



DIREÇÃO DE ACESSIBILIDADE, TELEMÁTICA E ITS

DIREÇÃO DE COMPRAS E LOGÍSTICA

COMPRAS - EMPREITADAS E SERVIÇOS

PROGRAMA PRELIMINAR - VOLUME 04

**MEMÓRIA DESCRITIVA – REDE DE SUPORTE À
EXPLORAÇÃO – ANEXO 1**

PROCESSO N.º:

DESIGNAÇÃO:

EMPREITADA DA “”

TIPO DE PROCEDIMENTO:

**CONCURSO PÚBLICO COM PUBLICAÇÃO
INTERNACIONAL**

Revisão	Data	Descrição das Alterações	
Versão 1	14/10/2024	Versão inicial	
		Elaborado por: DAT	Verificado por: Jaime Novo
Versão 2	28/06/2025		
		Elaborado por: DAT	Verificado por: Jaime Novo



ÍNDICE

1	ANEXO - ESPECIFICAÇÕES TÉCNICAS DOS PRINCIPAIS EQUIPAMENTOS E MATERIAIS	6
	INTRODUÇÃO	6
1.1	EQUIPAMENTOS MPLS	6
1.1.1	Introdução	6
1.1.2	Especificações do equipamento 7705 SAR-8 ou equivalente	7
1.1.3	Especificações do equipamento Nokia 7705 SAR-Ax ou equivalente	30
1.1.4	Componentes para o equipamento 7705 SAR 8	40
1.1.4.1	Módulo de 8 portas GigabitEthernet (3HE06151UA)	40
1.1.4.2	Carta com portas a 10GigabitEthernet	40
1.1.5	Componentes para o equipamento 7705 SAR 8 e 7705 SAR Ax	41
1.1.5.1	SFP – GIGE SX – LC ROHS 6/6 DDM -40/85°C	41
1.1.5.2	SFP – GIGE LX – LC ROHS 6/6 DDM -40/85°C	41
1.1.5.3	SFP – GIGE EX – LC ROHS 6/6 DDM -40/85°C	41
1.1.5.4	SFP – GIGE ZX – LC ROHS 6/6 DDM -40/85°C	41
1.1.5.5	SFP – GIGE EZX – LC ROHS 6/6 DDM -40/85°C	41
1.1.5.6	SFP+ – 10G SR – LC ROHS 6/6 0/70C (3HE04824AA)	41
1.1.5.7	SFP+ – 10G LR – LC ROHS 6/6 0/70C (3HE04823AA)	41
1.1.5.8	SFP+ – 10G ER – LC ROHS 6/6 0/70C (3HE05036AA)	41
1.1.5.8	SFP – 10G ZR – LC ROHS 6/6 DDM 0/70C (3HE05894AA)	42
1.1.5.9	SFP – Cabo em Y para sincronismo para Nokia 7705 SAR 8	42
1.1.5.10	Conversor AC/DC 230V/48V de 220W	42
1.2	EQUIPAMENTO SWITCHING E ROUTING	42
1.2.1	Introdução	42
1.2.2	OS6570M-U28 ou equivalente	42
1.2.3	Fonte de alimentação redundante AC OS6570-BP	63
1.2.4	Fonte de alimentação redundante AC OS6570-BP-D	63
1.2.5	OS6860N-U28 ou equivalente	63
1.2.6	OS6860E-24	81
1.2.7	Acessórios para os equipamentos OS6860N-U28 e OS6860E-24	81
1.2.8	OS6865-U28X	82
1.2.9	Acessórios para os equipamentos OS6865-U28X	89
1.2.9.1	Fonte de alimentação AC – OS6865-BP	89
1.2.9.2	Fonte de alimentação DC – OS6865-BP-D	89
1.2.9.3	SFPs Industriais	89
1.2.10	OS6560-24X4	89
1.2.10.1	Acessórios para os equipamentos OS6560-24X4	95
1.2.11	OS6560-48X4	95
1.2.12	OS6465-P28	101
1.2.12.1	Acessórios para OS6465-P28 ou equivalente	107
1.2.13	OS6465-P12	108



1.2.13.1	Acessórios para OS6465-P12 ou equivalente	108
1.2.14	OS6870-V12.....	108
1.2.15	SFP para os equipamentos Omniswitches	142
1.2.16	Equipamento Switch Industrial (Layer 2) BRS30 Hirschmann ou equivalente	146
1.2.12.1	Equipamento de rede layer 2 industrial	147
1.2.16.1	Acessórios para os equipamentos switchs industriais Hirschmann ou equivalentes	151
1.3	Conversor AC/DC 230V/48 de 50W (para o equipamento de segurança).....	153



Anexo 1 – Especificações dos equipamentos requeridos



1 ANEXO - ESPECIFICAÇÕES TÉCNICAS DOS PRINCIPAIS EQUIPAMENTOS E MATERIAIS

INTRODUÇÃO

O presente ponto refere-se às especificações mínimas dos equipamentos e acessórios que devem obedecer os equipamentos a serem utilizados no âmbito desta contratação. Todos os equipamentos a fornecer terão de ser geridos pelas plataformas de gestão de rede existentes na IP:

- Omnivista2500 para equipamentos ALE,
- NFM-P para equipamentos MPLS da Nokia e
- Hivision para equipamentos industriais Hirschmann.

Os equipamentos a serem fornecidos terão de integrar com as redes existentes bem como poderem ser inseridos nos anéis e redes existentes e em produção na IP sem perda de funcionalidades ao nível de tempos de latência, trânsito, ao nível dos protocolos de redundância utilizados na IP.

Caso seja proposto equipamento de outro fabricante diferente do indicado (Nokia, Alcatel Lucent e Hirschmann), o adjudicatário terá que apresentar uma declaração de um destes fabricantes, tendo presente a sua funcionalidade, que indique que o equipamento proposto é totalmente integrável e compatível (funcionalmente e protocolamente) com a rede desse fabricante em operação na IP, bem como que os equipamentos propostos são totalmente geridos e configurados através da sua plataforma de gestão também em operação na IP.

1.1 EQUIPAMENTOS MPLS

1.1.1 Introdução

Os equipamentos e placas a prever neste projeto, têm de ser totalmente integráveis com a rede IP/MPLS existente ao nível local e nacional. Os equipamentos e as placas a prever neste projeto são para ser inseridos em anéis e segmentos de rede com equipamentos Nokia/Alcatel Lucent pelo que têm de garantir todas as funcionalidades, tempos de convergência, latência entre outros requisitos não podendo degradar ou limitar as configurações em operação. Os equipamentos têm de ser totalmente integráveis e geridos na plataforma de gestão que a IP possui (NFM-P da Nokia) permitindo que a partir do centro de gestão se possa efetuar a criação e configuração de serviços MPLS envolvendo os novos equipamentos e os nós existentes.

O equipamento MPLS a fornecer, instalar, configurar e colocar ao serviço terá de ser:

- **Nokia 7705 SAR-8 ou equivalente**, com a seguinte constituição 7705 SAR-8 V2 ou equivalente com Chassis com PSU, 1 Módulo de FANS, 1 carta CSM+1 carta 8PortGE/FE v2 + licenças SAR+ licenças NFM-P + licenças IEEE1588.

- **Nokia 7705 SAR Ax ou equivalente** com:

- 4 x Combo SFP/RJ-45 10/100/1000 Mbit/s;
- 8 x SFP 10/100/1000 Mbit/s;
- licenças SAR+ licenças NFM-P + licenças IEEE1588.

Nota: Podem ser utilizados outros modelos MPLS da Nokia tais como 7705 SAR-18 e 7250 IXR para pontos de agregação.



1.1.2 Especificações do equipamento 7705 SAR-8 ou equivalente

1.1.2.1 Características gerais

- Taxa de transferência do sistema: 60 Gb/s (Half-Duplex);
- Capacidade de placas/cartas por chassis:
 - 2 slots de 10 Gb/s full duplex;
 - 4 Slots de 2.5 Gb/s full duplex.
 - Portas de sincronismo: Sync in, Sync out, ToD in, ToD out.
- O chassis deve permitir a montagem em rack standard de 19”.
- Redundância do equipamento: Carta de controlo (CSM), Switch fabric, power feeds, e ventoinhas de refrigeração.

Têm de incluir todo o licenciamento associado a funcionalidades e ao centro de gestão existente na IP.

1.1.2.2 Carta de Controlo (CSMv2) do 7705 SAR 8

- Carta de controlo terá de ser hot swappable;
- Com compact flash de 2Gbytes que pode ser utilizado para copiar e armazenar o software de boot de sistema, sistema operativo, ficheiros de configuração e logs;
- Carta CSMv2 terá de suportar largura de banda de 10 Gb/s, 2.5 Gb/s, e 1 Gb/s nas primeiras duas slots para cartas adaptadoras e 2.5 Gb/s e 1 Gb/s para as restantes slots;
- A carta de controlo CSMv2 tem de possuir fichas coaxiais 1.0/2.3 coaxial para entrada e saída de sincronismo. Terá de suportar sincronismo de 2 MHz e 10 MHz;
- No caso de se pretender redundância terá de ser possível instalar duas cartas de controlo CSMv2s. Uma das cartas estará em modo de espera (standby) e a outra em modo ativo. No caso da falha da carta de controlo ativa a carta de controlo que está em espera passa para modo ativo;
- Terá de possuir sensores de temperatura para monitorização contínua da sua temperatura.

1.1.2.3 Módulo de Ventoinhas

O módulo de ventoinhas para além fazer a refrigeração do equipamento tem de possuir leds para indicar alarmes, conector I/O para alarme externo e um botão para teste de leds e para anular o alarme audível.

1.1.2.4 Placas adaptadoras suportadas pelo 7705 SAR 8

O 7705 SAR-8 tem de suportar as seguintes placas adaptadoras:

- Placa adaptadora de 2 portas 10GigE ring (Ethernet);
- Placa adaptadora de 2 portas OC3/STM1 Channelized suportando ATM, ATM IMA, TDM, PPP/MLPPP e IP;
- Placa adaptadora de 4 portas OC3/STM1 / 1 porta OC12/STM4 suportando TDM e PPP/MLPPP em modo channelized e POS em modo clear channel;
- Placa adaptadora de 4 portas OC3/STM1 Clear Channel suportando ATM, POS e IP;
- Placa adaptadora de 4 portas DS3/E3 por clear channel serviços TDM, FR e PPP;
- Placa adaptadora de 6 portas E&M (6xRJ45);
- Placa adaptadora de 6 portas 10Gbps e GE;
- Placa adaptadora de 6 portas FXS voz suportando sinalização loop start/PLAR;



- Placa adaptadora de 8 portas FXO voz suportando sinalização loop start;
- Placa adaptadora de 8 portas Gigabit e Ethernet;
- Placa adaptadora de 8 portas Gigabit Ethernet;
- Placa adaptadora de 8 portas Voz e Teleproteção com 2 portas FXS, 2 portas FXO para voz analógica, 2 portas ITU-T G.703 codirecional 2 portas IEEE C37.94 óticas de teleproteção;
- Placa adaptadora de 12 portas Série de dados podendo ser configuradas para RS232, RS422/RS530, V35 ou X21;
- Placa adaptadora de 16 portas T1/E1 ASAP (ATM, ATM IMA, TDM, FR, HDLC, MCPPP/MLPPP e IP);
- Placa adaptadora de 32 portas T1/E1 ASAP (ATM, ATM IMA, TDM, FR, HDLC, MCPPP/MLPPP e IP);
- Placa de alarmes auxiliar – 24 portas digitais de entrada, 2 portas analógicas de entrada e 8 portas de saída;
- Placa recetora GNSS com 1 porta RF sincronismo de clock GPS
- Placa adaptadora CWDM passivo com variantes de 1,2,4 e 8 add/drop CWDM OADM;
- Placa de serviços Integrados com suporte de aplicações SCADA Multi-Drop Data Bridging (MDDB) e PCM multidrop bridging;
- Placa adaptadora micro-ondas de pacotes rádio (MPR);
- Placa Injetora de energia PoE para MPR.

De notar que todas as placas terão que possuir sensores de temperatura que monitorização a sua temperatura e disponibilizarão à placa de controlo os valores de temperatura de modo contínuo. No caso em que uma qualquer placa exceder os valores de temperatura específicos tem de ser gerado um alarme.

1.1.2.5 Dimensões e tipo de montagem

O equipamento a fornecer tem de permitir a montagem horizontal em rack 19” e não deverá ultrapassar a altura de 2Us.

1.1.2.6 Alimentação

O equipamento 7705 SAR 8 terá de suportar duas alimentações de -48V DC/-60V DC devendo suportar um intervalo de tensão entre -40 a -75 VDC.

1.1.2.7 Condições ambientais

O equipamento a fornecer terá de suportar em operação no mínimo as seguintes condições ambientais:

- - 40°C a + 65°C em modo permanente;
- Humidade: 5% a 95% sem condensação.

Em termos de Choque e vibração o equipamento terá de suportar no mínimo:

- Choque – 3g meia senoide 11ms;
- Vibração: 0,1g de 5 a 100Hz.

1.1.2.8 Serviços a suportar

O equipamento terá de suportar os seguintes serviços:

- VLL (Virtual Lease Line), serviços pseudowire PW ou túneis, que emula uma entidade layer 1 / 2 como uma linha alugada ou um cabo. Estes serviços emulados providenciam conectividade entre um ponto de acesso de serviço (SAP) num equipamento e outro SAP no mesmo router ou num router remoto; O serviço VLL terá



de oferecer entidades lógicas SAP como as VLAN ou a ligação virtual-visibilidade Layer 2 ou processamento (terminação IMA – multiplexagem inversa over ATM)

- Serviços VLL
 - ATM VLL (Apipe)— emulação serviço ATM pseudowire extremo-a-extremo sobre túneis MPLS, GRE e IP.
 - Emulação de circuito VLL (Cpipe)—serviço de emulação de circuito PWE3 sobre túneis MPLS e GRE.
 - Ethernet VLL (Epipe)— serviço de emulação Ethernet PWE3 Ethernet sobre túneis MPLS ou GRE para tramas Ethernet.
 - FR VLL (Fpipe)— serviço de emulação Frame Relay PWE3 sobre túneis MPLS ou GRE para tramas Frame Relay.
 - HDLC VLL (Hpipe)—Serviço de emulação HDLC PWE3 sobre túneis MPLS ou GRE para tramas HDLC.
 - IP interworking VLL (Ipipe)—serviço de emulação IP PWE3 entre dois hosts ligados por qualquer combinação de circuitos de acesso ponto-a-ponto. IP interworking VLLs pode funcionar sobre túneis MPLS e GRE. Alguns exemplos: Ethernet SAP para Ethernet SAP, Ethernet SAP para MLPPP SAP, Ethernet SAP para LAG SAP, FR SAP para Ethernet SAP, ou cHDLC SAP para Ethernet SAP.
- VPLS (serviços VPN multiponto layer 2);
 - VPLS providencia serviços de VPN nível 2 multiponto para os clientes finais. VPLS inclui VPLS hierárquico (H-VPLS). O equipamento terá de ter capacidade para participar em VPLS hierárquico (H-VPLS. Adicionalmente o equipamento terá de suportar gestão de VPLS (mVPLS) através de Rapid Spanning Tree Protocol (RSTP).
- VPRN (serviços VPN MPLS layer 3);
 - VPRN disponibiliza serviços de VPN Nível 3 para os clientes finais. Os serviços VPRN providenciam peering MP-BGP com os outros PEs, filtragem e políticas de QoS configuráveis, políticas de importação e exportação de VRF, e marcação SGT-QoS.
- Serviços IP/routing layer 3 (IPv4 e IPv6);
- Serviços de emulação de circuitos (CES);
- Serviço de emulação de circuitos através rede de comutação de pacotes (CESoPSN);
- Transporte de dados de porta série RS232 através de Raw Socket IP;
- MEF 8.

Tipos de pseudowires a suportar

Os tipos de pseudowires a suportar são os seguintes:

- IP Layer 2 transport;
- Ethernet tagged mode;
- Ethernet raw;
- HDLC;
- ATM N-to-one VCC cell mode;
- ATM N-to-one VPC cell mode;
- ATM transparent cell transport mode;
- SAToP E1;
- CESoPSN basic mode;
- CESoPSN TDM with CAS;
- FR DLCI.



Os tipos de serviços nas portas Ethernet e encapsulamentos SAP a suportar são os seguintes:

- null – suporte de um serviço simples numa porta;
- dot1q – suporte de múltiplos serviços para um cliente ou serviços para múltiplos clientes;
- qinq – suporte de múltiplos serviços de um cliente ou serviço para múltiplos clientes.

Os tipos de serviços nas portas SDH e encapsulamentos SAP a suportar são os seguintes:

- atm— suporte de múltiplas instâncias de serviço para um cliente bem como bridged llc-snap encapsulated ATM SAP termination para VPLS.

Os tipos de serviços nas portas TDM e Serie (TDM) e encapsulamentos SAP a suportar são os seguintes:

- atm— suporte de múltiplos serviços para um cliente (portas TDM);
- cem— suporte de múltiplos serviços para um cliente. Serviço OEM estruturado (circuit emulation service over packet switched network (CESoPSN ($n \times DS0$)) e serviço OEM não estruturado (structure-agnostic TDM over packet (SAToP)) são suportados. (portas TDM e SDI);
- ipcp—suporte de serviço simples IP por grupo de canais TDM. Utilizado para interligação de routers utilizando o protocolo ponto-a-ponto (PPP). (Portas TDM, e portas SDI V.35 e X.21 a alta velocidade);
- frame-relay (portas TDM, e portas SDI V.35 e X.21 a alta velocidade);
- cisco-hdlc (portas E1 e portas SDI V.35 e X21TDM a alta velocidade);
- hdlc (portas E1 e portas SDI V.35 e X.21 a alta velocidade).

1.1.2.9 Protocolos de rede

O equipamento terá de suportar os seguintes protocolos:

- Funções de MPLS Label Edge Router (LER) e Label Switch Router (LSR)
- Routing IP
 - Intermediate System-to-Intermediate System (IS-IS) (IPv4, IPv6)
 - Open Shortest Path First (OSPFv2 and OSPFv3);
 - Constraint-based Shortest Path First (CSPF);
 - Routing Information Protocol (RIP);
 - Border Gateway Protocol (BGP) com extensões multiprotocolo;
 - RFC 3107-labeled routes;
- IPv6
 - IPv6 VPN Provider Edge (6VPE) para MPLS e IPSec VPRN;
 - Dynamic Host Configuration Protocol (DHCP) v6 servidor/relay;
 - Túneis IPv6 sobre IPSecv4;
- Multicast nível 2 e 3
 - L2 multicasting via Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD) snooping em VPLS com fluxo de tráfego de nível 3 para nível 2;
 - Conversão IGMP/MLD snooping para Protocol Independent Multicast (PIM) para VPLS roteadas (RVPLS);
 - Protocol Independent Multicast – Source Specific Multicast (PIM-SSM) com IGMPv1/2/3 e MLD v1/2 Label Distribution Protocol (LDP);
- PIM (SSM) stitching via L2 PIM snooping;
- Next generation multicast VPNs com família de endereços MP-BGP MVPN-IPv4 e árvore dinâmica MLDP PMSI;
- Targeted LDP (T-LDP);



- Resource Reservation Protocol — Traffic Engineering (RSVP-TE)
 - RSVP-TE LSP shortcuts para a resolução de rotas IGP;
- Generic Routing Encapsulation (GRE).

1.1.2.10 Temporização e sincronismo

O equipamento terá de suportar 3 referências de sincronismo, um externo e dois internos devendo ser possível configurar segundo uma lista de prioridades alta a baixa. Terá de permitir configurar a reversão automática da fonte de sincronismo em caso de recuperação da fonte de sincronismo de alta prioridade. As portas de sincronismo externo podem ser configuradas como:

- 2.048MHZ (G.703 section 13 signal);
- Onda sinusoidal 10MHz.

O equipamento terá de suportar a recuperação adaptativa de relógio (Adaptive Clock Recovery – ACR) para MEF8 (emulação de circuitos PDH) quer no modo estruturado ou não estruturado.

O equipamento terá de suportar a recuperação diferencial de relógio (Differential Clock Recovery – DCR) para MEF8 (emulação de circuitos PDH) quer no modo estruturado ou não estruturado.

O equipamento terá de suportar alinhamento de tempo e frequência combinado Sync-E e IEEE1588.

O equipamento terá de suportar a norma IEEE 1588v2 nos seguintes tipos:

- Master Clock (MC);
- Slave Clock (SC);
- Boundary Clock (BC);
- End-to-End Transparent clock.

A sincronização baseada em pacotes através de UDP/IP e Ethernet.

O equipamento terá de suportar 6 referências de relógio.

O equipamento terá de permitir os seguintes perfis: Default IEEE 1588v2, ITU-T G.8265.1 e G.8275.1.

O equipamento terá de ter possibilidade para suportar uma carta recetora GNSS. O equipamento terá de suportar NTP como definido pelo RFC 1305, NTP versão 3, RFC 5905 Network Time Protocol (NTP) versão 4.

O equipamento deverá incluir um cliente SNTP como definido RFC2030 SNTP Versão 4.

1.1.2.11 Qualidade de serviço e gestão de tráfego

O equipamento terá de possuir um conjunto alargado de mecanismos de QoS para ambos os sentidos de tráfego de entrada e saída para suportar diferentes clientes e diferentes serviços ao nível de interface físicas ou cartas de forma concorrencial.

O equipamento terá de ter capacidade de classificação, controlo, modelagem e marcação de tráfego.

O equipamento terá de suportar Hierárquico QoS. Deverá também suportar tráfego de modelagem por classe de forwarding, SAP ou VLAN, por site de cliente multiserviço (MSS e por porta).

1.1.2.12 Operação Administração e Manutenção

Diagnósticos ICMP e ICMPv6

ICMP e ICMPv6 envia e recebe mensagens de controlo e erro utilizados para a gestão do stack TCP/IP.

Protocolo de Medição ativa nos dois sentidos (TWAMP)



O equipamento terá de suportar o RFC5357 referente ao Two-way active measurement protocol (TWAMP) que providência o método normalizado de medição do desempenho de round-trip (incluindo perdas de pacotes, atraso e jitter) de pacotes IP que são transmitidos entre dois dispositivos.

O equipamento terá de suportar funções de servidor TWAMP e de Reflector de sessão.

TWAMP tem de ser suportado em todas as interfaces IPv4 e em qualquer interface de base do router (incluindo endereços IP de Sistema e loopback).

Two-Way Active Measurement Protocol Light (TWAMP Light)

O equipamento terá de suportar o TWAMP light cumprindo o modelo opcional incluído no RFC5357.

Diagnósticos LSP

O equipamento terá de suportar diagnósticos LSP (LSP ping e LSP traceroute) conforme o RFC4379 – Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures.

Downstream Detailed Mapping (DDMAP) TLV

O equipamento terá de suportar DDMAP TLV com definido no RFC6424.

Diagnósticos SDP

O equipamento terá de suportar diagnósticos SDP (SDP ping e SDP MTU Path Discovery).

Diagnósticos VLL

O equipamento terá de suportar mecanismos de diagnóstico VLL permitindo testar a conectividade in-band de um VLL (VCCV ping), fazer o trace do caminho completo de um pseudowire (VCCV Trace).

Diagnósticos ITU-T Y.1564

O equipamento terá de suportar a funcionalidade ITU-T Y.1564 de teste de largura de banda e throughput para circuitos virtuais Ethernet.

Diagnósticos VPLS MAC

O equipamento terá de suportar um conjunto de ferramentas OAM para VPLS:

- MAC Ping;
- MAC Trace;
- CPE Ping;
- MAC Populate;
- MAC Purge.

Capacidades de OAM Ethernet

O equipamento terá de suportar as seguintes capacidades OAM Ethernet:

- Ethernet Connectivity Fault Management (ETH-CFM) — para a camada de rede OAM de acordo com o IEEE 802.1ag (dot1ag) e ITU-T Y.1731, incluindo loopbacks (LB), linktrace (LT), continuity checks (CC), e remote defect indicators (RDI);



- Performance Monitoring (PM) de acordo com o ITU-T Y.1731, incluindo medição de atrasos (DM) medição de variações de atrasos (DV) e medições de perdas (LM);
- Ethernet First Mile (EFM) OAM — para a camada de transporte OAM de acordo com IEEE 802.3ah (dot3ah).

Ethernet Loopbacks

O equipamento deverá disponibilizar a funcionalidade de loopback em portas Ethernet e suportar os seguintes loopbacks:

- loopback de linha de rede;
- loopback de linha de acesso;
- loopback interno;
- loopback de linha de acesso persistente;
- loopback de acesso interno persistente;
- Troca de endereço MAC (MAC swapping);
- Loopback CFM (Connectivity fault management) nas portas de rede e de acesso.

Sinalização do estado LDP

O equipamento terá de propagar falhas através de PW com um dos seguintes métodos:

- LDP Status via remoção de label (label withdrawal);
- LDP Status via TLV conforme RFC4447.

Ferramentas de debugging para Multicast IP

O equipamento terá de suportar ferramentas de debugging para multicast:

- Mtrace – Utilizado para conhecer o caminho da origem ao recetor, fornecendo informação que permita ao administrador de rede determinar o fluxo do stream multicast e onde o fluxo multicast para;
- Mstat – mostra o caminho multicast com a indicação das perdas, duplicados, TTL e atrasos em cada nó;
- Mrinfo – mostra a informação de configuração do router multicast alvo. O tipo de informação mostrada inclui as capacidades de multicast do router, versão, métricas, limites TTL, protocolos e estado.

Mirroring

O equipamento terá de suportar a funcionalidade de Mirroring de pacotes para qualquer interface Ethernet destino na rede.

O equipamento terá de suportar mirroring local ou remoto.

Bidirectional Forwarding Detection (BFD)

O equipamento terá de suportar BFD.

1.1.2.13 Resiliência

O equipamento terá de possuir funcionalidades de alta disponibilidade:

- Redundância;
- Nonstop Routing;
- Upgrade em operação;
- Comutação de carta de controlo;
- Sincronismo entre placas de controlo (configuração e base de dados de estados).



A redundância deverá ser conseguida através de:

- Redundância de software;
- Redundância de configuração – terá de suportar hot-standby de imagem do router, configuração e de estados permitindo a comutação imediata;
- Redundância de componentes – utilização de cartas de controlo redundantes, alimentações redundantes, ventoinhas redundantes e as cartas terão de ser hot swap;
- Redundância Multi-Chassis LAG permitindo que o dispositivo de cliente esteja ligado a dois nós redundantes mas que atuam como um do ponto de vista do dispositivo cliente.

O equipamento terá de suportar IEEE 802.3ad Link Aggregation Group (LAG) e multi-chassis (MC) LAG.

Redundância pseudowire

O equipamento terá de suportar redundância pseudowire.

LSP primário e secundário

O equipamento terá de suportar LSP primário e secundário.

Fast Reroute (FRR)

O equipamento terá de suportar Fast reroute (FRR) ao nível do:

- BGP;
- IP (OSPF & ISIS);
- LDP with loop-free alternate (LFA) policies (RFC 5286).

RSVP-TE

O equipamento terá de suportar RSVP-TE.

APS e MC APS

O equipamento terá de suportar Automatic Protection Switching (APS) e MC APS para SONET/SDH.

ECMP

O equipamento terá de suportar IPv4 e LDP LSR equal-cost multi-path (ECMP).

VRRP

O equipamento terá de suportar Virtual Router Redundancy Protocol (VRRP).

1.1.2.14 Segurança

Simple Network Management Protocol (SNMP) v3.

O equipamento terá de suportar SNMPv3.

Secure Shell (SSH)

O equipamento terá de suportar SSH.



Encriptação IP Security (IPSec) sobre MPLS

O equipamento terá de suportar IPSec.
O equipamento deverá suportar RFC4868.

Network address translation (NAT)

O equipamento terá de suportar NAT e NAT-Transversal.

Network Group Encryption (NGE) para serviços IP/MPLS

O equipamento terá de suportar a funcionalidade network group encryption (NGE) que permite a configuração da cifragem ponta-a-ponta de serviço numa rede MPLS.

O principais tipo de cifragem que terá de ser suportado:

- Cifragem SDP para uma variedade de serviços (VLL,VPLS,VPRN);
- Cifragem para serviços VPRN baseados em MP-BGP

Public Key Infrastructure (PKI) suportando certificados X.509v3, Certificate Management Protocol version 2 (CMPv2), Certificate Revocation List (CRL), Offensive Certified Security Professional (OCSP), Chaves RSA/DAS

O equipamento deverá suportar Certificados X.509v3.

A implementação PKI do equipamento deverá suportar as seguintes funcionalidades:

- Inscrição de certificado
 - Chave RSA/DAS gerada localmente;
 - Inscrição offline via PKCS#10;
 - Inscrição online via Certificate Management Protocol version 2 (CMPv2).
- Suporte de cadeia de CA;
- Verificação da revogação de certificado
 - Certificate Revocation List (CRL);
 - Offensive Certified Security Professional (OCSP).

1.1.2.15 Normas

Normas que terão de ser suportadas pelo equipamento:

- ANSI/TIA/EIA-232-C—Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange
- IEEE 802.1ad—IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks
- IEEE 802.1ag—Service Layer OAM
- IEEE 802.1p/q—VLAN Tagging
- IEEE 802.3—10BaseT
- IEEE 802.3ab—1000BaseT
- IEEE 802.3ah—Ethernet OAM
- IEEE 802.3u—100BaseTX
- IEEE 802.3x —Flow Control
- IEEE 802.3z—1000BaseSX/LX
- IEEE 802.3-2008—Revised base standard
- IEEE 802.1AX-2008—Link Aggregation Task Force (transferred from IEEE 802.3ad)
- IEEE C37.94-2002—N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment
- ITU-T G.704—Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels
- ITU-T G.707—Network node interface for the Synchronous Digital Hierarchy (SDH)



- ITU-T G.984.1—Gigabit-capable passive optical networks (GPON): general characteristics
- ITU-T Y.1564—Ethernet service activation test methodology
- ITU-T Y.1731—OAM functions and mechanisms for Ethernet-based networks

ATM

- AF-PHY-0086.001—Inverse Multiplexing for ATM (IMA)
- af-tm-0121.000—Traffic Management Specification Version 4.1, March 1999
- GR-1113-CORE—Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994
- GR-1248-CORE—Generic Requirements for Operations of ATM Network Elements (Nes). Issue 3 June 1996
- ITU-T Recommendation I.432.1—B-ISDN user-network interface – Physical layer specification: General characteristics
- ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions version 11/95
- RFC 2514—Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999
- RFC 2515—Definition of Managed Objects for ATM Management, February 1999
- RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5

BFD

- draft-ietf-bfd-mib-00.txt—Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-base-o5.txt—Bidirectional Forwarding Detection
- draft-ietf-bfd-v4v6-1hop-06.txt—BFD IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-06.txt—BFD for Multi-hop Paths

BGP

- RFC 1397—BGP Default Route Advertisement
- RFC 1997—BGP Communities Attribute
- RFC 2385—Protection of BGP Sessions via MDS
- RFC 2439—BGP Route Flap Dampening
- RFC 2547bis—BGP/MPLS VPNs
- RFC 2918—Route Refresh Capability for BGP-4
- RFC 3107—Carrying Label Information in BGP-4
- RFC 3392—Capabilities Advertisement with BGP-4
- RFC 4271—BGP-4 (previously RFC 1771)
- RFC 4360—BGP Extended Communities Attribute
- RFC 4364—BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)
- RFC 4456—BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)
- RFC 4486—Subcodes for BGP Cease Notification Message
- RFC 4684—Constrained Route Distribution for Border Gateway Protocol/
- MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
- RFC 4724—Graceful Restart Mechanism for BGP – GR Helper
- RFC 4760—Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4893—BGP Support for Four-octet AS Number Space
- RFC 6513—Multicast in MPLS/BGP IP VPNs
- RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs
- draft-ietf-idr-add-paths-04.txt—Advertisement of Multiple Paths in BGP
- draft-ietf-idr-add-paths-guidelines-00.txt—Best Practices for Advertisement of Multiple Paths in BGP



DHCP/DHCPv6

- RFC 1534—Interoperation between DHCP and BOOTP
- RFC 2131—Dynamic Host Configuration Protocol (REV)
- RFC 2132—DHCP Options and BOOTP Vendor Extensions
- RFC 3046—DHCP Relay Agent Information Option (Option 82)
- RFC 3315—Dynamic Host Configuration Protocol for IPv6
- RFC 3736—Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

Differentiated Services

- RFC 2474—Definition of the DS Field in the IPv4 and IPv6 Headers
- RFC 2597—Assured Forwarding PHB Group
- RFC 2598—An Expedited Forwarding PHB
- RFC 3140—Per-Hop Behavior Identification Codes

Digital Data Network Management

- V.35
- RS-232 (also known as EIA/TIA-232)
- X.21

ECMP

- RFC 2992—Analysis of an Equal-Cost Multi-Path Algorithm

Frame Relay

- ANSI T1.617 Annex D—Signalling Specification For Frame Relay Bearer Service
- ITU-T Q.922 Annex A—Digital Subscriber Signalling System No. 1 (DSS1) data link layer – ISDN data link layer specification for frame mode bearer services
- FRF.1.2—PVC User-to-Network Interface (UNI) Implementation Agreement
- FRF.12—Frame Relay Fragmentation Implementation Agreement
- RFC 2427—Multiprotocol Interconnect over Frame Relay

GRE

- RFC 2784—Generic Routing Encapsulation (GRE)

IPSec

- IETF draft-nourse-scep-21.txt—Cisco Systems' Simple Certificate Enrollment Protocol
- ITU-T X.690 (2002)—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- PKCS #12 Personal Information Exchange Syntax Standard
- RFC 2315—PKCS #7: Cryptographic Message Syntax
- RFC 2401—Security Architecture for the Internet Protocol
- RFC 2409—The Internet Key Exchange (IKE)
- RFC 2986—PKCS #10: Certification Request Syntax Specification
- RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3947—Negotiation of NAT-Traversal in the IKE
- RFC 3948—UDP Encapsulation of Ipsec ESP Packets
- RFC 4303—IP Encapsulating Security Payload (ESP)
- RFC 4210—Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 4211—Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
- RFC 4945—The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
- RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5996—Internet Key Exchange Protocol Version 2 (IKEv2)

IPv6

- RFC 2460—Internet Protocol, Version 6 (IPv6) Specification



- RFC 2462—IPv6 Stateless Address Autoconfiguration
- RFC 2464—Transmission of IPv6 Packets over Ethernet Networks
- RFC 3587—IPv6 Global Unicast Address Format
- RFC 3595—Textual Conventions for IPv6 Flow Label
- RFC 4007—IPv6 Scoped Address Architecture
- RFC 4193—Unique Local IPv6 Unicast Addresses
- RFC 4291—IPv6 Addressing Architecture
- RFC 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 4649—DHCPv6 Relay Agent Remote-ID Option
- RFC 4861—Neighbor Discovery for IP version 6 (IPv6)
- RFC 5095—Deprecation of Type 0 Routing Headers in IPv6
- RFC 5952—A Recommendation for IPv6 Address Text Representation

IS-IS

- RFC 1142—OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195—Use of OSI IS-IS for routing in TCP/IP & dual environments
- RFC 2763—Dynamic Hostname Exchange for IS-IS
- RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973—IS-IS Mesh Groups
- RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567—Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719—Recommendations for Interoperable Networks using IS-IS
- RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787—Recommendations for Interoperable IP Networks
- RFC 4205 for Shared Risk Link Group (SRLG) TLV
- RFC 5309—Point-to-Point Operation over LAN in Link State Routing Protocols

LDP

- RFC 5036—LDP Specification
- RFC 5283—LDP Extension for Inter-Area Label Switched Paths
- RFC 5443—LDP IGP Synchronization
- RFC 6388—Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths
- RFC 6512—Using Multipoint LDP When the Backbone Has No Route to the Root
- draft-pdutta-mpls-mldp-up-redundancy-00.txt—Upstream LSR Redundancy for Multipoint LDP Tunnels

LDP and IP FRR

- RFC 5286—Basic Specification for IP Fast Reroute: Loop-Free Alternates

MPLS

- RFC 3031—MPLS Architecture
- RFC 3032—MPLS Label Stack Encoding
- RFC 3815—Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)

MPLS – OAM

- RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 6424— Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

Multicast

- RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/IP VPNs
- draft-ietf-l2vpn-vpls-pim-snooping-07—Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)



