vila Chaud

37	Hemocentro	Rua Hosório Vieira Leite, São João
38	Hospital Materno Infantil	Rua Major Paulino, Nossa Senhora de Fátima
39	Posto de Saude Allan Cardec	Rua Rio de Janeiro
40	Praça 15 de Novembro	Centro
41	Praça Aguiar de Paula	Centro
42	Praça Brasil Cavalcante	Pio Gomes
43	Praça da Bíblia	Parque das Mangueiras
44	Praça da Fé	Vila Cruzeiro I
45	Praça da Fé	Vila Cruzeiro II
46	Praça da Liberdade	Vila Liberdade
47	Praça Das Bandeiras	Vila União
48	Praça das Dálías	Jardim Primavera
49	Praça Das Mães	São João
50	Praça do Estudante	Setor Boa Sorte
51	Praça do Rosário	Centro
52	Praça Dom Emanuel	Centro
53	Praça Duque de Caxias	Centro
54	Praça Emanuel B. dos Santos	Vila União
55	Praça Eutálio Pereira	Mãe de Deus
56	Praça Francisco Tozzi de Souza	Vila Liberdade
57	Praça Getúlio Vaz	Centro
58	Praça Marca Tempo	Centro
59	Praça Pontal Norte	Pontal Norte
60	Praça Publio de Souza	Bairro das Americas

61	Praça Tereza Müller Margon	Bairro Santo Antonio
62	Praça Uberlândia	Centro
63	Prefeitura Municipal de Catalão	R. Nassim Agel, 505 - Centro, Catalão - GO
64	Quadra Coberta Castelo Branco	Avenida Jose Marcelino, Castelo Branco
65	Quadra Coberta Pontal Norte	Pontal Norte
66	Quadra Coberta Vila Erondina	Rua São Salvador, Vila Erondina
67	Quadra de Esportes	Rua 28, Vila Margon
68	Quadra de Esportes Vila Mutirão	Vila Mutirão
69	Restaurante Popular	Avenida Raulina Fonseca Paschoal
70	SAE (Superintendencia de Tratamento de Água e Esgoto)	R. Ver. Kavefes Abraão, 660 - Lot. Leao, Catalão - GO
71	Secretaria de Esporte e Lazer	Rua 510, Setor Santa Cruz
72	Secretária de Habitação	Avenida 20 De Agosto, Centro
73	Secretaria de Saude	BR-050
74	Secretária do Meio Ambiente	Avenida Doutor Lamartine Pinto de Avelar, Vila Chaud
75	Serraria	Avenida Jeferson Barbosa de Melo
76	UBS (Unidade Básica de Saúde) - Bairro Castelo Branco	Marica Carolina de Mesquita Neto
77	UBS (Unidade Básica de Saúde) - Copacabana	
78	UBS (Unidade Básica de Saúde) - Cristina de Cassio Rodovalho	Rua Alberto Elias, Evelina Nour 2
79	UBS (Unidade Básica de Saúde) - Divano Elias da Silva	Rua Geraldo Belo da Silva, Setor Universitário
80	UBS (Unidade Básica de Saúde) - Joao Moreira de Castro	São João

81	UBS (Unidade Básica de Saúde) Willian Faiad	Pontal Norte
82	UBS(Unidade Basica de Saúde) - Albino da Silva Barbosa	Ipanema
83	UBS(Unidade Basica de Saúde) - Lamartine Pinto de Avelar	Bairro Santo Antônio
84	UBS(Unidade Basica de Saúde) - Silvana Maria Mesquita	Vila União
85	UBS(Unidade Básica de Saúde) - Doutor Paulo de Tarcio Campos	Avenida Ricardo Paranhos,Vila Liberdade
86	UPA (Unidade de Pronto Atendimento)	Avenida Pinto de Avelar
87	Vigilância Sanitária	BR- 050

O materiais que compõe a solução óptica devem possuir os seguintes requisitos mínimos:

Cabo Óptico Externo Monomodo autossustentado;

Este cabo óptico adotado para uso externo deverá ser do tipo “loose”, composto por 12 (doze) fibras ópticas do tipo monomodo dentro de tubo termoplástico com gel para acomodação das fibras, dois elementos de fibra de vidro pultrudada (FRP) para suporte mecânico (resistência à tração) e cobertos por uma capa externa de material termoplástico;

Cabo óptico deve possuir mínimo 12FO;

- Deverá ser totalmente dielétrico, ser resistente a intempéries e ação solar (proteção UV);
- Fabricante deste cabo óptico preferencialmente deverá possuir certificação ISO 9001 E ISO 14001;
- Apresentar Certificação Anatel;
- Este cabo deverá ser constituído por fibras monomodo 9/125 µm, proof-test 100 kpsi;
- Apresentar diâmetro do campo modal:
 - 9,3 +/- 0,5 µm em 1310 nm;
 - 10,4 +/- 0,8 µm em 1550 nm;
- Apresentar atenuação máxima de:
 - 0,37 dB/km em 1310 nm;
 - 0,23 dB/km em 1550 nm;

- Temperatura de operação de -10 a 65 graus, comprovada através de teste ciclo térmico;
- Permitir instalações aéreas entre postes com vãos livres de até 120 m sem cordoalha de aço;
- Possuir impresso na capa externa nome do fabricante, marca do produto, data de fabricação, gravação sequencial métrica (em sistema de medida internacional SI);
- Demais características de acordo com a norma ABNT NBR 14160.

