FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Caderno de Encargos

"AQUISIÇÃO DE EQUIPAMENTOS DE ENCAMINHAMENTO IP PARA NÓS DO PORTO"

GOVERNO DE PORTUGAL | MINISTRO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

Cofinanciado por:
COMPETE 2020 Lisb@20 20 CRESC ALGARVE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

ARTIGO 1.º

OBJECTO

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar entre a Fundação para a Ciência e a Tecnologia, I.P. e adjudicatário na sequência da adjudicação no âmbito da consulta para "Aquisição de equipamentos de encaminhamento IP para nós do Porto".
2. O Contrato a celebrar integra, para além do clausulado contratual:
   a) os suprimentos dos erros ou omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar, nos termos do artigo 50º do Código dos Contratos Públicos;
   b) os esclarecimentos e retificações relativos ao caderno de encargos que sejam emitidos ao abrigo do artigo 50º do Código dos Contratos Públicos;
   c) o caderno de encargos;
   d) a proposta adjudicada;
   e) os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos nas diferentes alíneas do número anterior, a prevalência obedece à ordem por que vêm enunciados nas suas diferentes alíneas.
4. Em caso de divergência entre os documentos referidos nas diferentes alíneas do nº 2 e o clausulado contratual, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101º do mesmo diploma.

ARTIGO 2.º

OBRIGAÇÕES DO ADJUDICATÁRIO

1. O adjudicatário obriga-se a executar o Contrato em termos que se conformem com o estabelecido no Caderno de Encargos, nos anexos que dele fazem parte integrante e na legislação aplicável.

2. Para além de outras obrigações previstas na lei ou no presente caderno de encargos, o adjudicatário obriga-se a:

   a) Assegurar que o objeto da prestação obedece às especificações técnicas exigidas;

   b) Cumprir os prazos estabelecidos, designadamente, para a execução das prestações a que se obriga;

   c) Prestar informação;

   d) Assegurar o sigilo.

ARTIGO 3.º

ESPECIFICAÇÕES TÉCNICAS

O adjudicatário obriga-se a assegurar que o objeto de aquisição obedece às especificações técnicas que constam do Anexo I ao presente Caderno de Encargos, do qual faz parte integrante.

ARTIGO 4.º

PRAZOS

O adjudicatário obriga-se ao pontual cumprimento de todos os prazos de execução das prestações objeto do contrato, os quais são os que constam do clausulado deste ou de outros documentos referidos no nº 2 do artigo 1º.

ARTIGO 5.º

ENTREGA

1. Os bens objeto de adjudicação consideram-se entregues após a respetiva aceitação por parte da FCT, I.P., a qual ocorre nos termos referidos nos nº 8 e 9 do anexo ao presente Caderno de Encargos.

2. Para os efeitos previstos no número anterior, a FCT, I.P. pode promover a realização de testes de aceitação nos termos definidos no nº 9 do anexo ao presente Caderno de Encargos, que se realizarão tendo por objetivo verificar o cumprimento dos requisitos estabelecidos no Anexo I ao presente Caderno de Encargos.

ARTIGO 6.º

OBRIGAÇÃO DE MANUTENÇÃO E GARANTIA

1. Caso se verifique qualquer anomalia nos bens objeto de adjudicação que impeça ou prejudique o desempenho da sua função, o adjudicatário obriga-se a proceder às operações necessárias à reposição deste nas mesmas condições que deram origem à aceitação nos termos e condições referidas no Anexo I ao presente Caderno de Encargos.

2. O prazo de garantia do equipamento fornecido será de 2 anos e incluirá os termos e abrangência previstos na lei aplicável.

ARTIGO 7.º

OBRIGAÇÃO DE PRESTAÇÃO DE INFORMAÇÃO

O adjudicatário obriga-se a prestar à FCT, I.P., por escrito, e no prazo que para tal for razoavelmente fixado pela FCT, toda a informação que lhe for solicitada relativa ao objeto da adjudicação ou à sua atuação em cumprimento das obrigações que para si decorrem do contrato.

ARTIGO 8.º

OBRIGAÇÃO DE SIGILO

O adjudicatário obriga-se a não divulgar informações que obtenha em virtude da execução do contrato durante a vigência deste e por um período de dois anos contados a partir da data da sua cessação.

ARTIGO 9.º

PREÇO E CONDIÇÕES DE PAGAMENTO

1. O preço base da aquisição a que se refere o presente caderno de encargos, entendido como o preço máximo que a FCT, I.P. se dispõe a pagar por todas as prestações objeto do presente

Caderno de Encargos é de 349.990€ (trezentos e quarenta e nove mil, novecentos e noventa euros); acrescidos de IVA à taxa legal em vigor[1].

2. Pela aquisição dos bens e serviços objeto do contrato, a FCT, I.P. pagará ao adjudicatário a quantia de ____ Euros [valor indicado na proposta adjudicada], acrescida de IVA à taxa legal em vigor nos termos do número seguinte.
3. A quantia prevista no número anterior deve ser satisfeita através do pagamento de uma fatura, a qual é emitida, após a entrega dos bens nos termos a que se refere o artigo 5º.
4. A fatura a emitir pelo adjudicatário assume a forma de fatura eletrónica, com os requisitos legais, nomeadamente os resultantes do artigo 299º-B do CCP.
5. A fatura referida no número 3 será paga no prazo máximo de trinta dias a contar da sua receção.

ARTIGO 10.º

VIGÊNCIA DO CONTRATO

1. O Contrato inicia a sua vigência na data da respetiva assinatura vigorando até estarem transcorridos três anos após a data da entrega na aceção do artigo 5º.
2. O artigo 8º cessa vigência na data em que cesse o prazo nele previsto.

ARTIGO 11.º

CAUÇÃO

1. Como forma de garantir o exato e pontual cumprimento de todas as obrigações legais e contratuais, bem como a celebração do contrato, o adjudicatário deve, no caso de o preço contratual ser igual ou superior a 200.000€, prestar caução nos termos e condições constantes estabelecido no artigo 90º do Código dos Contratos Públicos.

[1] O presente procedimento não prevê a adjudicação por lotes, uma vez que os equipamentos do tipo P e do tipo PE a adquirir farão parte da futura RCTS100 com arquitetura Segment Routing sobre MPLS. Dado que a interoperabilidade entre diversos fabricantes ao nível deste protocolo não é total assim com o das funcionalidades suportadas, a única forma de garantir o correto funcionamento da rede é garantindo que os equipamentos são da mesma marca, o que só é garantido pelo fornecimento por um único adjudicatário.

2. O valor da caução a prestar é de 5% do preço contratual

3. A caução é liberada nos termos previstos no artigo 295º do Código dos Contratos Públicos.

ARTIGO 12º

RESPONSABILIDADE DO ADJUDICATÁRIO

1. O adjudicatário responde pelos danos que causar à FCT, I.P. em razão do incumprimento culposo das obrigações que sobre ele impendam, nos termos das normas gerais de direito e do presente artigo.
2. O adjudicatário responde ainda perante a FCT, I.P. pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do Contrato, como se tais atos ou omissões fossem praticados por aquele.
3. O adjudicatário responde, independentemente de culpa, pelos danos causados à FCT, I.P. pela execução deficiente do Contrato.
4. Nenhuma das partes responde por danos causados à outra parte em virtude de incumprimento de obrigações emergentes do Contrato decorrente de caso fortuito ou força maior.
5. A parte que pretenda beneficiar-se do regime acolhido no número anterior deve, para o efeito, informar a outra parte da verificação de uma situação de incumprimento decorrente de caso fortuito ou de força maior, fazendo menção dos factos que, em seu entender, permitem atribuir esta origem ao incumprimento e, ainda, do prazo que estima necessário para cumprir a obrigação em causa.

ARTIGO 13º

CLÁUSULA PENAL

1. Sem prejuízo do n.º 4 do artigo anterior, pelo incumprimento, sob a forma de mora, de obrigações emergentes do contrato, a FCT, I.P. pode exigir do adjudicatário o pagamento de uma pena pecuniária nos seguintes termos:

   a) Pelo incumprimento do prazo para colocação dos bens objeto do contrato nas instalações do adjudicante nos termos do n.º 8 do Anexo I, um montante de 400€ (quatrocentos euros) por cada dia útil de atraso;

b) Pelo incumprimento da obrigação de prestação de informação, prevista no artigo 7º, um valor de 50€ (cinquenta euros) por cada dia útil de atraso na prestação da informação solicitada;

c) Pelo incumprimento do tempo de resposta, previsto no ponto 7.6. do Anexo I ao Caderno de Encargos, o montante de 300€ (trezentos euros) por cada hora de atraso, considerando-se que no caso de incumprimento do tempo de resposta definido para P4, um dia útil corresponde a 8 horas;

d) Pelo incumprimento do prazo estipulado para a substituição de equipamento, previsto no ponto 7.10 do Anexo I ao Caderno de Encargos, o montante de 1.000€ (mil euros) por cada dia útil de atraso;

e) Pela recusa de disponibilização de equipamento de substituição, tal como resultante do ponto 7.10 do Anexo I ao presente Caderno de Encargos, 10% do valor total do preço contratual pago em aplicação do nº 2 do artigo 9.º.

2. Sem prejuízo do disposto no número seguinte, os valores que resultem da aplicação das alíneas anteriores são calculados mensalmente, devendo o adjudicatário, na sequência de notificação da FCT, I.P., emitir a favor desta última uma nota de crédito para pagamento no prazo máximo de 30 dias.

3. As sanções de natureza pecuniária referidas no presente artigo têm como limite máximo o decorrente do artigo 329º do Código dos Contratos Públicos.

ARTIGO 14º

RESCISÃO

1. A FCT, I.P. pode rescindir o contrato:

   a) quando, estando o adjudicatário em mora, este não realize a prestação no prazo que lhe haja razoavelmente sido fixado pela FCT, I.P.;

   b) com fundamento em incumprimento das obrigações previstas no artigo 2º que determine a perda objetiva de interesse nas prestações que constituam o seu objeto;

2. A rescisão do contrato ao abrigo do disposto no número anterior determina a perda da caução prestada pelo adjudicatário, caso esta tenha sido prestada nos termos da lei e a extinção dos créditos de que este seja titular em virtude do referido contrato.

3. A perda da caução ao abrigo do número anterior não extingue o direito da FCT, I.P. de ser ressarcida da totalidade dos danos que lhe hajam sido causados pela conduta do adjudicatário que haja fundamentado a rescisão.

ARTIGO 15º

DESPESAS

Correm por conta do adjudicatário todas as despesas em que este haja de incorrer em virtude do cumprimento de obrigações emergentes do contrato.

ARTIGO 16º

LEI APLICÁVEL

O contrato rege-se pela lei portuguesa.

ARTIGO 17º

INTERPRETAÇÃO DO CONTRATO

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do Contrato, o adjudicatário deve solicitar por escrito um esclarecimento à FCT, I.P.
2. O adjudicatário obriga-se a ter em conta as orientações que lhe forem transmitidas por escrito pela FCT, I.P., na medida em que as mesmas não colidam com as regras aplicáveis à execução do Contrato.

ARTIGO 18º

COMUNICAÇÕES

1. Para efeitos de comunicações relativas à fase de execução do contrato, as partes podem recorrer aos seguintes meios de comunicação:
    a) correio postal, através de carta registada ou de carta registada com aviso de receção;
    b) correio eletrónico;

c) outro meio de transmissão eletrónica de dados.

2. Todas as comunicações devem ser escritas e redigidas em língua portuguesa.
3. Para efeitos de estabelecimento das comunicações a que se refere o presente artigo, as partes identificam os seguintes contactos, através dos quais as mesmas se devem concretizar:

a) Pela FCT, I.P.:

Nome do representante: Ana Tavares Pinto

Endereço postal: Av. do Brasil, 101 1700-066 Lisboa

Endereço eletrónico: compras@fccn.pt

Número de fax: +351 218472167

b) Pelo adjudicatário:

Nome do representante:

Endereço postal:

Endereço eletrónico:

Número de fax:

ARTIGO 19º

GESTOR DO CONTRATO

Para o exercício das funções de acompanhamento da execução do contrato nos termos regulados pelo artigo 290º-A do Código dos Contratos Públicos é designada Ana Pinto.