Network Management

- IANA-IFType-MIB
- ITU-T X.721—Information technology- OSI-Structure of Management Information
- ITU-T X.734—Information technology- OSI-Systems Management: Event Report Management Function
- M.3100/3120—Equipment and Connection Models
- RFC 1157—SNMPv1
- RFC 1850—OSPF-MIB
- RFC 1907—SNMPv2-MIB
- RFC 2011—IP-MIB
- RFC 2012—TCP-MIB
- RFC 2013—UDP-MIB
- RFC 2030—Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2096—IP-FORWARD-MIB
- RFC 2138—RADIUS
- RFC 2206—RSVP-MIB
- RFC 2571—SNMP-FRAMEWORKMIB
- RFC 2572—SNMP-MPD-MIB
- RFC 2573—SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574—SNMP-USER-BASED-SMMIB
- RFC 2575—SNMP-VIEW-BASED ACM-MIB
- RFC 2576—SNMP-COMMUNITY-MIB
- RFC 2588—SONET-MIB
- RFC 2665—EtherLike-MIB
- RFC 2819—RMON-MIB
- RFC 2863—IF-MIB
- RFC 2864—INVERTED-STACK-MIB
- RFC 3014—NOTIFICATION-LOG MIB
- RFC 3164—The BSD Syslog Protocol
- RFC 3273—HCRMON-MIB
- RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413—Simple Network Management Protocol (SNMP) Applications
- RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418—SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- TMF 509/613—Network Connectivity Model

OSPF

- RFC 1765—OSPF Database Overflow
- RFC 2328—OSPF Version 2
- RFC 2370—Opaque LSA Support
- RFC 2740—OSPF for IPv6
- RFC 3101—OSPF NSSA Option
- RFC 3137—OSPF Stub Router Advertisement
- RFC 3509—Alternative Implementations of OSPF Area Border Routers
- RFC 3623—Graceful OSPF Restart (support for Helper mode)



- RFC 3630—Traffic Engineering (TE) Extensions to OSPF
- RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV
- RFC 4577—OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) (support for basic OSPF at PE-CE links)

OSPFv3

- RFC 4552—Authentication/Confidentiality for OSPFv3

PPP

- RFC 1332—PPP Internet Protocol Control Protocol (IPCP)
- RFC 1570—PPP LCP Extensions
- RFC 1619—PPP over SONET/SDH
- RFC 1661—The Point-to-Point Protocol (PPP)
- RFC 1662—PPP in HDLC-like Framing
- RFC 1989—PPP Link Quality Monitoring
- RFC 1990—The PPP Multilink Protocol (MP)
- RFC 2686—The Multi-Class Extension to Multi-Link PPP

Pseudowires

- Metro Ethernet Forum—Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks
- RFC 3550—RTP: A Transport Protocol for Real-Time Applications
- RFC 3985—Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4385—Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446—IANA Allocation for PWE3
- RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 4448—Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4553—Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 4717—Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 4618—Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks
- RFC 4619—Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks
- RFC 4816—Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service
- RFC 5085—Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5086—Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
- draft-ietf-pwe3-redundancy-02.txt—Pseudowire (PW) Redundancy

RIP

- RFC 1058—Routing Information Protocol
- RFC 2453—RIP Version 2

RADIUS

- RFC 2865—Remote Authentication Dial In User Service
- RFC 2866—RADIUS Accounting

RSVP-TE and FRR

- RFC 2430—A Provider Architecture for DiffServ & TE
- RFC 2961—RSVP Refresh Overhead Reduction Extensions
- RFC 2702—Requirements for Traffic Engineering over MPLS
- RFC 2747—RSVP Cryptographic Authentication



- RFC 3097—RSVP Cryptographic Authentication – Updated Message Type Value
- RFC 3209—Extensions to RSVP for LSP Tunnels
- RFC 3210—Applicability Statement for Extensions to RSVP for LSP Tunnels
- RFC 3477—Signalling Unnumbered Links in Resource ReSerVation Protocol – Traffic Engineering (RSVP-TE)
- RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels

SONET/SDH

- GR-253-CORE—SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
- ITU-T Recommendation G.841—Telecommunication Standardization Section of
- ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

SSH

- draft-ietf-secsh-architecture.txt—SSH Protocol Architecture
- draft-ietf-secsh-userauth.txt—SSH Authentication Protocol
- draft-ietf-secsh-transport.txt—SSH Transport Layer Protocol
- draft-ietf-secsh-connection.txt—SSH Connection Protocol
- draft-ietf-secsh-newmodes.txt—SSH Transport Layer Encryption Modes
- draft-ietf-secsh-filexfer-13.txt—SSH File Transfer Protocol

Synchronization

- G.781—Synchronization layer functions, 2001/09/17
- G.803—Architecture of transport networks based on the synchronous digital hierarchy (SDH)
- G.813—Timing characteristics of SDH equipment slave clocks (SEC)
- G.823—The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy, 2003/03/16
- G.824—The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy, 2003/03/16
- G.8261—Timing and synchronization aspects in packet networks
- G.8262—Timing characteristics of synchronous Ethernet equipment slave clock
- GR 1244 CORE—Clocks for the Synchronized Network: Common Generic Criteria
- IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- ITU-T G.8264—Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008
- ITU-T G.8265.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010
- ITU-T G.8275.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014
- RFC 5905—Network Time Protocol Version 4: Protocol and Algorithms Specification

TACACS+

- IETF draft-grant-tacacs-02.txt—The TACACS+ Protocol

TCP/IP

- RFC 768—User Datagram Protocol
- RFC 791—Internet Protocol
- RFC 792—Internet Control Message Protocol
- RFC 793—Transmission Control Protocol
- RFC 826—Ethernet Address Resolution Protocol
- RFC 854—Telnet Protocol Specification
- RFC 1350—The TFTP Protocol (Rev. 2)
- RFC 1812—Requirements for IPv4 Routers



TWAMP

- RFC 5357—A Two-Way Active Measurement Protocol (TWAMP)

VPLS

- RFC 4762—Virtual Private LAN Services Using LDP

VRRP

- RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 3768 Virtual Router Redundancy Protocol
- RFC 5798 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6



Normas de Compatibilidade eletromagnética (EMC) Industrial segundo a Tabela 1 que terão de ser suportadas pelo equipamento

Tabela 1 – Normas de Compatibilidade eletromagnética (EMC) Industrial

Norma	Descrição	
IEEE 1613:2009 + A1:2011	IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations	Performance Class 1 (Class 2 with Optics interfaces only)
IEEE 1613.1-2013	IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Transmission and Distribution Facilities	Zone A; Performance Class 1 (Class 2 with Optics interfaces only)
IEEE Std C37.90	IEEE Standard for relays and relay systems associated with Electric Power Apparatus	
IEEE Std C37.90.1	Surge Withstand Capability (SWC) Tests	
IEEE Std C37.90.2	Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers	
IEEE Std C37.90.3	IEEE Standard Electrostatic Discharge Tests for Protective Relays	
EN 50121-4	Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus	
IEC 62236-4	Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus	
IEC 61000-6-2	Generic standards – Immunity for industrial environments	
IEC 61000-6-4	Generic standards – Emissions standard for industrial environments	
IEC 61000-6-5	Generic standards – immunity for equipment used in power station and substation environment	
IEC 61850-3	Communication networks and systems for power utility automation – Part 3: General requirements	
IEC/AS 60870.2.1	Telecontrol equipment and systems. Operating conditions. Power supply and electromagnetic compatibility	



Normas de Cliente e Regulamentos EMC segundo a Tabela 2 que terão de ser suportadas pelo equipamento

Tabela 2 - Normas de Cliente e Regulamentos EMC

Norma	Descrição	
IEC 61000-4-2	Electrostatic discharge immunity test	
IEC 61000-4-3	Radiated electromagnetic field immunity Test	
IEC 61000-4-4	Electrical fast transient/burst immunity Test	
IEC 61000-4-5	Surge immunity test	
IEC 61000-4-6	Immunity to conducted disturbances	
IEC 61000-4-8	Power frequency magnetic field immunity test	
IEC 61000-4-9	Pulse Magnetic field immunity test	
IEC 61000-4-10	Damped Oscillatory Magnetic Field	
IEC 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	With external AC/DC power supply
IEC 61000-4-12	Oscillatory wave immunity test	
IEC 61000-4-16	Conducted immunity 0 Hz – 150 kHz	
IEC 61000-4-17	Ripple on d.c. input power port immunity test	
IEC 61000-4-18	Damped oscillatory wave immunity test	
IEC 61000-4-29	Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests	
IEC 61000-3-2	Limits for harmonic current emissions (equipment input current <16A per phase)	With external AC/DC power supply
IEC 61000-3-3	Limits for voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <16A	With external AC/DC power supply



ITU-T K.20 (DC Ports)	Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents	
ETSI 300 132-2	Power supply interface at the input to telecommunications and 1gnali (ICT) equipment; Part 2: Operated by -48 V direct current (dc)	
EN 300 386	Telecommunication network equipment; ElectroMagnetic Compatibility (EMC)	
ES 201 468	Electromagnetic compatibility and Radio spectrum Matters (ERM); Additional ElectroMagnetic Compatibility (EMC) requirements and resistibility requirements for telecommunications equipment for enhanced availability of service in specific applications	
EN 55024	Information technology equipment – Immunity characteristics – Limits and methods of measurements	
Telcordia GR-1089-CORE	EMC and Electrical Safety – Generic Criteria for Network Telecommunications Equipment	
AS/NZS CISPR 22	Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement	Class A

FCC Part 15, Subpart B	Radio Frequency devices- Unintentional Radiators (Radiated & Conducted Emissions)	Class A
ICES-003	Information Technology Equipment (ITE) — Limits and methods of measurement	Class A
EN 55022	Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement	Class A
EN 55032	Electromagnetic compatibility of multimedia equipment – Emission requirements	Class A
CISPR 22	Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement	Class A
CISPR 32	Electromagnetic compatibility of multimedia equipment – Emission requirements	Class A
GS7 EMC	Electromagnetic Standard Compatibility (BT standard)	



Normas Ambientais segundo a Tabela 3 que terão de ser suportadas pelo equipamento

Tabela 3 - Normas Ambientais

Norma	Descrição	
IEEE 1613:2009 + A1:2011	Environmental and Testing Requirements for Communications Networking Devices	Forced air system; uses fans
IEC 61850-3	Communication networks and systems for power utility automation – Part 3: General requirements	Normal environmental conditions as per IEC 61850-3 ed.2
IEC 60068-2-1	Environmental testing – Part 2-1: Tests – Test A: Cold	
IEC 60068-2-2	Environmental testing – Part 2-2: Tests – Test B: Dry heat	
IEC 60068-2-30	Environmental testing – Part 2: Tests. Test Db and guidance: Damp heat, cyclic (12 + 12-hour cycle)	
IEC 60255-21-2	Electrical relays – Part 21: Vibration, shock, bump and seismic tests on measuring relays and protection equipment – Section Two: Shock and bump tests	
ETSI 300 753 Class 3.2	Acoustic noise emitted by telecommunications equipment	
Telcordia GR-63- CORE	NEBS Requirements: Physical Protection	
ETSI EN 300 019-2-1 v2.1.2, Class 1.2	Specification of environmental tests; Storage	
ETSI EN 300 019-2-2 V2.1.2, class 2.3	Specification of environmental tests; Transportation	
ETSI EN 300 019-2-3 V2.2.2, class 3.2	Specification of environmental tests; Stationary use at weatherprotected locations	
ETSI EN 300 019-2-4 v2.2.2 class T4.1	Specification of environmental tests; Stationary use at non-weatherprotected locations	

Normas de Segurança segundo a Tabela 4 que terão de ser suportadas pelo equipamento



Tabela 4 – Normas de Segurança

Norma	Descrição	
UL/CSA 60950-1	Information technology equipment – Safety – Part 1: General requirements	
IEC/EN 60950-1	Information technology equipment – Safety – Part 1: General requirements	
UL/CSA 62368-1	Audio/video, information and communication technology equipment – Part 1: Safety requirements	
IEC/EN 62368-1	Audio/video, information and communication technology equipment – Part 1: Safety requirements	
AS/NZS 60950-1	Information technology equipment – Safety – Part 1: General requirements	
IEC/EN 60825-1 and 2	Safety of laser products – Part 1: Equipment classification and requirements Part 2: Safety of optical fibre communication systems (OFCS)	
FDA CDRH 21-CFR 1040	PART 1040 Performance Standards for Light-Emitting Products	
IEC 60529	Degrees of Protection Provided by Enclosures (IP Code) – IP20	



Normas de Interface de Telecomunicações segundo a Tabela 5 que terão de ser suportadas pelo equipamento

Tabela 5 - Normas de Interface de Telecomunicações

Norma	Descrição	
IC CS-03 Issue 9	Compliance Specification for Terminal Equipment, Terminal Systems, Network Protection Devices, Connection Arrangements and Hearing Aids Compatibility	
ACTA TIA-968-B	Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network	
ATIS-06000403	Network and Customer Installation Interfaces- DS1 Electrical Interfaces	
ANSI/TIA/EIA-422-B (RS422)	Electrical Characteristics for balanced voltage digital interfaces circuits	
ITU-T G.825	The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)	
ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces	
ITU-T G.712 (E&M)	Transmission performance characteristics of pulse code modulation channels	
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy	
ITU-T V.24 (RS232)	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment(DCE)	
ITU-T V.36 (V35)	Modems for synchronous data transmission using 60-108 kHz group band circuits	
ITU-T V.11 / X.27 (RS-422)	Electrical characteristics for balanced double current interchange circuits operating at data signaling rates up to 10 Mbit/s	
ITU-T X.21 (RS-422)	Data Terminal Equipment Power via the Media Dependent Interfaces Enhancements	



ANSI/TIA/EIA-422-B (RS422)	Electrical Characteristics for balanced voltage digital interfaces circuits	
ITU-T G.825	The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)	
ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces	
ITU-T G.712 (E&M)	Transmission performance characteristics of pulse code modulation channels	
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy	
ITU-T V.24 (RS232)	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment(DCE)	
ITU-T V.36 (V35)	Modems for synchronous data transmission using 60-108 kHz group band circuits	
ITU-T V.11 / X.27 (RS-422)	Electrical characteristics for balanced double current interchange circuits operating at data signaling rates up to 10 Mbit/s	
ITU-T X.21 (RS-422)	Data Terminal Equipment Power via the Media Dependent Interfaces Enhancements	

Normas de Certificações e Diretivas segundo a Tabela 6 que terão de ser suportadas pelo equipamento Tabela 6 - Normas de Certificações e Diretivas

Norma	Descrição	
EU Directive 2014/30/ EU (EMC) (formerly 2004/108/EC)	Electromagnetic Compatibility (EMC)	
EU Directive 2014/35/ EU (LVD) (formerly 2006/95/ EC)	Low Voltage Directive (LVD)	
EU Directive 2012/19/ EU (WEEE)	Waste Electrical and Electronic Equipment (WEEE)	
EU Directive 2011/65/ EU (RoHS2)	Restriction of the use of certain Hazardous Substances in Electrical and Electronic Equipment (Recast)	
CE Mark		
TL9000 certified		
ISO 14001 certified		
ISO 9001:2008 certified		



1.1.3 Especificações do equipamento Nokia 7705 SAR-Ax ou equivalente

1.1.3.1 Características Gerais

O equipamento a fornecer será o Nokia 7705 SAR-Ax ou equivalente irão ser inseridos em anéis e segmentos de rede com equipamentos Nokia pelo que terão de garantir todas as funcionalidades, tempos de convergência, latência entre outros requisitos não podendo degradar ou limitar as configurações em operação.

Os equipamentos terão de ser totalmente integráveis e geridos na plataforma de gestão que a IP possui (NFM-P da Nokia) permitindo que a partir do centro de gestão se possa efetuar a criação e configuração de serviços MPLS envolvendo os novos equipamentos e os nós existentes.

Terá de possuir as seguintes características:

- Taxa de transferência do sistema (Half Duplex): 10 Gb/s
- 4 Portas Combo SFP/RJ-45 10/100/1000Mb/s
- 8 Portas SFP 10/100/1000Mb/s
- Portas de sincronismo: Sync in, ToD out.
- Dimensão 1U – montagem em rack 19”;
- 2 feeds: -48VDC/-60V DC
- Sem ventilação forçada (fanless)
- Condições de funcionamento:
 - Temperatura: -40°C a +65°C
 - Humidade: 5% a 95% sem condensação.

1.1.3.2 Serviços a suportar

O equipamento Nokia 7705 SAR-Ax ou equivalente terá de suportar os serviços descritos no ponto 1.2.2.8

1.1.3.3 Protocolos de rede

O equipamento Nokia 7705 SAR-Ax ou equivalente terá de suportar os protocolos descritos no ponto 1.2.2.9.

1.1.3.4 Qualidade de serviço e gestão de tráfego

O equipamento Nokia 7705 SAR-Ax ou equivalente terá de suportar as funcionalidades descritas no ponto 1.2.2.11.

1.1.3.5 Operação, Administração e Manutenção

O equipamento Nokia 7705 SAR-Ax ou equivalente terá de suportar as funcionalidades descritas no ponto 1.2.2.12.

1.1.3.6 Segurança

O equipamento Nokia 7705 SAR-Ax ou equivalente terá de suportar as funcionalidades descritas no ponto 1.2.2.14.

1.1.3.7 Normas suportadas

Normas de telecomunicações

- ANSI/TIA/EIA-232-C—Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange
- IEEE 802.1ad—IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks
- IEEE 802.1ag—Service Layer OAM
- IEEE 802.1p/q—VLAN Tagging
- IEEE 802.3—10BaseT



- IEEE 802.3ab—1000BaseT
- IEEE 802.3ah—Ethernet OAM
- IEEE 802.3u—100BaseTX
- IEEE 802.3x —Flow Control
- IEEE 802.3z—1000BaseSX/LX
- IEEE 802.3-2008—Revised base standard
- IEEE 802.1AX-2008—Link Aggregation Task Force (transferred from IEEE 802.3ad)
- IEEE C37.94-2002—N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment
- ITU-T G.704—Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels
- ITU-T G.707—Network node interface for the Synchronous Digital Hierarchy (SDH)
- ITU-T G.984.1—Gigabit-capable passive optical networks (GPON): general characteristics
- ITU-T Y.1564—Ethernet service activation test methodology
- ITU-T Y.1731—OAM functions and mechanisms for Ethernet-based networks

Protocolos suportados

ATM

- AF-PHY-0086.001—Inverse Multiplexing for ATM (IMA)
- af-tm-0121.000—Traffic Management Specification Version 4.1, March 1999
- GR-1113-CORE—Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994
- GR-1248-CORE—Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
- ITU-T Recommendation I.432.1—B-ISDN user-network interface - Physical layer specification: General characteristics
- ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions version 11/95
- RFC 2514—Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999
- RFC 2515—Definition of Managed Objects for ATM Management, February 1999
- RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5

BFD

- draft-ietf-bfd-mib-00.txt—Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-base-o5.txt—Bidirectional Forwarding Detection
- draft-ietf-bfd-v4v6-1hop-06.txt—BFD IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-06.txt—BFD for Multi-hop Paths

BGP

- RFC 1397—BGP Default Route Advertisement
- RFC 1997—BGP Communities Attribute
- RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 2439—BGP Route Flap Dampening
- RFC 2547bis—BGP/MPLS VPNs
- RFC 2918—Route Refresh Capability for BGP-4
- RFC 3107—Carrying Label Information in BGP-4
- RFC 3392—Capabilities Advertisement with BGP-4
- RFC 4271—BGP-4 (previously RFC 1771)
- RFC 4360—BGP Extended Communities Attribute
- RFC 4364—BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC



2574bis BGP/MPLS VPNs)

- RFC 4456—BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)
- RFC 4486—Subcodes for BGP Cease Notification Message
- RFC 4684—Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
- RFC 4724—Graceful Restart Mechanism for BGP - GR Helper
- RFC 4760—Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4893—BGP Support for Four-octet AS Number Space
- RFC 6513—Multicast in MPLS/BGP IP VPNs
- RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs
- draft-ietf-idr-add-paths-04.txt—Advertisement of Multiple Paths in BGP
- draft-ietf-idr-add-paths-guidelines-00.txt—Best Practices for Advertisement of Multiple Paths in BGP

DHCP/DHCPv6

- RFC 1534—Interoperation between DHCP and BOOTP
- RFC 2131—Dynamic Host Configuration Protocol (REV)
- RFC 2132—DHCP Options and BOOTP Vendor Extensions
- RFC 3046—DHCP Relay Agent Information Option (Option 82)
- RFC 3315—Dynamic Host Configuration Protocol for IPv6
- RFC 3736—Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

Differentiated Services

- RFC 2474—Definition of the DS Field in the IPv4 and IPv6 Headers
- RFC 2597—Assured Forwarding PHB Group
- RFC 2598—An Expedited Forwarding PHB
- RFC 3140—Per-Hop Behavior Identification Codes

Digital Data Network Management

- V.35
- RS-232 (also known as EIA/TIA-232)
- X.21

DSL Modules

- IEEE 802.2 LLC/SNAP bridged encapsulation while operating in ATM bonded mode
- ITU-T G.991.2 Annex A, B, F and ITU-T G.991.2 Amendment 2 Annex G—SHDSL
- standards compliance
- ITU-T G.991.2 Appendix F and G—Support for up to 5696 Kb/s per pair
- ITU-T G.992.1 (ADSL)
- ITU-T G.992.3 (G.dmt.bis), Annex A, B, J, M
- ITU-T G.992.3 Annex K.2 (ADSL2)
- ITU-T G.992.5, Annex A, B, J, M
- ITU-T G.992.5 Annex K (ADSL2+)
- ITU-T G.993.2 Amendment 1—Seamless Rate Adaptation
- ITU-T G.993.2 Annex A and Annex B—xDSL Standards Compliance (ADSL2/2+ and VDSL2)
- ITU-T G.993.2 Annex K.3—Supported Transport Protocol Specific Transmission
- Convergence functions
- ITU G.994.1 (2/07) Amendment 1 and 2—G.hs Handshake
- ITU-T G.998.2—SHDSL 4-pair EFM bonding
- ITU-T G.998.4 G.inp—Physical layer retransmission
- ITU-T Y.1564 Ethernet service activation test methodology



- TR-060—SHDSL rate and reach
- TR112 (U-R2 Deutsche Telekom AG) Version 7.0 and report of Self-Test-Result
- (ATU-T Register#3)

ECMP

- RFC 2992—Analysis of an Equal-Cost Multi-Path Algorithm

Frame Relay

- ANSI T1.617 Annex D—Signalling Specification For Frame Relay Bearer Service
- ITU-T Q.922 Annex A—Digital Subscriber Signalling System No. 1 (DSS1) data link layer - ISDN data link layer specification for frame mode bearer services
- FRF.1.2—PVC User-to-Network Interface (UNI) Implementation Agreement
- FRF.12—Frame Relay Fragmentation Implementation Agreement
- RFC 2427—Multiprotocol Interconnect over Frame Relay
- GRE
- RFC 2784—Generic Routing Encapsulation (GRE)

IPSec

- ITU-T X.690 (2002)—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- PKCS #12 Personal Information Exchange Syntax Standard
- RFC 2315—PKCS #7: Cryptographic Message Syntax
- RFC 2401—Security Architecture for the Internet Protocol
- RFC 2409—The Internet Key Exchange (IKE)
- RFC 2986—PKCS #10: Certification Request Syntax Specification
- RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3947—Negotiation of NAT-Traversal in the IKE
- RFC 3948—UDP Encapsulation of IPsec ESP Packets
- RFC 4303—IP Encapsulating Security Payload (ESP)
- RFC 4210—Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 4211—Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
- RFC 4945—The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
- RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5996—Internet Key Exchange Protocol Version 2 (IKEv2)

IPv6

- RFC 2460—Internet Protocol, Version 6 (IPv6) Specification
- RFC 2462—IPv6 Stateless Address Autoconfiguration
- RFC 2464—Transmission of IPv6 Packets over Ethernet Networks
- RFC 3587—IPv6 Global Unicast Address Format
- RFC 3595—Textual Conventions for IPv6 Flow Label
- RFC 4007—IPv6 Scoped Address Architecture
- RFC 4193—Unique Local IPv6 Unicast Addresses
- RFC 4291—IPv6 Addressing Architecture
- RFC 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 4649—DHCPv6 Relay Agent Remote-ID Option
- RFC 4861—Neighbor Discovery for IP version 6 (IPv6)
- RFC 5095—Deprecation of Type 0 Routing Headers in IPv6



- RFC 5952—A Recommendation for IPv6 Address Text Representation

IS-IS

- RFC 1142—OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195—Use of OSI IS-IS for routing in TCP/IP & dual environments
- RFC 2763—Dynamic Hostname Exchange for IS-IS
- RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973—IS-IS Mesh Groups
- RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567—Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719—Recommendations for Interoperable Networks using IS-IS
- RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787—Recommendations for Interoperable IP Networks
- RFC 4205 for Shared Risk Link Group (SRLG) TLV
- RFC 5304—IS-IS Cryptographic Authentication
- RFC 5308—Routing IPv6 with IS-IS
- RFC 5309—Point-to-Point Operation over LAN in Link State Routing Protocols
- RFC 5310—IS-IS Generic Cryptographic Authentication

LDP

- RFC 5036—LDP Specification
- RFC 5283—LDP Extension for Inter-Area Label Switched Paths
- RFC 5443—LDP IGP Synchronization
- RFC 6388—Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths
- RFC 6512—Using Multipoint LDP When the Backbone Has No Route to the Root
- draft-pdutta-mpls-mldp-up-redundancy-00.txt—Upstream LSR Redundancy for Multi-point LDP Tunnels
- LDP and IP FRR
- RFC 5286—Basic Specification for IP Fast Reroute: Loop-Free Alternates

MPLS

- RFC 3031—MPLS Architecture
- RFC 3032—MPLS Label Stack Encoding
- RFC 3815—Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 6790—The Use of Entropy Labels in MPLS Forwarding

MPLS – OAM

- RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 6424—Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

Multicast

- RFC 3956—Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
- RFC 3973—Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)
- RFC 4610—Anycast-RP Using Protocol Independent Multicast (PIM), which is similar to RFC 3446—Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery



- Protocol (MSDP)
- RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/IP VPNs
- cisco-ipmulticast/pim-autorp-spec—Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast, which is similar to RFC 5059—Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- draft-ietf-l2vpn-vpls-pim-snooping-07—Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)
- draft-ietf-mboned-msdp-deploy-nn.txt—Multicast Source Discovery Protocol
- (MSDP) Deployment Scenarios

Network Management

- IANA-IFTType-MIB
- ITU-T X.721—Information technology- OSI-Structure of Management Information
- ITU-T X.734—Information technology- OSI-Systems Management: Event Report
- Management Function
- M.3100/3120—Equipment and Connection Models
- RFC 1157—SNMPv1
- RFC 1850—OSPF-MIB
- RFC 1907—SNMPv2-MIB
- RFC 2011—IP-MIB
- RFC 2012—TCP-MIB
- RFC 2013—UDP-MIB
- RFC 2030—Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2096—IP-FORWARD-MIB
- RFC 2138—RADIUS
- RFC 2206—RSVP-MIB
- RFC 2571—SNMP-FRAMEWORKMIB
- RFC 2572—SNMP-MPD-MIB
- RFC 2573—SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574—SNMP-USER-BASED-SMMIB
- RFC 2575—SNMP-VIEW-BASED ACM-MIB
- RFC 2576—SNMP-COMMUNITY-MIB
- RFC 2588—SONET-MIB
- RFC 2665—EtherLike-MIB
- RFC 2819—RMON-MIB
- RFC 2863—IF-MIB
- RFC 2864—INVERTED-STACK-MIB
- RFC 3014—NOTIFICATION-LOG MIB
- RFC 3164—The BSD Syslog Protocol
- RFC 3273—HCRMON-MIB
- RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413—Simple Network Management Protocol (SNMP) Applications
- RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418—SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- TMF 509/613—Network Connectivity Model



OSPF

- RFC 1765—OSPF Database Overflow
- RFC 2328—OSPF Version 2
- RFC 2370—Opaque LSA Support
- RFC 2740—OSPF for IPv6
- RFC 3101—OSPF NSSA Option
- RFC 3137—OSPF Stub Router Advertisement
- RFC 3509—Alternative Implementations of OSPF Area Border Routers
- RFC 3623—Graceful OSPF Restart (support for Helper mode)
- RFC 3630—Traffic Engineering (TE) Extensions to OSPF
- RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV
- RFC 4577—OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP
- Virtual Private Networks (VPNs) (support for basic OSPF at PE-CE links)

OSPFv3

- RFC 4552—Authentication/Confidentiality for OSPFv3

PPP

- RFC 1332—PPP Internet Protocol Control Protocol (IPCP)
- RFC 1570—PPP LCP Extensions
- RFC 1619—PPP over SONET/SDH
- RFC 1661—The Point-to-Point Protocol (PPP)
- RFC 1662—PPP in HDLC-like Framing
- RFC 1989—PPP Link Quality Monitoring
- RFC 1990—The PPP Multilink Protocol (MP)
- RFC 2686—The Multi-Class Extension to Multi-Link PPP

Pseudowires

- Metro Ethernet Forum—Implementation Agreement for the Emulation of PDH
- Circuits over Metro Ethernet Networks
- RFC 3550—RTP: A Transport Protocol for Real-Time Applications
- RFC 3985—Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4385—Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446—IANA Allocation for PWE3
- RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 4448—Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4553—Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 4717—Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 4618—Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks
- RFC 4619—Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks
- RFC 4816—Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service
- RFC 5085—Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5086—Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)



- draft-ietf-pwe3-redundancy-02.txt—Pseudowire (PW) Redundancy

RIP

- RFC 1058—Routing Information Protocol
- RFC 2453—RIP Version 2

RADIUS

- RFC 2865—Remote Authentication Dial In User Service
- RFC 2866—RADIUS Accounting

RSVP-TE and FRR

- RFC 2430—A Provider Architecture for DiffServ & TE
- RFC 2961—RSVP Refresh Overhead Reduction Extensions
- RFC 2702—Requirements for Traffic Engineering over MPLS
- RFC 2747—RSVP Cryptographic Authentication
- RFC 3097—RSVP Cryptographic Authentication - Updated Message Type Value
- RFC 3209—Extensions to RSVP for LSP Tunnels
- RFC 3210—Applicability Statement for Extensions to RSVP for LSP Tunnels
- RFC 3477—Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)
- RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels
- RFC 5440—Path Computation Element (PCE) Communication Protocol (PCEP)
- draft-ietf-pce-stateful-pce—PCEP Extensions for Stateful PCE
- draft-ietf-pce-segment-routing—PCEP Extensions for Segment Routing
- draft-alvarez-pce-path-profiles—PCE Path Profiles

SONET/SDH

- GR-253-CORE—SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
- ITU-T Recommendation G.841—Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

SSH

- draft-ietf-secsh-architecture.txt—SSH Protocol Architecture
- draft-ietf-secsh-userauth.txt—SSH Authentication Protocol
- draft-ietf-secsh-transport.txt—SSH Transport Layer Protocol
- draft-ietf-secsh-connection.txt—SSH Connection Protocol
- draft-ietf-secsh-newmodes.txt—SSH Transport Layer Encryption Modes
- draft-ietf-secsh-filexfer-13.txt—SSH File Transfer Protocol

Synchronization

- G.781—Synchronization layer functions, 2001/09/17
- G.803—Architecture of transport networks based on the synchronous digital hierarchy (SDH)
- G.813—Timing characteristics of SDH equipment slave clocks (SEC)
- G.823—The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy, 2003/03/16
- G.824—The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy, 2003/03/16
- G.8261—Timing and synchronization aspects in packet networks
- G.8262—Timing characteristics of synchronous Ethernet equipment slave clock
- GR 1244 CORE—Clocks for the Synchronized Network: Common Generic Criteria



- IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- ITU-T G.8264—Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008
- ITU-T G.8265.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010
- ITU-T G.8275.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014
- RFC 5905—Network Time Protocol Version 4: Protocol and Algorithms Specification

TACACS+

- IETF draft-grant-tacacs-02.txt—The TACACS+ Protocol

TCP/IP

- RFC 768—User Datagram Protocol
- RFC 791—Internet Protocol
- RFC 792—Internet Control Message Protocol
- RFC 793—Transmission Control Protocol
- RFC 826—Ethernet Address Resolution Protocol
- RFC 854—Telnet Protocol Specification
- RFC 1350—The TFTP Protocol (Rev. 2)
- RFC 1812—Requirements for IPv4 Routers

TWAMP

- RFC 5357—A Two-Way Active Measurement Protocol (TWAMP)

VPLS

- RFC 4762—Virtual Private LAN Services Using LDP

VRRP

- RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 3768 Virtual Router Redundancy Protocol
- RFC 5798 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

Normas de Compatibilidade eletromagnética (EMC) Industrial

Norma	Descrição	
EN 50121-4	Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus	
IEC 62236-4	Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus	
IEC 61000-6-2	Generic standards – Immunity for industrial environments	



Norma	Descrição	
IEC 61000-6-4	Generic standards – Emissions standard for industrial environments	
IEC 61000-4-2	Electrostatic discharge immunity test	
IEC 61000-4-3	Radiated electromagnetic field immunity test	
IEC 61000-4-4	Electrical fast transient/burst immunity test	
IEC 61000-4-5	Surge immunity test	
IEC 61000-4-6	Immunity to conducted disturbances	
IEC 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	
IEC 61000-3-2	Limits for harmonic current emissions(equipment input current <16A per phase)	
IEC 61000-3-3	Limits for voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <16A	
ITU-T K.20(DC Ports)	Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents	
ETSI 300 132-2	Power supply interface at the input to telecommunications and Datacom (ICT) equipment; Part 2: Operated by -48 V direct current (dc)	
ETSI 300-132-3	Power supply interface at the input to telecommunications equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400V	
EN 300 386	Telecommunication network equipment; ElectroMagnetic Compatibility (EMC)	
EN 55024	Information technology equipment - Immunity characteristics - Limits and methods of measurements	

Normas Ambientais

Norma	Descrição	
IEC 60068-2-1	Environmental testing – Part 2-1: Tests – Test A: Cold	
IEC 60068-2-2	Environmental testing – Part 2-2: Tests – Test B: Dry heat	
IEC 60068-2-30	Environmental testing – Part 2: Tests. Test Db and guidance: Damp heat, cyclic (12 + 12-hour cycle)	
ETSI 300 753 Class 3.2	Acoustic noise emitted by telecommunications equipment	
Telcordia GR-63- CORE	NEBS Requirements: Physical Protection	
ETSI EN 300 019-2-1 v2.1.2, Class 1.2	Specification of environmental tests; Storage	
ETSI EN 300 019-2-2 V2.1.2, class 2.3	Specification of environmental tests; Transportation	
ETSI EN 300 019-2-3 V2.2.2, class 3.2	Specification of environmental tests; Stationary use at weatherprotected locations	

Normas de Segurança

Norma	Descrição	
UL/CSA 60950-1	Information technology equipment – Safety – Part 1: General requirements	



Norma	Descrição	
IEC/EN 60950-1	Information technology equipment – Safety – Part 1: General requirements	
AS/NZS 60950-1	Information technology equipment – Safety – Part 1: General requirements	
IEC/EN 60825-1 and 2	Safety of laser products – Part 1: Equipment classification and requirements Part 2: Safety of optical fibre communication systems (OFCS)	
FDA CDRH 21-CFR 1040	PART 1040 Performance Standards for Light-Emitting Products	
IEC 60529	Degrees of Protection Provided by Enclosures (IP Code) – IP40	

Normas ao nível da interface de telecomunicações

Norma	Descrição	
IC CS-03 Issue 9	Compliance Specification for Terminal Equipment, Terminal Systems, Network Protection Devices, Connection Arrangements and Hearing Aids Compatibility	
ACTA TIA-968-B	Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network	
ATIS-06000403	Network and Customer Installation Interfaces- DS1 Electrical Interfaces	

Certificações e diretivas

Norma	Descrição	
EU Directive 2014/30/ EU (EMC) (formerly 2004/108/EC)	Electromagnetic Compatibility (EMC)	
EU Directive 2014/35/ EU (LVD) (formerly 2006/95/ EC)	Low Voltage Directive (LVD)	
EU Directive 2012/19/ EU (WEEE)	Waste Electrical and Electronic Equipment (WEEE)	
EU Directive 2011/65/ EU (RoHS2)	Restriction of the use of certain Hazardous Substances in Electrical and Electronic Equipment (Recast)	
CE Mark		
TL9000 certified		
ISO 14001 certified		
ISO 9001:2008 certified		

1.1.4 Componentes para o equipamento 7705 SAR 8

1.1.4.1 Módulo de 8 portas GigabitEthernet (3HE06151UA)

Módulo de 8 portas GigabitEthernet incluindo Placa 1x8 Port GE SFP (3HE06151AA), 1xRTU– 6 Port FE Enablement (3HE06151LA) 6 x SFP GbE Base-T RJ45 DDM -40/85°C (3HE11904AA) e 6 portas 10/100 Mb/s RJ45. Terá de incluir 6 SFP-T de GbE.

1.1.4.2 Carta com portas a 10GigabitEthernet

Carta com capacidade para suportar 2 portas 10GE para 7705 SAR-8.



1.1.5 Componentes para o equipamento 7705 SAR 8 e 7705 SAR Ax

1.1.5.1 SFP – GIGE SX – LC ROHS 6/6 DDM -40/85°C

SFP Gigabit Ethernet (1000BASE-SX) (3HE00027CA) com comprimento de onda 850nm com conector LC para fibra multimodo com alcance até 300m. Temperatura de funcionamento: -40° a 85°C com Digital-diagnostic-monitoring (DDM).