Cabo Óptico DROP 02 FO

Cabo óptico adequado para aplicações internas e externas autossustentadas de acesso ao usuário final, tipo “drop”. Deve possuir características de baixa sensibilidade à curvatura (BLI). Permite instalação autossustentado ou através de eletrodutos ou eletrocalhas;

Características Técnicas:

- Possuir resistência à ação solar (proteção UV) e resistente à intempéries;
- Possuir fio de aço galvanizado que atuam contra esforços de tração e estabilidade térmica;
- Deve ser totalmente compatível com as fibras G652 D;
- Apresentar diâmetro nominal do mensageiro de até 3,0 mm;
- Deve possuir características não propagante a chamas com grau de proteção quanto a comportamento frente à chama classe LSZH (Cabo com baixa emissão de fumaça e livre de halogênios) e característica de atrito reduzido;
- Este cabo deverá ser constituído por fibras monomodo BLI A/B (Bending Loss Insensitive);
- Apresentar atenuação máxima de:
 - 0,35 dB/km em 1310nm;
 - 0,20 dB/km em 1550nm.
- Ser adequado para instalação em vãos máximos de 80 m;
- Raio mínimo de curvatura durante a instalação de 30 mm e durante a operação de 15mm;
- Coeficiente de atrito dinâmico máximo: 0,25;
- Possuir impresso na capa externa nome do fabricante, marca do produto, ano de fabricação, metragem linear do cabo (em sistema de medida internacional SI);
- Certificado de homologação expedido pela ANATEL;
- Fabricante deste cabo óptico preferencialmente deverá possuir certificação ISO 9001 E ISO 14001;

Cordão Óptico:

- Este cordão deverá ser constituído por uma fibra óptica monomodo 9/125 μm ;
- Utilizar padrão “zip-cord” de reunião das fibras para diâmetro nominal de 2mm;
- A fibra óptica deste cordão deverá possuir revestimento primário em acrilato e revestimento secundário em material termoplástico;

- Sobre o revestimento secundário deverão existir elementos de tração de fios dielétricos e capa em material termoplástico não propagante à chama;
- As extremidades deste cordão óptico duplo devem vir devidamente conectorizadas e testadas de fábrica;
- O fabricante preferencialmente deverá apresentar certificados ISO 9001 e ISO 14001;
- Possuir impresso na capa externa nome do fabricante, identificação do produto e data de fabricação;
- Ser disponibilizado nas opções de terminações com conectores ST / FC / SC / MT-RJ / LC e E2000-APC;
- O fabricante deve possuir certificação Anatel para os conectores ópticos ST / FC / SC / MT-RJ / LC e E2000-APC;
- O cordão deve estar de acordo com a norma ABNT 14106;
- Os conectores ópticos devem atender os requisitos mínimos previstos na norma ABNT NBR 14433;

Extensão Óptica:

- Atender os requisitos mínimos previstos na norma ANSI EIA/TIA 568-C.3;
- Este pigtail deverá ser constituído por 2 (duas) fibras ópticas monomodo 9/125 μm com revestimento primário em acrilato e revestimento secundário em PVC, com diâmetro nominal de 0,9mm e adaptador óptico para atender um canal óptico;
- Ser disponibilizado nas opções de terminações com conectores ST/ SC / LC;
- Uma das extremidades deve vir devidamente conectorizada e testada de fábrica;
- Os conectores ópticos devem atender os requisitos mínimos previstos na norma ABNT NBR 14433;
- O fabricante deverá apresentar certificados ISO 9001 e ISO 14001.

Distribuidor Interno Óptico:

- Distribuidor óptico para até 48 fibras para Rack de 19”;
- Deve suportar até 48 fibras com conectores SC e até 24 fibras com outros conectores;
- Deverá ter a função de acomodar e proteger as emendas de transição entre o cabo óptico e as extensões ópticas:
- Ser compatível com os adaptadores ópticos ST, SC, LC Duplex, FC;
- Ser modular permitindo expansão do sistema;
- Deve possuir áreas de armazenamento de excesso de fibras, acomodação e emenda, que devem estar internos à estrutura (conferindo maior segurança ao sistema);
- Deve possuir altura (1U) e ser compatíveis com o padrão 19”;
- Deve possuir áreas de armazenamento de excesso de fibras, acomodação e emenda, que devem ficar internos à estrutura (conferindo maior segurança ao sistema);
- Ser fornecido com bandejas de acomodação de emendas para até 24 Fibras;
- Ser fornecido com adaptadores ópticos;

- Ser fabricado em aço SAE 1020;
- Deve possuir gaveta deslizante para facilitar a manutenção e a instalação, e trabalhos posteriores sem retirá-los do rack;
- Deve possuir 02 acessos para cabos ópticos traseiros.