ARTIGO 20º

CESSÃO DA POSIÇÃO CONTRATUAL

1. A cessão da posição contratual do adjudicatário é possível nos termos do artigo 318º do Código dos Contratos Públicos.
2. Em caso de incumprimento contratual pelo adjudicatário que seja suscetível de conduzir à resolução do contrato, a sua posição contratual pode ser cedida aos concorrentes do

procedimento pré-contratual classificados nas posições subsequentes à do adjudicatário, nos termos do estabelecido no artigo 318º-A do Código dos Contratos Públicos.

ARTIGO 21º

ASSINATURA DO CONTRATO

O contrato a celebrar entre a FCT, I.P. e o adjudicatário será celebrado com recurso preferencial, por ambas as partes, à assinatura eletrónica qualificada, tal como definida pelo Decreto-lei nº 290D/99, de 2 de agosto, com as alterações introduzidas pelos Decretos-lei n.º 62/2003, de 3 de abril, 165/2004, de 6 de julho e 116-A/2006, de 16 de junho.

ARTIGO 22.º

TRIBUNAL DE CONTAS

1. O contrato poderá estar sujeito a fiscalização prévia do Tribunal de contas, nos termos do disposto nº 2, do artigo 318.º da LOE 2020, conjugado com o nº 2 do artigo 48.º da Lei de Organização e Processo do Tribunal de Contas, na sua redação atual
2. Caso se verifique o previsto no número anterior, o contrato apenas produz efeitos financeiros a partir data de obtenção do referido Visto;
3. Os emolumentos devidos, no valor legal, serão suportados pelo cocontratante.

ANEXO I

AQUISIÇÃO DE ROUTERS PROVIDER EDGE E PROVIDER PARA LISBOA

1. SOLUÇÃO A ADQUIRIR

O adjudicatário compromete-se a fornecer à FCT, I.P. dois (2) equipamentos de encaminhamento (routers) do tipo Provider Edge, doravante designados por Equipamentos do tipo PE, e quatro (4) equipamentos de encaminhamento (routers) do tipo Provider, doravante designados por Equipamentos do tipo P.

A solução descrita ficará dividida entre dois datacenters da FCT, sendo que um conjunto composto por um equipamento tipo PE e dois equipamentos tipo P será instalado na Faculdade de Engenharia da Universidade do Porto, e outro conjunto composto pelo mesmo número e tipo de equipamentos será instalado na Estação Porto Campanhã.

Os equipamentos a adquirir irão integrar a futura geração da rede académica Portuguesa, que estará suportada na tecnologia de *Segment Routing* usando MPLS e EVPN. A lista completa de requisitos para cada um dos tipos de equipamento P e PE consta do presente Anexo.

Os equipamentos do tipo PE e do tipo P a fornecer devem ser da mesma marca comercial dado a utilização prevista ser numa rede onde será implementado Segment Routing, assim como outras soluções avançadas de rede tais como TI-FLA, IP-FRR, etc. Uma vez que a interoperabilidade ao nível de protocolos avançados de rede entre fabricantes não é total, esta é a única forma de garantir o correto funcionamento da rede.

Todos os equipamentos a fornecer terão de ser novos e devidamente acondicionados na embalagem original. Não serão aceites quaisquer equipamentos, módulos ou placas recondicionados ou que tenham já sido previamente utilizados.

Não constitui obrigação do adjudicatário a configuração dos equipamentos, quer do tipo P ou do tipo PE, a fornecer.

2. SOFTWARE, REQUISITOS GERAIS

O licenciamento do *software* dos Equipamentos do tipo PE e Equipamentos do tipo P devem ser efetuados em nome do adjudicante.

O adjudicatário obriga-se a assegurar, sem qualquer custo adicional, a alteração de versão de *software* e licenciamento para todos os equipamentos fornecidos, de forma a suportar as funcionalidades mínimas descritas e requeridas no presente Anexo, de acordo com o tipo de equipamento a fornecer.

Futuras versões do software para os equipamentos fornecidos terão de ser fornecidas sem quaisquer encargos adicionais, durante a vigência do presente contrato. São consideradas futuras versões software as que corrijam erros/falhas da versão em utilização, assim como a disponibilização de novas funcionalidades. Nas novas versões de software não poderão ser perdidas quaisquer funcionalidades/licenciamentos que estejam em uso ou previstas neste caderno de encargos.

3. REQUISITOS TÉCNICOS GERAIS E OBRIGATÓRIOS DOS EQUIPAMENTOS DO TIPO PE

Os equipamentos do tipo PE deverão possuir uma arquitetura modular, compostos por chassis, assim como placas para módulos de portas (que encaixam nos chassis), módulos de portas (que encaixam nas placas mencionadas) e software. Os módulos de portas poderão, eles próprios, encaixar diretamente no chassis, não sendo, nesse caso, necessárias as placas para módulos de portas.

Estes serão os routers responsáveis pela iniciação/terminação de serviços avançados. Como tal têm de suportar a configuração de Multiprotocol BGP (com suporte para as *Address Families* necessárias), IGPs (ISIS e OSPF com extensões para *Segment Routing*), *Segment Routing*, Extensões para *Traffic Enfineering*, EVPN, VPNs L3, VPLS, VPWS, etc.

3.1. CARACTERÍSTICAS FÍSICAS

Os equipamentos do tipo PE devem obrigatoriamente possuir as seguintes características físicas:

- Arquitetura física modular. Chassis onde encaixam módulos com portas ou chassis onde encaixam placas que contêm módulos com portas;
- Chassis de tamanho máximo de 14 *rack-units*;
- Montável em rack 19 polegadas;
- Profundidade máxima de 80 cms;
- Cartas de processamento de *routing* redundantes (mínimo de duas independentes, e que ocupem no máximo uma baía cada uma);
- Processadores modulares, de encaixe no chassis. Sem necessidade de paragem do serviço no equipamento de encaminhamento proposto, para substituição das mesmas;

- No mínimo, quatro baías para placas para módulos de portas ou módulos de portas (caso encaixem diretamente no chassis), sendo que as baías para os processadores não são consideradas nesta contabilização;
- Suporte para portas de 400Gbps e 200Gbps;
- Capacidade mínima, do chassis, de 20 portas a 400Gbps sem qualquer contenção;
- Capacidade mínima, do chassis, de 20 portas a 200Gbps sem qualquer contenção;
- Capacidade mínima, do chassis, para 128 portas a 100 Gigabit Ethernet sem qualquer contenção;
- Capacidade mínima, do chassis, para 128 portas a 40 Gigabit Ethernet sem qualquer contenção. Este tipo de portas pode ser entregue tanto em portas de 40Gbps dedicadas como em portas de 100G às quais é acoplado um QSFP+ de 40Gbps;
- Capacidade mínima, do chassis, 192 portas a 10Gbps Ethernet em simultâneo com contenção máxima de 6:5. As portas 10Gbps deverão ser disponibilizadas através de SFP+;
- Capacidade do chassis, em cada baía, para placas para módulos de portas, ou módulos de portas, ter uma capacidade mínima, sem contenção, de 3.2Tbps full duplex;
- As placas ou módulos de portas ou módulos de portas deverão utilizar *chipsets* do próprio fabricante. Não será admitido equipamento que faça uso de *chipsets* de fabricantes generalistas ("também conhecidos por *merchant silicon vendors*");
- Capacidade para expandir o chassis através de equipamento remoto (satélite) com configuração e gestão integrada no equipamento principal;
- Temperatura de funcionamento do equipamento dos 5º aos 40º
- Fontes de alimentação para circuito elétrico AC (230v);
- Sistema de ventilação redundantes;
- Ventilação da frente para trás com pelo menos dois módulos de ventoinhas;
- Fontes de alimentação redundantes, assegurando a total funcionalidade e mantendo a redundância em caso de falha de uma delas (mínimo, três fontes de alimentação);
- Cada fonte de alimentação deverá ter dois cabos para ligação a duas réguas de potência diferentes;
- Existência no mercado, para o equipamento de encaminhamento proposto, de:
    - Placa para módulos de portas ou módulo de portas com, pelo menos, 5 portas a 400 Gigabit Ethernet sem contenção;

- Placa para módulos de portas ou módulo de portas com, pelo menos, 5 portas a 200 Gigabit Ethernet sem contenção;
- Placa para módulos de portas ou módulo de portas com, pelo menos, 32 portas a 100 Gigabit Ethernet sem contenção;
- Possibilidade de converter as portas de 400 Gigabit Ethernet em 200 Gigabit Ethernet, 100 Gigabit Ethernet e 40 Gigabit Ethernet mediante a utilização de um QSFP+ para o efeito.
- Possibilidade de converter as portas de 100 Gigabit Ethernet em 40 Gigabit Ethernet mediante a utilização de um QSFP+ para o efeito.

- Observância das seguintes normas NEBS (*Network Equipment Building Standards*):

  - NEBS nível 3 (SR-3580);

  - NEBS EMC and Safety (GR-1089);

  - NEBS *Physical Protection* (GR-63-CORE).

- Observância das seguintes normas EMC (*Electromagnetic compatibility*):

  - EN 61000-3-2: *Power Line Harmonics;*

  - EN 61000-3-3: *Voltage Fluctuations and Flicker*;

- Observância das seguintes normas de imunização:

  - EN-61000-4-2 *Electrostatic Discharge Immunity*
  - EN-61000-4-3 *Radiated Immunity*
  - EN-61000-4-4 *Electrical Fast Transient Immunity*
  - EN-61000-4-5 *Surge*
  - EN-61000-4-6 *Conducted Disturbances Immunity*
  - EN-61000-4-11 *Voltage Dips and Sags*

- Observância das seguintes normas ETSI (*European Telecommunications Standards Institute*):

  - EN 300 386: *Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements*;

  - EN 55022: *Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement*;

- EN 55024: *Information technology equipment - Immunity characteristics - Limits and methods of measurement.*

3.1.1. CARACTERÍSTICAS FÍSICAS DO PROCESSADOR E MÓDULOS

- Processador com, pelo menos, 8 cores a 1.9GHz;
- Cartas de processamento de routing 1 + 1, sem ponto de falha;
- Uma Porta de consola em cada carta de processamento de *routing*;
- No mínimo, 24GB de memória RAM em cada processador;
- Dispositivo de armazenamento não volátil (*Solid-State Drive*) com capacidade mínima de 128GB, em cada carta de processamento de routing;
- No mínimo, duas portas de gestão Fast Ethernet/Gigabit Ethernet em cada carta de processamento de *routing*;
- O equipamento deve suportar protocolos de timing de alta precisão, nomeadamente PTP (*Precision Time Protocol*), *Bidirectional Time of Day* (ToD) e *Centralized Integrated Timming Supply*;
- Deverá ser possível fazer, pelo menos, quatro *peerings* com routers com a tabela completa de *full routing* Internet (800.000 rotas IPv4 e 70.000 rotas IPv6) em qualquer uma das portas do equipamento - 10G, 40G/100G/200G/400G;
- Caso o adjudicatário possua placas para módulos de portas ou módulos de portas de vários tipos, aqueles que deverão ser disponibilizados deverão ser os com mais funcionalidades e mais recentes (estando já devidamente certificados pelo fabricante);
- As placas para módulos ou módulos com portas de 400/200/100G deverão respeitar as seguintes funcionalidades/características, bem como ser acompanhadas por licenciamento que permita atingir os valores máximo especificados ou, quando explicitamente indicado, um valor mais baixo do que o máximo suportado (caso das VRFs):
    - Performance Line Rate para as placas propostas em todas as portas
    - Ocupar, no máximo, 1 baía do chassis
    - Portas 400G com interfaces do tipo QSFP-DD
    - Portas 100G com interfaces do tipo QSFP28
    - 6.000.000 de rotas IPv4 / 6.000.000 IPv6 na *forwarding table (FIB)*
    - Capacidade para 16.000 VRFs
    - 32.000 Interfaces Layer 3 (por carta ou sistema)
    - 64.000 Bridge Domains