Terá de ser compatível com o 7705 SAR 8 e 7705 SAR A e do mesmo fabricante do equipamento.

1.1.5.2 SFP – GIGE LX – LC ROHS 6/6 DDM -40/85°C

SFP Gigabit Ethernet (1000BASE-LX) (3HE00028CA) com comprimento de onda 1310nm com conector LC com alcance até 10Km suportando SyncE. Temperatura de funcionamento: -40° a 85°C com Digital-diagnostic-monitoring (DDM) cumprindo a diretiva 2002/95/EC.

Terá de ser compatível com o 7705 SAR 8 e 7705 SAR A e do mesmo fabricante do equipamento.

1.1.5.3 SFP – GIGE EX – LC ROHS 6/6 DDM -40/85°C

SFP Gigabit Ethernet (1000BASE-EX) (3HE00867CA) com comprimento de onda 1310nm com conector LC com alcance até 40Km suportando SyncE. Temperatura de funcionamento: -40° a 85°C com Digital-diagnostic-monitoring (DDM) cumprindo a diretiva 2002/95/EC.

Terá de ser compatível com o 7705 SAR 8 e 7705 SAR A e do mesmo fabricante do equipamento.

1.1.5.4 SFP – GIGE ZX – LC ROHS 6/6 DDM -40/85°C

SFP Gigabit Ethernet (1000BASE-ZX) (3HE00029CA) com comprimento de onda 1550nm com conector LC com alcance até 70Km suportando SyncE. Temperatura de funcionamento: -40° a 85°C com Digital-diagnostic-monitoring (DDM) cumprindo a diretiva 2002/95/EC.

Terá de ser compatível com o 7705 SAR 8 e 7705 SAR A e do mesmo fabricante do equipamento.

1.1.5.5 SFP – GIGE EZX – LC ROHS 6/6 DDM -40/85°C

SFP Gigabit Ethernet (1000BASE-EZX) (3HE01389CA) com comprimento de onda 1550nm com conector LC com alcance até 120Km suportando SyncE. Temperatura de funcionamento: -40° a 85°C com Digital-diagnostic-monitoring (DDM) cumprindo a diretiva 2002/95/EC. Terá de ser compatível com o 7705 SAR 8 e 7705 SAR A e do mesmo fabricante do equipamento.

1.1.5.6 SFP+ – 10G SR – LC ROHS 6/6 0/70C (3HE04824AA)

Terá de ser compatível com o 7705 SAR 8

1.1.5.7 SFP+ – 10G LR – LC ROHS 6/6 0/70C (3HE04823AA)

Terá de ser compatível com o 7705 SAR 8

1.1.5.8 SFP+ – 10G ER – LC ROHS 6/6 0/70C (3HE05036AA)

Terá de ser compatível com o 7705 SAR 8



1.1.5.8 SFP – 10G ZR – LC ROHS 6/6 DDM 0/70C (3HE05894AA)

Terá de ser compatível com o 7705 SAR 8

1.1.5.9 SFP – Cabo em Y para sincronismo para Nokia 7705 SAR 8

Cabo mini coaxial em Y para ligar uma fonte de sincronismo a portas de entrada de duas CSMs.

1.1.5.10 Conversor AC/DC 230V/48V de 220W

Caraterísticas a ser suportadas pelo conversor a fornecer:

- Tensão AC de entrada: 100-240V ($\pm 15\%$);
- Frequência de entrada: 50-60Hz $\pm 6\%$;
- Tensão de saída DC: 48V com ajuste de 48 a 56V;
- Potência de saída mínima: 220W;
- Ripple de saída: $<100V_{pp}$ 20Hz a 20MHz;
- Temperatura de operação suportada: $-15^{\circ}C$ a $+70^{\circ}C$;
- Humidade: 5 a 95% - IEC60068-2-27;
- Montagem em calha DIN;
- Proteção: IP20 EN/IEC60529;
- Proteção de sobreaquecimento com corte da saída e com re-arranque automático;
- Resistência de Isolamento superior 5M Ω .
- Normas:
 - o EN61558-2-17;
 - o EN/IEC60204-1;
 - o EN/IEC61131-2;
 - o EN50178, IEC62103;
- Emissão EMC de acordo com as normas: EN61000-6-3 e EN61000-6-4;
- Emissão radiante: EN55011, EN55022 Classe B.

1.2 EQUIPAMENTO SWITCHING E ROUTING

1.2.1 Introdução

Os equipamentos a prever neste projeto, serão integrados nas redes existentes nos diferentes troços alvo de intervenção, devendo os mesmos serem totalmente compatíveis com os equipamentos Alcatel Lucent Enterprise e Hirschmann existentes e integráveis no centro de gestão Omnivista 2500 e Hivision que a IP possui em produção.

1.2.2 OS6570M-U28 ou equivalente

OS6570M-U28 ou equivalente: Switch Industrial Gigabit Ethernet L2 de 1 U de 20 portas SFP 100/1000 Base-X, 4 portas combo SFP/RJ45 de 1G, 4 portas SFP+ 1G/10G e 2 portas SFP+ 1G/10G uplink/VLF.

- Equipado com Fonte de alimentação modular primária AC e com possibilidade de possuir uma fonte redundante de backup AC ou DC.

E com as seguintes características:

- Montagem em rack 19”;
- Ser totalmente gerido através da plataforma de gestão Omnivista 2500 existente na IP e totalmente integrável com a rede existente no CCO de Lisboa e sem perda das funcionalidades em utilização nesse site;
- Capacidade de comutação: 168 Gbps;
- Capacidade de switching ASIC 210Gb/S;
- Throughput: 125Mpps



Terão de incluir todo o licenciamento associado a funcionalidades (Advanced Routing) e ao centro de gestão existente na IP.

1.2.2.1 Login

1.2.2.1.1 Métodos Login: Telnet, SSH, HTTP, SNMP.

1.2.2.1.2 Número de sessões telnet concorrentes: 6.

1.2.2.1.3 Número de sessões SSH concorrentes: 8.

1.2.2.1.4 Número de sessões HTTP concorrentes (Webview): 4.

1.2.2.2 Gestão de ficheiros

1.2.2.2.1 Métodos de transferência de ficheiros a suportar: FTP (v4/v6), SFTP (v4/v6), SCP (v4/v6), TFTP.

1.2.2.2.2 Suporte Cliente/Servidor:

FTP—Cliente (IPv4) ou Servidor;

SFTP—Cliente ou Servidor;

SCP—Cliente ou Servidor;

TFTP—Cliente.

1.2.2.2.3 Número de sessões FTP/SFTP concorrentes: 4.

1.2.2.3 SNMP

1.2.2.3.1 Os equipamentos terão que suportar as seguintes normas RFC para SNMPv2:

1902 até 1907 - SNMPv2c Management Framework;

1908 - Coexistence and transitions relating to SNMPv1 and SNMPv2c.

1.2.2.3.2 Os equipamentos terão que suportar as seguintes normas RFC para SNMPv3:

2570—Version 3 of the Internet Standard Network Management Framework;

2571—Architecture for Describing SNMP Management Frameworks;

2572—Message Processing and Dispatching for SNMP;

2573—SNMPv3 Applications;

2574/3414—User-based Security Model (USM) for version 3 SNMP;

2575—View-based Access Control Model (VACM) for SNMP;

2576—Coexistence between SNMP versions;

3586—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.

1.2.2.3.3 SNMPV3 Autenticação: SHA, MD5

1.2.2.3.4 Cifragem SMNPv3: DES, AES



1.2.2.4 Chassis Virtual

- 1.2.2.4.1 Número de switches físicos que podem constituir 1 chassis virtual:8.
- 1.2.2.4.2 Número de peers Virtual Fabric link:2.
- 1.2.2.4.3 Número de portas membro por link Virtual Fabric: 8.
- 1.2.2.4.4 Portas suportadas para VFL: 10G SFP+.
- 1.2.2.4.5 Vlan Control Vlan: 2-4094
- 1.2.2.4.6 Intervalo de tempo do protocolo Hello para Chassis virtuais válidos: 1-65535

1.2.2.5 NTP

- 1.2.2.5.1 Os equipamentos terão que suportar RFC 5905–Network Time Protocol v4.
- 1.2.2.5.2 Número de servidores NTP por cliente:12.
- 1.2.2.5.3 Número de associações: 512.

1.2.2.6 Nível 2 (Layer 2)

- 1.2.2.6.1 Os equipamentos terão que suportar as seguintes normas IEEE:
 - 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
 - 802.3u (100BaseTX)
 - 802.3ab (1000BaseT)
 - 802.3z (1000Base-X)
 - 802.3bz (2.5Base-T)
 - 802.3ae (10GBase-X)
 - 802.3ba (40GBase-X)
 - 802.3az (Energy Efficient Ethernet)

- 1.2.2.6.2 Portas suportadas:
 - Ethernet (10Mbps);
 - Fast Ethernet (100Mbps);
 - Gigabit Ethernet (1Gbps);
 - 10/40/100 Gigabit Ethernet (10/40/100Gbps).

- 1.2.2.6.3 Suporte 802.1Q Hardware tagging.

- 1.2.2.6.4 Os equipamentos terão que suportar nas Interfaces de 10/100Mbps jumbo Frames de 1553 bytes e nas interfaces de 1/10/40/100Gbps terão suportar Jumbo frames de 9216bytes.

1.2.2.7 Unidirectional Link Detection (UDLD)

Os equipamentos terão de suportar Unidirectional Link Detection(UDLD).

- 1.2.2.7.1 Número de portas UDLD por sistema: 128.



1.2.2.7.2 Número de vizinhos UDLD por portas:32.

1.2.2.8 Source learning

Os equipamentos terão de suportar o seguinte RFC: 2674—Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions.

O número de endereços MAC apreendidos quando o modo Source learning centralizado está ativo deverá ser pelo menos de 32 000.

1.2.2.9 VLAN

1.2.2.9.1 Os equipamentos terão que suportar o RFC 2674 - Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions e o RFC 5517 - Private VLAN.

1.2.2.9.2 Os equipamentos terão que suportar as seguintes normas IEEE:

- 802.1Q – Virtual Bridged Local Area Networks;
- 802.1D – Media Access Control Bridges.

1.2.2.9.3 Os equipamentos terão de suportar pelo menos:

- Número de vlans por VC: 4094;
- Número de tagged vlans por porta: 4093;
- Número de VLAN untagged por porta: 1.

1.2.2.10 Spanning Tree

Os equipamentos terão de suportar as seguintes normas IEEE:

- 802.1d—Media Access Control (MAC) Bridges;
- 802.1s—Multiple Spanning Trees;
- 802.1w—Rapid Spanning Tree Protocol.

Os equipamentos terão que suportar:

- Modos de operação SpanningTree:
 - O Modo Flat – 1 instância spanning tree por chassis virtual;
 - O Modo por VLAN – 1 instância spanning tree por VLAN.
- Elegibilidade de port Spanning Tree: Portas fixas, portas 802.1Q tagged e portas Link aggregate
- Número de instâncias spanning tree VLAN por chassis virtual:100;
- Número de instâncias Multiple Spanning Tree Instances (MSTI) modo flat por chassis virtual: 16 adicionais à instância de spanning tree interna e comum (MSTI 0).



1.2.2.11 SPB

1.2.2.11.1 Os equipamentos terão que suportar IEEE802.1aq Shortest Path Bridging (SPB-M) nomeadamente as seguintes normas:

- IEEE

802.1aq/D3.6: Draft February 10, 2011—Virtual Bridged Local Area Networks-Amendment 9: Shortest Path Bridging;

802.1ah/D4.2: DRAFT March 26, 2008— Virtual Bridged Local Area Networks—Amendment 6: Provider Backbone Bridging.

-IETF

draft-ietf-isis-ieee-aq-05.txt—ISIS Extensions Supporting IEEE 802.1aq Shortest Path Bridging;

IETF draft—IP/IPVPN services with IEEE 802.1aq SPBB networks;

IETF draft—IP/IPVPN services with IEEE 802.1aq SPB networks.

1.2.2.12 Detecção Loopback

Os equipamentos terão de suportar Loopback detection, Edge (Bridge) e SAP(Access).

1.2.2.12.1 Temporizador de transmissão: 5 a 600 segundos.

1.2.2.12.2 Temporizador de auto-recover: 30-86400 segundos.

1.2.2.13 Agregação de links estático

Os equipamentos terão de suportar agregação de links estáticos.

1.2.2.13.1 Número de grupos de agregação de links: 32;

1.2.2.13.2 Número de portas por grupo de link agregate:8.

1.2.2.14 Agregação de links dinâmico

Os equipamentos terão de suportar as especificações IEEE - 802.1ax/802.3ad—Aggregation of Multiple Link Segments.

1.2.2.14.1 Número de grupo de agregação de links:32.

1.2.2.14.2 Número de portas por grupo de agregação de link:8.

1.2.2.15 Dual Home Link

Os equipamentos terão de suportar Dual-Home Link (1 sessão).

1.2.2.16 ERP

1.2.2.16.1 Os equipamentos terão de suportar:

- ITU-T G8032 03/2010 – Ethernet Ring Protection version 2 ((Multi Rings and Ladder networks).

- ITU-T Y.1731/IEEE802.lag – Pacote ERP de acordo com o formato PDU OAM para CCM.

1.2.2.16.2 Número máximo de anéis por nó: 64.



1.2.2.16.3 Número máximo de nós por anel:16.

1.2.2.16.4 Número máximo de VLANs por portas:4094.

1.2.2.16.5 Intervalo de identificadores de anel: 1 – 2147483647.

1.2.2.16.6 Intervalo para remote MEPID: 1-8191.

1.2.2.16.7 Intervalo de valores para o temporizador wait-to restore:1-12minutos.

1.2.2.16.8 Intervalos de valores para guard timer: 1- 200 centésimas de segundo.

1.2.2.16.9 Multiple VLAN Registration Protocol (MVRP)

Os equipamentos terão de suportar Multiple VLAN Registration Protocol (MVRP) tal como definido nas normas IEEE 802.1ak-2007 Amendment 7: Multiple Registration Protocol e IEEE 802.1Q-2005 Corrigendum 2008.

O número de VLAN utilizando MVRP a suportar deverá ser de 512.

1.2.2.16.10 IEEE 802.1AB LLDP

Os equipamentos terão que suportar LLDP cumprindo a norma IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery e as seguintes especificações:

- Número máximo de políticas de rede que podem ser associados com a porta: 8;
- Número máximo de políticas de rede que podem ser configurados por chassis virtual: 32.

1.2.2.16.11 IPv4

1.2.2.16.11.1 Os equipamentos terão de suportar os seguintes RFC:

- 791–Internet Protocol;
- 792–Internet Control Message Protocol;
- 826–An Ethernet Address Resolution Protocol;
- 2784–Generic Routing Encapsulation (GRE);
- 2890–Key and Sequence Number Extensions to GRE (extensions defined are not supported);
- 1701–Generic Routing Encapsulation (GRE);
- 1702–Generic Routing Encapsulation over IPV4 Networks;
- 2003-IP Encapsulation within IP.
- 4292 – IP Forwarding Table MIB
- 4293 – Management Information Base for Internet Protocol (IP)

1.2.2.16.11.2 Os equipamentos terão de suportar os seguintes itens:

- Número de interfaces de router por Sistema: 128 e 4000 (Advanced Routing);
- Número de interfaces de router por vlan: 8 e 16 (Advanced Routing);
- Número de rotas de hardware: 256 e 16000 (Advanced Routing);
- Número de entradas de hardware ARP: 2048 e 8000(Advanced Routing);
- Número máximo de interfaces de tuneis GRE por sistema: 127(Advanced Routing);;
- Número máximo de interfaces túnel IPIP por chassis virtual: 127(Advanced Routing);



- Número máximo de gateways ECMP: 4 e 16 (Advanced Routing);
- Número máximo de rotas estáticas (incluindo Black Hole Routes): 256 e 4000 (Advanced Routing);

1.2.2.16.11.3 VRF (Virtual Routing and Forwarding)

1.2.2.16.11.3.1. Os equipamentos terão que suportar múltiplos VRF por cada equipamento permitindo configurar instâncias de routing separadas no mesmo equipamento. Cada instância de routing terá que manter independentemente o seu routing e table de forwarding, peer e informação de interface.

1.2.2.16.11.3.2. Os equipamentos terão que suportar:

- Maximum number of MAX profile VRF instances per VC (no LOW profiles): 8
- Maximum number of LOW profile VRF instances per VC (no MAX profiles): 16
- Número de instância VRF por vlan: 1;
- Número de instâncias routing VRF OSPFv2/v3 por chassis virtual: 8;
- Número de instâncias routing RIPv2/ng por chassis virtual: 8.

1.2.2.16.12 IPv6

1.2.2.16.12.1 Os equipamentos terão de suportar os seguintes RFC:

- 1981—Path MTU Discovery for IP version 6;
- 2375—IPv6 Multicast Address Assignments;
- 2460—Internet Protocol, Version 6 (IPv6) Specification;
- 2464—Transmission of IPv6 Packets over Ethernet Networks;
- 2465—Management Information Base for IP Version 6: Textual Conventions and General Group;
- 2466—Management Information Base for IP Version 6: ICMPv6 Group;
- 2711—IPv6 Router Alert Option;
- 3056—Connection of IPv6 Domains via IPv4 Clouds;
- 3484—Default Address Selection for Internet Protocol version 6 (IPv6);
- 3493—Basic Socket Interface Extensions for IPv6;
- 3542—Advanced Sockets Application Program Interface (API) for IPv6;
- 3587—IPv6 Global Unicast Address Format;
- 3595—Textual Conventions for IPv6 Flow Label;
- 3596—DNS Extensions to Support IP Version 6;
- 4007—IPv6 Scoped Address Architecture;
- 4022—Management Information Base for the Transmission Control Protocol (TCP);
- 4113—Management Information Base for the User Datagram Protocol (UDP);
- 4193—Unique Local IPv6 Unicast Addresses;
- 4213—Basic Transition Mechanisms for IPv6 Hosts and Routers;
- 4291—IP Version 6 Addressing Architecture;



- 4294—IPv6 Node Requirements;
- 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version (IPv6) Specification; 6
- 4861—Neighbor Discovery for IP version 6 (IPv6);
- 4862—IPv6 Stateless Address Autoconfiguration;
- 5095—Deprecation of Type 0 Routing Headers in IPv6;
- 5453—Reserved IPv6 Interface Identifiers;
- 5722—Handling of Overlapping IPv6 Fragments.

1.2.2.16.12.2 Os equipamentos terão que suportar:

- Número de Interfaces IPv6: 16 e 4000(Advanced Routing);
- Túneis 6to4: 1(Advanced Routing);;
- Número de túneis configurados: 255; (Advanced Routing);
- Número de Hosts IPv6 (Neighbor Discovery):128 e 3000(Advanced Routing);
- Número de endereços unicast global IPv6 ou anycast: 16 e 4000(Advanced Routing);
- Número de endereços unicast global IPv6 por interface IPv6: 1 e 50(Advanced Routing);
- Número de rotas estáticas IPv6 (incluindo rotas black hole): 128 e 512(Advanced Routing);
- Número de Peers RIPng:10 e 20(Advanced Routing);
- Número de interfaces RIPng:10 e 20(Advanced Routing);
- Número de rotas RIPng: 128 e 5000(Advanced Routing);
- Número de gateways ECMP:4 e 16(Advanced Routing).

1.2.2.17 Especificações RIP

1.2.2.17.1Os equipamentos terão de suportar os seguintes RFCs:

- RFC 1058—RIP v1;
- RFC 2453—RIP v2;
- RFC 1722—RIP v2 Protocol Applicability Statement;
- RFC 1724—RIP v2 MIB Extension;
- RFC 2080—RIPng for IPv6 RFC 2082—RIP-2 MD5 Authentication.
- RFC 2082 - RIP-2 MD5 Authentication
- RFC 4822 - RIPv2 Cryptographic Authentication

1.2.2.17.2 Especificações RIP que os equipamentos terão de suportar:



- Número de interfaces: 10;
- Número de peers: 8 e 100(Advanced Routing);
- Número de rotas: 256 e 10000(Advanced Routing);

1.2.2.18 Especificações DHCP Relay/Snooping

Os equipamentos terão que suportar os seguintes RFCs e as seguintes especificações:

- 0951–Bootstrap Protocol;
- 1534–Interoperation between DHCP and BOOTP;
- 1541–Dynamic Host Configuration Protocol;
- 1542–Clarifications and Extensions for the Bootstrap Protocol;
- 2132–DHCP Options and BOOTP Vendor Extensions;
- 3046–DHCP Relay Agent Information Option, 2001.

Implementação DHCP relay:- DHCP global;
- DHCP por Vlan.

Serviço DHCP Relay: BOOTP/DHCP (Bootstrap Protocol/Dynamic Host Configuration Protocol)

Número dos portos:- 67 para os pedidos
- 68 para as respostas.

Número de endereços IP suportados por cada serviço de relay: 256;
Número de endereços suportados em modo interface: 256;
Número de serviço relay UDP por chassis virtual: 30;
Número de vlans em que o serviço de forward UDP é permitido: 256;
Número de VLAN de entradas de filtragem por IP origem:
- 32 VLANs com 223 clientes;
- 16 VLANs com 239 clientes;
- 8 VLANs com 247 clientes;
- 4 VLANs com 251 clientes.

Maximum port level IP source filtering entries:254 Clients

1.2.2.19 Especificações DHCPv6 Relay / Snooping

Os equipamentos terão que suportar:

- RFC 3315 – Dynamic Host Configuration Protocol for Ipv6 (DHCPv6).
- Implementação de relay DHCP por VLAN DHCP



- Número dos portos destino UDP:
- 547 - DHCPv6 messages to a DHCPv6 Server ou Relay Agent
- 546 - DHCPv6 messages to a Client

- Número de destinos de relay por interface de relay DHCPv6:5;
- Número Vlan snooping DHCPv6 (por VLAN mode):64;
- Número de VLANs guard DHCPv6: 64;
- Número de serviços Relay UDP IPv6 genéricos:8;
- Número de portas relay UDP IPv6:8;
- Número de destino UDP IPv6 por porta:8.

1.2.2.20 Servidor DHCP

1.2.2.20.1 Os equipamentos terão que suportar a funcionalidade de servidor de DHCP cumprindo os seguintes RFC:

- RFC 2131—Dynamic Host Configuration Protocol;
- RFC 3315—Dynamic Host Configuration Protocol for IPv6;
- RFC 950—Internet Standard Subnetting Procedure;
- RFC 868—Time Protocol;
- RFC 1035—Domain Implementation and Specification;
- RFC 1191—Path MTU Discovery.

1.2.2.20.2 Implementação de servidor DHCP server: BOOTP/DHCP

1.2.2.20.3 Mecanismos de disponibilização de endereços:

- BootP estático;
- DHCP estático;
- DHCP dinâmico.

1.2.2.20.4 Os equipamentos terão que suportar:

- Número de leases: 8000;
- Tamanho de informação de lease: 375k.

1.2.2.21 Virtual Router Redundancy Protocol

1.2.2.21.1 Os equipamentos terão que suportar Virtual Router Redundancy Protocol.

1.2.2.21.2 Os RFC que terão de ser suportados são os seguintes:

- RFC 3768—Virtual Router Redundancy Protocol;
- RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol;
- RFC 5798 - Virtual Router Redundancy Protocol (VRRP) Version 3 para IPv4 e IPv6;



- RFC 6527 - Definitions of Managed Objects para VRRP Version 3 (VRRPv3) IPv6.

1.2.2.21.3 Especificações VRRP que os equipamentos terão de suportar:

- Número de routers virtuais VRRPv2 e VRRPv3: 255;
- Número de endereços IP por instância: 16.

1.2.2.22 Especificações IPMS

1.2.2.22.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 1112—Host Extensions for IP Multicasting
- RFC 2236—Internet Group Management Protocol, Version 2
- RFC 2710—Multicast Listener Discovery (MLD) for IPv6
- RFC 2933—Internet Group Management Protocol MIB
- RFC 3019—IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
- RFC 3376—Internet Group Management Protocol, Version 3
- RFC 3810—Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4541—Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4604—Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.

1.2.2.22.2 Os equipamentos terão de suportar as seguintes versões de IGMP: IGMPv1, IGMPv2, IGMPv3.

1.2.2.22.3 Número de fluxos multicast IPv4 (switched): 1000.

1.2.2.22.4 Número de fluxos multicast IPv4 (*,G routed): 1000.

1.2.2.22.5 Número de fluxos multicast IPv4 (S,G routed): 1000.

1.2.2.23 IPMSv6

1.2.2.23.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 2710—Multicast Listener Discovery for IPv6
- RFC 3019—IPv6 MIB for Multicast Listener Discovery Protocol
- RFC 3306—Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3810—Multicast Listener Discovery Version 2 for IPv6
- RFC 4541—Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4604—Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.



- 1.2.2.23.2 Os equipamentos terão de suportar as seguintes versões de MLD: MLDv1, MLDv2.
- 1.2.2.23.3 Intervalo de Query MLD: 1 a 65535 segundos.
- 1.2.2.23.4 MLD Router timeout: 1 a 65535 segundos.
- 1.2.2.23.5 MLD Source timeout: 1 a 65535 segundos.
- 1.2.2.23.6 MLD Query Response Interval: 1-65535 milisegundos.
- 1.2.2.23.7 MLD Last Member Query Interval: 1-65535 milisegundos.
- 1.2.2.23.8 Número de fluxos multicast IPv6 (switched): 1000.
- 1.2.2.23.9 Número de fluxos multicast IPV6 (*,G routed): 1000.
- 1.2.2.23.10 Número de fluxos multicast IPV6 (S,G routed): 1000.

1.2.2.24 QoS

- 1.2.2.24.1 Os equipamentos terão que suportar as seguintes especificações:
 - Número máximo de regras:384
 - Número de condições de políticas:384;
 - Número de ações de políticas: 384;
 - Número de grupos (rede, MAC, serviço, porta): 2047;
 - Número de entradas de grupo:384 por grupo (256 por grupo de serviço);
 - Número máximo de filas CoS por porta: 8;
 - Perfis Queue Set (QSP):2;
 - Número de listas de políticas QoS: 32.

1.2.2.25 LDAP Policy Server

- 1.2.2.25.1 Os equipamentos terão que suportar os seguintes RFCs:
 - RFC 2251–Lightweight Directory Access Protocol (v3);
 - RFC 3060–Policy Core Information Model—Version 1 Specification.
- 1.2.2.25.2 Número de policy servers (suportados num chassis virtual):5.
- 1.2.2.25.3 Número de policy servers(suportados por PolicyView):1.

1.2.2.26 Servidor de autenticação

- 1.2.2.26.1 Os equipamentos terão de suportar os seguintes RFCs:
 - RFC 2865–Remote Authentication Dial In User Service (RADIUS);
 - RFC 2866–RADIUS Accounting;
 - RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support;
 - RFC 2868–RADIUS Attributes for Tunnel Protocol Support;
 - RFC 2809–Implementation of L2TP Compulsory Tunneling through RADIUS;



- RFC 2869–RADIUS Extensions;
- RFC 2548–Microsoft Vendor-specific RADIUS Attributes;
- RFC 2882–Network Access Servers Requirements: Extended RADIUS Practices;
- RFC 1492–An Access Control Protocol;
- RFC 1789–Connectionless Lightweight X.5000 Directory Access Protocol;
- RFC 2247–Using Domains in LDAP/X.500 Distinguished Names;
- RFC 2251–Lightweight Directory Access Protocol (v3);
- RFC 2252–Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions;
- RFC 2253–Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names;
- RFC 2254–The String Representation of LDAP Search Filters
- RFC 2256–A Summary of the X.500(96) User Schema for Use with LDAPv3;
- RFC 2574–User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
- RFC 2924–Accounting Attributes and Record Formats;
- RFC 2975–Introduction to Accounting Management;
- RFC 2989–Criteria for Evaluating AAA Protocols for Network Access.

1.2.2.26.2 Os equipamentos terão de suportar:

- Número de servidores autenticação no modo de autoridade única (single authority): 8;
- Número de servidores de autenticação no modo de autoridade múltipla:8;
- Número de servidores por cada switch autenticado:8.

1.2.2.27 Universal Network Profiles (UNP)

Os equipamentos terão de suportar Universal Network Profiles (UNP) com as seguintes características:

- Número de UNPs por chassis virtual: 4000;
- Número de utilizadores UNP por chassis:256;
- Número de utilizadores por chassis virtual:2000;
- Tipo de autenticação: Por MAC e 802.1x;
- Tipo de perfil: VLAN.
- Tipo de porta UNP: Bridge;
- Número de lista de políticas de QoS por chassis virtual: 32 (incluindo a lista por defeito);
- Número de lista de políticas de QoS por UNP:1.

1.2.2.28 Access Guardian

1.2.2.28.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 2284–PPP Extensible Authentication Protocol (EAP);



- RFC 2865–Remote Authentication Dial In User Service (RADIUS);
- RFC 2866–RADIUS Accounting;
- RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support;
- RFC 2868–RADIUS Attributes for Tunnel Protocol Support;
- RFC 2869–RADIUS Extensions;
- RFC 3576--Change of Authorization-Request (COA) and Disconnect request (DM) for BYOD. RFC support is limited to ClearPass solution;
- RFC 3579–RADIUS Support for EAP.

1.2.2.28.2 Os equipamentos terão de suportar as seguintes normas IEEE:

- IEEE 802.1X-2001–Standard for Port-based Network Access Control;
- 802.1X RADIUS Usage Guidelines.

1.2.2.28.3 Métodos de autenticação que tem de suportar:

- 802.1X;
- Endereços MAC;
- Portal Captivo.

1.2.2.28.4 Número de utilizadores access guardian (sistema): 1000.

1.2.2.28.5 Número de utilizadores em quarentena por QMR: 256.

1.2.2.28.6 Número de utilizadores médio permitidos para login no portal captativo num dado instante:40.

1.2.2.28.7 Número de perfis de portal captativo:8.

1.2.2.28.8 Número de perfis AAA: 8.

1.2.2.28.9 Número de servidores de autenticação: 4 por tipo de autenticação (MAC, 802.1X, Portal Captativo).

1.2.2.28.10 Número de servidores de accounting: 4 por tipo de autenticação (MAC, 802.1X, Portal Captativo).

1.2.2.28.11 mDNS GRE Tunnel Supported Protocol:IPv4

1.2.2.28.12 SSDP GRE Tunnel Supported Protocol:IPv4

1.2.2.28.13 Maximum L2 GRE Access Tunnels:1.

1.2.2.29 Port mapping

1.2.2.29.1 Port mapping é uma facilidade de segurança que controla a comunicação entre utilizadores peers. Os equipamentos deverão possuir esta facilidade.

1.2.2.29.2 Número de sessões de port mapping: 8.

1.2.2.30 Especificações de Learned port security (LPS)



- 1.2.2.30.1 Os equipamentos terão que suportar Learned port security (LPS).
- 1.2.2.30.2 Portas eligíveis para Learned Port Security: Fixas e 802.1Q tagged.
- 1.2.2.30.3 Portas não eligíveis para Learned Port Security: Portas agregadas e portas agregadas 802.1Q(trunked).
- 1.2.2.30.4 Número máximo de MAC apreendidas por porta LPS:1000.
- 1.2.2.30.5 Número máximo de endereços MAC filtrados permitidos por porta LPS:100.
- 1.2.2.30.6 Número máximo de intervalos de endereços MAC configuráveis por porta LPS:8.

1.2.2.31 Port Mirroring

Os equipamentos terão que suportar Port mirroring com as seguintes especificações:

- Número de Sessões de mirroring: 7;
- Número de sessões combinadas Mirroring /monitoring por chassis: 7;
- Suportar N to 1 Mirroring: 128 to 1;
- Número máximo de destinos mirroring suportados:1;
- Número de Vlans RPMIR por sessão: 1.

1.2.2.32 Port monitoring

Os equipamentos terão que suportar Port monitoring com as seguintes especificações:

- Número de sessões a suportar:1;
- Sessões combinadas de mirroring/monitoring por chassis: 7;
- Tipo de ficheiro suportado: formato de ficheiro ENC (Network General Sniffer Network Analyzer Format).

1.2.2.33 SFlow

1.2.2.33.1 Os equipamentos terão de suportar SFlow e o RFC 3176.

1.2.2.33.2 Instância de receção/amostra/polling:2.

1.2.2.33.3 Amostragem:

- tamanho de pacote;
- tipo de trama;
- Endereços MAC de origem e destino;
- Vlans de origem e destino;
- Endereços IP de origem e destino;
- Portos de origem e destino;
- Flags TCP e TOS.

1.2.2.33.4 Polling:

- Octetos de entrada;
- Octetos de saída;
- Número de pacotes unicast de receção;



- Número de pacotes unicast de transmissão;
- Número de pacotes multicast de recepção;
- Número de pacotes multicast de transmissão;
- Número de pacotes de broadcast de recepção;
- Número de pacotes de broadcast de transmissão;
- Erros de entrada;
- Erros de saída.

1.2.2.34 RMON

Os equipamentos terão de suportar o RFC 2819 - Remote Network Monitoring Management Information Base.

Funcionalidades suportadas:

- Implementação de grupo RMON4 básico;
- Grupo de estatísticas ethernet;
- Grupo (controlo e estatísticas) histórico;
- Grupo de Alarmes;
- Grupo eventos.

Tipo de probe: Ethernet/History/Alarm

Status: Ativo/Criando/Inativo

History Control Interval (seconds):1-3600

History Sample Index Range:1-65535

Alarm Interval (seconds): 1–2147483647

Alarm Startup Alarm: Rising Alarm/Falling Alarm/
RisingOrFallingAlarm

Alarm Sample Type: Delta Value/Absolute;

RMON Traps Supported: RisingAlarm/FallingAlarm These traps are generated whenever an Alarm entry crosses either its Rising Threshold or its Falling Threshold and generates an event configured for sending SNMP traps.

1.2.2.35 Estado do Switch (Switch Health)

1.2.2.35.1 Funcionalidade Health a suportar:



- Estatísticas de utilização de CPU ao nível do switch (percentagem);
- Estatísticas de entrada ao nível Switch/modulo/porta (percentagem);
- Estatísticas de utilização Entrada/saída ao nível do Switch/modulo/porta (percentagem);
- Estatísticas de utilização de memória ao nível do switch (percentagem);
- Estatísticas da temperatura ao nível de dispositivo (por exemplo, Chassis/CMM).

1.2.2.35.2 Monitorização do nível de utilização dos recursos:

- Nível de utilização mais recente;
- Nível de utilização média no último minuto;
- Nível de utilização na última hora;
- Nível de utilização máximo na última hora.

1.2.2.36 Vlan Stacking

1.2.2.36.1 Os equipamentos terão de suportar as seguintes normas IEEE:

- IEEE 802.1Q, 2003 Edition,
- IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks P802.1ad/D6.0 (C/LM) Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

1.2.2.36.2 Número de serviços: 4.

1.2.2.36.3 Número de SVLANs: 4000.

1.2.2.36.4 Número de SAPs: 8000.

1.2.2.36.5 Número de perfis SAP: 8000.

1.2.2.36.6 Número de VLANs de cliente (CVLANs) por chassis virtual: 4000.

1.2.2.36.7 Número de associações Service-to-SAP:1000.

1.2.2.36.8 Maximum supported SAP-UNI-CVLAN:4000.

1.2.2.37 Switch logging

Os equipamentos terão de suportar o seguinte RFC: RFC-5424 Syslog Protocol.

Número de servidores Syslog: 12.

Dispositivo de logging: Memória Flash/Consola/Endereço IP.

Tipos / Níveis de severidade:

- 2 (Alarm - highest severity),
- 3 (Error),
- 4 (Alert),
- 5 (Warning)



- 6 (Info - default),
- 7 (Debug 1),
- 8 (Debug 2),
- 9 (Debug 3 - lowest severity).

1.2.2.38 Ethernet OAM

1.2.2.38.1 Os equipamentos terão de suportar as seguintes normas:

- IEEE 802.1ag Version 8.1—Connectivity Fault Management;
- IEEE 802.1D—Media Access Control (MAC) Bridges;
- IEEE 802.1Q—Virtual Bridged Local Area Networks ITU-T Y.1731—OAM Functions and Mechanisms for Ethernet-Based Networks.

1.2.2.38.2 Número de domínios de manutenção (MD) por bridge:8.

1.2.2.38.3 Número de associações de manutenção (MA) por bridge: 128.

1.2.2.38.4 Número de end points de manutenção (MEP) por bridge:256.

1.2.2.38.5 Tamanho da base de dados MEP: 1000.

1.2.2.38.6 Intervalo mínimo CCM: 100ms.

1.2.2.39 Link OAM

Os equipamentos terão de suportar as normas IEEE e RFC seguintes:

- IEEE 802.3ah—EFM LINK OAM
- RFC 4878 - Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) functions on Ethernet-Like Interfaces.

1.2.2.40 Routing avançado

Os equipamentos terão de suportar os seguintes protocolos dinâmicos:

- OSPF V2 e V3;
- IS-IS;
- BGP;

bem como protocolos de routing multicast.