OLT (Optical Line Networks)

- A OLT deve possuir no mínimo oito interfaces GPON;
- Seis Interfaces Giga Bit Ethernet baseadas em SFP;
- Duas portas Combo Elétricas de 10/100/1000 Mbps
- Duas Interfaces Óticas de 10GigE baseadas em XFP
- Uma Interface RS-232 para Console
- Uma interface 10/100/1000 para saída de gerenciamento de banda
- Ao total são 512 usuários concentrados em uma OLT de 2 U de Rack.
- Switching Fabric: 132 Gbps.
- Deve ser fornecida completa com transceivers GPON.
- Deve possuir fonte de alimentação Hot Swap, inclusa uma fonte redundante.
- Capacidades Layer 2:
 - IEEE 802.3ac – VLAN Tagging
 - IEEE 802.1S – Multiple Spanning Tree
 - IEEE 802.1W – Rapid Spanning Tree
 - IEEE 802.1D – Spanning Tree
 - IEEE 802.1Q – Virtual LANs with Port Based VLANs
- Até 4096 VLANs
- Completa operação com VLAN:
 - push, pop e translate
 - IEEE 802.1v – Protocol based VLANs
 - IEEE 802.1p – Prioritization of Traffic at the Data-Link Level
 - IEEE 802.3x – Flow Control
- Q-in-Q support
- Port Mirroring. Switched Port Analyzer (SPAN)
- Port Mirroring. Remote switched Port Analyzer (RSPAN)
- Storm Control
- Broadcast Storm filtering
- Marcação de tráfego: VLAN, IP, DSCP, CoS, Ethernet, etc
- Multicast Storm filtering
- IP Address Filtering
- DLF (Destination Lookup Failure) Storm Protection
- Rate Limiting (In/Out)

- MAC Static Filter
- MAC Address anti-spoofing
- IP Address anti-spoofing
- Ethernet Access List
- IP Access List
- BPDU's Filtering
- Mac freezing
- Proteção contra MAC Flooding
- Jumbo Frames support up to 16.374 bytes
- Radius/Tacacs+
- Access Control List L2 (ACLs Support)
- 8/16 k MAC Table
- EAPS (v1.0)
- Verificação de potência ONU remotamente via OLT
- Aging time
- Capacidades Layer 3:
 - RFC 1058 - RIP v1
 - RFC 2453 - RIP v2
 - RFC 2328 - OSPF v2
 - RFC 791 - Ipv4
- DHCP e DHCP option 82/60
- IP estático
- QOS
- Até 8 CoS por porta
- 802.1P VLAN
- IPv4 TOS priority
- Taxa de Entrada e Saída com shaping
- Alocação dinâmica de banda
- Filtering (L3/L4 Access Lists)
- IP Classification
- RFC 2474 - DiffServ Definition
- RFC 2475 - DiffServ Architecture
- RFC 2597 - Assured Forwarding PHB;
- RFC 3246 - An Expedited Forwarding PHB
- L3 "ACLs" Access Control List
- RFC 3260 - New Terminology and Clarifications for DiffServ
- Capacidades de Gerência:
 - Telnet
 - SSH v2
 - FTP

- SNMP
- SP + WRR
- ONT (Optical Network Unit)
- A ONT deve possuir no mínimo uma interface 10/100/1000 Base-T (RJ-45), Auto-Negociação, Auto-Sensing, Automática MDI / MDIX e 1x interface óptica GPON SC-APC;
- Deve implementar Fluxo de Controle (Flow Control);
- Deve possuir sensibilidade de -28 dB, compatível com ITU-T G.984.3;
- Camada física é compatível com a ITU-T G.984.2;
- Deve suportar FEC;
- Implementar AES com chave de comutação de 128 bit de downstream;
- Deve suporta a ativação com mecanismo de registro de identificação quando recém instalado.
- Deve suportar até 8 T-CONTs:
- A ONT deve suportar até 64 portas GEM:
- 1 para OMCI;
- 1 para Multicast;
- 1 para Broadcast;
- 61 para Ethernet;
- Suportar até 128 MACs por porta;
- MTU 2000 bytes;
- Classificação de upstream por:
- Porta Ethernet UNI;
- Ethernet Ether Type;
- 802.1Q VLAN ID;
- 802.1D campo de prioridade usuário do 802.1Q cabeçalho.
- Deve suportar pelo menos 10 VLANs;
- Suportar até 1000 grupos de multicast;
- Suportar IGMP v2/v3 Snooping:
- Suportar Proxy IGMP;
- Implementar 8 filas de prioridade por T-CONT;
- Ser gerenciável através de CLI;

