



**Computação Científica Nacional
FCCN**

Caderno de Encargos

**“EQUIPAMENTOS DE
TRANSPORTE E ACESSO IP a
100Gbps”**

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 “Equipamentos de Transporte e Acesso IP a 100Gbps”.
2. O Contrato a celebrar integra, para além do clausulado contratual:
 - a) os suprimientos 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) Assegurar a manutenção;
 - c) Cumprir os prazos estabelecidos, designadamente, para a execução das prestações a que se obriga;
 - d) Prestar informação;
 - e) 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 seu clausulado 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 6 e 7 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 7 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 623.000€ (seiscentos e vinte e três mil euros); acrescidos de IVA à taxa legal em vigor¹.

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

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 500.000€, prestar caução nos termos e condições constantes estabelecido no artigo 90º do Código dos Contratos Públicos.
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 11.º

VIGÊNCIA DO CONTRATO

¹ O presente procedimento não prevê a adjudicação por lotes, uma vez que a aquisição tem por objeto equipamentos de transporte e acesso numa rede com arquitetura Service Provider com Segment Routing sobre MPLS. Dado tratar-se da aquisição de cinco equipamentos, é necessário garantir que todos usam os mesmos chipsets, placas e sistema operativo para assegurar a total interoperabilidade, o que não aconteceria se fossem de diferentes fabricantes, modelos ou com arquitetura interna distinta. Tal só é garantido pelo fornecimento por um único adjudicatário e para uma única marca e modelo específicos.

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 12.º

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 13.º

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 6 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 5.6. 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 5.10 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 5.10 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 14.º

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 15.º

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 16.º

LEI APLICÁVEL

O contrato rege-se pela lei portuguesa.

ARTIGO 17.º

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 18.º

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

b) Pelo adjudicatário:

Nome do representante:

Endereço postal:

Endereço eletrónico:

ARTIGO 19.º

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 20.º

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.

ANEXO I

EQUIPAMENTOS DE TRANSPORTE E ACESSO IP A 100GBPS

1. SOLUÇÃO A ADQUIRIR

O adjudicatário compromete-se a fornecer à FCT, I.P. cinco (5) routers com as características descritas no presente Anexo.

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.

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

Não constitui obrigação do adjudicatário a configuração dos equipamentos a fornecer.

2. SOFTWARE, REQUISITOS GERAIS E COMUNS AOS EQUIPAMENTOS

O licenciamento do *software* dos Equipamentos deve ser efetuado 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.

3. REQUISITOS TÉCNICOS GERAIS E OBRIGATÓRIOS DOS EQUIPAMENTOS

3.1. CARACTERÍSTICAS FÍSICAS ESPECÍFICAS DOS CHASSIS

Os equipamentos devem possuir as seguintes características físicas:

- Dimensões:
 - altura máxima (3RU);
 - largura máxima 44.39 cms;
 - profundidade máxima de 60 cms;
- Capacidade de comutação de pelo menos 3.6Tbps, *full duplex*, com arquitetura não bloqueante;
- Arquitetura híbrida com suporte de interfaces fixas ao chassi e capacidade de expansão com, pelo menos, um módulo adicional para interfaces;
- Deverá suportar redundância e alta disponibilidade de carta de matriz de comutação (Switch Fabric);