1.2.2.41 Os equipamentos terão de suportar Open Shortest Path First (OSPF) v2

1.2.2.41.1 Os RFC que terão de ser suportados são os seguintes:

- 1370—Applicability Statement for OSPF;
- 4750—OSPF Version 2 Management Information Base;
- 2328—OSPF Version 2;
- 5250—The OSPF Opaque LSA Option;



- 3101—The OSPF Not-So-Stubby Area (NSSA) Option;
- 3623—Graceful OSPF Restart;
- 5709 - OSPFv2 HMAC-SHA Cryptographic Authentication.

1.2.2.41.2 Especificações OSPFv2 que os equipamentos terão de suportar:

- Número de áreas: 8;
- Número de interfaces: 128;
- Número de interfaces passivas: 200;
- Número de entradas da base de Link State: 20000;
- Número máximo de vizinhos por router: 128;
- Número máximo de rotas: 32000;
- Número máximo de entradas next hop ECMP: 16.

1.2.2.42 Os equipamentos terão de suportar OSPF versão 3

1.2.2.42.1 Os RFC que terão de ser suportados:

- RFC 1826—IP Authentication Header ;
- RFC 1827—IP Encapsulating Security Payload;
- RFC 2553—Basic Socket Interface Extensions for IPv6;
- RFC 2373—IPv6 Addressing Architecture;
- RFC 2374—An IPv6 Aggregatable Global Unicast Address Format;
- RFC 2460—IPv6 base specification;
- RFC 2740—OSPF for IPv6;
- RFC 5643—Management Information Base for OSPFv3.

1.2.2.42.2 Especificações OSPFv3 que os equipamentos terão de suportar:

- Número de áreas: 5;
- Número de interfaces: 128;
- Número de entradas na base de dados Link State: 20000;
- Número de vizinhos: 128;
- Número de rotas: 32000;
- Número de entrada ECMP next Hop: 16.

1.2.2.43 Os equipamentos terão de suportar Intermediate System to Intermediate System (IS-IS)

1.2.2.43.1 As normas que terão de ser suportados são os seguintes:

- 1142-OSI IS-IS Intra-domain Routing Protocol;
- 1195-OSI IS-IS for Routing in TCP/IP and Dual Environments;



- 3373-Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point- to-Point Adjacencies;
- 3567-Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication;
- 2966-Prefix Distribution with two-level IS-IS (Route Leaking) support;
- 2763-Dynamic Host name exchange support;
- 3719-Recommendations for Interoperable Networks using IS-IS;
- 3787-Recommendations for Interoperable IP Networks using IS-IS;
- 5308-IS-IS support for IPv6 (Routing IPv6 with IS-IS);
- IETF- draft-ietf-isis-igp-p2p-over-lan-05.txt-Point-to-point operation over LAN in link-state routing protocols.

1.2.2.43.2 Especificações IS-IS que os equipamentos terão de suportar:

- Número máximo de áreas por router: 3;
- Número máximo de adjacências L1 por interface por router: 70;
- Número máximo de adjacências L2 por interface por router: 70;
- Número máximo de interfaces IS-IS (por router): 70;
- Número máximo de entradas Link State Pack por adjacência: 255;
- Número máximo de rotas IS-IS: 24000;
- Número máximo de rotas L1 IS-IS: 12000;
- Número máximo de rotas L2 IS-IS: 12000.

1.2.2.44 Os equipamentos terão de suportar Border Gateway Protocol (BGP)

1.2.2.44.1 Os RFC que terão de ser suportados são os seguintes:

- 1771/4271–A Border Gateway Protocol 4 (BGP-4);
- 2439–BGP Route Flap Damping;
- 3392/5492–Capabilities Advertisement with BGP-4;
- 2385–Protection of BGP Sessions via the TCP MD5 Signature Option;
- 1997–BGP Communities Attribute;
- 4456–BGP Route Reflection: An Alternative to Full Mesh Internal BGP(IBGP);
- 3065–Autonomous System Confederations for BGP;
- 4273–Definitions of Managed Objects for BGP-4;
- 4486–Subcodes for BGP Cease Notification;
- 4760–Multiprotocol Extensions for BGP-4;
- 2545–Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing;
- 2918 – Route Refresh Capability for BGP-4;
- 4724 – Graceful Restart Mechanism for BGP;
- 6793 – BGP 4-octet ASN;



- 5668 – 4-Octet AS Specific BGP Extended Community;
- 2042 – Registering New BGP Attribute Types;
- 5396 – Textual Representation of Autonomous System (AS) Numbers.

1.2.2.44.2 Os equipamentos terão que ao nível do BGP suportar os seguintes atributos: Origin, AS Path, Next Hop (IPv4), MED, Local Preference, Atomic Aggregate, Aggregator (IPv4), Community, Originator ID, Cluster List, Multiprotocol Reachable NLRI (IPv6), Multiprotocol Unreachable NLRI (IPv6), AS4 Path, AS4 Aggregator (IPv4), e AS Specific Extended Community.

1.2.2.44.3 Especificações BGP que os equipamentos terão de suportar:

- Número máximo de peers por switch (32 peers por VRF): 512;
- Número máximo de redes: 4000;
- Número máximo de endereços agregados: 2000;
- Número máximo de rotas: 32000;
- Número máximo de políticas: 1000.

1.2.2.45 Multicast Boundary

1.2.2.45.1 Normas que os equipamentos terão de suportar:

- RFC 2365—Administratively Scoped IP Multicast;
- RFC 5132 - IP Multicast MIB.

1.2.2.45.2 Intervalo de endereços válidos: 239.0.0.0 to 239.255.255.255.

1.2.2.45.3 Intervalo de endereços extended Multicast route boundary: 224.0.0.0 to 239.255.255.255.

1.2.2.46 Protocol-Independent Multicast (PIM)

Os equipamentos terão de suportar os seguintes RFCs:

- 2365—Administratively Scoped IP Multicast;
- 4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification;
- 4007—IPv6 Scoped IP Multicast;
- 5060—Protocol Independent Multicast MIB;
- 5132—IP Multicast MIB 3569—An Overview of Source-Specific Multicast (SSM);
- 3973—Protocol Independent Multicast-Dense Mode (PIM-DM);
- 5015 - Bidirectional Protocol Independent Multicast (BIDIR-PIM);
- 5059—Bootstrap Router (BSR) Mechanism for PIM;
- 5240—Protocol Independent Multicast (PIM) Bootstrap Router MIB;
- 2715—Interoperability Rules for Multicast Routing Protocols.

1.2.2.46.1 Versão PIM a suportar: PIM-SMv2.

1.2.2.46.2 Atributos PIM



- Shared trees (also referred to as RP trees);
- Designated Routers (DRs);
- Designated Forwarders (DFs);
- Bootstrap Routers (BSRs);
- Candidate Bootstrap Routers (C-BSRs);
- Rendezvous Points (RPs) (applicable only for PIM-SM) and BIDIR-PIM;
- Candidate Rendezvous Points (C-RPs).

1.2.2.46.3 Temporizadores a suportar:

- C-RP expiry,
- C-RP holdtime,
- C-RP advertisement,
- Join/Prune, Probe,
- Register suppression,
- Hello,
- Expiry,
- Assert,
- Neighbor liveness,
- DF Election Timer.

1.2.2.46.4 Número de interfaces: 384 (combinados entre PIMv4, PIMv6 e DVMRP).

1.2.2.46.5 Rendezvous Point (RP):100.

1.2.2.46.6 Bootstrap Routers (BSRs): 1.

1.2.2.46.7 Protocolos multicast por interface:1.

1.2.2.46.8 Anycast RP Routers: 8.

1.2.3 Fonte de alimentação redundante AC OS6570-BP

Fonte de alimentação redundante AC de 150w para o OS6570U28.

1.2.4 Fonte de alimentação redundante AC OS6570-BP-D

Fonte de alimentação redundante DC de 150w para o OS6570U28.

1.2.5 OS6860N-U28 ou equivalente

O equipamento a fornecer terá de ser Omniswitch OS6860N-U28 Switch nível 2 e 3 ou equivalente terá que cumprir com os seguintes requisitos gerais:

- Chassis 1 U 19”;



- Número de portas mínimo: 24 portas x 100/1000BaseX, SFP, 4x1/10G SFP+ e 4x10/25G SFP28;
- Porta de gestão out-of-band ethernet: 1;
- Porta USB de gestão: 1;
- Porta RS232:1;
- Porta da consola (micro-USB): 1;
- Fonte de alimentação redundante 1+1 (com possibilidade de suportar 230 AC (intervalo de tensões admissíveis entre 180 a 264V) e -48V DC (intervalo de tensões admissíveis entre -36V a -72V);
- Ventoinhas: 3;
- Capacidade de switching agregada: 728Gb/s;
- Taxa de transferência:541,7Mpps;
- Temperatura de funcionamento: 0°C a 45°C;
- Humidade em operação: 5% a 95% sem condensação;
- Consumo inferior a 172W;
- Equipamento com acessórios para montagem em rack 19” ocupando 1 U de altura;
- Totalmente integrável e gerido no centro de gestão Omnivista existente na IP;
- Integrável e compatível com a rede de omniswitches existentes na IP;
- Terá de incluir todo o licenciamento necessário ao nível de funcionalidade e do centro de gestão.

Terão de incluir todo o licenciamento associado a funcionalidades (Advanced Routing) e ao centro de gestão existente na IP.

1.2.5.1 Login

- 1.2.5.1.1 Métodos Login: Telnet, SSH, HTTP, SNMP.
- 1.2.5.1.2 Número de sessões telnet concorrentes: 6.
- 1.2.5.1.3 Número de sessões SSH concorrentes: 8.
- 1.2.5.1.4 Número de sessões HTTP concorrentes (Webview):4.

1.2.5.2 Gestão de ficheiros

- 1.2.5.2.1 Métodos de transferência de ficheiros a suportar: FTP (v4/v6), SFTP (v4/v6), SCP (v4/v6), TFTP.
- 1.2.5.2.2 Suporte Cliente/Servidor:
 - FTP—Cliente (IPv4) ou Servidor;
 - SFTP—Cliente ou Servidor;
 - SCP—Cliente ou Servidor;
 - TFTP—Cliente.
- 1.2.5.2.3 Número de sessões FTP/SFTP concorrentes: 4.

1.2.5.3 SNMP

- 1.2.5.3.1 Os equipamentos terão que suportar as seguintes normas RFC para SNMPv2:
 - 1902 até 1907 - SNMPv2c Management Framework;
 - 1908 - Coexistence and transitions relating to SNMPv1 and SNMPv2c.
- 1.2.5.3.2 Os equipamentos terão que suportar as seguintes normas RFC para SNMPv3:
 - 2570—Version 3 of the Internet Standard Network Management Framework;
 - 2571—Architecture for Describing SNMP Management Frameworks;
 - 2572—Message Processing and Dispatching for SNMP;
 - 2573—SNMPv3 Applications;
 - 2574/3414—User-based Security Model (USM) for version 3 SNMP;
 - 2575—View-based Access Control Model (VACM) for SNMP;
 - 2576—Coexistence between SNMP versions;



3586—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.

1.2.5.4 Chassis Virtual

- 1.2.5.4.1 Número de switches físicos que podem constituir 1 chassis virtual:8.
- 1.2.5.4.2 Número de peers Virtual Fabric link:2.
- 1.2.5.4.3 Número de portas membro por link Virtual Fabric: 8.
- 1.2.5.4.4 Portas suportadas para VFL: 40G e 100G.

1.2.5.5 NTP

- 1.2.5.5.1 Os equipamentos terão que suportar RFC 5905—Network Time Protocol v4.
- 1.2.5.5.2 Número de servidores NTP por cliente:12.
- 1.2.5.5.3 Número de associações: 512.

1.2.5.6 Nível 2 (Layer 2)

- 1.2.5.6.1 Os equipamentos terão que suportar as seguintes normas IEEE:
 - 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD);
 - 802.3z (1000Base-X);
 - 802.3ae (10Gbase-X);
 - 802.3ba (40GBase-X);
 - 802.3az (Energy Efficient Ethernet).
- 1.2.5.6.2 Suporte 802.1Q Hardware tagging.
- 1.2.5.6.3 Os equipamentos terão que suportar Interfaces de 1/10/40/100Gbps e suportar Jumbo frames de 9216bytes.
- 1.2.5.6.4 Suporte MAC Sec.

1.2.5.7 Unidirectional Link Detection (UDLD)

Os equipamentos terão de suportar Unidirectional Link Detection(UDLD).

- 1.2.5.7.1 Número de portas UDLD por sistema: 128.
- 1.2.5.7.2 Número de vizinhos UDLD por portas:32.

1.2.5.8 Source learning

Os equipamentos terão de suportar o seguinte RFC: 2674—Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions.

O número de endereços MAC apreendidos quando o modo Source learning centralizado está ativo deverá ser pelo menos de 64000 (switch mode).

1.2.5.9 VLAN

- 1.2.5.9.1 Os equipamentos terão que suportar o RFC 2674.
- 1.2.5.9.2 Os equipamentos terão que suportar as seguintes normas IEEE:
 - 802.1Q – Virtual Bridged Local Area Networks;
 - 802.1D – Media Access Control Bridges.
- 1.2.5.9.3 Os equipamentos terão de suportar pelo menos:



- Número de vlans por VC: 4094;
- Número de tagged vlans por porta: 4093;
- Número de VLAN untagged por porta: 1.

1.2.5.10 VLAN de alta disponibilidade

As VLANs de alta disponibilidade permitem que seja enviado tráfego destinado a um endereço MAC a várias portas do switch.

Os equipamentos terão que suportar 16 VLAN de alta disponibilidade por chassis virtual.

1.2.5.11 Spanning Tree

Os equipamentos terão de suportar as seguintes normas IEEE:

- 802.1d—Media Access Control (MAC) Bridges;
- 802.1s—Multiple Spanning Trees;
- 802.1w—Rapid Spanning Tree Protocol.

Os equipamentos terão que suportar:

- Modos de operação SpanningTree:
 - o Modo Flat – 1 instância spanning tree por chassis virtual;
 - o Modo por VLAN – 1 instância spanning tree por VLAN.
- Elegibilidade de port Spanning Tree: Portas fixas, portas 802.1Q tagged e portas Link aggregate
- Número de instâncias spanning tree VLAN por chassis virtual:100;
- Número de instâncias Multiple Spanning Tree Instances (MSTI) modo flat por chassis virtual: 16 adicionais à instância de spanning tree interna e comum (MSTI0).

1.2.5.12 SPB

1.2.5.12.1 Os equipamentos terão que suportar IEEE802.1aq Shortest Path Bridging (SPB-M) nomeadamente as seguintes normas:

- IEEE
 - 802.1aq/D3.6: Draft February 10, 2011—Virtual Bridged Local Area Networks-Amendment 9: Shortest Path Bridging;
 - 802.1ah/D4.2: DRAFT March 26, 2008— Virtual Bridged Local Area Networks–Amendment 6: Provider Backbone Bridging.

-IETF

- draft-ietf-isis-ieee-aq-05.txt—ISIS Extensions Supporting IEEE 802.1aq Shortest Path Bridging;
- IETF draft—IP/IPVPN services with IEEE 802.1aq SPBB networks;
- IETF draft—IP/IPVPN services with IEEE 802.1aq SPB networks.

1.2.5.12.2 Os equipamentos terão que suportar o modo SPBM (MAC-in-MAC).

1.2.5.12.3 Os equipamentos terão que disponibilizar IP sobre SPBM:

- IPv4 (VPN-Lite e VPN L3);
- Mapeamento VRF-to-ISID (um a um, um a vários).



- 1.2.5.12.4 Terão que suportar uma instância de SPB-ISIS por chassis virtual.
- 1.2.5.12.5 Terão que suportar 16 BVLAN por chassis virtual.
- 1.2.5.12.6 Terá de suportar 70 adjacências IS-IS.
- 1.2.5.12.7 Número de identificadores de instâncias (I-SID) por virtual chassis: 2000.
- 1.2.5.12.8 Número máximo de VLAN ou SVLAN por I-SID: 2000.
- 1.2.5.12.9 O tamanho da MTU nos serviços SPB que os equipamentos terão de suportar é de 9000.

1.2.5.13 Detecção Loopback

Os equipamentos terão de suportar Loopback detection, Edge (Bridge) e SAP(Access).

- 1.2.5.13.1 Temporizador de transmissão: 5 a 600 segundos.
- 1.2.5.13.2 Temporizador de auto-recover: 30-86400 segundos.

1.2.5.14 Agregação de links estático

Os equipamentos terão de suportar agregação de links estáticos.

- 1.2.5.14.1 Número de grupos de agregação de links:128;
- 1.2.5.14.2 Número de portas por grupo de link aggregate:16.

1.2.5.15 Agregação de links dinâmico

Os equipamentos terão de suportar as especificações IEEE - 802.1ax/802.3ad—Aggregation of Multiple Link Segments.

- 1.2.5.15.1 Número de grupo de agregação de links:128.
- 1.2.5.15.2 Número de portas por grupo de agregação de link:16.

1.2.5.16 Dual Home Link

Os equipamentos terão de suportar Dual-Home Link (1 sessão).

1.2.5.17 ERP

- 1.2.5.17.1 Os equipamentos terão de suportar:
 - ITU-T G8032 03/2010 – Ethernet Ring Protection version 2 ((Multi Rings and Ladder networks).
 - ITU-T Y.1731/IEEE802.lag – Pacote ERP de acordo com o formato PDU OAM para CCM.
- 1.2.5.17.2 Número máximo de anéis por nó: 64.
- 1.2.5.17.3 Número máximo de nós por anel:16.
- 1.2.5.17.4 Número máximo de VLANs por portas:4094.
- 1.2.5.17.5 Intervalo de identificadores de anel: 1 – 2147483647.
- 1.2.5.17.6 Intervalo para remote MEPID: 1-8191.
- 1.2.5.17.7 Intervalo de valores para o temporizador wait-to restore:1-12minutos.
- 1.2.5.17.8 Intervalos de valores para guard timer: 1- 200 centésimas de segundo.



1.2.5.17.9 Multiple VLAN Registration Protocol (MVRP)

Os equipamentos terão de suportar Multiple VLAN Registration Protocol (MVRP) tal como definido nas normas IEEE 802.1ak-2007 Amendment 7: Multiple Registration Protocol e IEEE 802.1Q-2005 Corrigendum 2008.

O número de VLAN utilizando MVRP a suportar deverá ser de 512.

1.2.5.17.10 IEEE 802.1AB LLDP

Os equipamentos terão que suportar LLDP cumprindo a norma IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery e as seguintes especificações:

- Número máximo de políticas de rede que podem ser associados com a porta: 8;
- Número máximo de políticas de rede que podem ser configurados por chassis virtual: 32.

1.2.5.17.11 IPv4

1.2.5.17.11.1 Os equipamentos terão de suportar os seguintes RFC:

- 791—Internet Protocol;
- 792—Internet Control Message Protocol;
- 826—An Ethernet Address Resolution Protocol;
- 2784—Generic Routing Encapsulation (GRE);
- 2890—Key and Sequence Number Extensions to GRE (extensions defined are not supported);
- 1701—Generic Routing Encapsulation (GRE);
- 1702—Generic Routing Encapsulation over IPV4 Networks;
- 2003—IP Encapsulation within IP.

1.2.5.17.11.2 Os equipamentos terão de suportar os seguintes itens:

- Número de interfaces de router por Sistema: 4000;
- Número de interfaces de router por vlan: 16;
- Número de rotas de hardware: 12000 (switch mode);
- Número de entradas de hardware ARP: 24000 (modo switch);
- Número máximo de interfaces de tuneis GRE por sistema: 127;
- Número máximo de interfaces túnel IPIP por chassis virtual: 127;
- Número máximo de gateways ECMP: 16

1.2.5.17.11.3 VRF (Virtual Routing and Forwarding)

1.2.5.17.11.3.1 Os equipamentos terão que suportar múltiplos VRF por cada equipamento permitindo configurar instâncias de routing separadas no mesmo equipamento. Cada instância de routing terá que manter independentemente o seu routing e table de forwarding, peer e informação de interface.

1.2.5.17.11.3.2 Os equipamentos terão que suportar:

- Protocolos de routing suportados (VRF): Estático, IPv4, RIPv2, OSPFv2, BGP4;
- Número de instância VRF por vlan: 1;
- Número de instâncias routing VRF OSPFv2 por chassis virtual: 16;
- Número de instâncias routing RIPv2 por chassis virtual: 16;
- Número de instâncias routing VRF BGP por chassis virtual: 32.

1.2.5.17.12 IPv6

1.2.5.17.13 Os equipamentos terão de suportar os seguintes RFC:

- 1981—Path MTU Discovery for IP version 6;
- 2375—IPv6 Multicast Address Assignments;
- 2460—Internet Protocol, Version 6 (IPv6) Specification;
- 2464—Transmission of IPv6 Packets over Ethernet Networks;
- 2465—Management Information Base for IP Version 6: Textual Conventions and General Group;
- 2466—Management Information Base for IP Version 6: ICMPv6 Group;
- 2711—IPv6 Router Alert Option;



- 3056—Connection of IPv6 Domains via IPv4 Clouds;
- 3484—Default Address Selection for Internet Protocol version 6 (IPv6);
- 3493—Basic Socket Interface Extensions for IPv6;
- 3542—Advanced Sockets Application Program Interface (API) for IPv6;
- 3587—IPv6 Global Unicast Address Format;
- 3595—Textual Conventions for IPv6 Flow Label;
- 3596— DNS Extensions to Support IP Version 6;
- 4007—IPv6 Scoped Address Architecture;
- 4022—Management Information Base for the Transmission Control Protocol (TCP);
- 4113—Management Information Base for the User Datagram Protocol (UDP);
- 4193—Unique Local IPv6 Unicast Addresses;
- 4213—Basic Transition Mechanisms for IPv6 Hosts and Routers;
- 4291—IP Version 6 Addressing Architecture;
- 4294—IPv6 Node Requirements;
- 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification;
- 4861—Neighbor Discovery for IP version 6 (IPv6);
- 4862—IPv6 Stateless Address Autoconfiguration;
- 5095—Deprecation of Type 0 Routing Headers in IPv6;
- 5453—Reserved IPv6 Interface Identifiers;
- 5722—Handling of Overlapping IPv6 Fragments.

1.2.5.17.14 Os equipamentos terão que suportar:

- Número de Interfaces IPv6: 4096
- Túneis 6to4: 1;
- Número de túneis configurados: 255;
- Número de Hosts IPv6 (Neighbor Discovery): 12000 (switch mode);
- Número de endereços unicast global IPv6 ou anycast: 10000;
- Número de endereços unicast global IPv6 por interface IPv6: 50;
- Número de rotas hardware IPv6 (sem rotas IPv4 presentes): 6000 (64-bit) e 1000 (128-bit);
- Número de rotas estáticas IPv6 (incluindo rotas black hole): 512;
- Número de Peers RIPng:20;
- Número de interfaces RIPng:20;
- Número de rotas RIPng: 5000;
- Número de gateways ECMP:16;

1.2.5.18 Especificações IP Sec

Os equipamentos terão de suportar IPSEC sobre IPv4 e IPv6 cumprindo os seguintes RFC:

- 4301—Security Architecture for the Internet Protocol;
- 4302—IP Authentication Header (AH);
- 4303—IP Encapsulating Security Payload (ESP);
- 4305—Cryptographic Algorithm Implementation Requirements for ESP and AH;
- 4308—Cryptographic Suites for IPsec.

Algoritmos suportados para ESP: NULL, 3DES-CBC e AES-CBC;

Tamanhos das chaves suportados pelos algoritmos de cifragem:

- 3DES-CBC - 192 bits;
- AES-CBC – 128, 192, ou 256 bits;

Algoritmos de autenticação suportados para AH:

- HMAC-SHA1-96, HMAC-MD5-96, e AES-XCBC-MAC-96, HMAC-SHA256;
- HMACSHA384, HMAC-SHA512;



Tamanho das chaves suportados para os algoritmos de autenticação:

- HMAC-MD5 - 128 bits;
- HMAC-SHA1 - 160 bits;
- AES-XCBC-MAC - 128 bits.

Formato da chave mestra de segurança: Hexadecimal (16bytes) ou String (16 caracteres).

Intervalos de valores de prioridades para políticas IPsec: 1-1000 (1 = alta prioridade 1000 = baixa prioridade).

Intervalo de valores para regra das políticas IPsec: 1-10;

Intervalo SPI: 256-999999999;

Modos suportados: Transporte.

1.2.5.19 Especificações RIP

1.2.5.19.1 Os equipamentos terão de suportar os seguintes RFCs:

- RFC 1058–RIP v1;
- RFC 2453–RIP v2;
- RFC 1722–RIP v2 Protocol Applicability Statement;
- RFC 1724–RIP v2 MIB Extension;
- RFC 2080–RIPng for IPv6 RFC 2082–RIP-2 MD5 Authentication.

1.2.5.19.2 Especificações RIP que os equipamentos terão de suportar:

- Número de interfaces: 10;
- Número de peers: 100;
- Número de rotas: 10000;

1.2.5.20 Bidirectional Forwarding Detection (BFD)

1.2.5.20.1 Os equipamentos terão que suportar o protocolo BFD.

1.2.5.20.2 Terão que suportar os RFC seguintes:

- 5880—Bidirectional Forwarding Detection;
- 5881—Bidirectional Forwarding Detection for IPv4 and IPv6 (Single Hop);
- 5882—Generic Application of Bidirectional Forwarding Detection.

1.2.5.20.3 Os equipamentos terão que suportar:

- Número de sessões BFD:
- Chassis: 32;
- Virtual Chassis: 100;
- Protocolos: BGP, OSPF, VRRP Remote Address Tracking e rotas estáticas.
- Modos:
- Assíncrono;
- Echo.

1.2.5.21 Especificações DHCP Relay/Snooping

Os equipamentos terão que suportar os seguintes RFCs e as seguintes especificações:

- 0951—Bootstrap Protocol;
- 1534—Interoperation between DHCP and BOOTP;
- 1541—Dynamic Host Configuration Protocol;
- 1542—Clarifications and Extensions for the Bootstrap Protocol;
- 2132—DHCP Options and BOOTP Vendor Extensions;
- 3046—DHCP Relay Agent Information Option, 2001.

Implementação DHCP relay:

- DHCP global;



- DHCP por Vlan.
- Serviço DHCP Relay: BOOTP/DHCP (Bootstrap Protocol/Dynamic Host Configuration Protocol)
- Número dos portos:
 - 67 para os pedidos
 - 68 para as respostas.
- Número de endereços IP suportados por cada serviço de relay: 1536;
- Número de endereços suportados em modo interface: 1536;
- Número de serviço relay UDP por chassis virtual: 30;
- Número de vlans em que o serviço de forward UDP é permitido: 256;
- Número de VLAN de entradas de filtragem por IP origem:
 - 32 VLANs com 223 clientes;
 - 16 VLANs com 239 clientes;
 - 8 VLANs com 247 clientes;
 - 4 VLANs com 251 clientes.

1.2.5.22 Especificações DHCPv6 Relay / Snooping

Os equipamentos terão que suportar:

- RFC 3315 – Dynamic Host Configuration Protocol for Ipv6 (DHCPv6).
- Implementação de relay DHCP por VLAN DHCP
- Número dos portos destino UDP:
 - 547 - DHCPv6 messages to a DHCPv6 Server ou Relay Agent
 - 546 - DHCPv6 messages to a Client
- Número de destinos de relay por interface de relay DHCPv6:5;
- Número Vlan snooping DHCPv6 (por VLAN mode):64;
- Número de VLANs guard DHCPv6: 64;
- Número de serviços Relay UDP IPv6 genéricos:8;
- Número de portas relay UDP IPv6:8;
- Número de destino UDP IPv6 por porta:8.

1.2.5.23 Servidor DHCP

1.2.5.23.1 Os equipamentos terão que suportar a funcionalidade de servidor de DHCP cumprindo os seguintes RFC:

- RFC 2131—Dynamic Host Configuration Protocol;
- RFC 3315—Dynamic Host Configuration Protocol for IPv6;
- RFC 950—Internet Standard Subnetting Procedure;
- RFC 868—Time Protocol;
- RFC 1035—Domain Implementation and Specification;
- RFC 1191—Path MTU Discovery.

1.2.5.23.2 Implementação de servidor DHCP server: BOOTP/DHCP

1.2.5.23.3 Mecanismos de disponibilização de endereços:

- BootP estático;
- DHCP estático;
- DHCP dinâmico.

1.2.5.23.4 Os equipamentos terão que suportar:

- Número de leases: 8000;
- Tamanho de informação de lease: 375k.

1.2.5.24 Virtual Router Redundancy Protocol

1.2.5.24.1 Os equipamentos terão que suportar Virtual Router Redundancy Protocol.

1.2.5.24.2 Os RFC que terão de ser suportados são os seguintes:



- RFC 3768—Virtual Router Redundancy Protocol;
- RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol;
- RFC 5798 - Virtual Router Redundancy Protocol (VRRP) Version 3 para IPv4 e IPv6;
- RFC 6527 - Definitions of Managed Objects para VRRP Version 3 (VRRPv3) IPv6.

1.2.5.24.3 Especificações VRRP que os equipamentos terão de suportar:

- Número de routers virtuais VRRPv2 e VRRPv3: 255;
- Número de endereços IP por instância: 16.

1.2.5.25 Server Load balacing

1.2.5.25.1 Os equipamentos terão de suportar Server load balacing.

1.2.5.25.2 Número de clusters:32;

1.2.5.25.3 Número de servidores físicos por cluster:32;

1.2.5.25.4 Classificação layer 3:

- Endereço IP destino;
- Condição de política de QoS.

1.2.5.25.5 Classificação Layer 2: - Condição de política de QoS.

1.2.5.25.6 Verificação do estado do servidor: Ping, verificação de link.

1.2.5.25.7 Suporte de alta disponibilidade: Hardware-based failover, VRRP, Chassis Management Module(CMM) redundancy.

1.2.5.25.8 Protocolos de rede a suportar: Endereço IP virtual.

1.2.5.26 Especificações IPMS

1.2.5.26.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 1112—Host Extensions for IP Multicasting
- RFC 2236—Internet Group Management Protocol, Version 2
- RFC 2710—Multicast Listener Discovery (MLD) for IPv6
- RFC 2933—Internet Group Management Protocol MIB
- RFC 3019—IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
- RFC 3376—Internet Group Management Protocol, Version 3
- RFC 3810—Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4541—Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4604—Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.

1.2.5.26.2 Os equipamentos terão de suportar as seguintes versões de IGMP: IGMPv1, IGMPv2, IGMPv3.

1.2.5.26.3 Número de fluxos multicast IPv4 (switched): 40000.

1.2.5.26.4 Número de fluxos multicast IPV4 (*,G routed): 12000.

1.2.5.26.5 Número de fluxos multicast IPV4 (S,G routed): 12000.

1.2.5.27 IPMSv6

1.2.5.27.1 Os equipamentos terão de suportar os seguintes RFC:



- RFC 2710—Multicast Listener Discovery for IPv6
- RFC 3019—IPv6 MIB for Multicast Listener Discovery Protocol
- RFC 3306—Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3810—Multicast Listener Discovery Version 2 for IPv6
- RFC 4541—Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4604—Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.

- 1.2.5.27.2 Os equipamentos terão de suportar as seguintes versões de MLD: MLDv1, MLDv2.
- 1.2.5.27.3 Intervalo de Query MLD: 1 a 65535 segundos.
- 1.2.5.27.4 MLD Router timeout: 1 a 65535 segundos.
- 1.2.5.27.5 MLD Source timeout: 1 a 65535 segundos.
- 1.2.5.27.6 MLD Query Response Interval: 1-65535 milisegundos.
- 1.2.5.27.7 MLD Last Member Query Interval: 1-65535 milisegundos.
- 1.2.5.27.8 Número de fluxos multicast IPv6 (switched): 20000.
- 1.2.5.27.9 Número de fluxos multicast IPV6 (*,G routed): 6000.
- 1.2.5.27.10 Número de fluxos multicast IPV6 (S,G routed): 6000.

1.2.5.28 QoS

- 1.2.5.28.1 Os equipamentos terão que suportar as seguintes especificações:
- Número de condições de políticas (conditions hardware): 3072;
 - Número de ações de políticas: 3072;
 - Número de grupos (rede, MAC, serviço, porta): 3072;
 - Número de entradas de grupo: 1024 por grupo (256 por grupo de serviço);
 - Número máximo de filas CoS por porta: 8;
 - Perfis Queue Set (QSP): 4;
 - Número de listas de políticas QoS: 32.

1.2.5.29 LDAP Policy Server

- 1.2.5.29.1 Os equipamentos terão que suportar os seguintes RFCs:
- RFC 2251—Lightweight Directory Access Protocol (v3);
 - RFC 3060—Policy Core Information Model—Version 1 Specification.
- 1.2.5.29.2 Número de policy servers (suportados num chassis virtual): 5.
- 1.2.5.29.3 Número de policy servers (suportados por PolicyView): 1.

1.2.5.30 Servidor de autenticação

- 1.2.5.30.1 Os equipamentos terão de suportar os seguintes RFCs:
- RFC 2865—Remote Authentication Dial In User Service (RADIUS);
 - RFC 2866—RADIUS Accounting;
 - RFC 2867—RADIUS Accounting Modifications for Tunnel Protocol Support;
 - RFC 2868—RADIUS Attributes for Tunnel Protocol Support;
 - RFC 2809—Implementation of L2TP Compulsory Tunneling through RADIUS;
 - RFC 2869—RADIUS Extensions;
 - RFC 2548—Microsoft Vendor-specific RADIUS Attributes;
 - RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices;
 - RFC 1492—An Access Control Protocol;
 - RFC 1789—Connectionless Lightweight X.5000 Directory Access Protocol;
 - RFC 2247—Using Domains in LDAP/X.500 Distinguished Names;



- RFC 2251–Lightweight Directory Access Protocol (v3);
- RFC 2252–Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions;
- RFC 2253–Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names;
- RFC 2254–The String Representation of LDAP Search Filters
- RFC 2256–A Summary of the X.500(96) User Schema for Use with LDAPv3;
- RFC 2574–User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
- RFC 2924–Accounting Attributes and Record Formats;
- RFC 2975–Introduction to Accounting Management;
- RFC 2989–Criteria for Evaluating AAA Protocols for Network Access.

1.2.5.30.2 Os equipamentos terão de suportar:

- Número de servidores autenticação no modo de autoridade única (single authority): 8;
- Número de servidores de autenticação no modo de autoridade múltipla:8;
- Número de servidores por cada switch autenticado:8.

1.2.5.31 Universal Network Profiles (UNP)

Os equipamentos terão de suportar Universal Network Profiles (UNP) com as seguintes características:

- Número de UNPs por chassis virtual: 4000;
- Número de utilizadores UNP por chassis:2000;
- Número de utilizadores por chassis virtual:2000;
- Tipo de autenticação: Por MAC e 802.1x;
- Tipo de perfil: VLAN e SPB.
- Tipo de porta UNP: Bridge e acesso;
- Número de lista de políticas de QoS por chassis virtual: 32 (incluindo a lista por defeito);
- Número de lista de políticas de QoS por UNP:1.

1.2.5.32 Access Guardian

1.2.5.32.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 2284–PPP Extensible Authentication Protocol (EAP);
- RFC 2865–Remote Authentication Dial In User Service (RADIUS);
- RFC 2866–RADIUS Accounting;
- RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support;
- RFC 2868–RADIUS Attributes for Tunnel Protocol Support;
- RFC 2869–RADIUS Extensions;
- RFC 3576--Change of Authorization-Request (COA) and Disconnect request (DM) for BYOD. RFC support is limited to ClearPass solution;
- RFC 3579–RADIUS Support for EAP.

1.2.5.32.2 Os equipamentos terão de suportar as seguintes normas IEEE:

- IEEE 802.1X-2001–Standard for Port-based Network Access Control;
- 802.1X RADIUS Usage Guidelines.

1.2.5.32.3 Métodos de autenticação que tem de suportar:

- 802.1X;
- Endereços MAC;
- Portal Captivo.

1.2.5.32.4 Número de utilizadores access guardian (sistema): 1000.

1.2.5.32.5 Número de utilizadores em quarentena por QMR: 1000.

1.2.5.32.6 Número de utilizadores médio permitidos para login no portal captativo num dado instante:40.



- 1.2.5.32.7 Número de perfis de portal captativo:8.
- 1.2.5.32.8 Número de perfis AAA: 8.
- 1.2.5.32.9 Número de servidores de autenticação: 4 por tipo de autenticação (MAC, 802.1X, Portal Captativo).
- 1.2.5.32.10 Número de servidores de accounting: 4 por tipo de autenticação (MAC, 802.1X, Portal Captativo).

1.2.5.33 Port mapping

- 1.2.5.33.1 Port mapping é uma facilidade de segurança que controla a comunicação entre utilizadores peers. Os equipamentos deverão possuir esta facilidade.
- 1.2.5.33.2 Número de sessões de port mapping: 8.