- 10.000 Sessões BGP v4 (por carta ou para todo chassis)
- 6.000 sessões de peering OSPF/ISIS
- 3.800 PWHE
- 128.000 pseudo-wires (por sistema ou carta)
- 1.000.000 labels de MPLS
- Capacidade de *buffering* para, pelo menos 30ms por cada conjunto de 4 portas a 100G
- 2.000.000 de entradas MAC
- 48.000 *Egress Queues* (por porta ou carta)
- 64.000 EVPN Bridge Domains
- 64.000 instâncias EVPN
- Suporte para MACsec
- Suporte para Flexible Ethernet (FlexE)
- As portas da placa devem suportar transceivers de marcas diferentes da do equipamento que o adjudicatário fornecer;

- As placas para módulos ou módulos com portas de 10G deverão respeitar as seguintes funcionalidades/características, bem como ser acompanhadas por licenciamento que permita atingir os valores máximo especificados ou, quando explicitamente indicado, um valor mais baixo do que o máximo suportado (caso das VRFs):
  - Número mínimo de Portas a 10G por Carta: 24 (vinte e quatro)
  - Taxa de contenção máxima de 6:5
  - Ocupar no máximo 1 baía do chassis
  - Portas 10G com interfaces do tipo SFP+
  - 4.000.000 de rotas v4 na *forwarding table (FIB)*
  - Capacidade para 8.000 VRFs e, se aplicável, respetivo licenciamento para pelo menos 8 VRFs;
  - 64.000 Bridge Domains
  - 30.000 interfaces de layer 3 (por carta ou sistema)
  - 2.000.000 de entradas MAC
  - 6.500 Sessões BGP (por carta ou para todo chassis)
  - 128.000 pseudo-wires (por sistema ou carta)
  - 1.000.000 labels de MPLS
  - Capacidade de *buffering* para, pelo menos 70ms por porta
  - 256.000 Queues (por porta ou carta)
  - As portas da placa devem suportar transceivers de marcas diferentes da do equipamento que o adjudicatário fornecer;

3.1.2. CARACTERÍSTICAS FÍSICAS DAS PORTAS/TRANSCEIVERS

- 400 Gigabit Ethernet suportados no formato QSFP-DD. Não são permitidos outros formatos físicos;
- Suporte transceiver QDD-400G-DR4-S
- Suporte transceiver QDD-400G-FR4-S
- Suporte transceiver QDD-400G-LR8-S
- 100 Gigabit Ethernet suportados no formato QSFP-28. Não são permitidos outros formatos físicos;
- Suporte para transceiver QSFP28 100G-LR4-S;
- Suporte para transceiver QSFP28 100G-SR4-S;
- Suporte para transceiver QSFP28 100G-CWDM-S;
- Suporte para transceiver QSFP28 100G-SM-SR;
- Suporte para transceiver QSFP28 100G-ER4L-S;
- 40 Gigabit Ethernet suportados no formato QSFP+. Não são permitidos outros formatos físicos;
- Suporte para transceiver QSFP+ 40G-SR4-S;
- Suporte para transceiver QSFP+ 40G-LR4-S;
- Suporte para transceiver QSFP+ 4x10-LR-S;
- 10G suportados no formato SFP+ ou usando breakout de 4 x 10G em formato QSFP+ ou usando adaptador QSA.
- Suporte para portas a 10G usando transceiver SFP+ do tipo LR ou LR-S;
- Suporte para portas a 10G usando transceiver SFP+ do tipo SR ou SR-S;
- Suporte para portas a 10G usando transceiver SFP+ do tipo ER ou ER-S;
- Suporte para portas a 10G usando transceiver SFP+ do tipo ZR ou ZR-S;

3.2. CARACTERÍSTICAS DO SOFTWARE

Os equipamentos a fornecer têm de conseguir suportar as seguintes normas/ protocolos/ funcionalidades nas configurações:

- IEEE 802.1q VLAN e encapsulamento Q-in-Q;
- IEEE 802.1ad;
- Virtual Router Redundancy Protocol (VRRP);
- Jumbo frames em todas as portas de, pelo menos, 9200 bytes;
- Interfaces e sub-interfaces Layer 3;
- IPv4 e IPv6;
- Rotas estáticas, OSPFv2 e OSPFv3, ISIS e ISISv6, BGP;
- Equal-Cost Multipath (ECMP);

- Listas de acesso de entrada em layer 2, bem como listas de acesso de entrada e saída em layer 3, IPv4 e IPv6;
- Bidirectional Forwarding Detection (BFD);
- Multiprotocol Label Switching (MPLS), MPLS traffic engineering e ethernet sobre MPLS (EoMPLS);
- Segment Routing (SR) sobre ISIS ou OSPF, SR traffic engineering e topology Independent Loop Free Alternatives (TI-LFA);
- Suporte para mecanismos de QoS para Core MPLS (suporte EXP bits, marcação, remarcação)
- Suporte de mecanismos de alta disponibilidade, como TI-LFA, RSVP-TE FRR
- Virtual Private Network em layer 3 (L3VPN);
- Virtual Private LAN Service (VPLS);
- Virtual Private Wire Service (VPWS);
- Qualidade de serviço hierárquica (H-QoS);
- Multiprotocol BGP suporte para várias address families: IPv4, VPNv4 Unicast, L2VPN-EVPN;
- A EVPN deverá ser suportada sobre Segment Routing;
- A EVPN deverá suportar os modos multihoming – all active e single active. No modo *single active* deve ser possível designar o router PE principal e Backup por VLAN;
- EVPN IRB (Integrated Routing and Bridging);
- Deve suportar EVPN-VPWS;
- Deve ser possível fazer stitching entre *pseudowires* de acesso e EVPNs;
- Deve ser possível configurar multihoming cujos segmentos são pseudowires;
- Deve ser possível implementar um mecanismo de proteção de loops na EVPN quando esta interage com anéis de layer 2 de acessos existentes. Nesses acessos está a ser usado um mecanismo de Spannig Tree por VLAN (não o MST);
- Suporte para Traffic Engineering em Segment Routing com ISIS e OSPF;
- BGP (com suporte para as address Families EVPN), IGPs (ISIS e OSPF com extensões para Segment Routing), Segment Routing, Extensão para Traffic enfineering, EVPN, VPNs L3, VPLS, VPWS;

QoS:

- IEEE 802.1p filtragem/marcação/remarcação;
- IETF DSCP filtragem/marcação/remarcação;
- WRED Egress e Ingress;
- Policing e *Shapping* Egress e Ingress;
- *Policing* e *shapping* baseado no valor de DSCP e monitorização por SNMP dos valores em tempo real;
- Contadores para *Policers* de QoS;

RFCs:

- RFC 768 User Datagram Protocol
- RFC 791 INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION
- RFC 792 Internet Control Message Protocol - DARPA INTERNET Program to protocol specification
- RFC 793 Transmission Control Protocol - DARPA INTERNET Program to protocol specification

- RFC 826 Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Addressess for Transmission on Ethernet Hardware
- RFC 854 Telnet Protocol Specification
- RFC 855 Telnet Option Specification
- RFC 856 Telnet Binary Transmission
- RFC 857 File Transfer Protocol
- RFC 858 Telnet Suppress and Go Ahead Option
- RFC 859 Telnet Status Option
- RFC 862 Echo Protocol
- RFC 863 Discard Protocol
- RFC 894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC 896 Congestion Control in IP/TCP Internetworks
- RFC 906 Bootstrap loading using TFTP
- RFC 925 Multi-LAN address resolution
- RFC 926 Protocol for providing the connectionless mode network services
- RFC 931 Authentication server
- RFC 950 Internet Standard Subnetting Procedure
- RFC 951 Bootstrap Protocol (BOOTP)
- RFC 958 Network Time Protocol (NTP)
- RFC 959 File Transfer Protocol (FTP)
- RFC 988 Host extensions for IP multicasting
- RFC 1027 Using ARP to implement transparent subnet gateways
- RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks
- RFC 1058 Routing Information Protocol
- RFC 1059 Network Time Protocol (version 1) specification and implementation
- RFC 1073 Telnet Window Size Option
- RFC 1079 Telnet Terminal Speed Option
- RFC 1091 Path MTU Discovery
- RFC 1098 Simple Network Management Protocol (SNMP)
- RFC 1112 Host extensions for IP multicasting
- RFC 1119 Network Time Protocol (version 2) specification and implementation
- RFC 1122 Requirements for Internet Hosts - Communication Layers
- RFC 1136 Administrative Domains and Routing Domains: A model for routing in the Internet
- RFC 1141 Incremental updating of the Internet checksum
- RFC 1142 OSI IS-IS Intra-domain Routing Protocol
- RFC 1149 Standard for the transmission of IP datagrams on avian carriers
- RFC 1157 Simple Network Management Protocol (SNMP)
- RFC 1164 Application of the Border Gateway Protocol in the Internet
- RFC 1166 Internet Numbers
- RFC 1191 Path MTU discovery
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 1212 Concise MIB definitions
- RFC 1213 Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 1215 Convention for defining traps for use with the SNMP (only MIB II SNMP version 1 traps and version 2 notifications)
- RFC 1253 OSPF Version 2 Management Information
- RFC 1256 ICMP Router Discovery Messages
- RFC 1268 Application of the Border Gateway Protocol in the Internet
- RFC 1269 Definitions of Managed Objects for the Border Gateway Protocol: Version 3
- RFC 1271 Remote Network Monitoring Management Information Base
- RFC 1284 Definitions of Managed Objects for the Ethernet-like Interface Types

- RFC 1286 Definitions of Managed Objects for Bridges
- RFC 1294 Multiprotocol Interconnect over Frame Relay
- RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 1317 Definitions of Managed Objects for RS-232-like Hardware Devices
- RFC 1319 The MD2 Message-Digest Algorithm
- RFC 1323 TCP Extensions for High Performance
- RFC 1331 The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1338 Supernetting: an Address Assignment and Aggregation Strategy
- RFC 1349 Type of Service in the Internet Protocol Suite
- RFC 1350 The TFTP Protocol (Revision 2)
- RFC 1370 Applicability Statement for OSPF
- RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1450 Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1455 Physical Link Security Type of Service
- RFC 1473 The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
- RFC 1492 An Access Control Protocol, Sometimes Called TACACS
- RFC 1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
- RFC 1583 OSPF Version 2
- RFC 1587 The OSPF NSSA Option
- RFC 1597 Address Allocation for Private Internets
- RFC 1627 Network 10 Considered Harmful (Some Practices Shouldn't be Codified)
- RFC 1657 Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1700 Assigned Numbers
- RFC 1701 Generic Routing Encapsulation (GRE)
- RFC 1702 Generic Routing Encapsulation over IPv4 networks
- RFC 1771 A Border Gateway Protocol 4 (BGP-4)
- RFC 1772 Application of the Border Gateway Protocol in the Internet
- RFC 1793 Extending OSPF to Support Demand Circuits
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1828 IP Authentication using Keyed MD5
- RFC 1850 OSPF Version 2 Management Information Base
- RFC 1878 Variable Length Subnet Table for IPv4
- RFC 1902 Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1905 Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1918 Address Allocation for Private Internets
- RFC 1948 Defending Against Sequence Number Attackes
- RFC 1965 Autonomous System Confederations for BGP
- RFC 1966 BGP Route Reflection An alternative to full mesh IBGP
- RFC 1981 Path MTU Discovery for IP version 6
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)

- RFC 1997 BGP Communities Attribute
- RFC 1998 Application of the BGP Community Attribute in Multi-home Routing
- RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 2012 SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
- RFC 2013 SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 2018 TCP Selective Acknowledgment Options
- RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2037 Entity MIB using SMIv2
- RFC 2080 RIPng for IPv6
- RFC 2081 RIPng Protocol Applicability Statement
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2086 IMAP4 ACL extension
- RFC 2096 IP Forwarding Table MIB
- RFC 2104 HMAC: Keyed-Hashing for Message Authentication
- RFC 2113 IP Router Alert Option
- RFC 2205 Resource ReSerVation Protocol (RSVP)-Version 1 Functional Specification
- RFC 2206 RSVP Management Information Base using SMIv2
- RFC 2236 Internet Group Management Protocol Version 2
- RFC 2272 Message Processig and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 2273 SNMPv3 Applications
- RFC 2281 Cisco Hot Standby Router Protocol (HSRP)
- RFC 2328 OSPF Version 2
- RFC 2338 Virtual Router Redundancy Protocol
- RFC 2347 TFTP Option Extension
- RFC 2348 TFTP Blocksize Option
- RFC 2349 TFTP Timeout Interval and Transfer Size Options
- RFC 2362 Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
- RFC 2365 Administratively Scoped IP Multicast
- RFC 2370 The OSPF Opaque LSA Option
- RFC 2373 IP Version 6 Addressing Architecture
- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2402 IP Authentication Header
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2410 The NULL Encryption Algorithm and Its Use With Ipsec
- RFC 2428 FTP Extensions for IPv6 and NATs
- RFC 2439 BGP Route Flap Damping
- RFC 2451 The ESP CBC-Mode Cipher Algorithm
- RFC 2453 RIP Version 2

- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
- RFC 2472 IP Version 6 over PPP
- RFC 2474 Defininition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2475 An Architecture for Differentiated Service
- RFC 2544 Benchmarking Methodology for Network Interconnect Devices
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2547 BGP/MPLS VPNs
- RFC 2558 Definitions of Managed Objects for the SONET/SDH Interface Type
- RFC 2571 An Architecture for Describing SNMP Management Frameworks
- RFC 2572 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 2574 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 2575 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 2576 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
- RFC 2578 Structure of Management Information Version 2 (SMIv2)
- RFC 2581 TCP Congestion Control
- RFC 2597 Assured Forwarding PHB Group
- RFC 2615 PPP over SONET/SDH
- RFC 2625 IP and ARP over Fibre Channel
- RFC 2625 IP and ARP over Fibre Channel
- RFC 2631 Diffie-Hellman Key Agreement Method
- RFC 2644 Changing the Default for Directed Broadcasts in Routers
- RFC 2662 Definitions of Managed Objects for the ADSL Lines
- RFC 2670 Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces
- RFC 2697 A Single Rate Three Color Marker
- RFC 2698 A Two Rate Three Color Marker
- RFC 2702 Requirements for Traffic Engineering Over MPLS
- RFC 2711 IPv6 Router Alert Option
- RFC 2740 OSPF for IPv6
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation (GRE)
- RFC 2796 BGP Route Reflection - An Alternative to Full Support Mesh IBGP
- RFC 2842 Capabilities Advertisement with BGP-4
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 2865 Remote Authentication Dail In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2873 TCP Processing of the IPv4 Precedence Field
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 2961 RSVP Refresh Overhead Reduction Extensions
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 2991 OSPF Equal Cost Multipath

- RFC 2992 Analysis of an Equal-Cost Multi-Path Algorithm
- RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links
- RFC 3031 Multiprotocol Label Switching Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 3036 LDP Specification
- RFC 3037 LDP Applicability
- RFC 3042 Enhancing TCP's Loss of Recovery Using Limited Trasmit
- RFC 3046 DHCP Relay Agent Information Option
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3101 The OSPF Not-so-Stubby Area (NSSA) Option
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3162 RADIUS and IPv6
- RFC 3171 IANA Guidelines for IPv4 Multicast Address Assignments
- RFC 3180 GLOP Addressing in 233/8
- RFC 3201 Definitions of Managed Objects for Circuit to Interface Translation
- RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
- RFC 3235 Network Address Translators (NAT)-Friendly Application Design Guidelines
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
- RFC 3260 New Terminology and Clarifications for Diffserv
- RFC 3277 Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance
- RFC 3289 Management Information Base for the Differentiated Services Architecture
- RFC 3290 An Informal Management Model for Diffserv Routers
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3376 Internet Group Management Protocol, Version 3
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework
- 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 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3446 Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
- RFC 3468 The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols
- RFC 3471 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description

- RFC 3473 Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions
- RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
- RFC 3509 Alternative Implementations of OSPF Area Border Routers
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3569 An Overview of Source-Specific Multicast (SSM)
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3596 DNS Extensions to Support IP Version 6
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with Ipsec
- RFC 3618 Multicast Source Discovery Protocol (MSDP)
- RFC 3623 Graceful OSPF Restart
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 3667 IETF Rights in Contributions
- RFC 3668 Intellectual Property Rights in IETF Technology
- RFC 3682 The Generalized TTL Security Mechanism (GTSM)
- RFC 3697 IPv6 Flow Label Specification
- RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3785 Use of Interior Gateway Protocol (IGP) Metric as a second MPLS Traffic Engineering (TE) Metric
- RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
- RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)
- RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 3847 Restart Signaling for Intermediate System to Intermediate System (IS-IS)
- RFC 3879 Deprecating Site Local Addresses
- RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
- RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
- RFC 3954 Cisco Systems NetFlow Services Export Version 9
- RFC 3970 A Traffic Engineering (TE) MIB
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4001 Textual Conventions for Internet Network Addresses
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4061 PIM Sparse Mode shall be supported as specified
- RFC 4105 Requirements for Inter-Area MPLS Traffic Engineering
- RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
- RFC 4136 OSPF Refresh and Flooding Reduction in Stable Topologies
- RFC 4176 Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management
- RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4201 Link Bundling in MPLS Traffic Engineering (TE)
- RFC 4203 OSPF Extensions in Support of Generalized Multi-Protocol Lable Switching (GMPLS)

- RFC 4206 Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)
- RFC 4208 Generalized Multiprotocol Lable Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for Overlay Model
- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4257 Framework for Generalized Multi-Protocol Label Switching (GMPLS)-based Control of Synchronous Digital Hierarchy/Synchronous Optical Networking (SDH/SONET) Networks
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4292 IP Forwarding Table MIB
- RFC 4293 Management Information Base for the Internet Protocol (IP)
- RFC 4294 IPv6 Node Requirements
- RFC 4311 IPv6 Host-to-Router Load Sharing
- RFC 4364 BGP/MPLS IP Virtualized Private Networks (VPNs)
- RFC 4377 Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks
- RFC 4378 A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base
- RFC 4384 BGP Communities for Data Collection
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4444 Management Information Base for Intermediate System to Intermediate System (IS-IS)
- RFC 4446 IANA Allocations for Pseudowire Edge to Edge Emulation (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 4461 Signaling Requirements for Point-to-Multipoint Traffic-Engineered MPLS Label Switched Paths (LSPs)
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 4558 Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement
- RFC 4561 Definition of a Record Route Object (RRO) Node-Id Sub-Object
- RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Networks (VPNs)
- RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification
- RFC 4602 Protocol Independent Multicast - Sparse Mode (PIM-SM) Requirements Analysis
- RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
- RFC 4605 Supports IGMP / Multicast Listener Discovery MLD / Based Multicast Forwarding
- RFC 4607 Source-Specific Multicast for IP
- RFC 4610 Anycast RP for PIM-SM
- RFC 4649 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay-Agent Remote-ID Option
- RFC 4655 A Path Computation Element (PCE)-Based Architecture
- RFC 4657 Path Computation Element (PCE) Communication Protocol Generic Requirements

- RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
- RFC 4684 Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virual Private Networks (VPNs)
- RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4750 OSPF Version 2 Management Information Base
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4761 Virutal Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
- RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
- RFC 4781 Graceful Restart Mechanism for BGP with MPLS
- RFC 4797 Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virutal Private Networks
- RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
- RFC 4811 OSPF Out-of-Band Link State Database (LSDB) Resynchronization
- RFC 4812 OSPF Restart Signaling
- RFC 4813 OSPF Link-Local Signaling
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4872 RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol label Switching (GMPLS) Recovery
- RFC 4874 Exclude Routes - Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)
- RFC 4875 Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 4906 Transport of Layer 2 Frames over MPLS
- RFC 4915 Multi-Topology (MT) Routing in OSPF
- RFC 4970 Extensions to OSPF for Advertising Optional Router Capabilities
- RFC 4971 Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information
- RFC 5006 IPv6 Router Advertisement Option for DNS Configuration
- RFC 5015 Bidirectional Protocol Independent Multicast (BIDIR-PIM)
- RFC 5036 LDP Specification
- RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC 5065 Autonomous System Confederations for BGP
- RFC 5075 IPv6 Router Advertisement Flags Option
- RFC 5082 The Generalized TTL Security Mechanism (GTSM)
- 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)
- RFC 5088 OSPF Protocol Extensions for Path Computation Element (PCE) Discovery
- RFC 5089 IS-IS Protocol Extensions for Path Computation Element (PCE) Discovery
- RFC 5120 M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)
- RFC 5130 A Policy Control Mechanism in IS-IS Using Admistrative Tags
- RFC 5150 Label Switched Path Stitching with Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE)
- RFC 5151 Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol - Traffic Engineering (RSVP-TE) Extensions
- RFC 5152 A Per-Domain Path Computation Method for Establishing Inter-Domain Traffic Engineering (TE) Label Switched Paths (LSPs)

- RFC 5185 OSPF Multi-Area Adjacency
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5210 A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates
- RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks
- RFC 5292 Address-Prefix-Based Outbound Route Filter for BGP-4
- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-Wide Prefix Distribution with Two-Level IS-IS
- RFC 5303 Three-Way Handshake for IS-IS Point-to-Point Adjacencies
- RFC 5304 IS-IS Cryptographic Authentication
- RFC 5305 IS-IS Extensions for Traffic Engineering
- RFC 5306 Restart Signaling for IS-IS
- RFC 5307 IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
- 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
- RFC 5329 Traffic Engineering Extensions to OSPF Version 3
- RFC 5340 OSPF for IPv6
- RFC 5357 A Two-Way Active Measurement Protocol (TWAMP)
- RFC 5420 Encoding of Attributes for MPLS LSP Establishment Using RSVP-TE
- RFC 5424 The Syslog Protocol
- RFC 5426 Transmission of Syslog Messages over UDP
- RFC 5439 An Analysis of Scaling Issues in MPLS-TE Core Networks
- RFC 5440 Path Computation Element (PCE) Communication Protocol (PCEP)
- RFC 5441 A Backward-Recursive PCE-Based Computation (BRPC) Procedure to Compute Shortest Constrained Inter-Domain Traffic Engineering Label Switched Paths
- RFC 5443 LDP IGP Synchronization
- RFC 5455 Diffserv-Aware Class-Type Objet for the Path Computation Element Communication Protocol
- RFC 5462 Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field
- RFC 5492 Capabilities Advertisement with BGP-4
- RFC 5496 The Reverse Path Forwarding (RPF) Vector TLV
- RFC 5501 Requirements for Multicast Support in Virtual Private LAN Services
- RFC 5508 NAT Behavioral Requirements for ICMP
- RFC 5521 Extensions to the Path Computation Element Communication Protocol (PCEP) for Route Extensions
- RFC 5541 Encoding of Objective Functions in the Path Computation Element Communication Procotol (PCEP)
- RFC 5557 Path Computation Element Communication Protocol (PCEP) Requirements and Protocol Extensions in Support of Global Concurrent Optimization
- RFC 5561 LDP Capabilities
- RFC 5575 Dissemination of Flow Specification Rules
- RFC 5601 Pseudowire (PW) Management Information Base (MIB)
- RFC 5602 Pseudowire (PW) over MPLS PSN Management Information Base (MIB)
- RFC 5603 Ethernet Pseudowire (PW) Management Information Base (MIB)
- RFC 5635 Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)
- RFC 5643 Management Information Base for OSPFv3
- RFC 5668 4-Octet AS Specific BGP Extended Community