Instalação

- As atividades de planejamento, projeto e instalação da solução de interligação óptica dos Órgãos da Administração Pública compreendem:
- Desenvolver o projeto de liberação para uso compartilhado de Infraestrutura dos postes utilizados para interconexão óptica junto à concessionária de energia elétrica, desta forma deverá apresentar à Prefeitura Municipal de Catalão o projeto de compartilhamento da infraestrutura de postes de acordo com as respectivas normas da concessionária de energia elétrica ENEL Distribuição Goiás, com o

trajeto sugerido para a interligação. É de responsabilidade da Contratada definir qual melhor trajeto para interligação dos pontos mapeados pela Prefeitura;

- Após aprovação do projeto pela Prefeitura a Contratada deverá tomar as devidas providências junto a ENEL Distribuição Goiás para a aprovação do referido projeto de compartilhamento da infraestrutura de postes, estando ainda responsável pelo acompanhamento, eventuais esclarecimentos e correções que porventura sejam necessárias para a aprovação da ENEL Distribuição Goiás;
- Aprovação de quaisquer licenças, alvarás e demais liberações que porventura sejam necessárias para a execução dos serviços junto aos Órgãos Fiscalizadores e arcando com seus respectivos custos;
- A Contratada deverá fornecer e instalar todos os equipamentos (cordões ópticos, extensões ópticas, Distribuidores internos ópticos, rosetas ópticas, conectores e demais itens imprescindíveis ao funcionamento da solução), materiais, acessórios, fazer o lançamento dos cabos nos postes, fazer a fusão e certificar a infraestrutura de fibras ópticas, conforme segue as especificações do Termo de Referência - Projeto Técnico;
- Todos os serviços deverão seguir e estar em completo acordo com as normas e recomendações dos organismos governamentais competentes, ainda que não especificados no Termo de Referência - Projeto Técnico, nas versões vigentes quando da apresentação das propostas;
- Para garantir a qualidade dos cabos e serviços executados, a Contratada deverá executar e entregar os testes e medições nas fibras ópticas após o lançamento, emendas, e terminação dos cabos no DIO. Executar teste de enlace para avaliar a integridade das fibras, se há inversão de fibras, fibras quebradas ou fibras trincadas e a atenuação causada por emendas, conectores e pela distância. Executar teste de potência óptica para verificar a diferença da potência emitida e da recebida;
- Após a conclusão dos testes, os dados armazenados na memória do analisador deverão ser transferidos para meio magnético ou mídia, devendo também, serem impressos em forma de relatório em papel A-4 e entregue a equipe técnica da Prefeitura;
- Os links que forem diagnosticados com defeito deverão ser corrigidos antes da assinatura do Termo de Recebimento. O equipamento utilizado deverá possuir certificado de calibração dentro da validade, emitido por laboratório credenciado junto ao INMETRO.

Instalações – Criação do Espaço Físico do Data Center

Este item descreve os serviços de Montagens e Instalações, com aplicação de material, para reestruturação de Data Center;

Devem estar inclusos neste item:

- Instalação de Piso Elevado;
- Instalação de Piso Elevado para sala do Data Center faz necessário à vistoria técnica para elaboração de paginação, altura e instalação do piso, eximindo a Prefeitura de custos adicionais posteriores;

- As placas de piso elevado deverão possuir dimensão mínima de 500x500x20mm constituídas de chapas de aço ou material similar, possuir estrutura de sustentação com no mínimo 04 furos. As placas devem possuir tratamento antioxidante e pintura epóxi;
- Fornecimento e implantação de cabeamento elétrico com a instalação de quadros elétricos;
- A infraestrutura elétrica prevê toda a adequação elétrica no Data Center. Neste escopo estão incluídas as instalações de cabeamento e de quadro elétrico para ligação dos nobreaks. É de extrema importância que se realize a visita técnica in loco para que a licitante conheça o ambiente de instalação e as instalações atuais, propondo as alterações que sejam necessárias;
- Deverá estar previsto ainda a instalação de um quadro elétrico separado para os circuitos de ar condicionado, iluminação e tomadas de uso geral;
- Fornecimento e implantação de infraestrutura para a passagem dos cabos lógicos e elétricos;
- Sob o piso elevado deverão ser montados 2 níveis eletrocalhas do tipo aramada para a passagem dos cabos elétricos e lógicos. No nível mais baixo será instalada a infraestrutura para a passagem dos cabos elétricos e no nível superior deverão ser instaladas as eletrocalhas para a distribuição do cabeamento lógico;
- Todas as calhas instaladas deverão ser fixadas e não será aceita infraestrutura que contenha arestas, cantos mal acabados e acessórios feitos no local. Sempre que houver necessidade de curvas, reduções, derivações e demais conexões de eletrocalhas, estas deverão ser feitas utilizando acessórios específicos para este fim e respeitando os raios de curvaturas definidos em norma;
- Fornecimento e implantação de infraestrutura para iluminação e instalação de luminárias LED;
- A infraestrutura de iluminação será executada para atender somente a área do Data Center. A instalação das luminárias deverá ser feita de acordo com a nova paginação do forro e a Contratada fornecerá o leiaute com a nova disposição das luminárias;
- Deverá ser fornecida e instalada no ambiente do Data Center 01 (uma) porta corta fogo;