1.2.5.34 Especificações de Learned port security (LPS)

- 1.2.5.34.1 Os equipamentos terão que suportar Learned port security (LPS).
- 1.2.5.34.2 Portas eligíveis para Learned Port Security: Fixas e 802.1Q tagged.
- 1.2.5.34.3 Portas não eligíveis para Learned Port Security: Portas agregadas e portas agregadas 802.1Q(trunked).
- 1.2.5.34.4 Número máximo de MAC apreendidas por porta LPS:1000.
- 1.2.5.34.5 Número máximo de endereços MAC filtrados permitidos por porta LPS:100.
- 1.2.5.34.6 Número máximo de intervalos de endereços MAC configuráveis por porta LPS:8.

1.2.5.35 Port Mirroring

Os equipamentos terão que suportar Port mirroring com as seguintes especificações:

- Número de Sessões de mirroring: 2;
- Número de sessões combinadas Mirroring /monitoring por chassis: 2;
- Suportar N to 1 Mirroring: 128 to 1;
- Número de Vlans RPMIR por sessão: 1.

1.2.5.36 Port monitoring

Os equipamentos terão que suportar Port monitoring com as seguintes especificações:

- Número de sessões a suportar:1;
- Sessões combinadas de mirroring/monitoring por chassis: 2;
- Tipo de ficheiro suportado: formato de ficheiro ENC (Network General Sniffer Network Analyzer Format).

1.2.5.37 SFlow

- 1.2.5.37.1 Os equipamentos terão de suportar SFlow e o RFC 3176.
- 1.2.5.37.2 Instância de receção/amostra/polling:2.
- 1.2.5.37.3 Amostragem:
 - tamanho de pacote;
 - tipo de trama;
 - Endereços MAC de origem e destino;
 - Vlans de origem e destino;
 - Endereços IP de origem e destino;



- Portos de origem e destino;
- Flags TCP e TOS.

1.2.5.37.4 Polling:

- Octetos de entrada;
- Octetos de saída;
- Número de pacotes unicast de receção;
- Número de pacotes unicast de transmissão;
- Número de pacotes multicast de receção;
- Número de pacotes multicast de transmissão;
- Número de pacotes de broadcast de receção;
- Número de pacotes de broadcast de transmissão;
- Erros de entrada;
- Erros de saída.

1.2.5.38 RMON

Os equipamentos terão de suportar o RFC 2819 - Remote Network Monitoring Management Information Base.

Funcionalidades suportadas:

- Implementação de grupo RMON4 básico;
- Grupo de estatísticas ethernet;
- Grupo (controlo e estatísticas) histórico;
- Grupo de Alarmes;
- Grupo eventos.

1.2.5.39 Estado do Switch (Switch Health)

1.2.5.39.1 Funcionalidade Health a suportar:

- Estatísticas de utilização de CPU ao nível do switch (percentagem);
- Estatísticas de entrada ao nível Switch/modulo/porta (percentagem);
- Estatísticas de utilização Entrada/saída ao nível do Switch/modulo/porta (percentagem);
- Estatísticas de utilização de memória ao nível do switch (percentagem);
- Estatísticas da temperatura ao nível de dispositivo (por exemplo, Chassis/CMM).

1.2.5.39.2 Monitorização do nível de utilização dos recursos:

- Nível de utilização mais recente;
- Nível de utilização média no último minuto;
- Nível de utilização na última hora;
- Nível de utilização máximo na última hora.

1.2.5.40 Vlan Stacking

1.2.5.40.1 Os equipamentos terão de suportar as seguintes normas IEEE:

- IEEE 802.1Q, 2003 Edition,
- IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks P802.1ad/D6.0 (C/LM) Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

1.2.5.40.2 Número de serviços: 4.

1.2.5.40.3 Número de SVLANs: 4000.

1.2.5.40.4 Número de SAPs: 8000.

1.2.5.40.5 Número de perfis SAP: 8000.

1.2.5.40.6 Número de VLANs de cliente (CVLANs) por chassis virtual: 3500.

1.2.5.40.7 Número de associações Service-to-SAP:1000.



1.2.5.41 Switch logging

Os equipamentos terão de suportar o seguinte RFC: RFC-5424 Syslog Protocol.

Número de servidores Syslog: 12.

Dispositivo de logging: Memória Flash/Consola/Endereço IP.

Tipos / Níveis de severidade:

- 2 (Alarm - highest severity),
- 3 (Error),
- 4 (Alert),
- 5 (Warning)
- 6 (Info - default),
- 7 (Debug 1),
- 8 (Debug 2),
- 9 (Debug 3 - lowest severity).

1.2.5.42 Ethernet OAM

1.2.5.42.1 Os equipamentos terão de suportar as seguintes normas:

- IEEE 802.1ag Version 8.1–Connectivity Fault Management;
- IEEE 802.1D–Media Access Control (MAC) Bridges;
- IEEE 802.1Q–Virtual Bridged Local Area Networks ITU-T Y.1731–OAM Functions and Mechanisms for Ethernet-Based Networks.

1.2.5.42.2 Número de domínios de manutenção (MD) por bridge:8.

1.2.5.42.3 Número de associações de manutenção (MA) por bridge: 128.

1.2.5.42.4 Número de end points de manutenção (MEP) por bridge:256.

1.2.5.42.5 Tamanho da base de dados MEP: 1000.

1.2.5.42.6 Intervalo mínimo CCM: 100ms.

1.2.5.43 Link OAM

Os equipamentos terão de suportar as normas IEEE e RFC seguintes:

- IEEE 802.3ah–EFM LINK OAM
- RFC 4878 - Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) functions on Ethernet-Like Interfaces.

1.2.5.44 Service Assurance Agent (SAA)

1.2.5.44.1 Os equipamentos terão de suportar o Service Assurance Agent (SAA).

Nota:O SAA utiliza a monitorização ativa para gerar tráfego de modo contínuo, fiável e de modo preditivo permitindo efetuar medidas de desempenho de rede.

1.2.5.44.2 Número de SAAs: 128.

1.2.5.44.3 Número de sessões SAA SPB: 128 (por BVLAN).

1.2.5.45 Routing avançado

Os equipamentos terão de suportar os seguintes protocolos dinâmicos:

- OSPF V2 e V3;
- IS-IS;
- BGP;

bem como protocolos de routing multicast.

1.2.5.46 Os equipamentos terão de suportar Open Shortest Path First (OSPF) v2



1.2.5.46.1 Os RFC que terão de ser suportados são os seguintes:

- 1370—Applicability Statement for OSPF;
- 4750—OSPF Version 2 Management Information Base;
- 2328—OSPF Version 2;
- 5250—The OSPF Opaque LSA Option;
- 3101—The OSPF Not-So-Stubby Area (NSSA) Option;
- 3623—Graceful OSPF Restart;
- 5709 - SPfv2 HMAC-SHA Cryptographic Authentication.

1.2.5.46.2 Especificações OSPFv2 que os equipamentos terão de suportar:

- Número de áreas: 10;
- Número de interfaces: 200;
- Número de interfaces passivas: 200;
- Número de entradas da base de Link State: 100000;
- Número máximo de vizinhos por router: 254;
- Número máximo de rotas: 32000;
- Número máximo de entradas next hop ECMP: 16.

1.2.5.47 Os equipamentos terão de suportar OSPF versão 3

1.2.5.47.1 RFC que terão de ser suportados:

- RFC 1826—IP Authentication Header ;
- RFC 1827—IP Encapsulating Security Payload;
- RFC 2553—Basic Socket Interface Extensions for IPv6;
- RFC 2373—IPv6 Addressing Architecture;
- RFC 2374—An IPv6 Aggregatable Global Unicast Address Format;
- RFC 2460—IPv6 base specification;
- RFC 2740—OSPF for IPv6.

1.2.5.47.2 Especificações OSPFv3 que os equipamentos terão de suportar:

- Número de áreas: 5;
- Número de interfaces: 128;
- Número de entradas na base de dados Link State: 20000;
- Número de vizinhos: 128;
- Número de rotas: 32000;
- Número de entrada ECMP next Hop: 16.

1.2.5.48 Os equipamentos terão de suportar Intermediate System to Intermediate System (IS-IS)

1.2.5.48.1 As normas que terão de ser suportados são os seguintes:

- 1142-OSI IS-IS Intra-domain Routing Protocol;
- 1195-OSI IS-IS for Routing in TCP/IP and Dual Environments;
- 3373-Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point- to-Point Adjacencies;
- 3567-Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication;
- 2966-Prefix Distribution with two-level IS-IS (Route Leaking) support;
- 2763-Dynamic Host name exchange support;
- 3719-Recommendations for Interoperable Networks using IS-IS;
- 3787-Recommendations for Interoperable IP Networks using IS-IS;
- 5308-IS-IS support for IPv6 (Routing IPv6 with IS-IS);
- IETF- draft-ietf-isis-igp-p2p-over-lan-05.txt-Point-to-point operation over LAN in link-state routing protocols.



1.2.5.48.2 Especificações IS-IS que os equipamentos terão de suportar:

- Número máximo de áreas por router: 3;
- Número máximo de adjacências L1 por interface por router: 70;
- Número máximo de adjacências L2 por interface por router: 70;
- Número máximo de interfaces IS-IS (por router): 70;
- Número máximo de entradas Link State Pack por adjacência: 255;
- Número máximo de rotas IS-IS: 24000;
- Número máximo de rotas L1 IS-IS: 12000;
- Número máximo de rotas L2 IS-IS: 12000.

1.2.5.49 Os equipamentos terão de suportar Border Gateway Protocol (BGP)

1.2.5.49.1 Os RFC que terão de ser suportados são os seguintes:

- 1771/4271—A Border Gateway Protocol 4 (BGP-4);
- 2439—BGP Route Flap Damping;
- 3392/5492—Capabilities Advertisement with BGP-4;
- 2385—Protection of BGP Sessions via the TCP MD5 Signature Option;
- 1997—BGP Communities Attribute;
- 4456—BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP);
- 3065—Autonomous System Confederations for BGP;
- 4273—Definitions of Managed Objects for BGP-4;
- 4486—Subcodes for BGP Cease Notification;
- 4760—Multiprotocol Extensions for BGP-4;
- 2545—Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing;
- 2918 – Route Refresh Capability for BGP-4;
- 4724 – Graceful Restart Mechanism for BGP;
- 6793 – BGP 4-octet ASN;
- 5668 – 4-Octet AS Specific BGP Extended Community;
- 2042 – Registering New BGP Attribute Types;
- 5396 – Textual Representation of Autonomous System (AS) Numbers.

1.2.5.49.2 Os equipamentos terão que ao nível do BGP suportar os seguintes atributos: Origin, AS Path, Next Hop (IPv4), MED, Local Preference, Atomic Aggregate, Aggregator (IPv4), Community, Originator ID, Cluster List, Multiprotocol Reachable NLRI (IPv6), Multiprotocol Unreachable NLRI (IPv6), AS4 Path, AS4 Aggregator (IPv4), e AS Specific Extended Community.

1.2.5.49.3 Especificações BGP que os equipamentos terão de suportar:

- Número máximo de peers por switch (32 peers por VRF): 512;
- Número máximo de redes: 4000;
- Número máximo de endereços agregados: 2000;
- Número máximo de rotas: 128000;
- Número máximo de políticas: 1000.

1.2.5.50 Multicast Boundary

1.2.5.50.1 Normas que os equipamentos terão de suportar:

- RFC 2365—Administratively Scoped IP Multicast;
- RFC 5132 - IP Multicast MIB.

1.2.5.50.2 Intervalo de endereços válidos: 239.0.0.0 to 239.255.255.255.

1.2.5.50.3 Intervalo de endereços extended Multicast route boundary: 224.0.0.0 to 239.255.255.255.

1.2.5.51 Distance Vector Multicast Routing Protocol (DVMRP)

1.2.5.51.1 Normas que os equipamentos terão de suportar:

- RFC 1075—Distance Vector Multicast Routing Protocol, Version 1;
- RFC 4087—IP Tunnel MIB 2715—Interoperability Rules for Multicast Routing Protocols;



- IEEE draft-ietf-idmr-dvmrp-v3-09.txt - Distance Vector Multicast Routing Protocol, Version 3.

1.2.5.51.2 Versão DVMRP que terá de ser suportada: DVMRPv3.255

1.3.5.51.3 Atributos DVMRP:

- Reverse Path Multicasting,
- Neighbor Discovery,
- Multicast Source Location,
- Route Report Messages,
- Distance metrics,
- Dependent Downstream Routers,
- Poison Reverse,
- Pruning, Grafting,
- DVMRP Tunnels.

1.2.5.51.4 Temporizadores DVMRP:

- Flash update interval,
- Graft retransmissions,
- Neighbor probe interval,
- Neighbor timeout,
- Prune lifetime,
- Prune retransmission,
- Route report interval,
- Route hold-down,
- Route expiration timeout.

1.2.5.51.5 Número de interfaces: 384 (combinados entre PIMv4, PIMv6 e DVMRP).

1.2.5.51.6 Protocolos multicast por interface:1.

1.2.5.52 Protocol-Independent Multicast (PIM)

Os equipamentos terão de suportar os seguintes RFCs:

- 2365—Administratively Scoped IP Multicast;
- 4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification;
- 4007—IPv6 Scoped IP Multicast;
- 5060—Protocol Independent Multicast MIB;
- 5132—IP Multicast MIB 3569—An Overview of Source-Specific Multicast (SSM);
- 3973—Protocol Independent Multicast-Dense Mode (PIM-DM);
- 5015 - Bidirectional Protocol Independent Multicast (BIDIR-PIM);
- 5059—Bootstrap Router (BSR) Mechanism for PIM;
- 5240—Protocol Independent Multicast (PIM) Bootstrap Router MIB;
- 2715—Interoperability Rules for Multicast Routing Protocols.

1.2.5.52.1 Versão PIM a suportar: PIM-SMv2.

1.2.5.52.2 Atributos PIM

- Shared trees (also referred to as RP trees);
- Designated Routers (DRs);
- Designated Forwarders (DFs);
- Bootstrap Routers (BSRs);
- Candidate Bootstrap Routers (C-BSRs);
- Rendezvous Points (RPs) (applicable only for PIM-SM) and BIDIR-PIM;
- Candidate Rendezvous Points (C-RPs).

1.2.5.52.3 Temporizadores a suportar:

- C-RP expiry,
- C-RP holdtime,
- C-RP advertisement,
- Join/Prune, Probe,



- Register suppression,
- Hello,
- Expiry,
- Assert,
- Neighbor liveness,
- DF Election Timer.

1.2.5.52.4 Número de interfaces: 384 (combinados entre PIMv4, PIMv6 e DVMRP).

1.2.5.52.5 Rendezvous Point (RP):100.

1.2.5.52.6 Bootstrap Routers (BSRs): 1.

1.2.5.52.7 1.56.7 Protocolos multicast por interface:1.

1.2.5.52.8 1.56.8 Anycast RP Routers: 8.

1.2.5.52.9 MBR

1.2.5.52.9.1 Os equipamentos terão de suportar os seguintes RFCs:

- 4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification;
- 3973—Protocol Independent Multicast-Dense Mode (PIM-DM);
- 2715—Interoperability Rules for Multicast Routing Protocols.

1.2.5.52.9.2 Os equipamentos terão de suportar os seguintes IETF Internet-Drafts: draft-ietf-idmr-dvmrp-v3-09.txt - Distance Vector Multicast Routing Protocol, Version 3.

1.2.5.52.9.3 Interoperabilidade MBR: DVMRP interoperabilidade com IPv4 PIM (PIM-SM e PIM-DM).

1.2.6 OS6860E-24

1.2.6.1 Características principais do Equipamento

O equipamento a fornecer terá de suportar as seguintes características:

- Switch Layer 3 de 1U;
- Co processador para serviços avançados;
- Portas óticas: 24 100/1000Base RJ45;
- Portas SFP+ 1G/10G: 4;
- Portas Stacking 20G: 2;
- Portas USB: 1;
- Portas RS232: 1;
- Porta de Consola: 1;
- Fontes de alimentação: 1 +1 (backup);
- RAM: 2GB;
- Sem ventoinhas.
- Flash para Sistema de ficheiros: 2GB;
- Capacidade máxima "raw fabric": 224 Gb/s;
- Transferência (pacotes de 64 bytes):154,9 Mpps;
- Consumo máximo:72,2W.
- Altitude: 2 000m
- Temperatura em operação:0°C a 45°C;
- Humidade: 5% a 95% sem condensação.

Terão de incluir todo o licenciamento associado a funcionalidades (Advanced Routing) e ao centro de gestão existente na IP.

As restantes características estão expressas no ponto 1.3.2.2 a 1.3.2.41 do modelo OS6860E-U28.

1.2.7 Acessórios para os equipamentos OS6860N-U28 e OS6860E-24

1.2.7.1 Fonte de alimentação AC - OS6860-BP

Fonte alimentação AC para OS6860 com uma potência máxima de saída de 150W e corrente máxima de 12,5A, suportando uma tensão de entrada de 180V a 264 V AC/1,5A, e frequência de entrada entre 47Hz e 63Hz.

1.2.7.2 Fonte de alimentação DC - OS6860-BP-D

Fonte alimentação DC para OS6860 com uma potência máxima de saída de 150W e corrente máxima de 12,5A, suportando uma tensão de entrada de -36V a -72 V DC.



1.2.7.3 Cabo Virtual Chassis para OS6860 de 40 cm ou 1m (DAC cables for VC).

Cabo que permita agregar dois switches OS6860 em chassis virtual. Terá de ser fornecido o conjunto de cabos necessário para o estabelecimento desse chassis virtual.

1.2.8 OS6865-U28X

OS6865-U28X ou equivalente: Switch Industrial Gigabit Ethernet L3 de 1 U sem ventoinhas com capacidade de funcionar em ambientes com condições adversas.

Terá de ser fornecido com uma fonte de alimentação AC (OS6865-BP) e com uma fonte alimentação DC (OS6865-BP-D) bem como todo o licenciamento de funcionalidade bem como para o Omnivista 2500 existente na IP.

E com as seguintes características:

- Possuir 20 portas SFP Base X 4 portas fixas SFP+ (1G/10G), 4 portas HPOE 75w 10/100/1000Base-T e duas portas 20G VFL QSFP+;
- Temperatura de funcionamento: -40° a + 74°C;
- Humidade em operação: 5 a 95%;
- Capacidade de software rollback;
- Hot Swapping de fontes de alimentação e SFPs;
- Montagem em rack 19”;
- O equipamento terá de possuir uma fonte AC OS6865-BP ou equivalente e uma fonte DC OS6865-BP-D ou equivalente, Prateleira (power shelf), cabo de alimentação manual de utilizador e acessórios de montagem em rack;
- Ser totalmente gerido através da plataforma de gestão Omnivista 2500 existente na IP;
- Incluir todo o licenciamento associado a funcionalidades nomeadamente AOS com Advance IP routing e ao centro de gestão existente na IP;
- Proteção contra sobretensões nas portas UTP: 6KV;
- Capacidade de comutação: 208 Gbps;
- 28 Portas com capacidade 1588v2;
- Número de Vlans: 4 000;
- Número de MACs por sistema: 48 000;
- Terá de suportar Jumbo frames: 9216 bytes (1/10Gb/s);
- Número de rotas IPv4: 64 000;
- O equipamento terá de suportar a funcionalidade de virtual Chassis no mínimo duas unidades.
- O equipamento terá que suportar:
 - SNMPv1/2/3 através IPv4/IPv6
 - IEEE802.1AB – Layer Discover Protocol(LLDP)
 - NTP
 - DHCP v4 e DHCPv6
 - Remote Virtual Chassis até 10Km
 - ITU-T G.8032/Y1344 2010: Ethernet Ring Protection
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) encompasse IEEE 802.1D Spanning Tree Protocol (STP) and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Per-VLAN spanning tree (PVST+) and 1x1 STP mode
- IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules
- Dual-home link support for sub-second link protection without STP
- Virtual Router Redundancy Protocol (VRRP) with tracking capabilities
- IEEE protocol auto-discovery
- Bidirectional Forwarding Detection (BFD) for fast failure detection and reduced re-convergence times in a IPv4/IPv6 routed environment



- Split Virtual Chassis protection: Autodetection and recovery of Virtual Chassis splitting due to one or more VFL or stack element failures
- Controlo de Acesso
 - Autosensing IEEE 802.1X multi-client
 - Multi-VLAN support
 - MAC-based authentication for non-IEEE 802.1X hosts
 - Web based authentication (captive portal): a customizable web portal residing on the switch
- User Network Profile (UNP) simplifies NAC by dynamically providing pre-defined policy configuration to authenticated clients — VLAN, ACL, BW
- Secure Shell (SSH) with public key infrastructure (PKI) support
- Terminal Access Controller Access-Control System Plus (TACACS+) client
- Centralized Remote Access Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication
- Centralized RADIUS for device authentication and network access control authorization
- Learned Port Security (LPS) or MAC address lockdown
- Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)
- DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection
- ARP poisoning detection
- QoS
 - Priority queues: Eight hardware-based queues per port for flexible QoS management
 - Traffic prioritization: Flow-based QoS Flow-based traffic policing and bandwidth management
 - 32-bit IPv4/128-bit IPv6 non-contiguous mask classification
 - Egress traffic shaping
 - DiffServ architecture
 - Congestion avoidance: Support for end to end head-of-line (E2E-HOL) blocking prevention, IEEE 802.1Qbb Priority-based Flow Control (PFC) and IEEE 802.3x Flow Control (FC)
- Routing IPv4
 - Multiple VRF & inter-VRF route leaking
 - Static routing
 - Routing Information Protocol (RIP) v1 and v2
 - Open Shortest Path First (OSPF) v2 with Graceful Restart
 - Intermediate System to Intermediate System (IS-IS) with Graceful Restart
 - Border Gateway Protocol (BGP) v4 with Graceful Restart
 - Generic Routing Encapsulation (GRE) and IP/IP tunneling
 - Virtual Router Redundancy Protocol (VRRPv2)
 - DHCP relay (including generic UDP relay)
 - Address Resolution Protocol (ARP)
 - Policy-based routing and server load balancing
 - DHCPv4 server
- Routing IPv6
 - Multiple VRF & Inter-vrf route leaking
 - Internet Control Message Protocol version 6 (ICMPv6)
 - Static routing
 - Routing Information Protocol Next Generation (RIPng)
 - Open Shortest Path First (OSPF) v3 with Graceful Restart
 - Intermediate System to Intermediate System (IS-IS) with Graceful Restart
 - Multi-Topology IS-IS (M-ISIS)
 - BGP v4 multiprotocol extensions for IPv6 routing (MP-BGP)
 - Graceful Restart extensions for OSPF and BGP
 - Virtual Router Redundancy Protocol version 3 (VRRPv3)
 - Neighbor Discovery Protocol (NDP)



- Policy-based routing and server load balancing
- DHCPv6 server
- DHCPv6 Relay Agent
- Multicast IPv4/IPv6
 - Internet Group Management Protocol (IGMP) v1/v2/v3 snooping
- Protocol Independent Multicast – SparseMode (PIM-SM), Source Specific Multicast (PIM-SSM)
- Protocol Independent Multicast – DenseMode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir)
 - Distance Vector Multicast Routing Protocol (DVMRP)
 - Multicast Listener Discovery (MLD) v1/v2 snooping
 - PIM to DVMRP gateway support
- Serviços Layer 2 avançados
- Ethernet services support using IEEE 802.1ad Provider Bridges (also known as Q-in-Q or VLAN stacking)
 - Fabric virtualization services IEEE 802.1aq Shortest Path Bridging (SPB-M)
 - Ethernet network-to-network interface (NNI) and user network interface (UNI)
 - Service Access Point (SAP) profile identification
 - Service VLAN (SVLAN) and Customer VLAN (CVLAN) support
 - VLAN translation and mapping including CVLAN to SVLAN
 - Port mapping
 - DHCP Option 82: Configurable relay agent information
 - Multiple VLAN Registration Protocol (MVRP)
 - HA-VLAN for Layer 2 clusters such as MS-NLB and active-active Firewall clusters
 - Jumbo frame support
 - Bridge Protocol Data Unit (BPDU) blocking
 - STP Root Guard
 - STP Loop-Guard
 - Loopback Detection to auto-detect and prevent L2 loops
- Recomendação ITU-T
 - ITU-T G.8032/Y.1344 2010: Ethernet Ring Protection (ERPV2)
- Normas a suportar:
- Ambiente Industrial
 - IEC 60870-2-2 (operational temperature)
 - IEC 60068-2-1 (temperature type test– cold)
 - IEC 60068-2-2 (temperature type test– hot)
 - IEC 60721-3-1: Class 1K5 (storage temperature)
 - IEC 60068-2-30: 5% to 95% noncondensing humidity
 - IEC 60255-21-2 (mechanical shock)
 - IEC 60255-21-1 (vibration)
- Segurança Industrial
 - UL 508
 - UL 61010
 - EN 50021
 - Hazardous Location
 - ISA 12.12.01/UL 1604
 - CSA22.2/213
 - IP30
- Emissões Industriais
 - EN 61805-3
 - EN 55032 (Emission Standard)
 - EN 61000-3-2
 - EN 61000-3-3
 - EN 55024 (Immunity Standard)



- EN 61000-4-2 to EN 61000-4-8
 - EN 61000-4-11
 - EN 61000-4-12
 - EN 61000-4-16
 - EN 61000-4-17
 - EN 61000-4-29
 - IEC 60255-5
 - IEEE 1613
 - Normas industriais específicas para Subestações
 - IEEE 1613, Seção 4 a 8
 - IEC 61850-3
 - Aplicações Ferroviárias
 - EN 50121-4
 - EN 62236-4
 - Standards Suportados
 - IEEE standards
 - IEEE 802.1D STP
 - IEEE 802.1p CoS
 - IEEE 802.1Q VLANs
 - IEEE 802.1ab (LLDP)
 - IEEE 802.1ag (OA&M)
 - IEEE 802.1ad Provider Bridges Q-in-Q/
VLAN stacking
 - IEEE 802.1ak (Multiple VLAN Registration
Protocol (MVRP)
 - IEEE 802.1aq Shortest Path Bridging (SPB)
 - IEEE 802.1s MSTP
 - IEEE 802.3i 10BASE-T
 - IEEE 802.1w RSTP
 - IEEE 802.3x Flow Control
 - IEEE 802.3z Gigabit Ethernet
 - IEEE 802.3ab 1000Base-T
 - IEEE 802.3ac VLAN Tagging
 - IEEE 802.3ad/802.1AX Link Aggregation
 - IEEE 802.3ae 10 GigE
 - IEEE 802.3af Power over Ethernet
 - IEEE 802.3at PoE Plus
 - IEEE 802.3az Energy Efficient Ethernet (EEE)
 - IEEE 802.1x-2004
 - IEEE 1588-2008 (PTP)
 - ITU-T recommendations
 - ITU-T G.8032/Y.1344 2010: Ethernet Ring Protection (ERPv2)
 - IETF RFCs
- IPv4
- RFC 2003 IP/IP Tunneling
 - RFC 2131 Dynamic Host Configuration Protocol (DHCPv4)
 - RFC 2784 GRE Tunneling
 - RFC 4022/2452 MIB for IPv4 TCP
 - RFC 4087 IP Tunnel MIB
 - RFC 4113/2454 MIB for IPv4 UDP
 - RFC 4292/4293 IPv4 MIBs
- OSPF
- RFC 1765 OSPF Database Overflow
 - RFC 1850/2328/4570 OSPF v2 and MIB
 - RFC 2154 OSPF MD5 Signature



- RFC 2370/3630 OSPF Opaque LSA
- RFC 2740/5340 OSPFv3 for IPv6
- RFC 3101 OSPF NSSA Option
- RFC 3623/5187 OSPF Graceful Restart
- RFC 5838 MIB for OSPFv3
- RFC 4552 Authentication for OSPFv3

RIP

- RFC 1058 RIP v1
- RFC 1722/1723/2453/1724 RIP v2 and MIB
 - RFC 1812/2644 IPv4 Router Requirements
 - RFC 2080 RIPng for IPv6

BGP

- RFC 1269/1657/4273 BGP v3 and v4 MIB
- RFC 1403/1745 BGP/OSPF Interaction
- RFC 1771-1774/2842/2918/3392/4271 BGP v4
- RFC 1965 BGP AS Confederations
- RFC 1966/2796 BGP Route Reflection
- RFC 1997/1998/4360 BGP

Communities Attribute

- RFC 2042/5396 BGP New Attribute
- RFC 2385 BGP MD5 Signature
- RFC 2439 BGP Route Flap Damping
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Routing
- RFC 2858/4760 Multiprotocol Extensions for BGP-4
- RFC 3065 BGP AS Confederations
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification
- RFC 4724 Graceful Restart for BGP
- RFC 3392/5492/5668/6793 BGP 4-Octet ASN
- RFC 5082 Generalized TTL Security Mechanism (GTSM)

IS-IS

- RFC 1142/1195/3719/3787/5308 IS-IS v4
- RFC 2763/2966/3567/3373 Adjacencies and route management
- RFC 5120 M-ISIS: Multi Topology IS-IS
- RFC 5306 Graceful Restart
- RFC 5309/draft-ietf-isis-igp-p2p-over-lan Point to point over LAN
- RFC 6329 IS-IS Extensions Supporting IEEE 802.1aq SPB
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5310 IS-IS Generic Cryptographic Authentication

IP Multicast

- RFC 1075/draft-ietf-idmr-dvmrp-v3-11.txt DVMRP
- RFC 2362/4601/5059 PIM-SM
- RFC 2365 Multicast
- RFC 2710/3019/3810/MLD v2 for IPv6
- RFC 2715 PIM and DVMRP interoperability
- RFC 2933 IGMP MIB
- RFC 3376 IGMPv3 (includes IGMP v2/v1)
- RFC 3569 Source-Specific Multicast (SSM)
- RFC 3973 Protocol Independent MulticastDense Mode (PIM-DM)
- RFC 4541 Considerations for IGMP and MLD Snooping Switches
- RFC 5015 BiDIR PIM
- RFC 5060 Protocol Independent Multicast MIB
- RFC 5132 Multicast Routing MIB
- RFC 5240 PIM Bootstrap Router MIB

IPv6



- RFC 1981 Path MTU Discovery
- RFC 2460 IPv6 Specification
- RFC 2461 NDP
- RFC 2464 IPv6 over Ethernet
- RFC 2465 MIB for IPv6: Textual Conventions (TC) and General Group
- RFC 2466 MIB for IPv6: ICMPv6 Group
- RFC 2711 Router Alert Option
- RFC 3056 6to4 Tunnels
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3484 Default Address Selection
- RFC 3493/2553 Basic Socket API
- RFC 3542/2292 Advanced Sockets API
- RFC 3587/2374 Global Unicast Address Format
- RFC 3595 TC for IPv6 Flow Label
- RFC 3596/1886 DNS for IPv6
- RFC 4007 Scoped Address
- RFC 4022/2452 MIB for IPv6 TCP
- RFC 4087 IP Tunnel MIB
- RFC 4113/2454 MIB for IPv6 UDP
- RFC 4193 Unique Local Addresses
- RFC 4213/2893 Transition Mechanisms
- RFC 4291/3513/2373 Addressing Architecture (uni/any/multicast)
- RFC 4292/4293 IPv6 MIBs
- RFC 4301/2401 Security Architecture
- RFC 4302/2402 IP Authentication Header
- RFC 4303/2406 IP Encapsulating Security Payload (ESP)
- RFC 4308 Cryptographic Suites for IPsec
- RFC 4443/2463 ICMPv6
- RFC 4861/2461 Neighbor Discovery
- RFC 4862/2462 Stateless Address Autoconfiguration
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

Manageability

- RFC 854/855 Telnet and Telnet options
- RFC 959/2640 FTP
- RFC 1350 TFTP Protocol
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1867 Form-based File Upload in HTML
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2131 DHCP Server/Client
- RFC 2388 Returning Values from Forms: multipart/form-data
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2570-2576/3410-3415/3584 SNMP v3
- RFC 2616 /2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3023 XML Media Types
- RFC 3414 User-based Security Model
- RFC 3826 (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 4122 A Universally Unique Identifier (UUID) URN Namespace



- RFC 4234 Augmented BNF for Syntax Specifications: ABNF
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4253 SSH Transport Layer Protocol
- RFC 4254 SSH Connection Protocol
- RFC 4627 JavaScript Object Notation (JSON)
- RFC 6585 Additional HTTP Status Codes

Security

- RFC 1321 MD5
- RFC 1826/1827/4303/4305 Encapsulating Payload (ESP) and crypto algorithms
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension
- RFC 3162 RADIUS and IPv6
- RFC 4301 Security Architecture for IP
- RFC 5517 Private VLAN Security - With Common Criteria enabled
- RFC 5280 - Internet X.509 PKI Certificate and CRL Profile
- RFC 2560 - X.509 Internet PKI Online Certificate Status Protocol - OCSP
- RFC 2986 - PKCS #10: Certification Request Syntax Specification v 1.7
- RFC 5246 - TLS Protocol v 1.2
- RFC 4346 - TLS Protocol v 1.1
- RFC 3268 - AES Cipher suites for TLS
- RFC 6125 - Representation and Verification of Domain-Based Application Service Identity within Internet PKIX Certificates in the Context of TLS
- draft-ietf-radext-radsec-12 – TLS encryption for RADIUS

QoS

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246

DiffServ

- RFC 2697 srTCM
- RFC 2698 trTCM
- RFC 3635 Pause Control

Others

- RFC 791/894/1024/1349 IP and IP Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 2581 TCP Congestion Control
 - RFC 826 ARP
 - RFC 919/922 Broadcasting Internet Datagram
 - RFC 925/1027 Multi-LAN ARP/Proxy ARP
 - RFC 950 Subnetting
 - RFC 951 BOOTP
 - RFC 1151 RDP
 - RFC 1191 Path MTU Discovery
 - RFC 1256 ICMP Router RADIUS Discovery
 - RFC 1305/2030 NTP v3 and Simple NTP
 - RFC 1493 Bridge MIB
 - RFC 1518/1519 CIDR
 - RFC 1541/1542/2131/3396/3442 DHCP
 - RFC 1757/2819 RMON and MIB



- RFC 2581 TCP Congestion Control
 - RFC 2131/3046 DHCP/BootP Relay
 - RFC 2132 DHCP Options
 - RFC 2251 LDAP v3
 - RFC 2338/3768/2787 VRRP and MIB
 - RFC 3021 Using 31-bit Prefixes
 - RFC 3060 Policy Core
 - RFC 3176 sFlow
 - RGC 3621 Power Ethernet MIB
- Software Defined Networking (SDN)
- OpenFlow Switch Specification v1.3.1
 - OpenFlow Switch Specification v1.0.0

1.2.9 Acessórios para os equipamentos OS6865-U28X

1.2.9.1 Fonte de alimentação AC – OS6865-BP

Fonte alimentação AC para OS6865-U28X com uma potência máxima de saída de 180W e corrente máxima de 12,5A, suportando uma tensão de entrada de 100V a 240 V AC/1,5A.

1.2.9.2 Fonte de alimentação DC – OS6865-BP-D

Fonte alimentação DC para OS6865-U28X com uma potência máxima de saída de 180W, suportando uma tensão de entrada de -20 V DC a -72 V DC.

1.2.9.3 SFPs Industriais

- iSFP-GIG-T 1000Base-T industrial Gigabit Ethernet Transceiver (SFP MSA). SFP works at 1000 Mb/s speed and full-duplex mode.
- iSFP-GIG-SX 1000Base-SX industrial Gigabit Ethernet industrial optical transceiver (SFP MSA).
- iSFP-GIG-LX 1000Base-LX industrial Gigabit Ethernet optical transceiver (SFP MSA). Alcance de 10Km.
- iSFP-GIG-LH40 1000Base-LH industrial Gigabit Ethernet optical transceiver (SFP MSA). Alcance de 40 km on 9/125 µm SMF.
- iSFP-GIG-LH70 1000Base-LH industrial Gigabit Ethernet optical transceiver (SFP MSA). Alcance de 70 km on 9/125 µm SMF.
- ISFP-10G-LR - 10 Gigabit industrial optical transceiver (SFP+). Supports single mode fiber with an LC connector. Alcance de 10 Km.
- ISFP-10G-ER - 10 Gigabit industrial optical transceiver (SFP+). Supports single mode fiber with an LC connector. Alcance de 40Km.
- ISFP-10G-ZR - 10 Gigabit industrial optical transceiver (SFP+). Supports single mode fiber with an LC connector. Alcance de 80Km.
-

Nota: Todos os SFPs a serem utilizados terão de ser o fabricante dos mesmos devendo ser consultado a tabela de compatibilidade por modelo do fabricante.