- RFC 5701 IPv6 Address Specific BGP Extended Community Attribute
- RFC 5711 Node Behavior upon Originating and Receiving Resource Reservation Protocol (RSVP) Path Error Messages
- RFC 5714 IP Fast Reroute Framework
- RFC 5715 A Framework for Loop-Free Convergence
- RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
- RFC 5880 Bidirectional Forwarding Detection (BFD)
- RFC 5881 BFD for IPv4 and IPv6 (Single Hop)
- RFC 5883 Bidirectional Forwarding Detection (BFD) for Multihop Paths
- RFC 5884 Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)
- RFC 5885 Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verifictaion (VCCV)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 5921 A Framework for MPLS in Transport Networks
- RFC 5925 TCP authentication
- RFC 5950 Network Management Framework for MPLS-based Transport Networks
- RFC 6020 YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)
- RFC 6037 Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs
- RFC 6074 Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)
- RFC 6119 IPv6 Traffic Engineering in IS-IS
- RFC 6138 LDP IGP Synchronization for Broadcast Networks
- RFC 6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links
- RFC 6165 Extensions to IS-IS for Layer-2 Systems
- RFC 6177 IPv6 Address Assignment to End Sites
- RFC 6205 Generalized Labels for Lambda-Switch-Capable (LSC) Label Switching Routers
- RFC 6213 Support ISIS BFD-Enabled TLV
- RFC 6215 MPLS Transport Profile User-to-Network and Network-to-Network Interfaces
- RFC 6226 Support PIM Group-to-Rendezvous-Point Mapping
- RFC 6241 Network Configuration Protocol (NETCONF)
- RFC 6242 Using the NETCONF Protocol over Secure Shell (SSH)
- RFC 6371 Operations, Administration, and Maintenance Framework for Operations, MPLS-Based Transport Networks
- RFC 6374 Packet Loss and Delay Measurement for MPLS Networks
- RFC 6388 Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths
- RFC 6391 Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network
- RFC 6510 RSVP-TE extensions for signaling for point to multipoint LSPs
- RFC 6513 Multicast in MPLS/BGP IP VPNs
- RFC 6514 BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs
- RFC 6515 IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN
- RFC 6516 IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages
- RFC 6517 Mandatory Features in a Layer 3 Multicast BGP/MPLS VPN Solution
- RFC 6547 Using 127-Bit IPv6 Prefixes on Inter-Router Links
- RFC 6718 Pseudowire Redundancy
- RFC 6822 IS-IS Multi-Instance
- RFC 6987 OSPF Stub Router Advertisement
- RFC 7041 Extensions to the Virtual Private LAN Service (VPLS) PE Model for Provider Backbone Bridging
- RFC 7080 VPLS Interoperability with Provider Backbone Bridges

- RFC 7130 Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces
- RFC 7142 Reclassification of RFC 1142 to Historic
- RFC 7166 Authentication Trailer for OSPFv3
- RFC 7348 Virtual eXtensible Local Area Network (VXLAN)
- RFC 7311 Accumulated IGP Metric Attribute for BGP
- RFC 7432 BGP based MPLS Ethernet VPN
- RFC 7471 OSPF Traffic Engineering (TE) Metric Extensions
- RFC 7752 North-Bound Distribution of Link-State and Traffic Eng. (TE)
- RFC 7794 IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability
- RFC 7810 IS-IS Traffic Engineering (TE) Metric Extensions
- RFC 7876 UDP Return Path for Packet Loss and Delay Measurement for MPLS Networks
- RFC 7911 Advertisement of Multiple Paths in BGP shall be supported
- RFC 7916 Operational Management of Loop-Free Alternates
- RFC 8077 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 8092 Large Community Attributes
- RFC 8214 Virtual Private Wire Service Support in Ethernet VPN
- RFC 8231 Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE
- RFC 8233 Extensions to PCEP to Compute Service-Aware Label Switched Paths (LSPs)
- RFC 8281 PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model

Outros:

- IEEE 802.1 QinQ;
- IEEE 802.3ad LACP (Link Aggregation Control Protocol);
- Jumbo Frames de, pelo menos, 9200;
- Visibilidade e telemetria;
- Os equipamentos deverão possuir um conjunto de ferramentas com vista à automatização da sua operação e configuração, ferramentas estas que são executadas no próprio equipamento. Estas poderão ser scripts, macros, scripts baseadas em eventos.

4. REQUISITOS PARTICULARES E OBRIGATÓRIOS DOS EQUIPAMENTOS DO TIPO PE

Pretende-se ainda que os dois equipamentos do Tipo PE a fornecer cumpram um conjunto de requisitos particulares à solução que a FCT pretende construir.

Assim, caso estes equipamentos possuam licenciamento para funcionalidades e por utilização de portas, é obrigatório que:

- Todas as 16 portas de cada chassis a 100G estejam habilitadas e a suportar todos os serviços e sem restrições, indicados nos pontos 3 e 4 do presente anexo;
- Todas as 24 portas a 10G de cada chassis estejam habilitadas e a suportar todos os serviços e sem restrições, indicados no ponto 3 e 4 do presente anexo;

Cada um dos equipamentos do tipo PE deverá cumprir os seguintes requisitos:

a) Chassis Modular;
b) Possuir cartas de processamento de *routing* redundantes, de forma a permitirem a prestação do serviço sem interrupção no caso de falha de uma delas;
c) Disponibilizar um número mínimo de 16 (dezasseis) portas a 100Gbps sem taxa de contenção. As 16 (dezasseis) portas a 100G disponibilizadas deverão ser entregues em dois módulos/cartas diferentes, de forma a garantir que uma avaria numa delas não inviabiliza o uso do equipamento. Para perfazer as 16 portas, poderão ser usadas várias combinações, sendo que o mínimo de portas por módulo/carta não pode ser inferior a 4 (quatro). São exemplos de combinações (8 x 100G + 8 x 100G), (10 x 100G + 6 x 100G), (12 x 100G + 4 x 100G).
d) As cartas a fornecer com portas a 100G têm igualmente de suportar, pelo menos, portas a 200G ou a 400G;
e) Disponibilizar um número mínimo de 24 (vinte e quatro) portas a 10Gbps (SFP+ ou com transceiver com cabos de *breakout*) podendo estas ter uma taxa de contenção de 4:3;
f) Estar equipado com todas as fontes de alimentação possíveis para o chassis (para AC 230v), garantindo redundância das mesmas em caso de falha de uma e de forma a suportarem todos os módulos ou placas para módulos disponibilizados no âmbito do caderno de encargos. Caso haja diferentes versões de fontes, deverão ser fornecidas as mais recentes e que permitam usar, pelo menos, mais uma placa para módulos ou módulos de portas adicionais às adquiridas no âmbito da presente consulta (caso haja baías disponíveis para o efeito). Deverão também ser fornecidos todos os cabos, com terminação IEC-C21, necessários para ligação das fontes;
g) Estar equipado com todos os sistemas de ventilação possíveis para o equipamento de forma a haver redundância das mesmas;
h) Vir munidos de todos os módulos/cartas/*switch fabrics*/Interfaces (ou outra designação comercial) necessários para que cumpra os requisitos indicados na alínea 3 do presente Anexo, sem qualquer tipo de contenção de tráfego e ainda com um módulo/carta/*switch fabric*/Interface que garanta redundância em caso de falha de algum deles;
i) Vir dotado do Software e respetivo licenciamento para suportar todos os requisitos técnicos, funcionalidades, débitos ou outros, caso se aplique, tal como descritos no presente ponto. Caso se aplique, todo o licenciamento fornecido não deverá estar limitado temporalmente, sendo considerada a utilização da licença como perpétua;

5. REQUISITOS TÉCNICOS GERAIS E OBRIGATÓRIOS DOS EQUIPAMENTOS DO TIPO P

Os equipamentos do tipo P são responsáveis pelas configurações do tipo Provider numa arquitetura de operador.

5.1. CARACTERÍSTICAS FÍSICAS DOS CHASSIS

Os equipamentos do tipo P devem possuir as seguintes características físicas:

- Arquitetura física de chassis fixo ou modular;
- Chassis de tamanho máximo de 1 *rack-unit*;
- Montável em rack 19 polegadas
- Profundidade máxima de 77 cms
- Capacidade mínima, do chassis, para 24 portas a 100 Gigabit Ethernet com contenção máxima de 4:3;
- Capacidade para comutar, pelo menos, 1650Mpps
- Capacidade mínima do chassis que permita uma configuração de 12 portas a 100 Gigabit Ethernet e 48 portas a 10Gbps Ethernet, em simultâneo. As portas 10Gbps poderão ser disponibilizadas quer através de conversores para SFP+ ou *breakout cables*;
- Capacidade mínima do chassis que permita uma configuração de 96 portas a 25 ou 10 Gigabit Ethernet. As portas 25/10Gbps poderão ser disponibilizadas quer através de conversores para SFP+ ou *breakout cables*;
- Capacidade mínima do chassis para 24 portas a 40 Gigabit Ethernet. Este tipo de portas pode ser entregue tanto em portas de 40Gbps dedicadas como em portas de 100G às quais é acoplado um QSFP+ de 40Gbps;
- Temperatura de funcionamento do equipamento dos 0º aos 40º
- Fontes de alimentação para circuito elétrico AC (90-265V, 50-60Hz) redundantes;
- No mínimo três módulos com ventoinhas com ventilação da frente para trás e hot-swappable;
- Fontes de alimentação redundantes, assegurando a total funcionalidade e mantendo a redundância em caso de falha de uma delas;
- Fontes de alimentação com ventilação da frente para trás e hot-swappable;
- Observância das normas CE de acordo com as diretivas 004/108/EC and 2006/95/EC
- Observância das seguintes normas NEBS (*Network Equipment Building Standards*):
    - NEBS EMC and Safety (GR-1089-CORE);
    - NEBS *Physical Protection* (GR-63-CORE).
- Observância das seguintes normas EMC (*Electromagnetic compatibility*):

- 47CFR Part 15 (CFR 47) Class A
- AS/NZS CISPR22 Class A
- CISPR22 Class A
- EN55022 Class A
- ICES003 Class A
- VCCI Class A
- EN61000-3-2
- EN61000-3-3
- KN22 Class A
- CNS13438 Class A
- EN55024
- CISPR24
- EN300386
- Série EN-61000-4

- Observância das seguintes normas de segurança:
  - UL 60950-1 Second Edition
  - CAN/CSA-C22.2 No. 60950-1 Second Edition
  - EN 60950-1 Second Edition
  - IEC 60950-1 Second Edition
  - AS/NZS 60950-1
  - GB4943

5.2. CARACTERÍSTICAS FÍSICAS DO PROCESSADOR PARA OS EQUIPAMENTOS DO TIPO P

- Processador com, pelo menos, 8 cores a 1.6GHz
- Uma Porta de consola RJ45;
- Uma porta RJ45 Ethernet para gestão
- No mínimo, 32GB de memória do sistema;
- Dispositivo de armazenamento não volátil (*Solid-State Drive*) com capacidade mínima de 128 GB;
- O equipamento deve suportar protocolos de timing de alta precisão, nomeadamente *Time of Day* (ToD);

- Capacidade na base de dados de encaminhamento (*Forwarding Data Base* - FIB) de, pelo menos, 2.000.000 de entradas para IPv4/IPv6;
- Capacidade para 4.000 circuitos de layer 2
- Capacidade para pelo menos 1450 domínios de bridging /EVIs
- Capacidade de buffering para, pelo menos, 40 ms por porta
- Num mínimo de instâncias de EVPN: 1450
- Num mínimo de instâncias de Pseudowire: 940
- 8 Queues por porta
- 2.000 sessões de BGP

5.3. CARACTERÍSTICAS FÍSICAS DAS PORTAS/TRANSCEIVERS

- 100 Gigabit Ethernet suportados no formato QSFP-28. Não são permitidos outros formatos físicos;
- Suporte para transceiver QSFP28 100GBase-LR4-S
- Suporte para transceiver QSFP28 100GBase-SR4-S
- Suporte para transceiver QSFP28 100GBase CWDM4-S
- 40 Gigabit Ethernet suportados no formato QSFP+. Não são permitidos outros formatos físicos;
- Suporte para transceiver QSFP+ 40GBase-SR4-S;
- Suporte para transceiver QSFP+ 40GBase-LR4-S;
- Suporte para portas a 10G usando transceiver SFP+ do tipo LR ou, em alternativa, transceiver QSFP+ 40 Gigabit Ethernet com capacidade para transmissão em paralelo de 4 x 10GBase-LR (10 Kms - 4 x 10G-LR/LRL monomodo), com conetor MPO permitindo a terminação em fibra monomodo (breakout com conetor LC), tendo de ser garantida a interoperabilidade com equipamentos que cumpram a norma 10GBase-LR;
- Suporte para portas a 10G usando transceiver SFP+ do tipo SR ou, em alternativa, transceiver QSFP+ 40 Gigabit Ethernet com capacidade para transmissão em paralelo de 4 x 10GBase-SR (840 a 860nm), com conetor MPO permitindo a terminação em fibra multimodo (breakout com conetor LC) tendo de ser garantida a interoperabilidade com equipamentos que cumpram a norma 10GBase-SR;