Serviços de Instalação:

- A instalação e configuração dos equipamentos deve prever todos os cenários possíveis. Para isto se faz necessário à vistoria técnica obrigatória, eximindo a Prefeitura de custos adicionais posteriores;
- Este item descreve a execução dos seguintes serviços a serem executados pela Contratada;
- Durante a execução dos trabalhos deverá ser providenciado o isolamento do ambiente onde serão executados os serviços, afim de que os equipamentos existentes na sala não sejam afetados pela poeira. Será de responsabilidade da empresa contratada a limpeza do ambiente, remoção de entulhos, restos de materiais, etc. Toda a área do Data Center sob o piso elevado deverá ser limpa utilizando aspiradores e demais recursos necessários;
- Mobiliário, equipamentos de informática, pisos e rodapés, esquadrias e seus componentes, calhas e eletrodutos, bem como todo e qualquer material de expediente, deverão ser protegidos durante a execução dos trabalhos;
- Para preservar os ambientes adjacentes, bem como não prejudicar o andamento das atividades na Unidade/Gerência, a retirada dos entulhos deverá ser realizada diariamente, cercada de todos os cuidados necessários;

- No final da reestruturação, além do As Built dos sistemas instalados, desenhos, diagramas de interligação, manuais de projeto e manutenção, deverão ser entregues à Prefeitura.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DA REDE DE DADOS – INTEGRAÇÃO DE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

Todos os catálogos, manuais e especificações técnicas dos equipamentos/materiais deverão ser apresentados na íntegra para avaliação da comissão de licitação.

Instalações – Rede de dados – Integração de órgãos da Administração Pública – Ponto de Rede Categoria 6

Este item deverá ser cotado por UNIDADE DE PONTO. Para fins de composição de custos, será compreendido que a “unidade de ponto” para os cabos das redes horizontais UTP (cat 6), terão um comprimento estimado de 50 (cinquenta) metros. Não cabe as partes solicitarem revisão de valores devido a variação da metragem de cada ponto, seja para maior ou para menor;

Além do cabo UTP, deverão constar os miscelâneos: conector fêmea RJ45 (cat 6), Patch Cords e porta de patch panel, abraçadeiras plásticas, etiquetas para identificação de cabo e todo material de consumo necessário para instalação de cada ponto correspondente;

A licitante deverá prever materiais de infraestrutura para instalação de 01 (uma) unidade de ponto de rede lógico. Esta instalação deve prever todos os cenários possíveis, para isto faz-se necessário à vistoria técnica obrigatória, eximindo a Prefeitura, de quaisquer custos adicionais não previstos. Deverá ser composto, proporcionalmente, por todos os itens necessários à construção de infraestrutura seca tais como: Eletrocalha, Suportes de Fixação, tirante de Fixação, chumbadores para Tirante, curvas, abraçadeiras, eletrodutos galvanizado, Conduletes galvanizado, materiais de identificação e todos acessórios que se faça necessários para construção do ponto de rede de dados;

Toda a identificação do cabeamento deverá seguir o padrão da norma EIA/TIA 606 (Administration Standard for Telecommunications Infrastructure of Commercial Buildings).

Atividades que compreendem a instalação de ponto de rede lógico: lançamento de cabeamento de rede, instalação de tomadas fêmeas RJ, instalação física de patch panel, conectorização de cabos de rede em ambas extremidades, instalação de Patch cords, testes e certificações de cabeamento de acordo com as normas internacionais EIA/TIA 568-B e normas complementares, Identificação dos componentes do cabeamento (cabo, espelhos e painéis) com etiqueta adesiva;

Todo material de cabeamento estruturado utilizado para instalação do ponto de rede Cat.6 deverá ser do mesmo fabricante, exceto acessórios de instalação tais como parafusos, abraçadeiras e similares;

Os materiais de cabeamento estruturado deverão possuir as seguintes especificações mínimas:

Patch Panel Categoria 6 - 24 Portas;