1.2.10 OS6560-24X4

O equipamento a fornecer terá de ser Omniswitch OS6560-24X4 Switch nível 2 e 3 ou equivalente terá que cumprir com os seguintes requisitos gerais:

- Número de portas mínimo: 24 portas Gigabit Ethernet, 2 portas 1G SFP e 4 portas 1G/10G SFP+;
- Porta de gestão out-of-band ethernet: 1;
- Porta USB de gestão: 1;
- Porta da consola: 1;
- Fonte de alimentação redundante;
- Ventoinhas: 1
- Capacidade de comutação máxima: 168Gb/s;



- Temperatura de funcionamento: 0°C a 45°C;
- Humidade em operação: 5% a 95% sem condensação;
- Consumo inferior a 36W;
- Equipamento com acessórios para montagem em rack 19” ocupando 1 U de altura;
- Totalmente integrável e gerido no centro de gestão Omnivista existente na IP;
- Integrável e compatível com a rede de omniswitches existentes na IP;
- Terá de incluir todo o licenciamento necessário ao nível de funcionalidade e do centro de gestão.

Terá que suportar chassis virtual composto por um máximo de 8 switches físicos.

NTP

RFC 5905 – Network Time Protocol v4
Número máximo de servidores NTP por cliente: 12
Número máximo de associações: 521

Especificações Ethernet

IEEE suportados

802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
802.3u (10BaseTX)
802.3ab (100BaseT)
802.3z (1000Base-X)
802.3ae (10GBase-X)
802.3ba (40GBase-X)
802.3az (Energy Efficient Ethernet)

Portas Suportadas

Ethernet (10 Mbps)
Fast Ethernet (100 Mbps)
Gigabit Ethernet (1 Gbps)
10 Gigabit Ethernet (10Gbps)

802.1Q Hardware Tagging

Jumbo Frame Configuration: 1/10 Gigabit Ethernet ports
Maximum Frame Size: 1553 bytes (10/100 Mbps)
9216 bytes (1/10Gbps)

Terá que suportar MACsec em todas as portas 1G RJ45.

Número de portas UDLD por sistema: 128

Número de vizinhos ULLD: 32

Especificações Source Learning

RFC suportado: 2674

Maximum number of learned MAC addresses when centralized MAC source learning mode is enabled: 16 000

VLANS

-IEEE

802.1Q - Virtual Bridged Local Area Networks
802.1D - Media Access Control Bridges

Maximum VLANs per VC: 4093

Maximum Tagged VLANs per Port: 4093

Maximum Untagged VLANs per Port: One untagged VLAN (default VLAN) per port

Spanning Tree Specifications

IEEE

802.1d—Media Access Control (MAC) Bridges



- 802.1s—Multiple Spanning Trees
- 802.1w—Rapid Spanning Tree Protocol
- Spanning Tree operating modes supported
 - Flat mode—one spanning tree instance per VC
 - Per-VLAN mode—one spanning tree instance per VLAN
- Spanning Tree port eligibility
 - Fixed ports
 - 802.1Q tagged ports
 - Link aggregate of ports
- Maximum VLAN Spanning Tree instances per VC: 100
- Maximum flat mode Multiple Spanning Tree Instances (MSTI) per VC: 16 MSTI, in addition to the Common and Internal Spanning Tree instance (also referred to as MSTI 0).
- Especificações Static Link Aggregation Specifications
 - Maximum number of link aggregation groups: 32
 - Maximum number of ports per link aggregate group: 8
- Dynamic Link Aggregation Specifications
 - IEEE Specifications Supported
 - 802.1ax/802.3ad—Aggregation of Multiple Link Segments
 - Maximum number of link aggregation groups: 32
 - Maximum number of ports per link aggregate group: 8
- Especificação ERP
 - ITU-T G.8032 03/2010
 - Ethernet Ring Protection version 2 (Multi Rings and Ladder networks supported) (Hold off timer, Lockout, Signal degrade SD, RPL Replacement, Forced Switch, Manual Switch, Clear for Manual/Forced Switch, Dual end blocking not supported)
 - ITU-T Y.1731/IEEE 802.1ag : ERP packet compliant with OAM PDU format for CCM
 - Maximum number of rings per node: 64
 - Maximum number of nodes per ring: 16
 - Maximum number of VLANs per port: 4094
 - Range for ring ID: 1–2147483647
 - Range for remote MEPID: 1–8191
 - Range for wait-to-restore timer: 1-12 minutes
 - Range for guard timer: 1- 200 centi-seconds
- Especificações MVRP
 - Normas suportadas IEEE Standards Supported
 - IEEE 802.1ak-2007 Amendment 7: Multiple Registration Protocol
 - IEEE 802.1Q-2005 Corrigendum 2008
 - Maximum MVRP VLANs: 512
- Especificação 802.1AB
 - IEEE Specification: IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery
 - Maximum number of network policies that can be associated with a port: 8
 - Maximum number of network policies that can be configured on a VC: 32
 - Nearest Edge MAC Address: 01:20:da:02:01:73
 - Nearest Bridge MAC Address: 01:80:c2:00:00:0e
 - Nearest Customer MAC Address: 01:80:C2:00:00:00
 - Non-TPMR Address 01:80:C2:00:00:03
- Routing e Multicast Layer-2 e Layer-3



Switching Layer

- Up to 16k MAC Addresses
- Up to 4000 VLANs
- Up to 1.5k total system policies
- Latency: < 4 µs
- Max Frame: 9216 bytes (jumbo)

Routing IPv4 e IPv6

- Static routing for IPv4 and IPv6
- RIP v1 and v2 for IPv4; RIPv6 for IPv6
- Up to 256 IPv4 and 128 IPv6 static and RIP routes
- Up to 128 IPv4 and 16 IPv6 interfaces
- OSPFv2 & OSPFv3 routing
- OSPFv2, OSPFv3 support

Multicast

- IGMPv1/v2/v3 snooping to optimize multicast traffic
- Multicast Listener Discovery (MLD)v1/v2 snooping+
- Up to 1000 multicast groups
- IP Multicast VLAN (IPMVLAN) for optimized multicast replication at the edge, saving network core resources

Protocolos de rede

- DHCP relay (including generic UDP relay)
- ARP
- Generic User Datagram Protocol (UDP) relay per VLAN
- DHCP Option 82 — configurable relay agent information

Normas e certificações

EMI/EMC

- 47 CRF FCC Part 15: 2015 Subpart B (Class A)
- VCCI (Class A limits. Note: Class A with UTP cables)
- ICES-003:2012 Issue 5, Class A
- AS/NZS 3548 (Class A) - C-Tick
- AS/NZS 3548 (Class A limits. Note: Class A with UTP cables)
- CE-Mark: Marking for European countries (Class A limits. Note: Class A with UTP cables)
- CE Emission consists of:
 - EN 50581: Standard for technical documentation for RoHS recast
 - EN 55022 (EMI and EMC requirement)
 - EN 55024: 2010 (ITE Immunity characteristics)
 - EN 61000-3-2 (Limits for harmonic current emissions)
 - EN 61000-3-3
 - EN 61000-4-2
 - EN 61000-4-3
 - EN 61000-4-4
 - EN 61000-4-5
 - EN 61000-4-6
 - EN 61000-4-8
 - EN 61000-4-11
 - IEEE802.3: Hi-Pot Test (2250 V DC on all Ethernet ports)

Certificações de segurança

- CDRH Laser
- Compliant with Restriction on Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment (WEEE) directives.
- EN 60825-1 Laser



- EN 60825-2 Laser
- IEC 62368-1
- UL 60950-1, 2nd Edition, Information Technology Equipment
- CAN/CSA C22.2 No. 60950-1-07, 2nd Edition, Information Technology Equipment
- IEC 60950-1

Normas IEEE a suportar

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)
- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (Provider Bridge) Q-in-Q (VLAN stacking)*
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1AE MAC Security
- IEEE 802.1X (Port Based Network Access Protocol)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10 Gigabit Ethernet)
- IEEE 802.3af (Power-over-Ethernet)
- IEEE 802.3at (Power-over-Ethernet)
- IEEE 802.3bt (Power-over-Ethernet)
- IEEE 802.3az (Energy Efficient Ethernet)
- IEEE 802.3bz (2.5GE Multi-Gigabit Ethernet)
- IEEE 1588v2 Precision Timing Protocol (PTP)

Recomendações ITU-T

- G.8032/Y.1344 2010: Ethernet Ring Protection (ERPV2)

RFC do IETF

RIP

- RFC 1058 RIP v1
- RFC 1722/1723/1724/2453 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirement
- RFC 2080 RIPng for IPv6

OSPF

- RFC 1850/2328 OSPF v2 and MIB
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 3623 OSPF Graceful Restart
- RFC 1765 OSPF Database Overflow
- RFC 3101 OSPF NSSA
- RFC 5838 MIB for OSPFv3
- RFC 4552 Authentication for OSPFv3
- RFC 5340/5838 OSPF v3 and MIB

IP Multicast

- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2365 Multicast
- RFC 3376 IGMPv3 for IPv6



IPv6

- RFC 1886 DNS for IPv6
- RFC 2292/2373/2374/2460/2462
- RFC 2461 NDP
- RFC 2463/2466 ICMP v6 and MIB
- RFC 2452/2454 IPv6 TCP/UDP MIB
- RFC 2464/2553/2893/3493/3513
- RFC 3056 IPv6 Tunneling
- RFC 3542/3587 IPv6
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses

Gestão

- RFC 854/855 Telnet and Telnet options
- RFC 959/2640 FTP
- RFC 1350 TFTP Protocol
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1867 Form-based File Upload in HTML
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2131 DHCP Server/Client
- RFC 2388 Returning Values from Forms: multipart/form-data
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2570-2576/3410-3415/3584 SNMP v3
- RFC 2616 /2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3023 XML Media Types
- RFC 3414 User-based Security Model
- RFC 3826 (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 4122 A Universally Unique Identifier (UUID) URN Namespace
- RFC 4234 Augmented BNF for Syntax Specifications: ABNF
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4627 JavaScript Object Notation (JSON)
- RFC 5424 The Syslog protocol
- RFC 6585 Additional HTTP Status Codes

Segurança

- RFC 1321 MD5
- RFC 1826/1827/4303/4305 Encapsulating Payload (ESP) and crypto algorithms
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension
- RFC 4301 Security Architecture for IP

Qualidade de serviço

- RFC 896 Congestion control



- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Diversos

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826 ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BootP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3021 Using 31-bit Prefixes
- RFC 3060 Policy Core
- RFC 3176 sFlow

1.2.10.1 Acessórios para os equipamentos OS6560-24X4

1.2.10.1.1 Fonte de alimentação AC OS6560-BP

Fonte de alimentação OS6560-BP modular 150W AC para OS6560-24X4
Compatível com o equipamento do OS6560-24X4.

1.2.10.1.2 Fonte de alimentação DC OS6560-BP-D

Fonte de alimentação DC. Compatível com o equipamento do OS6560-24X4.

1.2.10.1.3 Cabo direto Staking

Cabo direto de stacking OS6560S-CBL-1M de 100 cm long SFP+ para OS6560-24X4.

1.2.11 OS6560-48X4

O equipamento a fornecer terá de ser Omniswitch OS6560-48X4 Switch nível 2 e 3 ou equivalente: Switch Gigabit Ethernet de 1U com as seguintes características:

- Número de portas mínimo: 48 portas Gigabit Ethernet, 2 portas 1G SFP e 4 portas 1G/10G SFP+;
- Porta de gestão out-of-band ethernet: 1;
- Porta USB de gestão: 1;
- Porta da consola: 1;
- Fonte de alimentação redundante;
- Ventoinhas: 1
- Capacidade de comutação máxima: 216Gb/s;
- Capacidade de Switching com todas as portas 1G/10G em full duplex: 216Gb/s
- Temperatura de funcionamento: 0°C a 45°C;
- Humidade em operação: 5% a 95% sem condensação;



- Consumo inferior a 87W;
- Equipamento com acessórios para montagem em rack 19” ocupando 1 U de altura;
- Totalmente integrável e gerido no centro de gestão Omnivista existente na IP;
- Integrável e compatível com a rede de omniswitches existentes na IP;
- Terá de incluir todo o licenciamento necessário ao nível de funcionalidade e do centro de gestão.

Especificações Ethernet

Norma IEEE a suportar

802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
802.3u (100BaseTX)
802.3ab (1000BaseT)
802.3z (1000Base-X)
802.3ae (10GBase-X)
802.3ba (40GBase-X)
802.3az (Energy Efficient Ethernet)

Portas a Suportar

Ethernet (10 Mbps)
Fast Ethernet (100 Mbps)
Gigabit Ethernet (1 Gbps)
10 Gigabit Ethernet (10Gbps)

802.1Q Hardware Tagging

Jumbo Frame Configuration: 1/10 Gigabit Ethernet ports
Maximum Frame Size: 1553 bytes (10/100 Mbps)
9216 bytes (1/10Gbps)

Terá que suportar MACsec em todas as portas 1G RJ45.

Número de portas UDLD por sistema: 128

Número de vizinhos ULLD:32

Especificações Source Learning

RFC a suportar:2674

Maximum number of learned MAC addresses when centralized MAC source learning mode is enabled : 16 000

VLANS

-IEEE

802.1Q - Virtual Bridged Local Area Networks

802.1D - Media Access Control Bridges

Maximum VLANs per VC: 4093

Maximum Tagged VLANs per Port:4093

Maximum Untagged VLANs per Port: One untagged VLAN (default VLAN) per port

Spanning Tree Specifications

IEEE

802.1d—Media Access Control (MAC) Bridges

802.1s—Multiple Spanning Trees

802.1w—Rapid Spanning Tree Protocol

Spanning Tree operating modes supported

Flat mode—one spanning tree instance per VC

Per-VLAN mode—one spanning tree instance per VLAN

Spanning Tree port eligibility

Fixed ports



802.1Q tagged ports
Link aggregate of ports

Maximum VLAN Spanning Tree instances per VC: 100
Maximum flat mode Multiple Spanning Tree Instances (MSTI) per VC: 16 MSTI, in addition to the Common and Internal Spanning Tree instance (also referred to as MSTI 0).

Especificações Static Link Aggregation

Maximum number of link aggregation groups: 32
Maximum number of ports per link aggregate group: 8

Especificações Dynamic Link Aggregation

IEEE a suportar
802.1ax/802.3ad—Aggregation of Multiple Link Segments
Maximum number of link aggregation groups:32
Maximum number of ports per link aggregate group: 8

Especificações ERP

ITU-T G.8032 03/2010
Ethernet Ring Protection version 2 (Multi Rings and Ladder networks supported) (Hold off timer, Lockout, Signal degrade SD, RPL Replacement, Forced Switch, Manual Switch, Clear for Manual/Forced Switch, Dual end blocking not supported)
ITU-T Y.1731/IEEE 802.1ag : ERP packet compliant with OAM PDU format for CCM
Maximum number of rings per node: 64
Maximum number of nodes per ring: 16
Maximum number of VLANs per port:4094
Range for ring ID: 1–2147483647
Range for remote MEPID: 1–8191
Range for wait-to-restore timer:1-12 minutes
Range for guard timer:1- 200 centi-seconds

Especificações MVRP

IEEE a suportar
IEEE 802.1ak-2007 Amendment 7: Multiple Registration Protocol
IEEE 802.1Q-2005 Corrigendum 2008
Maximum MVRP VLANs:512

Especificações 802.1AB

IEEE Specification: IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery
Maximum number of network policies that can be associated with a port:8
Maximum number of network policies that can be configured on a VC:32
Nearest Edge MAC Address: 01:20:da:02:01:73
Nearest Bridge MAC Address: 01:80:c2:00:00:0e
Nearest Customer MAC Address: 01:80:C2:00:00:00
Non-TPMR Address 01:80:C2:00:00:03

Routing e Multicast Layer-2 e Layer-3

Switching Layer-2

- Up to 16k MAC Addresses
- Up to 4000 VLANs
- Up to 1.5k total system policies
- Latency: < 4 µs
- Max Frame: 9216 bytes (jumbo)

Routing IPv4 e IPv6

- Static routing for IPv4 and IPv6



- RIP v1 and v2 for IPv4; RIPv6 for IPv6
- Up to 256 IPv4 and 128 IPv6 static and RIP routes
- Up to 128 IPv4 and 16 IPv6 interfaces
- OSPFv2 & OSPFv3 routing
- OSPFv2, OSPFv3 support

Multicast

- IGMPv1/v2/v3 snooping to optimize multicast traffic
- Multicast Listener Discovery (MLD)v1/v2 snooping+
- Up to 1000 multicast groups
- IP Multicast VLAN (IPMVLAN) for optimized multicast replication at the edge, saving network core resources

Protocolos de rede

- DHCP relay (including generic UDP relay)
- ARP
- Generic User Datagram Protocol (UDP) relay per VLAN
- DHCP Option 82 — configurable relay agent information

Normas e certificações

EMI/EMC comercial

- 47 CRF FCC Part 15: 2015 Subpart B (Class A)
- VCCI (Class A limits. Note: Class A with UTP cables)
- ICES-003:2012 Issue 5, Class A
- AS/NZS 3548 (Class A) - C-Tick
- AS/NZS 3548 (Class A limits. Note: Class A with UTP cables)
- CE-Mark: Marking for European countries (Class A limits. Note: Class A with UTP cables)
- CE Emission consists of:
 - EN 50581: Standard for technical documentation for RoHS recast
 - EN 55022 (EMI and EMC requirement)
 - EN 55024: 2010 (ITE Immunity characteristics)
 - EN 61000-3-2 (Limits for harmonic current emissions)
 - EN 61000-3-3
 - EN 61000-4-2
 - EN 61000-4-3
 - EN 61000-4-4
 - EN 61000-4-5
 - EN 61000-4-6
 - EN 61000-4-8
 - EN 61000-4-11
 - IEEE802.3: Hi-Pot Test (2250 V DC on all Ethernet ports)

Certificações de segurança

- CDRH Laser
- Compliant with Restriction on Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment (WEEE) directives.
- EN 60825-1 Laser
- EN 60825-2 Laser
- IEC 62368-1
- UL 60950-1, 2nd Edition, Information Technology Equipment
- CAN/CSA C22.2 No. 60950-1-07, 2nd Edition, Information Technology Equipment
- IEC 60950-1

Normas IEEE a suportar

- IEEE 802.1D (STP)
- IEEE 802.1p (CoS)



- IEEE 802.1Q (VLANs)
- IEEE 802.1ad (Provider Bridge) Q-in-Q (VLAN stacking)*
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1AE MAC Security
- IEEE 802.1X (Port Based Network Access Protocol)
- IEEE 802.3i (10Base-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (1000Base-T)
- IEEE 802.3ac (VLAN Tagging)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10 Gigabit Ethernet)
- IEEE 802.3af (Power-over-Ethernet)
- IEEE 802.3at (Power-over-Ethernet)
- IEEE 802.3bt (Power-over-Ethernet)
- IEEE 802.3az (Energy Efficient Ethernet)
- IEEE 802.3bz (2.5GE Multi-Gigabit Ethernet)
- IEEE 1588v2 Precision Timing Protocol (PTP)

Recomendações ITU-T

- G.8032/Y.1344 2010: Ethernet Ring Protection (ERPV2)

RFC do IETF

RIP

- RFC 1058 RIP v1
- RFC 1722/1723/1724/2453 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirement
- RFC 2080 RIPng for IPv6

OSPF

- RFC 1850/2328 OSPF v2 and MIB
- RFC 2154 OSPF MD5 Signature
- RFC 2370/3630 OSPF Opaque LSA
- RFC 3623 OSPF Graceful Restart
- RFC 1765 OSPF Database Overflow
- RFC 3101 OSPF NSSA
- RFC 5838 MIB for OSPFv3
- RFC 4552 Authentication for OSPFv3
- RFC 5340/5838 OSPF v3 and MIB

Multicast IP

- RFC 1112 IGMP v1
- RFC 2236/2933 IGMP v2 and MIB
- RFC 2365 Multicast
- RFC 3376 IGMPv3 for IPv6

IPv6

- RFC 1886 DNS for IPv6
- RFC 2292/2373/2374/2460/2462
- RFC 2461 NDP
- RFC 2463/2466 ICMP v6 and MIB
- RFC 2452/2454 IPv6 TCP/UDP MIB
- RFC 2464/2553/2893/3493/3513
- RFC 3056 IPv6 Tunneling
- RFC 3542/3587 IPv6
- RFC 4007 IPv6 Scoped Address Architecture



- RFC 4193 Unique Local IPv6 Unicast Addresses

Gestão

- RFC 854/855 Telnet and Telnet options
- RFC 959/2640 FTP
- RFC 1350 TFTP Protocol
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1867 Form-based File Upload in HTML
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2131 DHCP Server/Client
- RFC 2388 Returning Values from Forms: multipart/form-data
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2570-2576/3410-3415/3584 SNMP v3
- RFC 2616 /2854 HTTP and HTML
- RFC 2667 IP Tunneling MIB
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3023 XML Media Types
- RFC 3414 User-based Security Model
- RFC 3826 (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 4122 A Universally Unique Identifier (UUID) URN Namespace
- RFC 4234 Augmented BNF for Syntax Specifications: ABNF
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4627 JavaScript Object Notation (JSON)
- RFC 5424 The Syslog protocol
- RFC 6585 Additional HTTP Status Codes

Segurança

- RFC 1321 MD5
- RFC 1826/1827/4303/4305 Encapsulating Payload (ESP) and crypto algorithms
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension
- RFC 4301 Security Architecture for IP

Qualidade de serviço

- RFC 896 Congestion control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 3635 Pause Control

Diversos

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB



- RFC 826 ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030 NTP v3 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BootP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3021 Using 31-bit Prefixes
- RFC 3060 Policy Core
- RFC 3176 sFlow

1.2.12 OS6465-P28

Equipamento OS6865-P28 ou equivalente sem ventilação mecânica para rack de 19" com 22 portas 10/100/1000 Base-T PoE+, 8 com capacidade para HPoE de 60W, duas portas 100/1000Base-X e 4 portas SFP+ 1G/10G.

Temperatura de funcionamento: -40°C a 75°C

Capacidade máxima de comutação: 128Gb/s

Capacidade de transferência: 95,3Mpps

Portas 1588v2: 26

Portas MACsec:26

Contactos de alarme: 1 de entrada, 1 de saída

Fontes de alimentação:2

Orçamento de Potência máximo: 285W

Altitude funcionamento: 13 000ft

Dissipação de calor (BTU/H):98,95

Proteção de descarga máxima:6KV

MTBF (horas) só o equipamento: superior a 2 100 000

Instalação em Rack 19"

Chassis virtual: Número máximo de unidades num chassis virtual: 4

Ligações remotas de Chassis Virtual: usando iSFP-GIG-SX, iSFP-GIG-LX

Jumbo frame size: 9216 bytes (para 1 Gb/s)

Número total de endereços MAC: 16 000

Número total de rotas IPv4: 128

Número de VLANs: 4 000

Certificações

- UL 60950-1, 2nd Ed.
- IEC 60950-1; all national deviations
- EN 60950-1; all deviations
- EN 60825-1 Laser
- EN 60825-2 Laser
- CDRH Laser
- RoHS and WEEE directives compliant
- REACH directive

EMI/EMC



- 47 CRF FCC Part 15: 2015 Subpart B (Class A)VCCI (Class A, with UTP Cables)
- ICES–003:2012 Issue 5, Class A • AS/NZS 3548 (Class A) – C-Tick
- CE marking for European countries (Class A)
- CE Emission
- EN50581 (RoHS Recast)
- EN 55032 (EMI & EMC requirement)
- EN 55024 (Immunity Characteristics)
- EN 61000-3-2(Harmonic Current emissions)
- EN 61000-3-3
- EN 61000-4-2
- EN 61000-4-3
- EN 61000-4-4
- EN 61000-4-5 (Surge Immunity, Class 4)
- EN 61000-4-6
- EN 61000-4-8
- EN 61000-4-9
- EN 61000-4-11
- IEEE802.3: Hi-pot Test (2.25 KV DC on all Ethernet Ports)

Ambiente Industrial

- IEC 60870-2-2 (operational temperature)
- IEC 60068-2-1 (temperature type test – cold)
- IEC 60068-2-2 (temperature type test – hot)
- IEC 60721-3-1: Class 1K5 (storage temperature)
- IEC 60068-2-30: 5% to 95% non-condensing humidity
- IEC 60255-21-2 (mechanical shock)
- IEC 60255-21-1 (vibration)

Segurança Industrial

- UL 508
- UL 61010
- EN 50021
- Hazardous location
 - ISA 12.12.01 (UL 1604)
 - CSA22.2/213
- IP30 Industrial emission
- EN 61805-3
- EN 55032 (Emission Standard)
- EN 61000-3-2
- EN 61000-3-3
- EN 55024/EN 55035 (Immunity Standard)
- EN 61000-4-2 to EN 61000-4-8
- EN 61000-4-11
- EN 61000-4-12
- EN 61000-4-16
- EN 61000-4-17
- EN 61000-4-29
- IEC 60255-5
- IEEE 1613

Normas industriais Subestações

- IEEE 1613, Secção 4 a 8
- IEC 61850-3

Aplicações ferroviárias

- EN 50121-4
- EN 50155:2017
- EN 61373
- EN 62236-4
- EN61000-6-4



- EN61000-6-2
- ITS (estradas)
- NEMA TS-2

Gestão e configuração

- Intuitive CLI in a scriptable Python & BASH environment via console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6
- Powerful WebView Graphical Web Interface via HTTP and HTTPS over IPv4/IPv6
- Network Automation and Programmability Abstraction Layer with Multivendor (NAPALM) support
- Fully programmable RESTful web services interface with XML and JSON support. API enables access to CLI and individual mib objects
- Integrated with Alcatel-Lucent OmniVista® products for network management
- Integrated with Nokia Network Services Platform (NSP)© for network management
- Full configuration and reporting using SNMPv1/2/3 to facilitate thirdparty network management over IPv4/IPv6
- File upload using USB, TFTP, FTP, SFTP or SCP using IPv4/IPv6
- Human-readable ASCII-based configuration files for off-line editing, bulk configuration and out-of-the-box auto-provisioning
- Non-volatile memory for start-up configuration
- Multiple microcode image support with fallback recovery
- Dynamic Host Configuration Protocol (DHCP) relay for IPv4/IPv6
- IEEE 802.1AB Link Layer Discover Protocol (LLDP) with Media Endpoint Discover (MED) extensions
- Network Time Protocol (NTP)
- DHCPv4 and DHCPv6 server managed by Nokia VitalQIP® DNS/ DHCP IP Address Management
- Access to the AOS console via USBAdapter with Bluetooth technology provides wireless management access, eliminating the need of console cables

Monitorização e deteção de avarias

- Local (on the flash) and remote server logging (Syslog): event and command logging
- IP tools: ping and trace route
- Dying Gasp support via SNMP and syslog messages
- Loopback IP address support for management per service
- Policy- and port-based mirroring
- Remote port mirroring
- sFlow v5 and Remote Monitoring (RMON)
- Unidirectional Link Detection (UDLD), Digital Diagnostic Monitoring (DDM)

Alta Disponibilidade

- Unified management, control and virtual chassis technology
- Virtual Chassis 1+N redundant supervisor manager
- Smart continuous switching technology
- ITU-T G.8032/Y1344 2010: Ethernet Ring Protection
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) encompasses IEEE 802.1D spanning Tree Protocol (STP) and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Per-VLAN spanning tree (PVST+) and 1x1 STP mode
- IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules
- Dual-home link support for subsecond link protection without STP
- Virtual Router Redundancy Protocol
- (VRRP) with tracking capabilities
- IEEE protocol auto-discovery
- Redundant and hot-swappable power supplies
- Built-in CPU protection against malicious attacks
- Split Virtual Chassis protection: Autodetection and recovery of Virtual Chassis splitting due to one or more VFL or stack element failures*

Segurança

- AOS secured diversified code solution is available on OmniSwitch® 6465, hardening it at both the software source code and binary executable levels to enhance overall



network security.

- AOS secured diversified code protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise mission critical operations.
- AOS secured diversified code is a proactive, defense approach toward network security that continuously defines and implements value-add capabilities to address both current and future threats.

Controlo de Acesso

- Alcatel-Lucent Access Guardian framework for comprehensive user policy-based NAC
- Autosensing IEEE 802.1X multiclient, multi-VLAN support
- MAC-based authentication for non-IEEE 802.1X hosts
- Web based authentication (captive portal): a customizable web portal residing on the switch
- policy configuration to authenticated clients — VLAN, ACL, BW
- Secure Shell (SSH) with public key infrastructure (PKI) support
- Terminal Access Controller Access Control System Plus (TACACS+) client
- Centralized Remote Access Dial In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication
- Centralized RADIUS for device authentication and network access control authorization
- Learned Port Security (LPS) or MAC address lockdown
- Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)
- DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection
- ARP poisoning detection
- IP Source Filtering as a protective and effective mechanism against ARP attacks
- LLDP Security mechanism for rogue device detection and restriction

QoS

- Priority queues: Eight hardware-based queues per port for flexible QoS management
- Traffic prioritization: Flow-based QoS Flow-based traffic policing and bandwidth management
- 32-bit IPv4/128-bit IPv6 noncontiguous mask classification
- Egress traffic shaping
- DiffServ architecture
- Congestion avoidance: Support for end-to-end head-of-line (E2E-HOL) blocking prevention, IEEE 802.1Qbb Priority-based Flow Control (PFC) and IEEE 802.3x Flow Control (FC)
- Auto-QoS support for Generic Object Oriented Substation Events (GOOSE) messages

Layer 3 Routing e Multicast

Routing IPv4

- Static routing
- Routing Information Protocol (RIP) v1 and v2
- Virtual Router Redundancy Protocol (VRRPv2)
- DHCP relay (including generic UDP relay)
- Address Resolution Protocol (ARP)
- Policy-based routing and server load balancing
- DHCPv4 server

Routing IPv6

- Internet Control Message Protocol version 6 (ICMPv6)
- Static routing
- Virtual Router Redundancy Protocol version 3 (VRRPv3)
- Neighbor Discovery Protocol (NDP)
- Policy-based routing and server load balancing
- DHCPv6 server



Multicast IPv4 e IPv6

- Internet Group Management Protocol (IGMP) v1/v2/v3 snooping
- Multicast Listener Discovery (MLD) v1/v2 snooping

Serviços Layer 2

- Ethernet services support using IEEE 802.1ad Provider Bridges (also known as Q-in-Q or VLAN stacking)
- Ethernet OAM (802.1ag, ITU-T Y.1731): Connectivity Fault Management (L2 ping & Link trace)
- Ethernet in First mile: Link OAM(802.3ah)
- Ethernet network-to-network interface (NNI) and user network interface (UNI)
- Service Access Point (SAP) profile identification
- Service VLAN (SVLAN) and Customer VLAN (CVLAN) support
- VLAN translation and mapping including CVLAN to SVLAN
- Port mapping
- DHCP Option 82: Configurable relay agent information
- Multiple VLAN Registration Protocol (MVRP)
- HA-VLAN for Layer 2 clusters such as MS-NLB and active-active Firewall clusters
- Customer Provider Edge (CPE) test head traffic generator and analyzer tool
- TR-101 Point-to-Point Protocol over Ethernet (PPPoE) Intermediate Agent allowing for the PPPoE network access method
- Service Assurance Agent (SAA) for proactively measuring network health, reliability and performance.
- Jumbo frame support
- Bridge Protocol Data Unit (BPDU) blocking
- STP Root Guard

Normas suportadas

IEEE

- IEEE 802.1D STP
- IEEE 802.1p CoS
- IEEE 802.1Q VLANs
- IEEE 802.1ab (LLDP)
- IEEE 802.1ag (OA&M)
- IEEE 802.1ad Provider Bridges Q-in-Q/ VLAN stacking
- IEEE 802.1ak (Multiple VLAN Registration Protocol (MVRP)
- IEEE 802.1s MSTP • IEEE 802.3i 10BASE-T
- IEEE 802.1w RSTP • IEEE 802.3x Flow Control
- IEEE 802.3z Gigabit Ethernet
- IEEE 802.3ab 1000Base-T
- IEEE 802.3ac VLAN Tagging
- IEEE 802.3ad/802.1AX Link Aggregation
- IEEE 802.3ae 10 GigE
- IEEE 802.3af Power over Ethernet
- IEEE 802.3at PoE Plus
- IEEE 1588v2 Precision Time Protocol ITU-T recommendations
- ITU-T G.8032/Y.1344 2010: Ethernet Ring Protection (ERPv2)
- ITU-T Y.1731 OA&M fault and performance management IETF RFCs IPv4
- RFC 2131 Dynamic Host Configuration Protocol (DHCPv4)
- RFC 4022/2452 MIB for IPv4 TCP • RFC 4113/2454 MIB for IPv4 UDP
- RFC 4292/4293 IPv4 MIBs RIP
- RFC 1058 RIP v1
- RFC 1722/1723/2453/1724 RIP v2 and MIB
- RFC 1812/2644 IPv4 Router Requirements
- RFC 2080 RIPng for IPv6 IP Multicast
- RFC 2365 Multicast
- RFC 2710/3019/3810/MLD v2 for IPv6



- RFC 2933 IGMP MIB
- RFC 3376 IGMPv3 (includes IGMP v2/v1)
- RFC 4541 Considerations for IGMP and MLD Snooping Switches
- RFC 5132 Multicast Routing MIB IPv6
- RFC 1981 Path MTU Discovery
- RFC 2460 IPv6 Specification
- RFC 2464 IPv6 over Ethernet
- RFC 2465 MIB for IPv6: Textual Conventions (TC) and General Group
- RFC 2466 MIB for IPv6: ICMPv6 Group
- RFC 3484 Default Address Selection
- RFC 3493/2553 Basic Socket API
- RFC 3542/2292 Advanced Sockets API
- RFC 3587/2374 Global Unicast Address Format
- RFC 3595 TC for IPv6 Flow Label
- RFC 3596/1886 DNS for IPv6
- RFC 4007 Scoped Address
- RFC 4022/2452 MIB for IPv6 TCP
- RFC 4113/2454 MIB for IPv6 UDP
- RFC 4193 Unique Local Addresses
- RFC 4213/2893 Transition Mechanisms
- RFC 4291/3513/2373 Addressing Architecture (uni/any/multicast)
- RFC 4292/4293 IPv6 MIBs
- RFC 4443/2463 ICMPv6
- RFC 4861/2461 Neighbor Discovery*
- RFC 4862/2462 Stateless Address Autoconfiguration
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6*

Gestão

- RFC 854/855 Telnet and Telnet options
- RFC 959/2640 FTP
- RFC 1350 TFTP Protocol
- RFC 1155/2578-2580 SMI v1 and SMI v2
- RFC 1157/2271 SNMP
- RFC 1212/2737 MIB and MIB-II
- RFC 1213/2011-2013 SNMP v2 MIB
- RFC 1215 Convention for SNMP Traps
- RFC 1573/2233/2863 Private Interface MIB
- RFC 1643/2665 Ethernet MIB
- RFC 1867 Form-based File Upload in HTML
- RFC 1901-1908/3416-3418 SNMP v2c
- RFC 2096 IP MIB
- RFC 2131 DHCP Server/Client
- RFC 2388 Returning Values from Forms: multipart/form-data
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2570-2576/3410-3415/3584 SNMP v3
- RFC 2616 /2854 HTTP and HTML
- RFC 2668/3636 IEEE 802.3 MAU MIB
- RFC 2674 VLAN MIB
- RFC 3023 XML Media Types
- RFC 3414 User-based Security Model
- RFC 3826 (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 4122 A Universally Unique Identifier (UUID) URN Namespace
- RFC 4234 Augmented BNF for Syntax Specifications: ABNF
- RFC 4251 Secure Shell Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4627 JavaScript Object Notation (JSON)



- RFC 6585 Additional HTTP Status Codes Security
- RFC 1321 MD5
- RFC 1826/1827/4303/4305 Encapsulating Payload (ESP) and crypto algorithms
- RFC 2104 HMAC Message Authentication
- RFC 2138/2865/2868/3575/2618 RADIUS Authentication and Client MIB
- RFC 2139/2866/2867/2620 RADIUS Accounting and Client MIB
- RFC 2228 FTP Security Extensions
- RFC 2284 PPP EAP
- RFC 2869/2869bis RADIUS Extension
- RFC 4301 Security Architecture for IP

QoS

- RFC 896 Congestion Control
- RFC 1122 Internet Hosts
- RFC 2474/2475/2597/3168/3246 DiffServ
- RFC 2697 srTCM
- RFC 2698 trTCM
- RFC 3635 Pause Control

Outras normas

- RFC 791/894/1024/1349 IP and IP/Ethernet
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793/1156 TCP/IP and MIB
- RFC 826 ARP
- RFC 919/922 Broadcasting Internet Datagram
- RFC 925/1027 Multi-LAN ARP/Proxy ARP
- RFC 950 Subnetting
- RFC 951 BOOTP
- RFC 1151 RDP
- RFC 1191 Path MTU Discovery
- RFC 1256 ICMP Router Discovery
- RFC 1305/2030/5905 NTP v4 and Simple NTP
- RFC 1493 Bridge MIB
- RFC 1518/1519 CIDR
- RFC 1541/1542/2131/3396/3442 DHCP
- RFC 1757/2819 RMON and MIB
- RFC 2131/3046 DHCP/BootP Relay
- RFC 2132 DHCP Options
- RFC 2251 LDAP v3
- RFC 2338/3768/2787 VRRP and MIB
- RFC 3021 Using 31-bit Prefixes
- RFC 3060 Policy Core
- RFC 3176 sFlow
- RFC 4562 MAC-Forced Forwarding

1.2.12.1 Acessórios para OS6465-P28 ou equivalente

Fonte de alimentação OS6465-BPR-xx

Fonte de alimentação AC modular para instalação em rack para o OS6465. Fornece energia ao equipamento e energia para PoE para um OS6465-P28 switch.