- Deverá suportar redundância de carta Processadora de Encaminhamento (2 cartas). Cada carta deverá ter, pelo menos, o seguinte conjunto de interfaces/capacidades:
 - CPU baseado na geração Intel Xeon 64-bit
 - 32G memória DDR4 SDRAM
 - 2 x 128G SSD para armazenamento
 - Timing Interfaces: 2 x BITS RJ45
 - GPS Interfaces: 10Mhz, 1 PPS, ToD
 - Consola: RJ45 RS232
 - AUX: RJ45 RS232
 - 2 x 10/100/1000M OOB
 - 1 x USB A
- Deverá suportar redundância das fontes de alimentação:
 - 1.6 kW DC power module (até 4 módulos), redundância: 2+2
 - 1.6 kW AC power module (até 4 módulos), redundância:
 - AC high line (200-240V): 2+2
 - AC low line (90-130V): 3+1
- Deverá suportar ventilação, frente-trás, com ventoinhas redundantes;
- Suporte de, pelo menos 16, interfaces fixas no chassis do tipo QSFP28 com capacidade de 10, 40 e 100G e, um mínimo, de 20 interfaces SFP+ adicionais, com uma performance total de 1.6T, *full duplex*. Deve permitir configurações sem bloqueio das 16 x 100G, ou 15 x 100G + 10 x 10G ou 14 x 100G + 20 x 10G. Não são permitidos outro tipo de formatos de transceivers além dos QSFP28 para 100G e SFP+ para os 10G nestas interfaces;
 - Suporte de MACsec
 - AES-128 / AES-256
 - AES-XPB-128 / AES-XPB-256
 - Point-to-Multipoint
 - LACP/Link Bundle Member Support
 - Physical Links
 - Suporte MACsec nos interfaces de breakout
- Suporte de G.8273.2 PTP Class C;
- Suporte de satélites para expansão de interfaces;
- O equipamento deve ser disponibilizado com todas as fontes de alimentação redundantes que permitam o uso de duas cartas Processadoras de Encaminhamento, todos os *switch fabric*, assim como dos interfaces fixos no chassis e ainda com o *slot* de expansão com uma carta de alto desempenho para AC 90-265V, 50-60Hz;
- Passível de instalação em rack de 19 polegadas;
- Suporte para transceivers de 100G (QSFP-28) do tipo QSFP-100G-CWDM4-S, QSFP-100G-SM-SR, QSFP-100G-SR4-S, QSFP-100G-LR4-S, QSFP-100G-ER4L-S;

- Suporte no chassis para portas a 40 Gigabit Ethernet do tipo QSFP+. Não são permitidos outros formatos físicos;
- Suporte no chassis para transceivers de 40G QSFP-40G-SR4-S, QSFP-40G-SR4, QSFP-40G-CSR4, QSFP-40G-LR4-S, QSFP-40G-LR4, QSFP-40G-ER4, QSFP-4x10G-LR-S;
- Suporte para portas a 10 Gigabit Ethernet do tipo SFP+. Não são permitidos outros formatos físicos;
- Suporte para transceivers de 10G do tipo SFP-10G-SR, SFP-10G-LR, SFP-10G-ER, SFP-10G-ZR;
- Consumo máximo por Gbps de 0.5W
- Suporte de modulo de expansão com capacidade mínima de 2Tbps de desempenho, *full duplex*, com um suporte mínimo das seguintes densidades de portas:
 - 15 interfaces QSFP28 com suporte de 10,25,40 e 100G (com suporte de *breakout cable* para 4X10G)
 - 5 interfaces QSFPDD com suporte de 10,25,40,100,200 e 400G (com suporte de *breakout cable* para suporte de 4X10G);
 - Suporte para transceivers de 400G do tipo QDD-400G-DR4-S, QDD-400G-FR4-S, QDD-400G-LR8-S, QDD-400G-ZR-S (40kms), QDD-400G-ZRP-S (40Kms a 100/200/300/400Gbps), além do suporte para transceivers de 100G e 40G indicados anteriormente suportados no chassis;
 - As portas a 200 e 400 Gigabit Ethernet são suportados no formato QSFPDD. Não são permitidos outros formatos físicos;
 - Suporte de MACsec
 - AES-128 / AES-256
 - AES-XPB-128 / AES-XPB-256
 - Point-2-Multipoint
 - LACP/Link Bundle Member Support
 - Physical Links
 - Suporte MACsec nos interfaces de breakout
 - FlexE suportado no hardware
 - Suporte de satélites para expansão de interfaces
- Suporte de modulo de expansão com capacidade mínima de 800Gbps de desempenho, *full duplex*, com um suporte mínimo das seguintes densidades de portas:
 - 32 interfaces SFP28 com suporte de 10 ou 25G
 - 48 interfaces SFP+ com suporte de 10G
 - Suporte para transceivers SFP-25G-SR-S, SFP-10/25G-CSR-S, SFP-10/25G-LR-S, CWDM-SFP10G-xxxx (onde x é o comprimento de onda CWDM para 40Kms), além dos SFP+ de 10G indicados anteriormente suportados no chassis
- Temperatura de funcionamento: 5°C a 40°C;
- Humidade em operação: 10% a 85%;
- Standards ETSI/EN
 - EN300 386: Telecommunications Network Equipment (EMC)
 - ETSI 300 019 Storage Class 1.1