- Possuir Certificação UL ou ETL LISTED;
- O produto deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS;
- Painel frontal em termoplástico de alto impacto, não propagante a chama que atenda a norma UL 94 V-0 (flamabilidade), com porta etiquetas de identificação em acrílico para proteção; O painel deverá ser de cor preta;
- Apresentar largura de 19", e altura de 1U ou 44,5mm para os Patch Panels de 24 portas;
- Ser disponibilizado em 24 portas com conectores RJ-45 fêmea na parte frontal, estes devem ser fixados a circuitos impressos (para proporcionar melhor performance elétrica);
- Ser fornecido em módulos de 08 ou 06 posições;
- Os conectores fêmea RJ-45 devem possuir as seguintes características: Atender a ANSI/TIA/EIA-568-C.2 Categoria 6, possuir vias de contato produzidas em bronze fosforoso com camadas de 2,54 µm de níquel e 1,27 µm de ouro, possuir terminação do tipo 110 IDC (conexão traseira) estanhados para a proteção contra oxidação, permitindo inserção de condutores de 22 AWG a 26 AWG;
- Identificação do fabricante no corpo do produto;
- Possuir local para aplicação de ícones de identificação (para codificação);
- Fornecido de fábrica com ícones de identificação (nas cores azul e vermelha);
- Ser fornecido com guia traseiro perfurado, em material termoplástico de alto impacto, não propagante a chama que atenda a norma UL 94 V-0 (flamabilidade) com possibilidade fixação individual dos cabos, proporcionando segurança, flexibilidade e rapidez na montagem;
- Ser fornecido com acessórios para fixação dos cabos (cintas de amarração);
- Possuir em sua estrutura, elementos laterais em material metálico, que eliminem o risco de torção do corpo do Patch Panel;
- Suportar ciclos de inserção, igual ou superior a 200 (duzentas) vezes com terminações 110 IDC;
- Suportar ciclos de inserção, na parte frontal, igual ou superior a 750 (setecentas e cinquenta) vezes com conectores RJ-45 e 200 inserções com RJ11;
- Fornecido com instrução de montagem na língua Portuguesa;
- Exceder as características elétricas contidas na norma ANSI/TIA/EIA-568-C.2 Categoria 6;
- Compatível com as terminações T568A e T568B, segundo a norma ANSI/TIA/EIA-568-C.2, sem a necessidade de trocas de etiqueta;

Cordão de Conexão – Patch Cord;

- Possui Certificação UL ou ETL LISTED;

- Deve ter duas certificações Anatel conforme regulamento da entidade: a do cabo flexível e do cordão de manobra;
- Deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS;
- Deve possuir certificação de canal para 4 conexões por laboratório de 3a. Parte ETL;
- Deverão ser montados e testados em fábrica, com garantia de performance.

Cabeamento:

- O acessório deve ser confeccionado em cabo par trançado, U/UTP Categoria 6 (Unshielded Twisted Pair), 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina e capa externa em PVC não propagante a chama, conectizados à RJ-45 macho Categoria 6 nas duas extremidades, estes conectores (RJ-45 macho), devem atender às especificações contidas na norma ANSI/TIA/EIA-568-C.2 Categoria 6, ter corpo em material termoplástico de alto impacto não propagante a chama que atenda a norma UL 94 V-0 (flamabilidade), possuir vias de contato produzidas em bronze fosforoso com camadas de 2,54 µm de níquel e 1,27 µm de ouro, para a proteção contra oxidação, garras duplas para garantia de vinculação elétrica com as veias do cabo;
- Deve possuir classe de flamabilidade no mínimo CM;
- O Cabo utilizado deve apresentar Certificação ETL em conformidade com a norma ANSI/TIA/EIA-568-C.2 CATEGORIA 6 (stranded cable);
- Deve possuir capa protetora (boot) do mesmo dimensional do RJ-45 plug e proteção à lingueta de travamento. Esta capa protetora deve ajudar a evitar a curvatura excessiva do cabo em movimentos na conexão bem como proteger o pino de destravamento dos conectores contra enroscamentos e quebras;
- Deve ser disponibilizado pelo fabricante em pelo menos 8 cores atendendo às especificações da ANSI/TIA/EIA-606-A;
- Exceder as características elétricas contidas na norma ANSI/TIA/EIA-568-C.2 Categoria 6;

Cabo U/UTP – Categoria 6;

- Possuir certificado de performance elétrica (VERIFIED) pela UL ou ETL, conforme especificações da norma ANSI/TIA-568-C.2 CATEGORIA 6 e ISO/IEC 11801 bem como certificado para flamabilidade (UL LISTED ou ETL LISTED) CMR;
- O cabo utilizado deverá possuir certificação Anatel impressa na capa;
- O produto deve cumprir com os requisitos quanto a taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS;
- Possuir certificação de canal para 6 conexões por laboratório de 3a. Parte ETL ou UL;
- Possuir impresso na capa externa nome do fabricante, marca do produto, e sistema de rastreabilidade que permita identificar a data de fabricação dos cabos;

- Ser composto por condutores de cobre sólido; capa externa em PVC não propagante à chama, com possibilidade de fornecimento nas cores azul, amarelo, preto, verde, branco, bege, marrom, laranja, vermelha ou cinza;
- Deve atender ao código de cores especificado abaixo:
 - par 1: azul-branco, com uma faixa azul (stripe) no condutor branco;
 - par 2: laranja-branco, com uma faixa laranja (stripe) no condutor branco;
 - par 3: verde-branco, com uma faixa verde (stripe) no condutor branco;
 - par 4: marrom-branco, com uma faixa marrom (stripe) no condutor branco;
- Exceder as características elétricas contidas na norma ANSI/TIA-568-C.2 Categoria 6;
- Impedância característica de 100Ω (Ohms);
- Deverá ser apresentado através de catálogos, testes das principais características elétricas em transmissões de altas velocidades (valores típicos) de ATENUAÇÃO (dB/100m), NEXT (dB), PSNEXT(dB), RL(dB), ACR(dB), para frequências de 100, 200, 350 e 550Mhz;