Fonte de alimentação OS6465-BPRD

Fonte de alimentação C modular para instalação em rack para o OS6465. Fornece energia ao equipamento e energia para PoE para um OS6465-P28 switch.

SFPs Industriais

- iSFP-GIG-T 1000Base-T industrial Gigabit Ethernet Transceiver (SFP MSA). SFP works at 1000 Mb/s speed and full-duplex mode



- iSFP-GIG-SX 1000Base-SX industrial Gigabit Ethernet industrial optical transceiver (SFP MSA)
- iSFP-GIG-LX 1000Base-LX industrial Gigabit Ethernet optical transceiver (SFP MSA)
- iSFP-GIG-LH40 1000Base-LH industrial Gigabit Ethernet optical transceiver (SFP MSA). Typical reach of 40 km on 9/125 µm SMF
- iSFP-GIG-LH70 1000Base-LH industrial Gigabit Ethernet optical transceiver (SFP MSA). Typical reach of 70 km on 9/125 µm SMF

1.2.13 OS6465-P12

Equipamento OS6465-P12 ou equivalente sem ventilação mecânica para montagem DIN com 8 portas 10/100/1000 Base-T PoE+, 4 com capacidade para HPoE de 60W, 4 portas 100/1000Base-X.

Temperatura de funcionamento: -40°C a 75°C

Capacidade máxima de comutação: 24Gb/s

Capacidade de transferência: 17,9Mpps

Portas 1588v2: 12

Portas MACsec: 12

Contactos de alarme: 1 de entrada, 1 de saída

Fontes de alimentação: 2

Orçamento de Potência máximo: 150W

Dissipação de calor (BTU/H): 40,22

Proteção de descarga máxima: 6KV

MTBF (horas) só o equipamento: superior a 1 400 000

Instalação em DIN, Parede e painel.

Chassis virtual: Número máximo de unidades num chassis virtual: 4

Ligações remotas de Chassis Virtual: usando iSFP-GIG-SX, iSFP-GIG-LX

Jumbo frame size: 9216 bytes (para 1 Gb/s)

Número total de endereços MAC: 16 000

Número total de rotas IPv4: 128

Número de VLANs: 4 000

As restantes especificações são iguais à especificação OS6465-P28 descritas no ponto 1.2.9 deste Anexo.

1.2.13.1 Acessórios para OS6465-P12 ou equivalente

Fonte de alimentação OS6465-BPN de 75W para OS6465-P12 e OS6465-P6. Tensão de entrada entre 100 e 240 VAC. Siporte IEEE 802.3at e iEEE802.3af.

SFPs industriais ver ponto 1.3.9.1 deste Anexo.

1.2.14 OS6870-V12

O equipamento a fornecer terá de ser Omniswitch OS6870-V12 Router/Switch L2/3 ou equivalente com uma fonte de alimentação OS6870-BPH que terá que cumprir com os seguintes requisitos gerais:

- Chassis 1 U 19”;
- Número de portas mínimo: 12 portas SFP28 1G/10G/25G e 2 portas QSFP56 100/200G;
- Módulo de expansão Uplink;
- Porta de gestão out-of-band ethernet: 1;
- Porta USB (Type-A): 1;
- Porta da consola (RJ45): 1;



- Com possibilidade de ter Fonte de alimentação redundante;
- Ventoinhas: 3+1 redundante;
- Fluxo de Ar: Frente-Traseira
- Capacidade de switching agregada: 2 000 Gb/s;
- Taxa de transferência: 1 488 Mpps;
- Temperatura de funcionamento: 0°C a 45°C;
- Humidade em operação: 5% a 95% sem condensação;
- Equipamento com acessórios para montagem em rack 19" ocupando 1 U de altura;
- Totalmente integrável e gerido no centro de gestão Omnivista existente na IP;
- Integrável e compatível com a rede de omniswitches existentes na IP;
- Terá de incluir todo o licenciamento associado a funcionalidades (Advanced Routing) e ao centro de gestão existente na IP

1.2.14.1 Login

1.2.14.1 Métodos Login: Telnet, SSH, HTTP, SNMP.

1.2.14.2 Número de sessões telnet concorrentes: 6.

1.2.14.3 Número de sessões SSH concorrentes: 8.

1.2.14.4 Número de sessões HTTP concorrentes (Webview): 4.

1.2.14.2 Gestão de ficheiros

1.2.14.2.1 Métodos de transferência de ficheiros a suportar: FTP (v4/v6), SFTP (v4/v6), SCP (v4/v6), TFTP.

1.2.14.2.2 Suporte Cliente/Servidor:

FTP—Cliente (IPv4) ou Servidor;

SFTP—Cliente ou Servidor;

SCP—Cliente ou Servidor;

TFTP—Cliente.

1.2.14.2.3 Número de sessões FTP/SFTP concorrentes: 4.

1.2.14.2.3 SNMP



1.2.14.2.3.1 Os equipamentos terão que suportar as seguintes normas RFC para SNMPv2:

1902 até 1907 - SNMPv2c Management Framework;

1908 - Coexistence and transitions relating to SNMPv1 and SNMPv2c.

1.2.14.2.3.2 Os equipamentos terão que suportar as seguintes normas RFC para SNMPv3:

2570—Version 3 of the Internet Standard Network Management Framework;

2571—Architecture for Describing SNMP Management Frameworks;

2572—Message Processing and Dispatching for SNMP;

2573—SNMPv3 Applications;

2574/3414—User-based Security Model (USM) for version 3 SNMP;

2575—View-based Access Control Model (VACM) for SNMP;

2576—Coexistence between SNMP versions;

3586—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.

1.2.14.2.3.3 SNMPV3 Autenticação:SHA,MD5

1.2.14.2.3.4 Cifragem SMNPv3: DES,AES

1.2.14.2.4 Chassis Virtual

1.2.14.2.4.1 Número de switches físicos que podem constituir 1 chassis virtual:8.

1.2.14.2.4.2 Número de peers Virtual Fabric link:2.

1.2.14.2.4.3 Número de portas membro por link Virtual Fabric: 8.

1.2.14.2.4.4 Portas suportadas para VFL: 10G SFP+,25G SFP28, 40G QSFP+, 100G QSFP28 e 200GQSFP56.

1.2.14.2.5 NTP

1.2.14.2.5.1 Os equipamentos terão que suportar RFC 5905—Network Time Protocol v4.

1.2.14.2.5.2 Número de servidores NTP por cliente:12.



1.2.14.2.5.3 Número de associações: 512.

1.2.14.2.6 Nível 2 (Layer 2)

1.2.14.2.6.1 Os equipamentos terão que suportar as seguintes normas IEEE:

- 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- 802.3u (100BaseTX)
- 802.3ab (1000BaseT)
- 802.3z (1000Base-X)
- 802.3bz (2.5Base-T)
- 802.3ae (10GBase-X)
- 802.3ba (40GBase-X)
- 802.3az (Energy Efficient Ethernet)

1.2.14.2.6.2 Suporte 802.1Q Hardware tagging.

1.2.14.2.6.3 Os equipamentos terão que suportar Interfaces de 1/10/40/100Gbps e suportar Jumbo frames de 9216bytes.

1.2.14.2.6.4 Suporte MAC Sec.

1.2.14.2.7 Unidirectional Link Detection (UDLD)

Os equipamentos terão de suportar Unidirectional Link Detection(UDLD).

1.2.14.2.7.1 Número de portas UDLD por sistema: 128.

1.2.14.2.7.2 Número de vizinhos UDLD por portas:32.

1.2.14.2.8 Source learning

Os equipamentos terão de suportar o seguinte RFC: 2674—Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions.

O número de endereços MAC apreendidos quando o modo Source learning centralizado está ativo deverá ser pelo menos de 128000 (switch mode) e 80000 Edge router mode.

1.2.14.2.9 VLAN



1.2.14.2.9.1 Os equipamentos terão que suportar o RFC 2674 - Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions e o RFC 5517 - Private VLAN.

1.2.14.2.9.2 Os equipamentos terão que suportar as seguintes normas IEEE:

- 802.1Q – Virtual Bridged Local Area Networks;
- 802.1D – Media Access Control Bridges.

1.2.14.2.9.3 Os equipamentos terão de suportar pelo menos:

- Número de vlans por VC: 4094;
- Número de tagged vlans por porta: 4093;
- Número de VLAN untagged por porta: 1.

1.2.14.2.10 VLAN de alta disponibilidade

As VLANs de alta disponibilidade permitem que seja enviado tráfego destinado a um endereço MAC a várias portas do switch.

Os equipamentos terão que suportar 16 VLAN de alta disponibilidade por chassis virtual.

1.2.14.2.11 Spanning Tree

Os equipamentos terão de suportar as seguintes normas IEEE:

- 802.1d—Media Access Control (MAC) Bridges;
- 802.1s—Multiple Spanning Trees;
- 802.1w—Rapid Spanning Tree Protocol.

Os equipamentos terão que suportar:

- Modos de operação SpanningTree:
 - o Modo Flat – 1 instância spanning tree por chassis virtual;
 - o Modo por VLAN – 1 instância spanning tree por VLAN.
- Elegibilidade de port Spanning Tree: Portas fixas, portas 802.1Q tagged e portas Link aggregate
- Número de instâncias spanning tree VLAN por chassis virtual:100;



- Número de instâncias Multiple Spanning Tree Instances (MSTI) modo flat por chassis virtual: 16 adicionais à instância de spanning tree interna e comum (MSTI0).

1.2.14.2.12 SPB

1.2.14.2.12.1 Os equipamentos terão que suportar IEEE802.1aq Shortest Path Bridging (SPB-M) nomeadamente as seguintes normas:

- IEEE

802.1aq/D3.6: Draft February 10, 2011—Virtual Bridged Local Area Networks—Amendment 9: Shortest Path Bridging;

802.1ah/D4.2: DRAFT March 26, 2008— Virtual Bridged Local Area Networks—Amendment 6: Provider Backbone Bridging.

-IETF

draft-ietf-isis-ieee-aq-05.txt—ISIS Extensions Supporting IEEE 802.1aq Shortest Path Bridging;

IETF draft—IP/IPVPN services with IEEE 802.1aq SPBB networks;

IETF draft—IP/IPVPN services with IEEE 802.1aq SPB networks.

1.2.14.2.12.2 Os equipamentos terão que suportar o modo SPBM (MAC-in-MAC).

1.2.14.2.12.3 Os equipamentos terão que disponibilizar IP sobre SPBM:

- IPv4 (VPN-Lite e VPN L3);

- Mapeamento VRF-to-ISID (um a um, um a vários).

1.2.14.2.12.4 Terão que suportar uma instância de SPB-ISIS por chassis virtual.

1.2.14.2.12.5 Terão que suportar 16 BVLAN por chassis virtual.

1.2.14.2.12.6 Terá de suportar 128 adjacências IS-IS.

1.2.14.2.12.7 Número máximo de interfaces IS-IS:128

1.2.14.2.12.8 Número de identificadores de instâncias (I-SID) por virtual chassis: 2000.

1.2.14.2.12.9 Número máximo de VLAN ou SVLAN por I-SID: 2000.

1.2.14.2.12.10 O tamanho da MTU nos serviços SPB que os equipamentos terão de suportar é de 9000.



1.2.14.2.13 Detecção Loopback

Os equipamentos terão de suportar Loopback detection, Edge (Bridge) e SAP(Access).

1.2.14.2.13.1 Temporizador de transmissão: 5 a 600 segundos.

1.2.14.2.13.2 Temporizador de auto-recover: 30-86400 segundos.

1.2.14.2.14 Agregação de links estático

Os equipamentos terão de suportar agregação de links estáticos.

1.2.14.2.14.1 Número de grupos de agregação de links:252;

1.2.14.2.14.2 Número de portas por grupo de link aggregate:16.

1.2.14.2.15 Agregação de links dinâmico

Os equipamentos terão de suportar as especificações IEEE - 802.1ax/802.3ad—Aggregation of Multiple Link Segments.

1.2.14.2.15.1 Número de grupo de agregação de links:128.

1.2.14.2.15.2 Número de portas por grupo de agregação de link:16.

1.2.14.2.16 Dual Home Link

Os equipamentos terão de suportar Dual-Home Link (1 sessão).

1.2.14.2.17 ERP

1.2.14.2.17.1 Os equipamentos terão de suportar:

- ITU-T G8032 03/2010 – Ethernet Ring Protection version 2 ((Multi Rings and Ladder networks).
- ITU-T Y.1731/IEEE802.lag – Pacote ERP de acordo com o formato PDU OAM para CCM.

1.2.14.2.17.2 Número máximo de anéis por nó: 64.

1.2.14.2.17.3 Número máximo de nós por anel:16.

1.2.14.2.17.4 Número máximo de VLANs por portas:4094.



- 1.2.14.2.17.5 Intervalo de identificadores de anel: 1 – 2147483647.
- 1.2.14.2.17.6 Intervalo para remote MEPID: 1-8191.
- 1.2.14.2.17.7 Intervalo de valores para o temporizador wait-to restore:1-12minutos.
- 1.2.14.2.17.8 Intervalos de valores para guard timer: 1- 200 centésimas de segundo.
- 1.2.14.2.17.9 Multiple VLAN Registration Protocol (MVRP)

Os equipamentos terão de suportar Multiple VLAN Registration Protocol (MVRP) tal como definido nas normas IEEE 802.1ak-2007 Amendment 7: Multiple Registration Protocol e IEEE 802.1Q-2005 Corrigendum 2008.

O número de VLAN utilizando MVRP a suportar deverá ser de 512.

1.2.14.2.17.10 VXLAN

Os equipamentos terão de suportar o RFC 7348 —VXLAN: A Framework for Overlaying Layer 2 Virtualized Networks over Layer 3 Networks.

Segmentos VXLAN (redees overlay L2): 16 milhões

Instâncias de serviço VXLAN: 8000

Número de endpoints de túneis VXLAN numa rede VXLAN:500

Portas destino UDP VXLAN: 8 (incluindo a porta UDP default que é 4789)

Service Access Points VXLAN(SAPs):8000 por dispositivo ou por chassis virtual

Service access ports with SAPs that contain a VLAN ID range:255

VXLAN Network IDs (VNIs):4 000

Grupos Multicast: 500

Protocolo multicast suportado: Bidireccional PIM(BIDIR-PIM)

1.2.14.2.17.10 IEEE 802.1AB LLDP

Os equipamentos terão que suportar LLDP cumprindo a norma IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery e as seguintes especificações:

- Número máximo de políticas de rede que podem ser associados com a porta: 8;
- Número máximo de políticas de rede que podem ser configurados por chassis virtual: 32.

1.2.14.2.17.11 IPv4

1.2.14.2.17.11.1 Os equipamentos terão de suportar os seguintes RFC:

791–Internet Protocol;



792–Internet Control Message Protocol;
826–An Ethernet Address Resolution Protocol;
2784–Generic Routing Encapsulation (GRE);
2890–Key and Sequence Number Extensions to GRE (extensions defined are not supported);
1701–Generic Routing Encapsulation (GRE);
1702–Generic Routing Encapsulation over IPV4 Networks;
2003-IP Encapsulation within IP.
4292 – IP Forwarding Table MIB
4293 – Management Information Base for Internet Protocol (IP)

1.2.14.2.17.11.2 Os equipamentos terão de suportar os seguintes itens:

- Número de interfaces de router por Sistema: 4000;
- Número de interfaces de router por vlan: 16;
- Número de rotas de hardware: 113000
- Número de entradas de hardware ARP: 24000 (modo switch) e 64 000 (ER – edge router mode);
- Número máximo de interfaces de tuneis GRE por sistema: 127;
- Número máximo de interfaces túnel IPIP por chassis virtual: 127;
- Número máximo de gateways ECMP: 16
- Número máximo de rotas estáticas (incluindo Black Hole Routes):4094

1.2.14.2.17.11.3 VRF (Virtual Routing and Forwarding)

1.2.14.2.17.11.3.1. Os equipamentos terão que suportar múltiplos VRF por cada equipamento permitindo configurar instâncias de routing separadas no mesmo equipamento. Cada instância de routing terá que manter independentemente o seu routing e table de forwarding, peer e informação de interface.

1.2.14.2.17.11.3.2. Os equipamentos terão que suportar:

- Maximum number of MAX profile VRF instances per VC (no LOW profiles): 64
- Maximum number of LOW profile VRF instances per VC (no MAX profiles): 128



- Número de instância VRF por vlan: 1;
- Número de instâncias routing VRF OSPFv2/v3 por chassis virtual: 16;
- Número de instâncias routing RIPv2/ng por chassis virtual: 16;
- Número de instâncias routing VRF BGP por chassis virtual: 32.

1.2.14.2.17.12 IPv6

1.2.14.2.17.12.1 Os equipamentos terão de suportar os seguintes RFC:

- 1981—Path MTU Discovery for IP version 6;
- 2375—IPv6 Multicast Address Assignments;
- 2460—Internet Protocol, Version 6 (IPv6) Specification;
- 2464—Transmission of IPv6 Packets over Ethernet Networks;
- 2465—Management Information Base for IP Version 6: Textual Conventions and General Group;
- 2466—Management Information Base for IP Version 6: ICMPv6 Group;
- 2711—IPv6 Router Alert Option;
- 3056—Connection of IPv6 Domains via IPv4 Clouds;
- 3484—Default Address Selection for Internet Protocol version 6 (IPv6);
- 3493—Basic Socket Interface Extensions for IPv6;
- 3542—Advanced Sockets Application Program Interface (API) for IPv6;
- 3587—IPv6 Global Unicast Address Format;
- 3595—Textual Conventions for IPv6 Flow Label;
- 3596— DNS Extensions to Support IP Version 6;
- 4007—IPv6 Scoped Address Architecture;
- 4022—Management Information Base for the Transmission Control Protocol (TCP);
- 4113—Management Information Base for the User Datagram Protocol (UDP);
- 4193—Unique Local IPv6 Unicast Addresses;
- 4213—Basic Transition Mechanisms for IPv6 Hosts and Routers;



- 4291—IP Version 6 Addressing Architecture;
- 4294—IPv6 Node Requirements;
- 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification;
- 4861—Neighbor Discovery for IP version 6 (IPv6);
- 4862—IPv6 Stateless Address Autoconfiguration;
- 5095—Deprecation of Type 0 Routing Headers in IPv6;
- 5453—Reserved IPv6 Interface Identifiers;
- 5722—Handling of Overlapping IPv6 Fragments.

1.2.14.2.17.12.2 Os equipamentos terão que suportar:

- Número de Interfaces IPv6: 4096
- Túneis 6to4: 1;
- Número de túneis configurados: 255;
- Número de Hosts IPv6 (Neighbor Discovery): 16000 (switch mode e edge router);
- Número de endereços unicast global IPv6 ou anycast: 10000;
- Número de endereços unicast global IPv6 por interface IPv6: 50;
- Número de rotas estáticas IPv6 (incluindo rotas black hole): 512;
- Número de Peers RIPng:20;
- Número de interfaces RIPng:20;
- Número de rotas RIPng: 5000;
- Número de gateways ECMP:16;

1.2.14.2.18 Especificações IP Sec

Os equipamentos terão de suportar IPSEC sobre IPv4 e IPv6 cumprindo os seguintes

RFC:

- 4301—Security Architecture for the Internet Protocol;



- 4302—IP Authentication Header (AH);
- 4303—IP Encapsulating Security Payload (ESP);
- 4305—Cryptographic Algorithm Implementation Requirements for ESP and AH;
- 4308—Cryptographic Suites for IPsec.

Algoritmos suportados para ESP: NULL, 3DES-CBC e AES-CBC;

Tamanhos das chaves suportados pelos algoritmos de cifragem:

- 3DES-CBC - 192 bits;
- AES-CBC – 128, 192, ou 256 bits;

Algoritmos de autenticação suportados para AH:

- HMAC-SHA1-96, HMAC-MD5-96, e AES-XCBC-MAC-96, HMAC-SHA256;
- HMACSHA384, HMAC-SHA512;

Tamanho das chaves suportados para os algoritmos de autenticação:

- HMAC-MD5 - 128 bits;
- HMAC-SHA1 - 160 bits;
- AES-XCBC-MAC - 128 bits.

Formato da chave mestra de segurança: Hexadecimal (16bytes) ou String (16 caracteres).

Intervalos de valores de prioridades para políticas IPsec: 1-1000 (1 = alta prioridade 1000 = baixa prioridade).

Intervalo de valores para regra das políticas IPsec: 1-10;

Intervalo SPI: 256-9999999999;

Modos suportados: Transporte.

1.2.14.2.19 Especificações RIP



1.2.14.2.19.1 Os equipamentos terão de suportar os seguintes RFCs:

- RFC 1058–RIP v1;
- RFC 2453–RIP v2;
- RFC 1722–RIP v2 Protocol Applicability Statement;
- RFC 1724–RIP v2 MIB Extension;
- RFC 2080–RIPng for IPv6 RFC 2082–RIP-2 MD5 Authentication.
- RFC 2082 - RIP-2 MD5 Authentication
- RFC 4822 - RIPv2 Cryptographic Authentication

1.2.14.2.19.2 Especificações RIP que os equipamentos terão de suportar:

- Número de interfaces: 10;
- Número de peers: 100;
- Número de rotas: 10000;

1.2.14.2.20 Bidirectional Forwarding Detection (BFD)

1.2.14.2.20.1 Os equipamentos terão que suportar o protocolo BFD.

1.2.14.2.20.2 Terão de suportar os RFC seguintes:

- 5880—Bidirectional Forwarding Detection;
- 5881—Bidirectional Forwarding Detection for IPv4 and IPv6 (Single Hop);
- 5882—Generic Application of Bidirectional Forwarding Detection.

1.2.14.2.20.3 Os equipamentos terão que suportar:

- Número de sessões BFD:
- Chassis: 32;
- Virtual Chassis: 100;
- Protocolos: BGP, OSPF, VRRP Remote Address Tracking e rotas estáticas.
- Modos: Assíncrono Echo.



1.2.14.2.21 Especificações DHCP Relay/Snooping

Os equipamentos terão que suportar os seguintes RFCs e as seguintes especificações:

- 0951–Bootstrap Protocol;
- 1534–Interoperation between DHCP and BOOTP;
- 1541–Dynamic Host Configuration Protocol;
- 1542–Clarifications and Extensions for the Bootstrap Protocol;
- 2132–DHCP Options and BOOTP Vendor Extensions;
- 3046–DHCP Relay Agent Information Option, 2001.

Implementação DHCP relay:

- DHCP global;
- DHCP por Vlan.

Serviço DHCP Relay: BOOTP/DHCP (Bootstrap Protocol/Dynamic Host Configuration Protocol)

Número dos portos:

- 67 para os pedidos
- 68 para as respostas.

Número de endereços IP suportados por cada serviço de relay: 1536;

Número de endereços suportados em modo interface: 1536;

Número de serviço relay UDP por chassis virtual: 30;

Número de vlans em que o serviço de forward UDP é permitido: 256;

Número de VLAN de entradas de filtragem por IP origem:

- 32 VLANs com 223 clientes;
- 16 VLANs com 239 clientes;
- 8 VLANs com 247 clientes;
- 4 VLANs com 251 clientes.

Maximum port level IP source filtering entries:254 Clients



1.2.14.2.22 Especificações DHCPv6 Relay / Snooping

Os equipamentos terão que suportar:

- RFC 3315 – Dynamic Host Configuration Protocol for Ipv6 (DHCPv6).
- Implementação de relay DHCP por VLAN DHCP
- Número dos portos destino UDP:
 - 547 - DHCPv6 messages to a DHCPv6 Server ou Relay Agent
 - 546 - DHCPv6 messages to a Client
- Número de destinos de relay por interface de relay DHCPv6:5;
- Número Vlan snooping DHCPv6 (por VLAN mode):64;
- Número de VLANs guard DHCPv6: 64;
- Número de serviços Relay UDP IPv6 genéricos:8;
- Número de portas relay UDP IPv6:8;
- Número de destino UDP IPv6 por porta:8.

1.2.14.2.23 Servidor DHCP

1.2.14.2.23.1 Os equipamentos terão que suportar a funcionalidade de servidor de DHCP cumprindo os seguintes RFC:

- RFC 2131—Dynamic Host Configuration Protocol;
- RFC 3315—Dynamic Host Configuration Protocol for IPv6;
- RFC 950—Internet Standard Subnetting Procedure;
- RFC 868—Time Protocol;
- RFC 1035—Domain Implementation and Specification;
- RFC 1191—Path MTU Discovery.

1.2.14.2.23.2 Implementação de servidor DHCP server: BOOTP/DHCP

1.2.14.2.23.3 Mecanismos de disponibilização de endereços:



- BootP estático;
- DHCP estático;
- DHCP dinâmico.

1.2.14.2.23.4 Os equipamentos terão que suportar:

- Número de leases: 8000;
- Tamanho de informação de lease: 375k.

1.2.14.2.24 Virtual Router Redundancy Protocol

1.2.14.2.24.1 Os equipamentos terão que suportar Virtual Router Redundancy Protocol.

1.2.14.2.24.2 Os RFC que terão de ser suportados são os seguintes:

- RFC 3768—Virtual Router Redundancy Protocol;
- RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol;
- RFC 5798 - Virtual Router Redundancy Protocol (VRRP) Version 3 para IPv4 e IPv6;
- RFC 6527 - Definitions of Managed Objects para VRRP Version 3 (VRRPv3) IPv6.

1.2.14.2.24.3 Especificações VRRP que os equipamentos terão de suportar:

- Número de routers virtuais VRRPv2 e VRRPv3: 255;
- Número de endereços IP por instância: 16.

1.2.14.2.25 Server Load balacing

1.2.14.2.25.1 Os equipamentos terão de suportar Server load balacing.

1.2.14.2.25.2 Número de clusters:32;

1.2.14.2.25.3 Número de servidores físicos por cluster:32;

1.2.14.2.25.4 Classificação layer 3:

- Endereço IP destino;
- Condição de política de QoS.

1.2.14.2.25.5 Classificação Layer 2: - Condição de política de QoS.



1.2.14.2.25.6 Verificação do estado do servidor: Ping, verificação de link.

1.2.14.2.25.7 Suporte de alta disponibilidade: Hardware-based failover, VRRP, Chassis Management Module(CMM) redundancy.

1.2.14.2.25.8 Protocolos de rede a suportar: Endereço IP virtual.

1.2.14.2.26 Especificações IPMS

1.2.14.2.26.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 1112—Host Extensions for IP Multicasting
- RFC 2236—Internet Group Management Protocol, Version 2
- RFC 2710—Multicast Listener Discovery (MLD) for IPv6
- RFC 2933—Internet Group Management Protocol MIB
- RFC 3019—IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
- RFC 3376—Internet Group Management Protocol, Version 3
- RFC 3810—Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4541—Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4604—Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.

1.2.14.2.26.2 Os equipamentos terão de suportar as seguintes versões de IGMP: IGMPv1, IGMPv2, IGMPv3.

1.2.14.2.26.3 Número de fluxos multicast IPv4 (switched): 12000.

1.2.14.2.26.4 Número de fluxos multicast IPV4 (*,G routed): 12000.

1.2.14.2.26.5 Número de fluxos multicast IPV4 (S,G routed): 12000.

1.2.14.2.27 IPMSv6

1.2.14.2.27.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 2710—Multicast Listener Discovery for IPv6
- RFC 3019—IPv6 MIB for Multicast Listener Discovery Protocol



- RFC 3306—Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3810—Multicast Listener Discovery Version 2 for IPv6
- RFC 4541—Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4604—Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.

1.2.14.2.27.2 Os equipamentos terão de suportar as seguintes versões de MLD: MLDv1, MLDv2.

1.2.14.2.27.3 Intervalo de Query MLD: 1 a 65535 segundos.

1.2.14.2.27.4 MLD Router timeout: 1 a 65535 segundos.

1.2.14.2.27.5 MLD Source timeout: 1 a 65535 segundos.

1.2.14.2.27.6 MLD Query Response Interval: 1-65535 milisegundos.

1.2.14.2.27.7 MLD Last Member Query Interval: 1-65535 milisegundos.

1.2.14.2.27.8 Número de fluxos multicast IPv6 (switched): 6000.

1.2.14.2.27.9 Número de fluxos multicast IPV6 (*,G routed): 6000.

1.2.14.2.27.10 Número de fluxos multicast IPV6 (S,G routed): 6000.

1.2.14.2.28 QoS

1.2.14.2.28.1 Os equipamentos terão que suportar as seguintes especificações:

- Número máximo de regras:2000
- Número de condições de políticas: 2000;
- Número de ações de políticas: 2000;
- Número de grupos (rede, MAC, serviço, porta): 2047;
- Número de entradas de grupo:1024 por grupo (256 por grupo de serviço);
- Número máximo de filas CoS por porta: 8;
- Perfis Queue Set (QSP):2;
- Número de listas de políticas QoS: 32.



1.2.14.2.29 LDAP Policy Server

1.2.14.2.29.1 Os equipamentos terão que suportar os seguintes RFCs:

- RFC 2251–Lightweight Directory Access Protocol (v3);
- RFC 3060–Policy Core Information Model—Version 1 Specification.

1.2.14.2.29.2 Número de policy servers (suportados num chassis virtual):5.

1.2.14.2.29.3 Número de policy servers(suportados por PolicyView):1.

1.2.14.2.30 Servidor de autenticação

1.2.14.2.30.1 Os equipamentos terão de suportar os seguintes RFCs:

- RFC 2865–Remote Authentication Dial In User Service (RADIUS);
- RFC 2866–RADIUS Accounting;
- RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support;
- RFC 2868–RADIUS Attributes for Tunnel Protocol Support;
- RFC 2809–Implementation of L2TP Compulsory Tunneling through RADIUS;
- RFC 2869–RADIUS Extensions;
- RFC 2548–Microsoft Vendor-specific RADIUS Attributes;
- RFC 2882–Network Access Servers Requirements: Extended RADIUS Practices;
- RFC 1492–An Access Control Protocol;
- RFC 1789–Connectionless Lightweight X.5000 Directory Access Protocol;
- RFC 2247–Using Domains in LDAP/X.500 Distinguished Names;
- RFC 2251–Lightweight Directory Access Protocol (v3);
- RFC 2252–Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions;
- RFC 2253–Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names;
- RFC 2254–The String Representation of LDAP Search Filters
- RFC 2256–A Summary of the X.500(96) User Schema for Use with LDAPv3;



- RFC 2574–User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
- RFC 2924–Accounting Attributes and Record Formats;
- RFC 2975–Introduction to Accounting Management;
- RFC 2989–Criteria for Evaluating AAA Protocols for Network Access.

1.2.14.2.30.2 Os equipamentos terão de suportar:

- Número de servidores autenticação no modo de autoridade única (single authority): 8;
- Número de servidores de autenticação no modo de autoridade múltipla:8;
- Número de servidores por cada switch autenticado:8.

1.2.14.2.31 Universal Network Profiles (UNP)

Os equipamentos terão de suportar Universal Network Profiles (UNP) com as seguintes características:

- Número de UNPs por chassis virtual: 4000;
- Número de utilizadores UNP por chassis:2000;
- Número de utilizadores por chassis virtual:2000;
- Tipo de autenticação: Por MAC e 802.1x;
- Tipo de perfil: VLAN,SPB e VXLAN.
- Tipo de porta UNP: Bridge e acesso;
- Número de lista de políticas de QoS por chassis virtual: 32 (incluindo a lista por defeito);
- Número de lista de políticas de QoS por UNP:1.

1.2.14.2.32 Access Guardian

1.2.14.2.32.1 Os equipamentos terão de suportar os seguintes RFC:

- RFC 2284–PPP Extensible Authentication Protocol (EAP);
- RFC 2865–Remote Authentication Dial In User Service (RADIUS);
- RFC 2866–RADIUS Accounting;



- RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support;
- RFC 2868–RADIUS Attributes for Tunnel Protocol Support;
- RFC 2869–RADIUS Extensions;
- RFC 3576--Change of Authorization-Request (COA) and Disconnect request (DM) for BYOD.
RFC support is limited to ClearPass solution;
- RFC 3579–RADIUS Support for EAP.

1.2.14.2.32.2 Os equipamentos terão de suportar as seguintes normas IEEE:

- IEEE 802.1X-2001–Standard for Port-based Network Access Control;
- 802.1X RADIUS Usage Guidelines.

1.2.14.2.32.3 Métodos de autenticação que tem de suportar:

- 802.1X;
- Endereços MAC;
- Portal Captivo.

1.2.14.2.32.4 Número de utilizadores access guardian (sistema): 1000(NI) e 2000(VC).

1.2.14.2.32.5 Número de utilizadores em quarentena por QMR: 1000(NI) e 2000(VC).

1.2.14.2.32.6 Número de utilizadores médio permitidos para login no portal captativo num dado instante:40.

1.2.14.2.32.7 Número de perfis de portal captativo:8.

1.2.14.2.32.8 Número de perfis AAA: 8.

1.2.14.2.32.9 Número de servidores de autenticação: 4 por tipo de autenticação (MAC, 802.1X, Portal Captativo).

1.2.14.2.32.10 Número de servidores de accounting: 4 por tipo de autenticação (MAC, 802.1X, Portal Captativo).

1.2.14.2.32.11 mDNS GRE Tunnel Supported Protocol:IPv4

1.2.14.2.32.12 SSDP GRE Tunnel Supported Protocol:IPv4



1.2.14.2.32.13 Maximum L2 GRE Access Tunnels:1

1.2.14.2.32.14 Maximum L2 GRE Aggregation Tunnels:2 000.

1.2.14.2.33 Port mapping

1.2.14.2.33.1 Port mapping é uma facilidade de segurança que controla a comunicação entre utilizadores peers. Os equipamentos deverão possuir esta facilidade.

1.2.14.2.33.2 Número de sessões de port mapping: 8.

1.2.14.2.34 Especificações de Learned port security (LPS)

1.2.14.2.34.1 Os equipamentos terão que suportar Learned port security (LPS).

1.2.14.2.34.2 Portas eligíveis para Learned Port Security: Fixas e 802.1Q tagged.

1.2.14.2.34.3 Portas não eligíveis para Learned Port Security: Portas agregadas e portas agregadas 802.1Q(trunked).

1.2.14.2.34.4 Número máximo de MAC apreendidas por porta LPS:1000.

1.2.14.2.34.5 Número máximo de endereços MAC filtrados permitidos por porta LPS:100.

1.2.14.2.34.6 Número máximo de intervalos de endereços MAC configuráveis por porta LPS:8.

1.2.14.2.35 Port Mirroring

Os equipamentos terão que suportar Port mirroring com as seguintes especificações:

- Número de Sessões de mirroring: 7;
- Número de sessões combinadas Mirroring /monitoring por chassis: 7;
- Suportar N to 1 Mirroring: 128 to 1;
- Número máximo de destinos mirroring suportados
- Número de Vlans RPMIR por sessão: 1.



1.2.14.2.36 Port monitoring

Os equipamentos terão que suportar Port monitoring com as seguintes especificações:

- Número de sessões a suportar:1;
- Sessões combinadas de mirroring/monitoring por chassis: 7;
- Tipo de ficheiro suportado: formato de ficheiro ENC (Network General Sniffer Network Analyzer Format).

1.2.14.2.37 SFlow

1.2.14.2.37.1 Os equipamentos terão de suportar SFlow e o RFC 3176.

1.2.14.2.37.2 Instância de receção/amostra/polling:2.

1.2.14.2.37.3 Amostragem:

- tamanho de pacote;
- tipo de trama;
- Endereços MAC de origem e destino;
- Vlans de origem e destino;
- Endereços IP de origem e destino;
- Portos de origem e destino;
- Flags TCP e TOS.

1.2.14.2.37.4 Polling:

- Octetos de entrada;
- Octetos de saída;
- Número de pacotes unicast de receção;
- Número de pacotes unicast de transmissão;
- Número de pacotes multicast de receção;
- Número de pacotes multicast de transmissão;
- Número de pacotes de broadcast de receção;
- Número de pacotes de broadcast de transmissão;
- Erros de entrada;



- Erros de saída.

1.2.14.2.38 RMON

Os equipamentos terão de suportar o RFC 2819 - Remote Network Monitoring Management Information Base.

Funcionalidades suportadas:

- Implementação de grupo RMON4 básico;
- Grupo de estatísticas ethernet;
- Grupo (controlo e estatísticas) histórico;
- Grupo de Alarmes;
- Grupo eventos.