- ETSI 300 019 Transportation Class 2.3
- ETSI 300 019 Stationary Use Class 3.1
- EN55022: Information Technology Equipment (Emissions)
- EN55024: Information Technology Equipment (Immunity)
- EN50082-1/EN-61000-6-1: Generic Immunity Standard
- Standards EMC
 - FCC Class A
 - ICES 003 Class A
 - AS/NZS 3548 Class A
 - CISPR 22 (EN55022) Class A
 - VCCI Class A
 - BSMI Class A
 - IEC/EN 61000-3-2: Power Line Harmonics
 - IEC/EN 61000-3-3: Voltage Fluctuations and Flicker
 - EN50121-4 Railway Applications Part 4: Emission and immunity of the signaling and telecommunications apparatus
- Imunidade
 - IEC/EN-61000-4-2: Electrostatic Discharge Immunity (8kV Contact, 15kV Air)
 - IEC/EN-61000-4-3: Radiated Immunity (10V/m)
 - IEC/EN-61000-4-4: Electrical Fast Transient Immunity (2kV Power, 1kV Signal)
 - IEC/EN-61000-4-5: Surge AC Port (4kV CM, 2kV DM)
 - IEC/EN-61000-4-5: Signal Ports (1kV)
 - IEC/EN-61000-4-5: Surge DC Port (1kV)
 - IEC/EN-61000-4-6: Immunity to Conducted Disturbances (10Vrms)
 - IEC/EN-61000-4-8: Power Frequency Magnetic Field Immunity (30A/m)
 - IEC/EN-61000-4-11: Voltage DIPS, Short Interruptions, and Voltage Variations
 - EN 50121-4: Railway EMC
- Segurança
 - UL/CSA/IEC/EN 60950-1
 - IEC/EN 60825 Laser Safety
 - ACA TS001
 - AS/NZS 60950
 - FDA: Code of Federal Regulations Laser Safety
- Network Equipment Building Systems (NEBS)
 - SR-3580: NEBS Criteria Levels (Level 3)
 - GR-1089-CORE: NEBS EMC and Safety
 - GR-63-CORE: NEBS Physical Protection
- Capacidade mínima, do chassis, para 156 portas a 10 Gigabit Ethernet;
- Capacidade mínima, do chassis, para 144 portas a 10 Gigabit Ethernet;
- Capacidade mínima, do chassis, para 36 portas a 40 Gigabit Ethernet;
- Capacidade mínima, do chassis, para 36 portas a 100 Gigabit Ethernet;

- Capacidade mínima, do chassis, para 5 portas a 400 Gigabit Ethernet.