Conector RJ-45 Fêmea - Categoria 6;

- Possuir Certificação UL ou ETL LISTED;
- Possuir certificação de canal para 4 conexões por laboratório de 3a. Parte ETL;
- Ter corpo em material termoplástico de alto impacto não propagante à chama que atenda a norma UL 94 V-0 (flamabilidade);
- Possuir protetores 110 IDC traseiros para as conexões;
- Possuir vias de contato produzidas em bronze fosforoso com camadas de $2,54\ \mu\text{m}$ de níquel e $1,27\ \mu\text{m}$ de ouro;
- Apresentar disponibilidade de fornecimento nas cores (branca, bege, vermelha, azul e preta);
- O keystone deve ser compatível para as terminações T568A e T568B, segundo a ANSI/TIA/EIA-568-C.2;
- Possuir terminação do tipo 110 IDC (conexão traseira) estanhados para a proteção contra oxidação e permitir inserção de condutores de 22 AWG a 26 AWG;
- O conector fêmea deverá possibilitar a crimpagem dos 8 condutores ao mesmo tempo proporcionando deste modo uma conectorização homogênea;
- Suportar ciclo/s de inserção, na parte frontal, igual ou superior a 750 (setecentas e cinquenta) vezes com conectores RJ-45 e 200 inserções com RJ11;
- Suportar ciclos de inserção, igual ou superior a 200 (duzentas) vezes com terminações 110 IDC;
- Identificação da Categoria gravado na parte frontal do conector;
- Exceder as características elétricas contidas na norma ANSI/TIA/EIA-568-C.2 Categoria 6;
- O produto deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a diretiva RoHS;

Instalação:

- Lançamento de cabo UTP Cat.6 do ponto de concentração (rack principal) até o ponto de instalação do equipamento;
- Conectorização de cabos de rede;
- Instalação física de Patch Panel seguindo padrões previamente definidos;
- Testes e certificações de cabeamento de acordo com as normas internacionais EIA/TIA 568-B e normas complementares;
- Identificação dos componentes do cabeamento (cabo, espelhos e painéis) com etiqueta adesiva;
- Fornecidos com todos os acessórios para fixação e identificação, tais como: velcro para amarração, etiquetas, etc.;
- Os serviços de instalação compreendem: a construção de infraestrutura seca para o lançamento do cabo, e a conectorização de ambas as extremidades do cabo;
- Ficará sob responsabilidade da empresa instaladora, a limpeza do local de trabalho, bem como todo e qualquer acabamento necessário;
- Todos os enlaces devem ser certificados e o relatório desta certificação deve constar da documentação da obra;
- Toda a infraestrutura necessária para instalação do referido enlace será responsabilidade da Contratada, devendo a mesma obter todas as aprovações necessárias para a implantação, além do fornecimento dos materiais adequados a cada tipo de instalação;
- Deverá ser apresentado valor por ponto.

Capacitação em Software

A proponente deverá ministrar os treinamentos e repasse de conhecimento acerca das soluções adquiridas com no mínimo as seguintes características:

01 turma, 03 participantes, com carga horária total de 16 horas;

08 horas aula por dia, de segunda a sexta-feira, exceto feriados;

O local a ser utilizado será de responsabilidade do Contratante e deverá acomodar com o conforto necessário para um bom rendimento todos os participantes;

A data e os horários de início e término da ação deverão ser acordadas entre Contratante e Contratada.

RELAÇÃO ORIENTATIVA DE MATERIAIS OU SERVIÇOS A SEREM EXECUTADOS

ITEM	DESCRIÇÃO	UND	QTD.
	PRODUTOS		
01	Nobreak – Implantação ou reestruturação de datacenter	Und	3,00
02	Switch Core – Implantação ou reestruturação de datacenter	Und	1,00
03	Switch Tor – Implantação ou reestruturação de datacenter	Und	3,00
04	Switch 24P – Implantação ou Reestruturação de datacenter	Und	25,00
05	Switch 48P – Implantação ou Reestruturação de datacenter	Und	10,00
06	Ativos de rede WLAN – Controladora	Und	1,00
07	Ativos de rede WLAN – Access Point	Und	40,00
08	Servidores – Implantação ou reestruturação de datacenter	Und	4,00
09	Fibras Óticas – Integração de órgãos da Administração Pública ou Rede de conectividade	M	60000,00
10	Obras civis, montagem e instalações – Criação do espaço físico do Data Center	M ²	31,00
11	Obras civis, montagem e instalações – Rede de dados – Integração de órgãos da Administração Pública	M	550,00
12	Capacitação em Software	Und	1,00

DOCUMENTOS QUE COMPOEM O PROJETO

Juntamente com esse memorial, seguem duas plantas em formato A0 contendo informações sobre as conexões das fibras, lay out do datacenter e detalhes gerais.