Tipo de probe: Ethernet/History/Alarm

Status: Ativo/Criando/Inativo

History Control Interval (seconds):1-3600

History Sample Index Range:1-65535

Alarm Interval (seconds): 1–2147483647

Alarm Startup Alarm: Rising Alarm/Falling Alarm/

RisingOrFallingAlarm

Alarm Sample Type: Delta Value/Absolute;

RMON Traps Supported: RisingAlarm/FallingAlarm These traps are generated whenever an Alarm entry crosses either its Rising Threshold or its Falling Threshold and generates an event configured for sending SNMP traps

1.2.14.2.39 Estado do Switch (Switch Health)

1.2.14.2.39.1 Funcionalidade Health a suportar:

- Estatísticas de utilização de CPU ao nível do switch (percentagem);
- Estatísticas de entrada ao nível Switch/modulo/porta (percentagem);
- Estatísticas de utilização Entrada/saída ao nível do Switch/modulo/porta (percentagem);



- Estatísticas de utilização de memória ao nível do switch (percentagem);
- Estatísticas da temperatura ao nível de dispositivo (por exemplo, Chassis/CMM).

1.2.14.2.39.2 Monitorização do nível de utilização dos recursos:

- Nível de utilização mais recente;
- Nível de utilização média no último minuto;
- Nível de utilização na última hora;
- Nível de utilização máximo na última hora.

1.2.14.2.40 Vlan Stacking

1.2.14.2.40.1 Os equipamentos terão de suportar as seguintes normas IEEE:

- IEEE 802.1Q, 2003 Edition,
- IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks P802.1ad/D6.0 (C/LM) Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

1.2.14.2.40.2 Número de serviços: 4.

1.2.14.2.40.3 Número de SVLANs: 4000.

1.2.14.2.40.4 Número de SAPs: 8000.

1.2.14.2.40.5 Número de perfis SAP: 8000.

1.2.14.2.40.6 Número de VLANs de cliente (CVLANs) por chassis virtual: 4000.

1.2.14.2.40.7 Número de associações Service-to-SAP:1000.

1.2.14.2.40.8 Maximum supported SAP-UNI-CVLAN:4000.

1.2.14.2.41 Switch logging

Os equipamentos terão de suportar o seguinte RFC: RFC-5424 Syslog Protocol.

Número de servidores Syslog: 12.

Dispositivo de logging: Memória Flash/Consola/Endereço IP.

Tipos / Níveis de severidade:



- 2 (Alarm - highest severity),
- 3 (Error),
- 4 (Alert),
- 5 (Warning)
- 6 (Info - default),
- 7 (Debug 1),
- 8 (Debug 2),
- 9 (Debug 3 - lowest severity).

1.2.14.2.42 Ethernet OAM

1.2.14.2.42.1 Os equipamentos terão de suportar as seguintes normas:

- IEEE 802.1ag Version 8.1–Connectivity Fault Management;
- IEEE 802.1D–Media Access Control (MAC) Bridges;
- IEEE 802.1Q–Virtual Bridged Local Area Networks ITU-T Y.1731–OAM Functions and Mechanisms for Ethernet-Based Networks.

1.2.14.2.42.2 Número de domínios de manutenção (MD) por bridge:8.

1.2.14.2.42.3 Número de associações de manutenção (MA) por bridge: 128.

1.2.14.2.42.4 Número de end points de manutenção (MEP) por bridge:256.

1.2.14.2.42.5 Tamanho da base de dados MEP: 1000.

1.2.14.2.42.6 Intervalo mínimo CCM: 100ms.

1.2.14.2.43 Link OAM

Os equipamentos terão de suportar as normas IEEE e RFC seguintes:

- IEEE 802.3ah–EFM LINK OAM
- RFC 4878 - Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) functions on Ethernet-Like Interfaces.



1.2.14.2.44 Service Assurance Agent (SAA)

1.2.14.2.44.1 Os equipamentos terão de suportar o Service Assurance Agent (SAA).

Nota: O SAA utiliza a monitorização ativa para gerar tráfego de modo contínuo, fiável e de modo preditivo permitindo efetuar medidas de desempenho de rede.

1.2.14.2.44.2 Número de SAAs: 128.

1.2.14.2.44.3 Número de sessões SAA SPB: 128 (por BVLAN).

1.2.14.2.45 Routing avançado

Os equipamentos terão de suportar os seguintes protocolos dinâmicos:

- OSPF V2 e V3;
- IS-IS;
- BGP;

bem como protocolos de routing multicast.

1.2.14.2.46 Os equipamentos terão de suportar Open Shortest Path First (OSPF) v2

1.2.14.2.46.1 Os RFC que terão de ser suportados são os seguintes:

- 1370—Applicability Statement for OSPF;
- 4750—OSPF Version 2 Management Information Base;
- 2328—OSPF Version 2;
- 5250—The OSPF Opaque LSA Option;
- 3101—The OSPF Not-So-Stubby Area (NSSA) Option;
- 3623—Graceful OSPF Restart;
- 5709 - SPFv2 HMAC-SHA Cryptographic Authentication.

1.2.14.2.46.2 Especificações OSPFv2 que os equipamentos terão de suportar:

- Número de áreas: 10;
- Número de interfaces: 200;



- Número de interfaces passivas: 200;
- Número de entradas da base de Link State: 100000;
- Número máximo de vizinhos por router: 254;
- Número máximo de rotas: 32000;
- Número máximo de entradas next hop ECMP: 16.

1.2.14.2.47 Os equipamentos terão de suportar OSPF versão 3

1.2.14.2.47.1 RFC que terão de ser suportados:

- RFC 1826—IP Authentication Header ;
- RFC 1827—IP Encapsulating Security Payload;
- RFC 2553—Basic Socket Interface Extensions for IPv6;
- RFC 2373—IPv6 Addressing Architecture;
- RFC 2374—An IPv6 Aggregatable Global Unicast Address Format;
- RFC 2460—IPv6 base specification;
- RFC 2740—OSPF for IPv6;
- RFC 5643—Management Information Base for OSPFv3.

1.2.14.2.47.2 Especificações OSPFv3 que os equipamentos terão de suportar:

- Número de áreas: 5;
- Número de interfaces: 128;
- Número de entradas na base de dados Link State: 20000;
- Número de vizinhos: 128;
- Número de rotas: 32000;
- Número de entrada ECMP next Hop: 16.

1.2.14.2.48 Os equipamentos terão de suportar Intermediate System to Intermediate System (IS-IS)

1.2.14.2.48.1 As normas que terão de ser suportados são os seguintes:



- 1142-OSI IS-IS Intra-domain Routing Protocol;
- 1195-OSI IS-IS for Routing in TCP/IP and Dual Environments;
- 3373-Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point- to-Point Adjacencies;
- 3567-Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication;
- 2966-Prefix Distribution with two-level IS-IS (Route Leaking) support;
- 2763-Dynamic Host name exchange support;
- 3719-Recommendations for Interoperable Networks using IS-IS;
- 3787-Recommendations for Interoperable IP Networks using IS-IS;
- 5308-IS-IS support for IPv6 (Routing IPv6 with IS-IS);
- IETF- draft-ietf-isis-igp-p2p-over-lan-05.txt-Point-to-point operation over LAN in link-state routing protocols.

1.2.14.2.48.2 Especificações IS-IS que os equipamentos terão de suportar:

- Número máximo de áreas por router: 3;
- Número máximo de adjacências L1 por interface por router: 70;
- Número máximo de adjacências L2 por interface por router: 70;
- Número máximo de interfaces IS-IS (por router): 70;
- Número máximo de entradas Link State Pack por adjacência: 255;
- Número máximo de rotas IS-IS: 24000;
- Número máximo de rotas L1 IS-IS: 12000;
- Número máximo de rotas L2 IS-IS: 12000.

1.2.14.2.49 Os equipamentos terão de suportar Border Gateway Protocol (BGP)

1.2.14.2.49.1 Os RFC que terão de ser suportados são os seguintes:

- 1771/4271–A Border Gateway Protocol 4 (BGP-4);



- 2439–BGP Route Flap Damping;
- 3392/5492–Capabilities Advertisement with BGP-4;
- 2385–Protection of BGP Sessions via the TCP MD5 Signature Option;
- 1997–BGP Communities Attribute;
- 4456–BGP Route Reflection: An Alternative to Full Mesh Internal BGP(IBGP);
- 3065–Autonomous System Confederations for BGP;
- 4273–Definitions of Managed Objects for BGP-4;
- 4486–Subcodes for BGP Cease Notification;
- 4760–Multiprotocol Extensions for BGP-4;
- 2545–Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing;
- 2918 – Route Refresh Capability for BGP-4;
- 4724 – Graceful Restart Mechanism for BGP;
- 6793 – BGP 4-octet ASN;
- 5668 – 4-Octet AS Specific BGP Extended Community;
- 2042 – Registering New BGP Attribute Types;
- 5396 –Textual Representation of Autonomous System (AS) Numbers.

1.2.14.2.49.2 Os equipamentos terão que ao nível do BGP suportar os seguintes atributos: Origin, AS Path, Next Hop (IPv4), MED, Local Preference, Atomic Aggregate, Aggregator (IPv4), Community, Originator ID, Cluster List, Multiprotocol Reachable NLRI (IPv6), Multiprotocol Unreachable NLRI (IPv6), AS4 Path, AS4 Aggregator (IPv4), e AS Specific Extended Community.

1.2.14.2.49.3 Especificações BGP que os equipamentos terão de suportar:

- Número máximo de peers por switch (32 peers por VRF): 512;
- Número máximo de redes: 4000;
- Número máximo de endereços agregados: 2000;
- Número máximo de rotas: 128000;
- Número máximo de políticas: 1000.



1.2.14.2.50 Multicast Boundary

1.2.14.2.50.1 Normas que os equipamentos terão de suportar:

- RFC 2365—Administratively Scoped IP Multicast;
- RFC 5132 - IP Multicast MIB.

1.2.14.2.50.2 Intervalo de endereços válidos: 239.0.0.0 to 239.255.255.255.

1.2.14.2.50.3 Intervalo de endereços extended Multicast route boundary: 224.0.0.0 to 239.255.255.255.

1.2.14.2.51 Distance Vector Multicast Routing Protocol (DVMRP)

1.2.14.2.51.1 Normas que os equipamentos terão de suportar:

- RFC 1075—Distance Vector Multicast Routing Protocol, Version 1;
- RFC 4087—IP Tunnel MIB
- 2715—Interoperability Rules for Multicast Routing Protocols;
- IEEE draft-ietf-idmr-dvmrp-v3-09.txt - Distance Vector Multicast Routing Protocol, Version 3.

1.2.14.2.51.2 Versão DVMRP que terá de ser suportada: DVMRPv3.255

1.2.14.2.51.3 Atributos DVMRP:

- Reverse Path Multicasting,
- Neighbor Discovery,
- Multicast Source Location,
- Route Report Messages,
- Distance metrics,
- Dependent Downstream Routers,
- Poison Reverse,
- Pruning, Grafting,
- DVMRP Tunnels.



1.2.14.2.51.4 Temporizadores DVMRP:

- Flash update interval,
- Graft retransmissions,
- Neighbor probe interval,
- Neighbor timeout,
- Prune lifetime,
- Prune retransmission,
- Route report interval,
- Route hold-down,
- Route expiration timeout.

1.2.14.2.51.5 Número de interfaces: 384 (combinados entre PIMv4, PIMv6 e DVMRP).

1.2.14.2.51.6 Protocolos multicast por interface:1.

1.2.14.2.52 Protocol-Independent Multicast (PIM)

Os equipamentos terão de suportar os seguintes RFCs:

- 2365—Administratively Scoped IP Multicast;
- 4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification;
- 4007—IPv6 Scoped IP Multicast;
- 5060—Protocol Independent Multicast MIB;
- 5132—IP Multicast MIB 3569—An Overview of Source-Specific Multicast (SSM);
- 3973—Protocol Independent Multicast-Dense Mode (PIM-DM);
- 5015 - Bidirectional Protocol Independent Multicast (BIDIR-PIM);
- 5059—Bootstrap Router (BSR) Mechanism for PIM;
- 5240—Protocol Independent Multicast (PIM) Bootstrap Router MIB;
- 2715—Interoperability Rules for Multicast Routing Protocols.



1.2.14.2.52.1 Versão PIM a suportar: PIM-SMv2.

1.2.14.2.52.2 Atributos PIM

- Shared trees (also referred to as RP trees);
- Designated Routers (DRs);
- Designated Forwarders (DFs);
- Bootstrap Routers (BSRs);
- Candidate Bootstrap Routers (C-BSRs);
- Rendezvous Points (RPs) (applicable only for PIM-SM) and BIDIR-PIM;
- Candidate Rendezvous Points (C-RPs).

1.2.14.2.52.3 Temporizadores a suportar:

- C-RP expiry,
- C-RP holdtime,
- C-RP advertisement,
- Join/Prune, Probe,
- Register suppression,
- Hello,
- Expiry,
- Assert,
- Neighbor liveness,
- DF Election Timer.

1.2.14.2.52.4 Número de interfaces: 384 (combinados entre PIMv4, PIMv6 e DVMRP).

1.2.14.2.52.6 Bootstrap Routers (BSRs): 1.

1.2.14.2.52.7 1.56.7 Protocolos multicast por interface:1.

1.2.14.2.52.8 1.56.8 Anycast RP Routers: 8.

1.2.14.2.52.9 MBR

1.2.14.2.52.9.1 Os equipamentos terão de suportar os seguintes RFCs:



- 4601—Protocol Independent Multicast-Sparse Mode (PIM-SM) Protocol Specification;
- 3973—Protocol Independent Multicast-Dense Mode (PIM-DM);
- 2715—Interoperability Rules for Multicast Routing Protocols.

1.2.14.2.52.9.2 Os equipamentos terão de suportar os seguintes IETF Internet-Drafts: draft-ietf-idmr-dvmrp-v3-09.txt - Distance Vector Multicast Routing Protocol, Version 3.

1.2.14.2.52.9.3 Interoperabilidade MBR: DVMRP interoperabilidade com IPv4 PIM (PIM-SM e PIM-DM somente).

1.2.14.3 ACESSÓRIOS PARA OS6870-V12

1.2.14.3.1 Fonte de alimentação AC - OS6870-BPH

Fonte alimentação AC (PS-550W-AC-2/OS6870-BPH) para OS6870-V12 com uma potência máxima de saída de 550W, suportando uma tensão de entrada de 100V a 240 V AC, e frequência de entrada entre 50Hz e 60Hz.

1.2.14.3.2 OS6870-BP-D

Fonte de alimentação OS6870-BPD modular 250W DC para OS6870-V12.

1.2.14.3.3 Cabo Chassis Virtual para OS6870 de 1m (SFP-25G-C1M, SFP28).

Cabo que permita agregar dois switches OS6870 em chassis virtual. Terá de ser fornecido o conjunto de cabos necessário para o estabelecimento desse chassis virtual.

1.2.14.3.4 Cabo Chassis Virtual para OS6870 de 1m (QSFP-100G-C1M 100 Gigabit direct attached copper cable 1m, QSFP28)

Cabo que permita agregar dois switches OS6870 em chassis virtual. Terá de ser fornecido o conjunto de cabos necessário para o estabelecimento desse chassis virtual.



1.2.14.5 SFP-GIG-T 1000Base-T Gigabit Ethernet Transceiver (SFP MAS). SFP trabalha a 1000 Mb/s e em modo full-duplex

1.2.14.6 SFP-GIG-SX 1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA) – Multimodo

1.2.14.5 OS6-REAR-MNT2

Acessório de montagem em rack 19” para estabilização traseira de um OS6870.

1.2.15 SFP para os equipamentos Omniswitches

1.2.15.1 SFP 10G SR Multimodo

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3 Clause 52;
- Ligações a suportar: 10/100/1000Base-T
- Tipo de Fibra: Multimodo;
- Potência ótica de saída: -7,3 a -3,0 dBm @1G
- Sensibilidade de receção:-11,1 dBm;
- Distância: 300m
- Temperatura de funcionamento: -5°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.

1.2.15.2 SFP 10G-GIG-SR Dual Multimodo

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3-2005;
- Ligações a suportar: 10GBASE-SR/SW, 1000BASE-SX;
- Tipo de fibra: Fibra multimodo;
- Comprimento de onda: 850nm;



- Potência ótica de saída: -5 a -1 dBm @10G e -9,5 a -1 dBm @1G
- Sensibilidade de receção:-11,1 dBm @10G e -17dBm @1G;
- Alcance:
OM1: ~33m @ 10G, ~275m @ 1G
OM2: ~82m @ 10G, ~550m @ 1G
OM3: ~300m @ 10G, ~550m @ 1G
- Temperatura de funcionamento: 0°C a 70°C;
- SFP compatível com os equipamentos Omniswitch a fornecer e do mesmo fabricante.

1.2.15.3 SFP 10G-LR

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3 Clause 52;
- Ligações a suportar: 10GBASE-LR;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1310nm;
- Potência ótica de saída: -8.2 a +0.5 dBm;
- Sensibilidade de receção: -10,3dBm,
- Alcance: 10km;
- Temperatura de funcionamento: -5°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante.
- Suporte DDM.

1.2.15.4 SFP-10G-ER

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3 Clause 52;
- Ligações a suportar: 10GBASE-ER;
- Tipo de fibra: Fibra monomodo;



- Comprimento de onda: 1550nm;
- Potência ótica de saída: -4.7 to 4.0 dBm;
- Sensibilidade de receção: -14.1 dBm;
- Alcance: 40km;
- Temperatura de funcionamento: -5°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante.
- Suporte DDM.

1.2.15.5 SFP 10G-ZR

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3ae;
- Ligações a suportar: 10GBASE-ZR;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1550nm;
- Potência ótica de saída: 0 to +4 dBm;
- Sensibilidade de receção: -24 dBm;
- Alcance: 80km;
- Temperatura de funcionamento: 0°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante.
- Suporte DDM.

1.2.15.6 SFP 1000BASE-T

- Tipo de conector a suportar: RJ-45;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 10/100/1000Base-T
- Tipo de cabo: Cat5, Cat5e, Cat 6;
- Distância: 100m
- Temperatura de funcionamento: 0°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.

1.2.15.7 SFP 1000BASE-SX

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-SX;



- Tipo de fibra: Fibra multimodo;
- Comprimento de onda: 850nm;
- Potência ótica de saída: -9.5 a -4 dBm;
- Sensibilidade de receção: -17dBm,
- Alcance:
 - ~275 m on 62.5/125µm
 - ~550 m on 50/125µm
- Temperatura de funcionamento: 0°C a 70°C;
- SFP compatível com os equipamentos Omniswitch a fornecer e do mesmo fabricante.

1.2.15.8 SFP 1000BASE-LH-70 70Km

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-LX70;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1550nm;
- Potência ótica de saída: 0 a +5 dBm;
- Sensibilidade de receção: -22dBm,
- Alcance: 70km;
- Temperatura de funcionamento: 0°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante.
- Suporte DDM.

1.2.15.9 SFP 1000BASE-LH-120/ EZX 120Km

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-EZX;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1550nm;
- Alcance: 120km;
- Temperatura de funcionamento: -5°C a 70°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante.
- Suporte DDM.

1.2.15.10 iSFP 1000BASE-T

- Tipo de conector a suportar: RJ-45;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 10/100/1000Base-T
- Tipo de cabo: Cat5, Cat5e, Cat 6;
- Distância: 100m
- Temperatura de funcionamento: -40°C a 85°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.

1.2.15.11 iSFP 1000BASE-SX

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-SX;
- Tipo de fibra: Fibra multimodo;
- Comprimento de onda: 850nm;
- Potência ótica de saída: -9.5 a -3.5 dBm;
- Sensibilidade de receção: -18dBm,
- Alcance:



- ~275 m on 62.5/125µm
- ~550 m on 50/125µm
- Temperatura de funcionamento: -40°C a 85°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.

1.2.15.12 iSFP 1000BASE-LX 20Km

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-LX;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1310nm;
- Alcance: 20km;
- Temperatura de funcionamento: -40°C a 85°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.
- Suporte DDM.

1.2.15.13 iSFP 1000BASE-LH-40 40Km

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-LX40;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1310nm;
- Potência ótica de saída: -2 a +3 dBm;
- Sensibilidade de receção: -22dBm,
- Alcance: 40km;
- Temperatura de funcionamento: -40°C a 85°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.
- Suporte DDM.

1.2.15.14 iSFP 1000BASE-LH-70 70Km

- Tipo de conector a suportar: LC;
- Normas a suportar: 802.3z, SFP MAS;
- Ligações a suportar: 1000Base-LX70;
- Tipo de fibra: Fibra monomodo;
- Comprimento de onda: 1550nm;
- Potência ótica de saída: 0 a +5 dBm;
- Sensibilidade de receção: -22dBm;
- Alcance: 70km;
- Temperatura de funcionamento: -40°C a 85°C;
- SFP compatível com os equipamentos Omniswitch e do mesmo fabricante do equipamento.
- Suporte DDM.

1.2.16 Equipamento Switch Industrial (Layer 2) BRS30 Hirschmann ou equivalente

Para a construção dos anéis Layer 2 da rede multisserviço IP (Rede A) terá de ser utilizados equipamentos de rede industriais sem ventilação mecânica e com 8,16 ou 20 portas compatíveis com os equipamentos em produção na IP e sendo geríveis totalmente através da plataforma de gestão Hivision existente.

:



1.2.12.1 Equipamento de rede layer 2 industrial

Tipo 1

- Switch Industrial Hirschmann BRS30 sem ventoinhas (Store and forward) de 8 portas 10/100Base-T – RJ45 e 4 portas SFP Gigabit (Uplinks) com software Layer 2 Professional HiOS9.6 (BRS30-0804OOOO-SFCTV9HHSEAXX.X.XX.) ou equivalente

Tipo 2

- Switch Industrial Hirschmann BRS30 sem ventoinhas (Store and forward) de 16 portas 10/100Base-T – RJ45 e 4 portas SFP Gigabit (Uplinks) com software Layer 2 Professional HiOS9.6 (BRS30-1604OOOO-SFCTV9HHSEAXX.X.XX.) ou equivalente

Tipo 3

- Switch Industrial Hirschmann BRS30 sem ventoinhas (Store and forward) de 20 portas 10/100Base-T – RJ45 e 4 portas SFP Gigabit (Uplinks) com software Layer 2 Professional HiOS9.6 (BRS30-2004OOOO-SFCTV9HHSEAXX.X.XX.) ou equivalente

Terão de possuir no mínimo as seguintes características:

- Switch Industrial sem ventoinhas (Store and forward) de XX portas 10/100Base-T – RJ45 e 4 portas SFP Gigabit (Uplinks).
- O equipamento terá de permitir ser montado em DIN Rail.
- O equipamento terá de funcionar no seguinte intervalo de temperaturas: 0º a +60ºC. e em relação à Humidade relativa (sem condensação): 1% a 95%.
- O equipamento terá que ter gestão via TFTP, SFTP, SCP, LLDP (802.1AB), LLDP-MED, SSHv2, HTTP, HTTPS, Traps, SNMP v1/v2/v3, Telnet, IPv6 Management , DNS Client , OPC UA Server.
- O equipamento terá de suportar Dual Software Image.



- Conjuntamente com o equipamento terá de ser fornecido o rack DIN para instalação em bastidor 19”.
- Terá de incluir todo o licenciamento necessário para que o equipamento possa ser gerido pela plataforma HVision existente na IP.

Switching

- Independent VLAN Learning,
- Fast Aging,
- Static Unicast/Multicast Address
- Entries, QoS / Port Prioritization (802.1D/p),
- TOS/DSCP Prioritization,
- Interface Trust Mode,
- CoS Queue Management,
- Queue-Shaping / Max. Queue Bandwidth,
- Flow Control (802.3X), Egress Interface Shaping,
- Ingress Storm Protection,
- Jumbo Frames, VLAN (802.1Q),
- GARP VLAN Registration Protocol (GVRP),
- Voice VLAN,
- GARP Multicast Registration Protocol (GMRP),
- IGMP Snooping/Querier per VLAN (v1/v2/v3),
- Unknown Multicast Filtering,
- Multiple VLAN Registration Protocol (MVRP),
- Multiple MAC Registration Protocol (MMRP),
- Multiple Registration Protocol (MRP)

Diagnósticos

O equipamento terá de possuir os seguintes mecanismos de diagnóstico:

- Detecção de conflitos de endereços de gestão;
- Detecção de reaprendizagem de endereços;
- Detecção de erros de rede
- Notificação de MAC;
- RMON (1,2,3,9);
- Port Mirroring 1:1;
- Port Mirroring 8:1;
- Port Mirroring N:1;
- Realização de testes de diagnósticos automáticos em caso de Cold Start;
- Teste de cabo de cobre;
- Gestão de SFPs (temperatura, potência ótica de entrada e de saída (µW e dBm));
- Estado de funcionamento;
- Syslog;
- Detecção de Sobrecarga;



- Detecção de Link Flap;
- Detecção de Duplex Mismatch;
- Port-monitoring com auto-disable;
- Monitorização de Velocidade de link e duplex.
- Sincronização de tempo
- O equipamento terá que suportar:
 - Cliente SNTP;
 - Servidor SNTP;
 - 802.1AS
 - Buffered Real Time Clock;
 - PTPv2 Transparent Clock two-step;
 - PTPv2 Boundary Clock.

O equipamento terá de suportar perfis industriais:

- protocolo IEC61850 (Servidor MMS, Switch Model).
- Protocolo EtherNet/IP,
- Protocolo IEC61850 (MMS Server, Switch Model)
- Protocolo Modbus TCP
- Protocolo PROFINET Switching

Segurança

O equipamento terá de suportar:

- ISASecure CSA / IEC 62443-4-2 certificado
- MAC-based Port Security,
- Port-based Access Control with 802.1X, Guest/unauthenticated VLAN,
- Integrated Authentication Server (IAS),
- RADIUS VLAN Assignment,
- Denial-of-Service Prevention,
- DoS Prevention Drop Counter,
- VLAN-based ACL,
- Ingress VLAN-based ACL,
- Basic ACL, Access to Management restricted by VLAN,
- Device Security Indication, Audit Trail,
- CLI Logging, HTTPS
- Certificate Management,
- Restricted Management Access,
- Appropriate Use Banner,
- Configurable Password Policy,
- Configurable Number of Login Attempts,
- SNMP Logging,
- Multiple Privilege Levels,
- Local User Management,
- Remote Authentication via RADIUS,
- User Account Locking,
- Password change on first login
- RADIUS Policy Assignment,
- Multi-Client Authentication per Port,
- MAC Authentication Bypass,
- Format options for MAC authentication bypass,
- LDAP;

O equipamento terá de suportar tensão de alimentação DC entre 24 VDC e 48 VDC.



O equipamento terá que ter um consumo no máximo de 16W.

Configuração

O equipamento terá de suportar as seguintes funcionalidades:

- Automatic Configuration Undo (roll-back),
- Configuration Fingerprint,
- Text-based Configuration File (XML),
- Backup config on a remote server when saving,
- Clear config but keep IP settings,
- BOOTP/DHCP Client with Auto-Configuration,
- DHCP Server: per Port,
- DHCP Server: Pools per VLAN,
- AutoConfiguration Adapter ACA21/22 (USB),
- HiDiscovery,
- USB-C Management support,
- Command Line Interface (CLI),
- CLI Scripting,
- CLI script handling over ENVN at boot,
- Full-featured MIB Support,
- Context-sensitive Help,
- HTML5 based Management

Redundância

O equipamento terá de suportar os seguintes protocolos de redundância:

- HIPER-Ring (Ring Switch),
- Link Aggregation with LACP,
- Link Backup, Media Redundancy Protocol (MRP) (IEC62439-2),
- Redundant Network Coupling,
- RSTP 802.1D-2004 (IEC62439-1),
- RSTP Guards ,
- Sub Ring Manager

Estabilidade mecânica

O equipamento terá de suportar:

- IEC 60068-2-6 vibration 5 Hz ... 8,4 Hz with 3,5 mm amplitude; 2 Hz ... 13,2 Hz with 1 mm amplitude; 8,4 Hz ... 200 Hz with 1 g; 13,2 Hz ... 100 Hz with 0,7 g
- IEC 60068-2-27 shock 15 g, 11 ms duration

Imunidade interferências Eletromagnéticas



O equipamento terá de suportar:

- EN61000-4-2 electrostatic discharge (ESD): 6 kV contact discharge, 8 kV air discharge;
- EN61000-4-3 electromagnetic field: 10 V/m (80-1000 MHz) 5 V/m (2000-2700 MHz); 3 V/m (5100-6000 MHz);
- EN61000-4-4 fast transients (bursts): 2 kV power line, 2 kV data line;
- EN61000-4-5 surge voltage: power line: 2 kV (line/earth), 1 kV (line/line), 2 kV data line;
- EN61000-4-6 conducted immunity: 10 V (150 kHz-80 MHz);
- EN 55022 Class A.

Outras normas

- O equipamento terá que possuir aprovação nas seguintes normas:
- EN 50121;
- IEC61850.

1.2.16.1 Acessórios para os equipamentos switches industriais Hirschmann ou equivalentes

1.2.16.1.1 M-SFP-LX/LC ou equivalente: SFP Gigabit para Switch Hirschmann BRS30 modelo M-SFP-LX/LC (20Km) ou equivalente devendo possuir no mínimo as seguintes características:

- Módulo SFP Gigabit Ethernet para fibra ótica monomodo com conector LC.
- Alcance: 20Km.
- Link Budget a 1310nm: 0 – 11 dB (A=0,4dB/km, 3dB reserva, D=3,5ps(nm×km)).
- Diagnósticos: Potência ótica de entrada e saída e temperatura.
- Condições ambientais
 - - Temperatura de funcionamento: 0° a 60°C;
 - - Humidade relativa (sem condensação): 10% a 95%.
- MTBF: superior a 13 000 000 horas.
- Estabilidade mecânica
 - IEC 60068-2-27 shock: 15 g, 11 ms duration, 18 shocks;
 - IEC 60068-2-6 vibration: 1 mm, 2 Hz-13.2 Hz, 90 min.; 0.7 g, 13.2 Hz-100 Hz, 90 min.; 3.5 mm, 3Hz-9 Hz, 10 cycles, 1 octave/min.; 1 g, 9 Hz-150 Hz, 10 cycles, 1 octave/min.
- Imunidade interferências Eletromagnéticas
 - EN61000-4-2 electrostatic discharge (ESD): 6 kV contact discharge, 8 kV air discharge;
 - EN61000-4-3 electromagnetic field: 10 V/m (80-1000 MHz);
 - - EN61000-4-4 fast transients (bursts): 2 kV power line, 1 kV data line;
 - - EN61000-4-5 surge voltage: power line: 2 kV (line/earth), 1 kV (line/line), 1 kV data line;
 - - EN61000-4-6 conducted immunity: 3 V (10 kHz-150 kHz), 10 V (150 kHz-80 MHz).
- Cumprir a norma EN55022 Class A.
- O SFP terá de ser do mesmo fabricante que o equipamento de rede.

1.2.16.1.2 M-SFP-LX+/LC ou equivalente: SFP Gigabit para Switch Hirschmann BRS30 modelo M-SFP-LX+/LC (40Km) ou equivalente devendo possuir no mínimo as seguintes características:

- Módulo SFP Gigabit Ethernet para fibra ótica monomodo com conector LC.
- Alcance: 40Km.
- Link Budget a 1310nm: 5 – 20 dB (A=0,4dB/km, 3dB reserve).
- Diagnósticos: Potência ótica de entrada e saída e temperatura.
- Condições ambientais



- - Temperatura de funcionamento: 0° a 60°C;
 - - Humidade relativa (sem condensação): 10% a 95%.
- MTBF: superior a 13 000 000 horas.
- Estabilidade mecânica
 - IEC 60068-2-27 shock: 15 g, 11 ms duration, 18 shocks;
 - IEC 60068-2-6 vibration: 1 mm, 2 Hz-13.2 Hz, 90 min.; 0.7 g, 13.2 Hz-100 Hz, 90 min.; 3.5 mm, 3Hz-9 Hz, 10 cycles, 1 octave/min.; 1 g, 9 Hz-150 Hz, 10 cycles, 1 octave/min.
- Imunidade interferências Eletromagnéticas
 - EN61000-4-2 electrostatic discharge (ESD): 6 kV contact discharge, 8 kV air discharge;
 - EN61000-4-3 electromagnetic field: 10 V/m (80-1000 MHz);
 - EN61000-4-4 fast transientes (bursts): 2 kV power line, 1 kV data line;
 - EN61000-4-5 surge voltage: power line: 2 kV (line/earth), 1 kV (line/line), 1 kV data line;
 - EN61000-4-6 conducted immunity: 3 V (10 kHz-150 kHz), 10 V (150 kHz-80 MHz).
- Cumprir a norma EN55022 Class A.
- O SFP terá de ser do mesmo fabricante que o equipamento de rede.

1.2.16.1.3 M-SFP-LH/LC ou equivalente: SFP Gigabit para Switch Hirschmann BRS30 modelo M-SFP-LH/LC (70Km) ou equivalente devendo possuir no mínimo as seguintes características:

- Módulo SFP Gigabit Ethernet para fibra ótica monomodo com conector LC.
- Alcance: 70Km.
- Link Budget a 1550nm: 6 – 22 dB (A=0,25dB/km, 2dB reserve.
- Diagnósticos: Potência ótica de entrada e saída e temperatura.
- Condições ambientais
 - - Temperatura de funcionamento: 0° a 60°C;
 - - Humidade relativa (sem condensação): 10% a 95%.
- MTBF: superior a 13 000 000 horas.
- Estabilidade mecânica
 - IEC 60068-2-27 shock: 15 g, 11 ms duration, 18 shocks;
 - IEC 60068-2-6 vibration: 1 mm, 2 Hz - 13.2 Hz, 90 min.; 0.7g, 13.2 Hz - 100 Hz, 90 min.; 3.5 mm, 3 Hz - 9 Hz, 10 cycles, 1 octave/min.; 1g, 9 Hz - 150 Hz, 10 cycles, 1 octave/min.
- Imunidade interferências Eletromagnéticas
 - EN61000-4-2 electrostatic discharge (ESD): 6 kV contact discharge, 8 kV air discharge;
 - EN61000-4-3 electromagnetic field: 10 V/m (80-1000 MHz);
 - EN61000-4-4 fast transientes (bursts): 2 kV power line, 1 kV data line;
 - EN61000-4-5 surge voltage: power line: 2 kV (line/earth), 1 kV (line/line), 1 kV data line;
 - EN61000-4-6 conducted immunity: 3 V (10 kHz-150 kHz), 10 V (150 kHz-80 MHz).
- Cumprir a norma EN55022 Class A.
- O SFP terá de ser do mesmo fabricante que o equipamento de rede.

1.2.16.2 Conversor Pulls Modelo ML50-105 ou equivalente:

Conversor de 50W Vin 230VAC/110VDC Vout para 48VDC. O conversor terá que ter as seguintes características:

- Tensão de entrada: 100-240V AC 47 a 63 Hz;
- Tensão de entrada (limites): 85 .. 264V;
- Corrente de entrada:
 - <1.0A (AC 100V, Pout: 50W);



- < 0.6A(AC 196V, Pout: 50W);
- Imunidade a transientes: resistência a transientes de acordo com VDE 0160/W2 (750V/1.3ms);
- Hold-up time: > 170ms para AC 230V, 48V/1.05A;
- Tensão de saída: DC 48 – 56V (devendo ser ajustável por potenciômetro);
- Corrente de saída: 1,05A;
- Regulação de tensão: stat. <1% Vout dyn. $\pm 2\%$ Vout over all;
- Ripple/Noise: <200mVPP (20MHz bandw., 50 Ω measurement);
- Proteção de sobretensão (OVP) <60V;
- Power back immunity: 63V;
- A unidade deverá estar protegida contra curtos circuitos, sobretensões e circuito aberto;
- Montagem em DIN Rail;
- Eficiência: 90% (AC 230V, 48V/1.05A);
- Perdas: 6W (AC 230V, 48V/1.05A);
- MTBF: 600 000 horas (48V/1.05A AC230V e Tamb=+40°C);
- Condições ambientais
 - Temperatura de funcionamento: -10°C a +70°C;
 - Humidade (IEC60068-2-30): 5% a 95% (sem condensação);
 - Vibração (IEC60068-2-6): 2g;
 - Choque (IEC60068-2-27): 15g 6ms, 10g 11ms;
 - Prot. class/degree: Class I (EN60950) / IP20 (EN60529);
 - Safety approvals: EN 60 950, EN 60204-1, EN 50178.

1.3 Conversor AC/DC 230V/48 de 50W (para o equipamento de segurança)

- a) Tensão de entrada: 100-240V AC 47 a 63 Hz; 230VAC;
- b) Tensão de saída: DC 48 – 56V (devendo ser ajustável por potenciômetro);
- c) Potência mínima: 50W.

A unidade deverá estar protegida contra curtos circuitos, sobretensões e circuito aberto;

Condições ambientais

- o Temperatura de funcionamento: -10°C a +70°C;
- o Humidade (IEC60068-2-30): 5% a 95% (sem condensação);
- o Vibração (IEC60068-2-6): 2g;
- o Choque (IEC60068-2-27): 15g 6ms, 10g 11ms;