3.2. ESCALABILIDADE

Os equipamentos a fornecer deverão, pelo menos, suportar a capacidade indicada para cada um dos itens seguintes:

- Unicast FIB: 6M IPv4, 6M IPv6
- MRoute/MFib: 128K IPv4, 64K IPv6
- VRF: 16K
- mVPN VRF: 2k
- OIFs: 64K/NP; 300K/Sistema
- Logical Intfs BVI, GRE: 32K/NP, 32K/System
- Bridge Domains: 64K
- PWs (VPWS, VPLS, EoMPLS): 128K /NPU/System
- PWHE: 3800/NP, 15,200/System, 8 Members per GIL
- VxLAN: 64K /NPU /System
- ARP: 128K/System
- Packet Buffer – Egress: 3GB /4x100G (~ 100ms)
- Egress Queues: 48K /NPU
- Ingress Queues: Não Suportadas
- Policers: Max Reg./Color-aware 128K/NPU - feature policer, Conform-Aware – 64k/NP
- BFD SW Sessions: 8K /NP /System @ 1s
- BFD HW Sessions - Max Sessions: 3K/NP 8K/System @ 50ms
- BFD HW Sessions: Min Timer: 300/NP 600/System @ 3.3ms
- MPLS Labels: 1M
- Label Stack: 10
- MAC Entries: 2M
- NetFlow: 1:1K, Cache# 1M records /LC; 200KPPS /System
- L2 sub-interfaces (EFPs): 64K/NP, 128K/System, 8k/LAG
- EFP Filtering: 64K/NP, 64K /LC, 128K/System, 8k/LAG
- L3 interfaces /sub-interfaces: 32K / NP, 32K/System, 8k/LAG
- QoS Policy-map x class-map entries: 64K v4 + 16k v6 /Port, /NPU
- Unique Policy Maps: 2k /NP Both direction, 51,200 /System, pQoS: 51,200/Sys
- Unique Class Maps: 1k/ Policy, 10k/System
- Microflow Policer: 256k (1k granularity)
- Num of ACL's: 4K /NPU (v4); 4K /NPU (v6)
- Total num of ACE's: 64K (v4) +16K (v6) /Port, /NPU; Mix as long as 64K 160bit entry can fit.

- PBR / ABF: 2k/NP Ingress
- LI Taps: 2K (v4), 1K (v6)
- Ethernet Data Plane Loopback: 200 lines
- BGP peering sessions: 10k
- OSPF / ISIS peering sessions: 6K v4 + 250 v6
- BGP Flow Spec: 3K
- IGP Routes: 40k OSPF or ISIS
- Y.1731 Monitoring PPS per System: 38k/NP
- MEPS w/ CCM @ 3.3mSec per NP (HW offload): 240 sessions/NP
- MEPS w/ CCM @ 10mSec per NP (HW offload) : 1K sessions/NP
- # CFM Sessions (/NP /LC); Services (/System): 32K/NP, 32K/LC, 64K/System
- OpenFlow Entries 64K v4 1-D, 16K v6 1-DMPLS TE Head-End: 15k
- MPLS TE Mid-Points: 128k
- MPLS TE Tail Ends: 64k
- P2MP TE Head End: 15k
- P2MP TE Mid-Points: 64k
- P2MP/mLDP TE Core OIF: 512
- Etherchannel Links per Bundle: 64
- Etherchannel per System: 1600
- EVPN: BD-> 64K, EVI-> 64K, MAC-> 2M

3.3. CARACTERÍSTICAS DO SOFTWARE

Os equipamentos a fornecer, além de suportarem os RFCs e drafts enunciados no presente anexo, têm ainda de suportar as seguintes normas/ protocolos/ configurações que estão no momento a ser usados na rede:

- Portas switching em layer 2;
- IEEE 802.1q VLAN e encapsulamento Q-in-Q (802.1ad);
- Virtual Router Redundancy Protocol (VRRP);
- Jumbo frames em todas as portas;
- Interfaces e sub-interfaces Layer 3;
- Rotas estáticas, OSPFv2 e OSPFv3, ISIS, Multiprotocol BGP;
- BMP – BGP Monitoring Protocol;
- Equal-Cost Multipath (ECMP);
- Bidirectional Forwarding Detection (BFD) e sBFP (Seamless BFD);
- Multiprotocol Label Switching (MPLS), MPLS traffic engineering e Ethernet sobre MPLS (EoMPLS);