5.4. CARACTERÍSTICAS DO SOFTWARE

Os equipamentos a fornecer têm de conseguir suportar as seguintes normas/ protocolos/ configurações:

- Portas switching em layer 2;
- IEEE 802.1q VLAN e encapsulamento Q-in-Q;
- IEEE 802.1ad;
- Virtual Router Redundancy Protocol (VRRP);
- Jumbo frames em todas as portas;
- Interfaces e sub-interfaces Layer 3;
- IPv4 e IPv6;
- Rotas estáticas, OSPFv2 e OSPFv3, ISIS e ISISv6, BGP;
- Equal-Cost Multipath (ECMP);
- Listas de acesso de entrada em layer 2, bem como listas de acesso de entrada e saída em layer 3, IPv4 e IPv6;
- Bidirectional Forwarding Detection (BFD);
- Multiprotocol Label Switching (MPLS), MPLS traffic engineering e ethernet sobre MPLS (EoMPLS);
- Segment Routing (SR) sobre ISIS ou OSPF, SR traffic engineering e topology Independent Loop Free Alternatives (TI-LFA);
- Virtual Private Network em layer 3 (L3VPN);
- Qualidade de serviço hierárquica (H-QoS);
- Marcação DSCP;
- Classificação com base na classe de serviço (L2), tipo de serviço (L3) e listas de acesso (L3/L4);
- Priority queuing;
- Zero-Touch Provisioning (ZTP);
- Suporte de funcionalidades para Segment Routing, ISIS e OSPF com extensão para Segment Routing, multiprotocol BGP, IPv6, MPLS
- Suporte para, pelo menos 8 VRFs para gestão;
- Suporte para mecanismos de QoS para Core MPLS (suporete EXP bits, marcação, remarcação)
- Suporte de mecanismos de alta disponibilidade, como TI-LFA, RSVP-TE FRR
- Suporte para traffic engineering MPLS-TE, SR-TE
  Suporte para EVPN – EVPN-VPWS (virtual Private Wire Service) e EVPN Multihoming, EVPN IRB (Integrated Routing and Bridging);
- IEEE 802.1p filtragem/marcação/remarcação

- IETF DSCP filtragem/marcação/remarcação
- WRED Egress
- Policing Ingress
- Shapping Egress
- Policing e shapping baseado no valor de DSCP e monitorização por SNMP dos valores em tempo real
- Contadores para mecanismos de QoS por SNMP
- Estar em cumprimento com a certificação FIPS 140-2

Ao nível da Gestão, aprovisionamento e Monitorização deverão suportar:

- Visibilidade e telemetria;
- Hosting de aplicações nativamente ou através de containers;
- Proteção a nível de control-plane e management plane;
- Autenticação, autorização e accounting (AAA);
- TACACS+;
- SSH;
- SNMPv3;
- MIB, XML, JSON e GPB;
- Operação, administração e manutenção Ethernet e MPLS (OAM);
- NETCONF e YANG;

RFCs e drafs suportados:

- draft-agrawal-spring-srv6-mpls-interworking SRv6 and MPLS interworking
- draft-ali-spring-sr-traffic-accounting Traffic Accounting in Segment Routing Networks
- draft-barth-pce-segment-routing-policy-cp PCEP extension to support Segment Routing Policy Candidate Paths
- draft-bashandy-rtgwg-segment-routing-uloop Loop avoidance using Segment Routing
- draft-filsfils-spring-net-pgm-extension-srv6-usid Network Programming extension: SRv6 uSID instruction
- draft-filsfils-spring-sr-policy-considerations SR Policy Implementation and Deployment Considerations
- draft-gandhi-mpls-rfc6374-sr Performance Measurement for Segment Routing Networks with MPLS Data Plane
- draft-gandhi-spring-sr-enhanced-plm Enhanced Performance and Liveness Monitoring in Segment Routing Networks
- draft-gandhi-spring-stamp-srpmPerformance Measurement Using STAMP for Segment Routing Networks
- draft-gandhi-spring-twamp-srpm Performance Measurement Using TWAMP Light and STAMP for Segment Routing Networks
- draft-ietf-idr-bgp-ls-flex-algo Flexible Algorithm Definition Advertisement with BGP Link-State

- draft-ietf-idr-bgpls-segment-routing-epe BGP-LS extensions for Segment Routing BGP Egress Peer Engineering
- draft-ietf-idr-bgpls-segment-routing-epe-17 Segment Routing BGP Egress Peer Engineering BGP-LS Extensions
- draft-ietf-idr-bgp-ls-segment-routing-ext BGP Link-State extensions for Segment Routing
- draft-ietf-idr-bgp-ls-segment-routing-msd Signaling MSD (Maximum SID Depth) using Border Gateway Protocol Link-State
- draft-ietf-idr-bgp-prefix-sid-27 Segment Routing Prefix SID extensions for BGP
- draft-ietf-idr-segment-routing-te-policy-05 Advertising Segment Routing Policies in BGP
- draft-ietf-isis-segment-routing-extensions IS-IS Extensions for Segment Routing
- draft-ietf-isis-segment-routing-extensions-21 Segment Routing Extension for ISIS
- draft-ietf-lsr-flex-algo IGP Flexible Algorithm
- draft-ietf-lsr-isis-srv6-extensions IS-IS Extension to Support Segment Routing over IPv6 Dataplane
- draft-ietf-ospf-segment-routing-extensions OSPF Extensions for Segment Routing
- draft-ietf-ospf-segment-routing-extensions-27 OSPF Extensions for Segment Routing
- draft-ietf-ospf-segment-routing-msd Signaling MSD (Maximum SID Depth) using OSPF
- draft-ietf-pce-association-diversity PCEP extension for signaling LSP diversity constraint
- draft-ietf-pce-association-policy PCEP extension for associating Policies and LSPs
- draft-ietf-pce-binding-label-sid Carrying Binding Label/Segment-ID in PCE-based Networks
- draft-ietf-rtgwg-segment-routing-ti-lfa Topology Independent Fast Reroute using Segment Routing
- draft-ietf-spring-mpls-anycast-segments Anycast Segments in MPLS based Segment Routing
- draft-ietf-spring-mpls-path-segment Path Segment in MPLS Based Segment Routing Network
- draft-ietf-spring-segment-routing-ldp-interop-15 Segment Routing interworking with LDP
- draft-ietf-spring-segment-routing-mpls-18 Segment Routing with MPLS data plane
- draft-ietf-spring-segment-routing-policy Segment Routing Policy Architecture
- draft-koldychev-pce-multipath PCEP Extensions for Signaling Multipath Information
- draft-koldychev-pce-operational PCEP Operational Clarification
- draft-litkowski-pce-state-sync Inter Stateful Path Computation Element communication procedures
- draft-tokar-pce-sid-algo Carrying SID Algorithm information in PCE-based Network
- draft-voyer-pim-sr-p2mp-policy Segment Routing Point-to-Multipoint Policy
- draft-voyer-spring-sr-replication-segment SR Replication Segment for Multi-point Service Delivery

- ietf-6man-spring-srv6-oam Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)
- ietf-idr-bgpls-srv6-ext BGP Link State Extensions for SRv6
- RFC 1112 Host Extensions for IP Multicasting (Snooping)
- RFC 1142 IS-IS Intra-domain Routing Protocol
- RFC 1195 IS-IS for Routing in TCP/IP and Dual Environments
- RFC 1305 NTPv3
- RFC 1323 TCP Extensions for High Performance
- RFC 1350 The TFTP Protocol
- RFC 1519 CIDR
- RFC 1812 Requirements for IPv4 Routers
- RFC 1981 Path MTU Discovery for IP version 6
- RFC 1997 BGP Communities Attribute
- RFC 2104 HMAC: Keyed-Hashing for Message Authentication
- RFC 2236 Support IGMPv2
- RFC 2328 OSPF Version 2
- RFC 2362 Protocol Independent Multicast - Sparse Mode (PIM-SM)
- RFC 2385 Protection of BGP Sessions via MD5
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2462 IPv6 Stateless Address Auto configuration
- RFC 2464 Transmission of IPv6 over Ethernet Networks
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2547 BGP/MPLS VPNs
- RFC 2702 Requirements for Traffic Engineering over MPLS
- RFC 2711 Support Router-Alert option
- RFC 2740 OSPF for IPv6 (OSPFv3)
- RFC 2796 BGP Route Reflection: Alternative to Full-mesh IBGP
- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 2973 IS-IS Mesh Groups
- RFC 2991 OSPF Equal Cost Multipath
- RFC 2992 Analysis of an Equal-Cost Multi-Path Algorithm
- RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links
- RFC 3031 Multi Protocol Label Switching Architecture (MPLS)
- RFC 3046 DHCP Relay Agent Information Option
- RFC 3101 OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3277 ISIS Transient Black hole Avoidance
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3376 Support for IGMPv3
- RFC 3392 Capabilities Advertisement with BGP4
- RFC 3412 Message Processing and Dispatching for the SNMP
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the SNMPv3
- RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

- RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
- RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
- RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3579 RADIUS (Remote Authentication Dial In User Service),Support For Extensible Authentication Protocol (EAP)
- RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS),Usage Guidelines
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3618 Multicast Source Discovery Protocol (MSDP)
- RFC 3618 Support MSDP
- RFC 3623 Graceful Restart for OSPF
- RFC 3630 OSPF Traffic-engineering
- RFC 3719 Recommendations for Interoperable Networks using IS-IS
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
- RFC 3916 Requirement for Pseudo- Wire Emulation Edge-to-Edge (PWE3)
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
- RFC 4061 PIM Sparse Mode shall be supported as specified
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Transition Mechanisms for IPv6 Hosts and Routers - Dual IP Layer
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4291 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4444 MIB for ISIS
- RFC 4446 IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4486 Subcodes for BGP Cease Notification Messages
- RFC 4552 OSPFv3 authentication
- RFC 4558 Node-ID Based Resource Reservation Protocol (RSVP) Hello and Hello A Clarification Statement
- RFC 4561 Definition of a Record Route Object (RRO) Node-Id Sub-Object
- RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM) Specification
- RFC 4602 Protocol Independent Multicast - Sparse Mode (PIM-SM) Requirements Analysis
- RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast
- RFC 4605 Supports IGMP / Multicast Listener Discovery MLD / Based Multicast Forwarding
- RFC 4607 Source-Specific Multicast for IP
- RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
- RFC 4655 A Path Computation Element (PCE)-Based Architecture
- RFC 4655 A Path Computation Element (PCE)-Based Architecture
- RFC 4657 Path Computation Element (PCE) Communication Protocol Generic Requirements

- RFC 4657 Path Computation Element (PCE) Communication Protocol Generic Requirements
- RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
- RFC 4684 Constrained Route Distribution for BGP/MPLS IP VPNs.
- RFC 4724 Graceful Restart Mechanism for BGP – GR Helper
- RFC 4750 MIB support for OPSFv2
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4761 VPLS, BGP-AD and Signaling
- RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
- RFC 4762 VPLS, LDP Signalling
- RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
- RFC 4781 Graceful Restart Mechanism for BGP with MPLS Interconnect IPv6 islands over a Multiprotocol
- RFC 4798 Interconnect IPv6 islands over a Multiprotocol
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
- RFC 4875, RFC 6510 RSVP-TE extensions for signaling for point to multipoint LSPs
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5006 IPv6 Router Advertisement Option for DNS Configuration
- RFC 5059 Support Bootstrap Router (BSR) Mechanism for PIM
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5120 ISIS Multi Topology (MT) Routing
- RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags
- RFC 5151 Inter-Domain MPLS and GMPLS Traffic Engineering –Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5250 OSPF opaque LSA Option
- RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates
- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Support redistribution between different levels of ISIS
- RFC 5303 Three-Way Handshake for IS-IS Point-to-Point Adjacencies
- RFC 5304 Support for HMAC-MD5 authentication
- RFC 5305 IS-IS Extensions for Traffic Engineering
- RFC 5306 Restart Signaling for IS-IS
- RFC 5308 Routing IPv6 with IS-IS
- RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols
- RFC 5329 OSPFv3 Traffic-Engineering
- RFC 5340 OSPFv3
- RFC 5357 A Two-Way Active Measurement Protocol (TWAMP)
- RFC 5420 Encoding of Attributes for MPLS LSP Establishment Using RSVP-TE
- RFC 5440 Path Computation Element (PCE) Communication Protocol (PCEP)
- RFC 5440 Path Computation Element (PCE) Communication Protocol (PCEP)
- RFC 5462 Multiprotocols Label Switching (MPLS) Label Stack Entry: “EXP” Field Renamed to “Traffic Class” Field
- RFC 5496 Support The Reverse Path Forwarding (RPF) Vector TLV.
- RFC 5561 LDP Capabilities