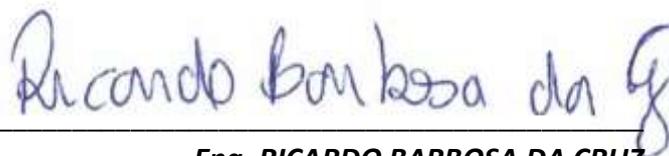
Em arquivo digital, será entregue um arquivo do Google Earth com o referenciamento das localidades atendidas e também os pontos de instalação das caixas e encaminhamento de fibras óticas.

CONSIDERAÇÕES FINAIS

Este memorial tem a função de orientar as instalações e modificações na obra serão aceitas, desde que sejam respeitadas as premissas básicas, contidas neste documento, desde que sejam respeitados os dimensionamentos apresentados e aprovação previa da Fiscalização e anuência do projetista.

Estamos a disposição para eventuais esclarecimentos que se fizerem necessário

Catalão, 06 de julho de 2018

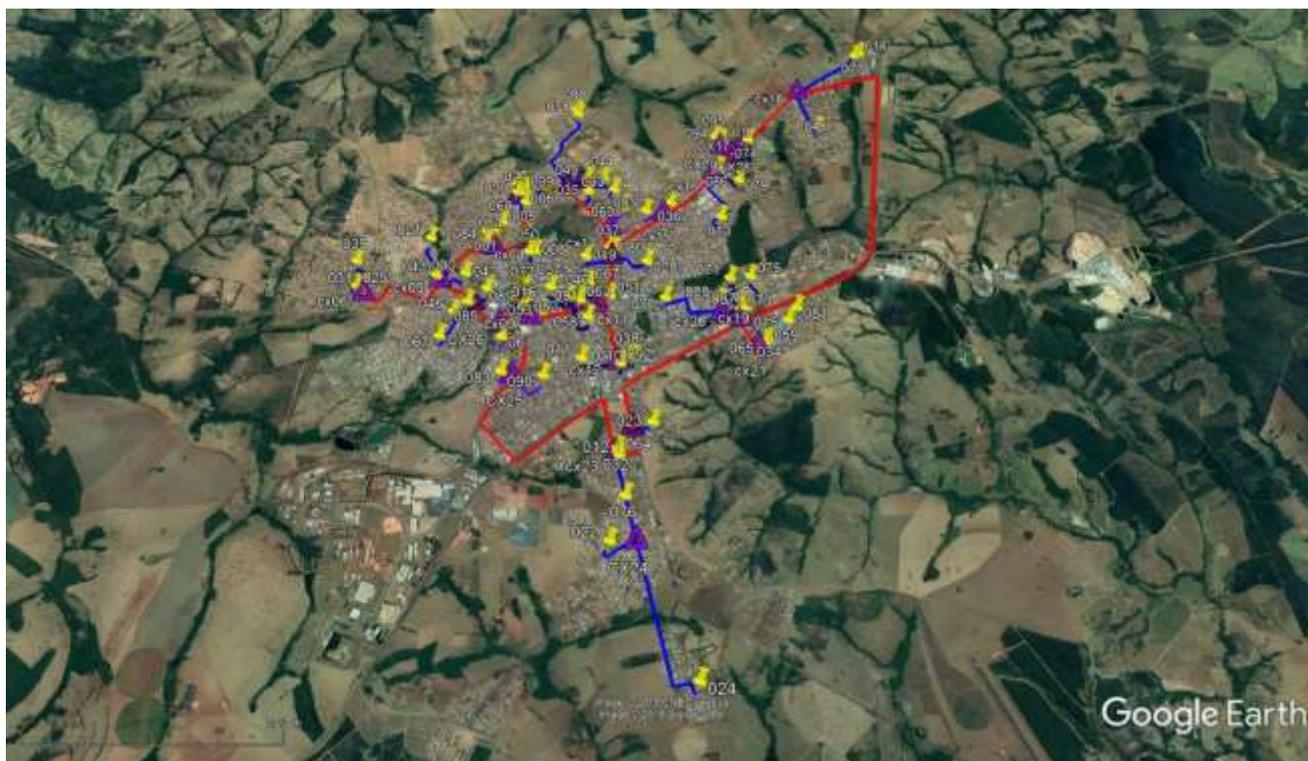


Eng. RICARDO BARBOSA DA CRUZ
CREA-GO 9538/D

ANEXO 01 – TRAÇADO DE FIBRAS 12 VIAS



ANEXO 02 – LOCALIDADES ATENDIDAS



ANEXO 3 – POSIÇÃO DAS CAIXAS DE DERIVAÇÃO