- Segment Routing (SR) sobre ISIS e OSPF
- SR traffic engineering e Topology Independent Loop Free Alternatives (TI-LFA);
- SR com suporte de Microloop Avoidance usando OSPF e ISIS
- Flex Algorithm com SR-TE
- Suporte de *dark bandwidth measurement* com SR
- LDP com FRR e RLFA
- Virtual Private Network em layer 3 (L3VPN);
- Qualidade de serviço hierárquica (H-QoS);
- Marcação DSCP do pacote IP;
- Classificação com base na classe de serviço (L2), tipo de serviço (L3) e listas de acesso (L3/L4);
- Suporte para mecanismos de QoS para Core MPLS (suporte EXP bits, marcação, remarcação)
- IEEE 802.1p filtragem/marcação/remarcação
- IETF DSCP filtragem/marcação/remarcação
- WRED Egress
- Priority queuing;
- Policing Ingress/Egress
- Shapping Ingress/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
- Dynamic and Static Buffer Allocation
- Sampled Flow
- Zero-Touch Provisioning (ZTP);
- Suporte para, pelo menos 8 VRFs;
- 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), EVPN Multihoming, EVPN IRB (Integrated Routing and Bridging);
- Suporte dos modos EVPN Nativo com MAC learning: Single Home Network, Dual Home Device – All Active Load Balancing, Dual Home Device – Single -Active Load Balancing
- A EVPN deve ainda suportar as seguintes funcionalidades: flow-based load balancing; Port-Active Multihoming; Single-Flow-Active Load Multihoming Balancing Mode;
- EVPN MPLS Seamless Integration com VPLS;
- Mecanismos de EVPN Core Isolation Protection, EVPN Roting Policy; EVPN Attribute Set;
- EVPN - BGP Multiple Sourced or Redistributed Paths;

- EVPN – Highest Random Weight Mode for EVPN DF Election
- EVPN – Layer 2 Fast Reroute
- EVPN preferred Nexthop
- EVPN Access-drive DF Election
- EVPN Head End Multi-Homed
- Hierarchical EVPN Access Pseudowire
- Inter-AS EVPN Option B
- EVPN E-Tree Per-PE (Scenario 1b)
- EVPN E-TREE Per-AC (Scenario 2)
- Virtual Ethernet Segment - AC-based
- DHCP on PWHE Interfaces
- EVPN E-Tree Using RT Constraints
- EVPN (EVPN & EVPN-VPWS multi-homing) On-Demand Next Hop
- SR-TE PCE Groups
- BGP PIC over SR-TE
- Segment Routing Conditional Prefix Advertisement for OSPF
- SR-PCE Flexible Algorithm Multi-Domain Path Computation
- SR-MPLS over GRE as TI-LFA Backup Path
- Segment Routing Conditional Prefix Advertisement for IS-IS
- Segment Routing Flexible Algorithm Affinity Constraints for IS-IS
- Segment Routing Protected Adjacency SID Backup Timer for IS-IS
- Segment Routing Performance Measurement using RFC5357 (TWAMP Light) Encoding
- Segment Routing Ping and Traceroute for Flexible Algorithm
- SR-TE IPv4 SR policy over BGPv6 session
- Anycast SID-Aware Path Computation
- Segment Routing Data Plane Monitoring
- SR Policy End-to-End Delay Measurement
- Segment Routing Tree Segment Identifier (Tree-SID)
- OSPF Flexible Algorithm
- 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 drafts suportados:

- draft-ietf-spring-segment-routing-mpls-18 Segment Routing with MPLS data plane
- draft-ietf-isis-segment-routing-extensions-21 Segment Routing Extension for ISIS
- draft-ietf-ospf-segment-routing-extensions-27 OSPF Extensions for Segment Routing
- draft-ietf-idr-bgppls-segment-routing-epe-17 Segment Routing BGP Egress Peer Engineering
BGP-LS Extensions
- draft-ietf-idr-bgp-prefix-sid-27 Segment Routing Prefix SID extensions for BGP
- draft-ietf-idr-bgp-ls-segment-routing-ext-11 BGP Link-State extensions for Segment
Routing
- draft-ietf-spring-segment-routing-ldp-interop-15 Segment Routing interworking with LDP
- draft-voyer-6man-extension-header-insertion Deployments With Insertion of IPv6 Segment
Routing Headers
- draft-ietf-bess-evpn-vpws
- draft-ietf-bess-evpn-vpls-seamless-integ EVPN Seamless Integration with VPLS with support of
draft-ietf-bess-evpn-vpls-seamless-integ
- draft-ietf-bess-evpn-inter-subnet-forwarding IP Inter-Subnet Forwarding in EVPN with
support of draft-ietf-bess-evpn-inter-subnet-forwarding
- draft-ietf-bess-evpn-prefix-advertisement EVPN IP Prefix Advertisement with support of draft-ietf-
bess-evpn-prefix-advertisement
- draft-ietf-bess-evpn-prefix-advertisement EVPN-IRBs with support of draft-ietf-bess-evpn-prefix-
advertisement
- draft-ietf-mpls-soft-preemption MPLS Traffic Engineering Soft preemption with draft-ietf-mpls-
soft-preemption
- RFC 0768 User Datagram Protocol
- RFC 0791 Internet Protocol Version 4
- RFC 0792 Internet Control Message Protocol
- RFC 0793 Transmission Control Protocol
- RFC 0813 Window and Acknowledgement Strategy in TCP
- RFC 0826 Address Resolution Protocol
- RFC 0854 Telnet
- RFC 0855 Telnet Option Specification
- RFC 0856 Telnet Binary Transmission
- RFC 0857 File Transfer Protocol
- RFC 0858 Telnet Suppress and Go Ahead Option
- RFC 0859 Telnet Status Option
- RFC 0862 Echo Protocol
- RFC 0863 Discard Protocol
- RFC 0894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC 0896 Congestion Control in IP/TCP Internetworks
- RFC 0906 Bootstrap loading using TFTP
- RFC 0925 Multi-LAN address resolution
- RFC 0926 Protocol for providing the connectionless mode network services
- RFC 0931 Authentication server

- RFC 0950 Internet Standard Subnetting Procedure
- RFC 0958 Network Time Protocol
- RFC 0959 File Transfer Protocol (FTP)
- RFC 0988 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 (Snooping)
- 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 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 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 1247 OSPF Version 2
- RFC 1248 OSPF Version 2 Management Information Base
- RFC 1252 OSPF Version 2 Management Information Base
- 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 NTPv3
- 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
- RFC 1364 BGP OSPF Interaction
- RFC 1370 Applicability Statement for OSPF

- RFC 1398 Definitions of Managed Objects for the Ethernet-Like Interface Types
- 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 CIDR
- RFC 1541 Dynamic Host Configuration Protocol
- 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 1654 A Border Gateway Protocol 4 (BGP-4)
- 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 1706 DNS NSAP Resource Records
- RFC 1771 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 IPv4 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 Attacks
- 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 1997 BGP Communities Attribute
- RFC 1998 An 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 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 2117 Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
- RFC 2132 DHCP Options and BOOTP Vendor Extensions
- RFC 2178 OSPF Version 2
- RFC 2205 Resource ReSerVation Protocol (RSVP)-Version 1 Functional Specification
- RFC 2206 RSVP Management Information Base using SMIv2
- RFC 2236 Support IGMPv2
- 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)
- 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 MD5
- 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 Auto configuration
- RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464 Transmission of IPv6 over Ethernet Networks
- RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
- RFC 2472 IP Version 6 over PPP
- RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2475 An Architecture for Differentiated Service
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- 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 2631 Diffie-Hellman Key Agreement Method
- RFC 2638 A Two-bit Differentiated Services Architecture for the Internet
- 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 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 Support Router-Alert option
- RFC 2737 Entity MIB (Version 2)
- RFC 2740 OSPF for IPv6 (OSPFv3)
- RFC 2746 RSVP Operation Over IP Tunnels
- RFC 2747 RSVP Cryptographic Authentication
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2770 GLOP Addressing in 233/8
- RFC 2784 Generic Routing Encapsulation (GRE)
- RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 2796 BGP Route Reflection: Alternative to Full-mesh IBGP
- RFC 2842 Capabilities Advertisement with BGP-4
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 2865 Remote Authentication Dial 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 2922 Physical Topology MIB
- 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 Multi Protocol Label Switching Architecture (MPLS)
- RFC 3032 MPLS Label Stack Encoding
- RFC 3036 LDP Specification