- RFC 5575 Dissemination of Flow Specification Rules
- RFC 5643 OSPFv3 MIB
- RFC 5668 4 Octet AS Specific BGP Extended Community
- RFC 5701 IPv6 Address Specific BGP Extended Community Attribute
- RFC 5711 Node Behavior upon Originating and Receiving Resource Reservation Protocol (RSVP) Path Error Messages
- RFC 5714 IP Fast Reroute Framework
- RFC 5880 Bidirectional Forwarding Detection (BFD)
- RFC 5925 TCP authentication
- RFC 6074 Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)
- RFC 6119 IPv6 Traffic Engineering in IS-IS
- RFC 6165 Extensions to IS-IS for Layer-2 Systems
- RFC 6177 IPv6 Address Assignment to End Sites
- RFC 6213 Support ISIS BFD-Enabled TLV
- RFC 6226 Support PIM Group-to-Rendezvous-Point Mapping
- RFC 6241 Network Configuration Protocol (NETCONF)
- RFC 6242 Using the NETCONF Protocol over Secure Shell (SSH)
- RFC 6374 Packet Loss and Delay Measurement for MPLS Networks
- RFC 6374 Packet Loss and Delay Measurement for MPLS Networks
- RFC 6388 Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path
- RFC 6391 Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network
- RFC 6514 BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPN
- RFC 6514 BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs
- RFC 6515 IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN
- RFC 6516 IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages
- RFC 6517 Mandatory Features in a Layer 3 Multicast BGP/MPLS VPN Solution
- RFC 6547 Using 127-Bit IPv6 Prefixes on Inter-Router Links
- RFC 6549 OSPFv2 Multi-Instance Extension
- RFC 6718 Pseudowire Redundancy
- RFC 6822 IS-IS Multi-Instance
- RFC 6936 Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums
- RFC 6987 OSPF Stub Router Advertisement
- RFC 7041 Extensions to the Virtual Private LAN Service (VPLS) PE Model for Provider Backbone Bridging
- RFC 7080 VPLS Interoperability with Provider Backbone Bridges
- RFC 7142 Reclassification of RFC 1142 to Historic
- RFC 7166 Authentication Trailer for OSPFv3
- RFC 7311 Accumulated IGP Metric Attribute for BGP
- RFC 7432 BGP MPLS-Based Ethernet VPN
- RFC 7470 Conveying Vendor-Specific Constraints in the Path Computation Element Communication Protocol
- RFC 7471 OSPF Traffic Engineering (TE) Metric Extensions
- RFC 7471 OSPF Traffic Engineering (TE) Metric Extensions

- RFC 768 User Datagram Protocol
- RFC 7752 North-Bound Distribution of Link-State and Traffic Eng. (TE)
- RFC 7752 North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP
- RFC 7794 IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability
- RFC 7794 IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability
- RFC 7810 IS-IS Traffic Engineering (TE) Metric Extensions
- RFC 7820 UDP Checksum Complement in the One-Way Active Measurement Protocol (OWAMP) and Two-Way Active Measurement Protocol (TWAMP)
- RFC 7855 Source Packet Routing in Networking (SPRING) Problem Statement and Requirements
- RFC 7876 UDP Return Path for Packet Loss and Delay Measurement for MPLS Networks
- RFC 7876 UDP Return Path for Packet Loss and Delay Measurement for MPLS Networks
- RFC 791 Internet Protocol Version 4
- RFC 7911 Advertisement of Multiple Paths in BGP shall be supported
- RFC 7916 Operational Management of Loop-Free Alternates
- RFC 792 Internet Control Message Protocol
- RFC 793 Transmission Control Protocol
- RFC 8051 Applicability of a Stateful Path Computation Element (PCE)
- RFC 8077 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 8092 Large Community Attributes
- RFC 8186 Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)
- RFC 8214 Virtual Private Wire Service Support in Ethernet VPN
- RFC 8231 Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE
- RFC 8231 Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE
- RFC 8233 Extensions to PCEP to Compute Service-Aware Label Switched Paths (LSPs)
- RFC 8233 Extensions to PCEP to Compute Service-Aware Label Switched Paths (LSPs)
- RFC 826 Address Resolution Protocol
- RFC 8281 PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model
- RFC 8281 PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model
- RFC 8287 Label Switched Path (LSP) Ping/Traceroute for Segment Routing (SR) IGP-Prefix and IGP-Adjacency Segment Identifiers (SIDs) with MPLS Data Planes
- RFC 8287 Label Switched Path (LSP) Ping/Traceroute for Segment Routing (SR) IGP-Prefix and IGP-Adjacency Segment Identifiers (SIDs) with MPLS Data Planes
- RFC 8354 Use Cases for IPv6 Source Packet Routing in Networking (SPRING)
- RFC 8356 Experimental Codepoint Allocation for the Path Computation Element Communication Protocol (PCEP)
- RFC 8402 Segment Routing Architecture
- RFC 8403 A Scalable and Topology-Aware MPLS Dataplane Monitoring System
- RFC 8408 Conveying path setup type in PCEP messages
- RFC 8408 Conveying path setup type in PCEP messages
- RFC 8491 Signaling MSD (Maximum SID Depth) using IS-IS

- RFC 854 Telnet
- RFC 8570, RFC 7810 IS-IS Traffic Engineering (TE) Metric Extensions
- RFC 8571 BGP-LS Advertisement of IGP Traffic Engineering Performance Metric Extensions
- RFC 8660 Segment Routing with MPLS data plane
- RFC 8661 Segment Routing interworking with LDP
- RFC 8664 PCEP Extensions for Segment Routing
- RFC 8668 Advertising L2 Bundle Member Link Attributes in IS-IS
- RFC 8669 Segment Routing Prefix SID extensions for BGP
- RFC 8679 PCEP Extensions for Establishing Relationships Between Sets of LSPs
- RFC 8697 Path Computation Element Communication Protocol (PCEP) Extensions for Establishing Relationships between Sets of Label Switched Paths (LSPs)
- RFC 8741 Ability for a Stateful PCE to Request and Obtain Control of a LSP
- RFC 8754 IPv6 Segment Routing Header (SRH)
- RFC 8762 Simple Two-Way Active Measurement Protocol
- RFC 958 Network Time Protocol
- RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in ISIS
- RFC 5310 IS-IS Generic Cryptographic authentication
- EVPN Seamless Integration with VPLS with support of draft-ietf-bess-evpn-vpls-seamless-integ
- IP Inter-Subnet Forwarding in EVPN with support of draft-ietf-bess-evpn-inter-subnet-forwarding
- EVPN IP Prefix Advertisement with support of draft-ietf-bess-evpn-prefix-advertisement
- EVPN All active multihoming with support of RFC7432
- IGMP-snooping and S,G state synch with EVPN using ESI-label with support of RFC7432
- Interconnect Solution for EVPN Overlay networks according to draft-ietf-bess-dci-evpn-overlay
- Network Virtualization Overlay Solution using EVPN according to draft-ietf-bess-evpn-overlay

6. REQUISITOS PARTICULARES E OBRIGATÓRIOS DOS EQUIPAMENTOS DO TIPO P

Os quatro equipamentos do tipo P são responsáveis pelas configurações do tipo Provider numa arquitetura de operador. Como tal, no nível mais simples de licenciamento (caso se aplique), pelo menos 15 (quinze) das 24 (vinte e quatro) portas de cada chassis (60 portas no conjunto dos quatro chassis) têm de suportar funcionalidades tais como:

- ISIS e OSPF com suporte para Segment Routing, BGP;
- MPLS, Segment Routing, PIM
- Telemetria, SSH, SNMP, Netflow, ACLs, Radius
- Policy Based Routing e ACL Based Routing
- Para tempos de convergência mais baixos TI-LFA, IP Fast Reroute, BGP PIC;
- Suporte para QoS e Qos Hierárquico
- Funcionalidades tais como Dot1Q, QinQ, VLAN, L2Transport, PWHE, IRB

Uma vez que estes equipamentos serão cruciais durante a fase de transição da atual arquitetura para o novo modelo de rede, é obrigatório que no conjunto dos quatro routers do tipo P a fornecer, pelo menos 5 portas em cada um deles (20 portas no total dos quatro equipamentos), suportem todas as funcionalidades detalhadas no presente ponto e no ponto 5, cumprindo todos os requisitos técnicos aí indicados. São consideradas funcionalidades avançadas:

- Serviços de L2 avançados: Bridging, VPLS, EVPN L2 GW, EVPN IRB com gateway anycast;
- Serviços de L3 avançados: L3VPN, VRFs, Multicast VPN, IPv6 Provider Edge (6PE);
- Traffic Engineering: SR-TE, IGP Flex-Algo

Para além de todos requisitos técnicos detalhados nos pontos 5 e 6 do presente anexo, um equipamento do tipo P deverá ainda cumprir os seguintes requisitos:

a) Estar equipado com todas as fontes de alimentação possíveis para o chassis (para AC 230v), garantindo redundância das mesmas em caso de falha de uma. Deverão vir equipados com cabos com terminação IEC-C13;
b) Estar equipado com todos os sistemas de ventilação possíveis para o equipamento de forma a haver redundância das mesmas;
c) Disponibilização de, no mínimo, 24 (vinte e quatro) portas a 100Gbps com uma taxa de contenção máxima de 4:3;
d) Vir dotado do software e respetivo licenciamento para suportar todos os requisitos técnicos, funcionalidades, débitos ou outros, caso se aplique, tal como descritos no presente ponto e ponto 5. Caso se aplique, todo o licenciamento fornecido não deverá estar limitado temporalmente, sendo considerada a utilização da licença como perpétua;

7. MANUTENÇÃO

O adjudicatário compromete-se a assegurar, durante a vigência do contrato e sem custos adicionais, a manutenção da totalidade do equipamento fornecido. Os serviços de manutenção, apoio técnico e outros com eles relacionados deverão obedecer aos requisitos enunciados nos pontos seguintes.

7.1. SERVIÇO DE ABERTURA DE OCORRÊNCIAS

É responsabilidade da FCT, I.P. definir os seus contactos autorizados para Abertura de Ocorrências. Como meios para abertura de ocorrências deverão ser disponibilizados pelo adjudicatário os seguintes:

- Web (https)
- E-mail
- Telefone
- Fax

O adjudicatário comunicará à FCT, I.P. os meios de contacto acima referidos no prazo de 5 dias após a assinatura do contrato.

Na comunicação de uma Ocorrência a FCT, I.P. compromete-se a remeter a seguinte informação, por um dos meios de abertura disponibilizados:

- Nome do Cliente
- Número Contrato
- Nome de contacto
- Número telefone
- Endereço de e-mail
- Prioridade
- Número de série do equipamento
- Modelo
- Resumo da anomalia verificada

A informação a disponibilizar pela FCT, I.P. poderá ser alvo de alterações, caso a FCT, I.P. verifique que tal se justifica.

7.2. ACESSO REMOTO

Para determinadas ocorrências a FCT, I.P. poderá disponibilizar acesso remoto aos seus equipamentos. De acordo com as situações, este acesso poderá ser disponibilizado via SSH ou SNMP.

7.3. APOIO TÉCNICO

A FCT pode solicitar ao adjudicatário apoio técnico, que poderá consistir essencialmente em esclarecimentos de dúvidas sobre a utilização operacional, sob suspeita de erros ou mau funcionamento do equipamento e *software* objeto de manutenção.

O Apoio Técnico deverá ser assegurado pelo adjudicatário durante o Horário de Cobertura definido no presente Anexo.

É responsabilidade do adjudicatário garantir que o Apoio Técnico é sempre prestado por técnicos certificados na gama de equipamento, objeto de adjudicação, no âmbito da presente consulta. As equipas responsáveis pelo apoio técnico deverão estar localizadas em áreas onde seja possível garantir a prestação de serviços tal como descritas no presente Caderno de Encargos, nomeadamente para realização de troca de equipamento de substituição.