- RFC 3037 LDP Applicability
- RFC 3042 Enhancing TCP's Loss of Recovery Using Limited Transmit
- RFC 3046 DHCP Relay Agent Information Option
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3086 Definition of Differentiated Services Per Domain Behaviors
- RFC 3101 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 3164 The BSD syslog Protocol
- 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 ISIS Transient Black hole Avoidance
- RFC 3289 Management Information Base for the Differentiated Services Architecture
- RFC 3290 An Informal Management Model for Diffserv Routers
- RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3376 Support for IGMPv3
- RFC 3392 Capabilities Advertisement with BGP4
- 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 SNMP
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the 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 Rendezvous 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 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
- RFC 3509 Alternative Implementations of OSPF Area Border Routers
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3527 Link Selection sub-option for the Relay Agent Information Option for DHCPv4

- RFC 3567 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 Restart for OSPF
- RFC 3630 OSPF Traffic-engineering
- RFC 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
- 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 IS-IS
- RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- 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 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management
- 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 Requirement for Pseudo- Wire Emulation Edge-to-Edge (PWE3)
- RFC 3917 Requirements for IP Flow Information Export (IPFIX)
- RFC 3954 Cisco Systems NetFlow Services Export Version 9
- RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
- RFC 3970 A Traffic Engineering (TE) MIB
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
- RFC 4001 Textual Conventions for Internet Network Addresses
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4023 Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
- 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 Label Switching (GMPLS)