7.4. HELPDESK

A FCT, I.P. deve ter acesso a um *helpdesk* que deverá responder às seguintes solicitações: abertura de ocorrências, acompanhamento de ocorrências abertas e prestação de apoio técnico. Este serviço tem obrigatoriamente de ser prestado durante o Horário de Cobertura definido abaixo, tendo de obedecer ao Tempo de Resposta igualmente definido.

Todos os contactos feitos pela FCT, I.P., via *helpdesk*, consideram-se como realizados ao abrigo do presente contrato, não dando, pois, lugar a qualquer pagamento adicional.

Os contactos referentes ao *helpdesk* deverão ser fornecidos, no prazo de cinco dias após a entrega prevista no artigo 5º.

7.5. HORÁRIO DE COBERTURA

O Horário de Cobertura é o período durante o qual o adjudicatário se compromete a prestar o Serviço de Abertura de Ocorrências e o Apoio Técnico.

O Horário de Cobertura do serviço de manutenção deverá ser assegurado durante o horário das 9 horas às 18 horas, todos os dias úteis da semana.

7.6. TEMPO DE RESPOSTA

O tempo de resposta é o tempo máximo entre a abertura da ocorrência pela FCT, I.P. e a receção de resposta do adjudicatário, sendo que a resposta considerada para o efeito tem de ser obrigatoriamente fornecida por técnico certificado para o equipamento alvo de adjudicação. Não é considerada, para este efeito, uma resposta de um sistema automático de resposta/registo de ocorrências. O tempo de resposta deverá estar de acordo com a prioridade definida pela FCT, I.P. na abertura da ocorrência.

Independentemente do meio da abertura da Ocorrência, deve ser respeitado o Tempo de Resposta, de acordo com o nível de prioridade da ocorrência:

Nível de Prioridade da Ocorrência	Tempo de Resposta máximo
P1 (Crítico)	1 hora
P2 (Seriamente Degradado)	2 horas
P3 (Degradado)	4 horas
P4 (Informativo)	Dia útil seguinte

7.7. NÍVEL DE PRIORIDADE

Cabe à FCT, I.P. a definição da severidade da ocorrência aquando da Abertura de Ocorrência no âmbito do serviço de manutenção. Os níveis de prioridade estabelecidos pela FCT, I.P. são os seguintes:

- P1 (Crítico): A anomalia reportada tem um impacto crítico na atividade da FCT, I.P.;

- P2 (Seriamente Degradado): A anomalia verificada causa degradação de performance e afeta a funcionalidade, com impacto significativo na atividade da FCT, I.P.;

- P3 (Degradado): A anomalia verificada causa a degradação de performance e afeta a funcionalidade, embora sem impacto significativo na atividade da FCT, I.P.;

- P4 (Informativo): A FCT, I.P. pretende informações sobre determinado assunto.

De acordo com o nível de prioridade indicado pela FCT, I.P. na altura de abertura da ocorrência, o adjudicatário tem obrigatoriamente de cumprir o respetivo Tempo de Resposta definido no presente anexo.

7.8. SERVIÇO DE ACOMPANHAMENTO DE OCORRÊNCIAS *ONLINE*

A FCT, I.P. deve ter acesso a um sistema informático *online* (via Internet), onde possa recorrer ao Serviço de Abertura de Ocorrências e Apoio Técnico. Através deste sistema deve ser possível à FCT, I.P. acompanhar o estado de Ocorrências reportadas.

Os contactos referentes ao Serviço de Acompanhamento de Ocorrências Online deverão ser fornecidos à FCT, I.P., nos primeiros cinco dias úteis após a entrega prevista no artigo 5º.

7.9. GESTOR DE CONTA TÉCNICO

O Gestor de Conta Técnico deverá ser o representante do adjudicatário para assuntos relacionados com o serviço de manutenção/apoio técnico/garantia, devendo o mesmo ter elevado grau de conhecimento e experiência em redes. O Gestor de Conta Técnico deve adquirir um conhecimento profundo da rede da FCT, I.P. É responsabilidade do Gestor de Conta Técnico:

- Garantir que a informação relativa a ocorrências é trocada de forma eficiente;

- Supervisionar e acompanhar ocorrências;

- Assegurar que as ocorrências são resolvidas o mais rapidamente possível;

- Zelar pelo sigilo da informação obtida sobre a infraestrutura da FCT, I.P. obtida no contexto das ações de apoio técnico;

- Elaborar relatórios do serviço de manutenção, caso tal seja requerido.

7.10. EQUIPAMENTO DE SUBSTITUIÇÃO

O adjudicatário é responsável por garantir que equipamento de substituição seja disponibilizado sempre que se verifique uma ocorrência que o torne necessário. Cabe à FCT, I.P. decidir sobre a necessidade de substituição de equipamento, sendo que o adjudicatário deverá respeitar essa decisão e deverá agir em conformidade. O adjudicatário não pode, em caso algum, recusar a disponibilização de equipamento de substituição, caso tenha sido essa a decisão da FCT, I.P. Por Equipamento de Substituição, entende-se o equipamento que, não só garanta as mesmas funcionalidades do original, mas também possua as mesmas capacidades ou superiores (por exemplo, ao nível de densidade de portas, capacidade de comutação/encaminhamento, funcionalidades e tipo de portas).

O equipamento de substituição deverá assegurar as funções do equipamento avariado até que o mesmo seja reparado, caso se verifique que pode ser reparado. Com o equipamento avariado em sua posse, o adjudicatário dispõe do prazo de cinco dias úteis para aferir da viabilidade da sua reparação, sendo a decisão sobre a reparação comunicada, através de meios eletrónicos, à FCT, I.P. dentro desse prazo.

Caso o adjudicatário confirme a viabilidade de reparação do equipamento avariado, o equipamento avariado enviado para reparação deverá ser disponibilizado no prazo máximo de trinta dias corridos contados desde o dia de abertura da ocorrência pela FCT, I.P. O adjudicatário deverá sempre disponibilizar com o equipamento reparado à FCT, I.P., um relatório descritivo das operações efetuadas no equipamento alvo de reparação.

Caso o adjudicatário conclua pela inviabilidade de reparação do equipamento avariado, e sujeito à expressa aceitação por escrito da FCT, I.P., o equipamento de substituição torna-se automaticamente propriedade da FCT, I.P. Caso o adjudicatário tenha disponibilizado equipamento

de substituição diferente ao danificado, a FCT, I.P. tem o direito de exigir equipamento de substituição exatamente igual ao avariado. A FCT, I.P. não aceitará nunca equipamento com performance inferior à do equipamento avariado. A aceitação de equipamento diferente do avariado implica sempre a expressa aceitação por escrito e não poderá nunca acarretar custos para a FCT, I.P.

No caso de a avaria implicar a substituição definitiva do equipamento, o equipamento novo deverá obrigatoriamente ser disponibilizado à FCT, I.P. devidamente acondicionado e selado pelo fabricante.

O adjudicatário deverá disponibilizar o equipamento de substituição no dia útil seguinte à comunicação da ocorrência, caso esta comunicação ocorra até às 14h. Caso a comunicação da ocorrência seja efetuada após esta hora ou ao fim de semana ou num feriado nacional, considera-se, para efeitos de disponibilização pelo adjudicatário do equipamento de substituição, o segundo dia útil seguinte à comunicação da ocorrência pela FCT, I.P.

O local de recolha do equipamento de substituição não poderá distar mais de 30 km da Avenida do Brasil, 101, Lisboa. É responsabilidade da FCT, I.P. a recolha do equipamento nessa localização.

7.11. ÁREA PRIVADA

O adjudicatário deverá proceder à criação de uma área privada de cliente, exclusiva para a FCT, I.P., que seja acessível via Internet, e onde possam ser disponibilizados: atualizações de *software*, relatórios e documentos técnicos.

A FCT, I.P., pode solicitar ao adjudicatário a disponibilização de *software* para o equipamento objeto de adjudicação, nesta área privada, sem que tal implique qualquer encargo adicional para a FCT, I.P.

7.12. SOFTWARE

Como parte integrante da obrigação de manutenção, o adjudicatário deverá disponibilizar qualquer versão de *software*, dentro da gama de licenciamento incluída no equipamento objeto de adjudicação, sem que tal implique qualquer encargo adicional para a FCT, I.P.

8. COLOCAÇÃO DOS EQUIPAMENTOS NAS INSTALAÇÕES DO ADJUDICANTE

O equipamento a fornecer ao abrigo do contrato deve ser colocado à disposição da FCT, I.P, para efeitos de realização dos testes de aceitação a que se refere o número seguinte no prazo de e cinquenta dias após a assinatura do contrato, devendo esse equipamento ser objeto de instalação física, por parte do adjudicatário, em bastidor a indicar pela FCT, I.P.

A colocação à disposição dos bens da FCT, I.P. tem de ser obrigatoriamente coordenado com esta sendo que o agendamento deverá ser efetuado com a antecedência mínima de 7 dias úteis.

A disponibilização do equipamento ocorrerá em duas moradas no Porto, com um conjunto de um equipamento do tipo PE e dois do tipo P a ser entregue em cada uma:

- R. Dr. Roberto Frias, Universidade do Porto, Centro Informática (CICA), Ed. D, Sala 102, 4200-465;
- Largo da Estação de Campanhã, Estação Porto Campanhã, Sala IP Telecom, 1º andar, 4300-173;

É da responsabilidade do adjudicatário o transporte do equipamento até às moradas indicadas.

A instalação do equipamento em bastidor deverá ocorrer na mesma data da sua disponibilização à FCT, I.P. e da responsabilidade do adjudicatário.

9. TESTES DE ACEITAÇÃO

O adjudicante poderá promover a realização de testes de aceitação, destinados à verificação da conformidade dos bens com os requisitos técnicos constantes do presente Caderno de Encargos, devendo os mesmos ocorrer nos 30 dias corridos após a receção dos bens objeto do contrato nas salas usadas pela FCT, I.P para comutação de tráfego no Porto, nomeadamente na FEUP – CICA e na Estação Porto Campanhã, Sala IPTELECOM, nos termos descritos no presente anexo.

Os bens consideram-se entregues na aceção do artigo 5º na data da sua aceitação por escrito por parte da FCT, I.P. ou na ausência de qualquer notificação no 31º dia corrido subsequente à receção de todos os bens objeto de adjudicação nas instalações referidas no parágrafo anterior.

Se nos termos dos testes de aceitação a FCT, I.P. constatar que os bens não cumprem os requisitos técnicos constantes do presente Caderno de Encargos, disso dará conhecimento ao adjudicatário, abrindo-se um prazo de 7 (sete) dias corridos para que este desenvolva as diligências necessárias a que aqueles requisitos sejam cumpridos, e o equipamento seja de novo submetido a testes.

Se, estes testes de aceitação não forem concluídos com êxito, persistindo a desadequação aos requisitos técnicos exigidos, a FCT, I.P. poderá dar novo prazo de sete dias ao adjudicatário para correção das anomalias detetadas, aplicando-se com as devidas adaptações o estabelecido neste nº 9 ou, em alternativa, considerar incumprida a obrigação de fornecimento dos equipamentos para reforço de equipamento de encaminhamento IP da RCTS e rescindir o Contrato.

10. FORMAÇÃO

A FCT poderá solicitar a realização de ações de formação de forma a adquirir os conhecimentos necessários para operar com total autonomia os equipamentos alvo desta aquisição. O tempo máximo para formação que a FCT poderá solicitar ao adjudicatário é de duas semanas para os elementos da equipa, sendo as ações de formação realizadas ou nas instalações da FCT, ou em local a designar na área da Grande Lisboa. A FCT poderá ainda solicitar os manuais dos equipamentos e outros utilizados em ações de formação ministrados para os equipamentos em causa. Os manuais são fornecidos sem qualquer custo adicional para a FCT num prazo máximo de 10 dias úteis após a sua solicitação. As ações de formação serão realizadas em data a combinar entre as partes. Na falta de acordo, a FCT indicará as respetivas datas, as quais são fixadas atendendo a critérios de razoabilidade.

Assinado por : **ANA MANUELA TAVARES AMARAL PINTO**
Num. de Identificação: BI10764067