- RFC 4206 Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)
- RFC 4208 Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Support for Overlay Model
- RFC 4213 Transition Mechanisms for IPv6 Hosts and Routers - Dual IP Layer
- RFC 4220 Traffic Engineering Link Management Information Base
- RFC 4243 Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option
- RFC 4257 Framework for Generalized Multi-Protocol Label Switching (GMPLS)-based Control of Synchronous Digital Hierarchy/Synchronous Optical Networking (SDH/SONET) Networks
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4273 Definitions of Managed Objects for BGP-4
- RFC 4291 Internet Protocol Version 6 (IPv6) 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 Virtual 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 MIB for ISIS
- 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
- RFC 4486 Subcodes for BGP Cease Notification Messages
- RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
- RFC 4552 OSPFv3 authentication
- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- 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 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) 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 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 BGP/MPLS IP VPNs.
- RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 4724 Graceful Restart Mechanism for BGP – GR Helper
- RFC 4736 Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Loosely Routed Label Switched Path (LSP)
- RFC 4750 MIB support for OPSFv2
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4761 Virtual 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 LDP Capabilities
- RFC 4797 Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC 4798 Interconnect IPv6 islands over a Multiprotocol
- RFC 4804 Aggregation of Resource ReSerVation Protocol (RSVP) Reservations over MPLS TE/DS-TE Tunnels
- 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 IP version 6 (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 RSVP-TE extensions for signaling for point to multipoint 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 5004 Avoid BGP Best Path Transitions from One External to Another
- RFC 5006 IPv6 Router Advertisement Option for DNS Configuration
- RFC 5015 Support Bidirectional Protocol Independent Multicast (BIDIR-PIM)
- RFC 5036 LDP Specification
- RFC 5059 Support Bootstrap Router (BSR) Mechanism for 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 5107 DHCP Server Identifier Override Suboption
- RFC 5120 ISIS Multi Topology (MT) Routing
- RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative 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 OSPF opaque LSA Option
- RFC 5277 NETCONF Event Notifications
- 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 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 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 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 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 Object for the Path Computation Element Communication Protocol
- RFC 5462 Multiprotocols Label Switching (MPLS) Label Stack Entry: “EXP” Field Renamed to “Traffic Class” Field
- RFC 5492 Capabilities Advertisement with BGP-4
- RFC 5496 Support 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 5512 BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute
- RFC 5521 Extensions to the Path Computation Element Communication Protocol (PCEP) for Route Exclusions
- RFC 5541 Encoding of Objective Functions in the Path Computation Element Communication Protocol (PCEP)
- RFC 5549 Advertising IPv4 NLRI (Network Layer Reachability Information with) an IPv6 Next Hop
- 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 5613 OSPF Link-Local Signaling
- RFC 5635 Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)
- RFC 5643 OSPFv3 MIB
- RFC 5668 4 Octet AS Specific BGP Extended Community
- RFC 5701 IPv6 Address Specific BGP Extended Community Attribute
- RFC 5709 OSPFv2 HMAC-SHA Cryptographic Authentication
- 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 Bidirectional Forwarding Detection (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 Verification (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 6016 Support for the Resource Reservation Protocol (RSVP) in Layer 3 VPNs
- RFC 6020 YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)
- RFC 6037 Support for draft rosen mvpn (profile 0)
- RFC 6073 Segmented Pseudowire
- 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 6151 Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms
- 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 6232 Purge Originator Identification TLV for IS-IS
- RFC 6233 IS-IS Registry Extension for Purges
- RFC 6241 Network Configuration Protocol (NETCONF)
- RFC 6242 Using the NETCONF Protocol over Secure Shell (SSH)
- RFC 6286 Autonomous-System-Wide Unique BGP Identifier for BGP-4
- RFC 6368 Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 6371 Operations, Administration, and Maintenance Framework for Operations, MPLS-Based Transport Networks
- RFC 6372 MPLS Transport Profile (MPLS-TP) Survivability Framework
- RFC 6373 MPLS Transport Profile (MPLS-TP) Control Plane Framework
- RFC 6374 Packet Loss and Delay Measurement for MPLS Networks
- RFC 6382 Unique Origin Autonomous System Numbers

- 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 6482 A Profile for Route Origin Authorizations (ROAs)
- RFC 6510 Resource Reservation Protocol (RSVP) Message Formats for Label Switched Path (LSP) Attributes Objects
- RFC 6513 Support NG-MVPN (Multicast in MPLS / BGP IP VPNs
- RFC 6514 BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPN
- 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 6608 Subcodes for BGP Finite State Machine Error
- RFC 6718 Pseudowire Redundancy
- RFC 6754 Support for Protocol Independent Multicast Equal-Cost Multipath (ECMP) Redirect
- RFC 6793 BGP Support for Four-Octet Autonomous System (AS) Number Space
- RFC 6810 The Resource Public Key Infrastructure (RPKI) to Router Protocol The Resource Public Key Infrastructure (RPKI) to Router Protocol
- RFC 6811 BGP Prefix Origin Validation
- RFC 6822 IS-IS Multi-Instance
- RFC 6860 Hiding Transit-Only Networks in OSPF
- RFC 6936 Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums
- RFC 6987 OSPF Stub Router Advertisement
- RFC 6991 Common YANG Data Types
- RFC 6996 Autonomous System (AS) Reservation for Private Use
- 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 7153 IANA Registries for BGP Extended Communities
- RFC 7166 Authentication Trailer for OSPFv3
- RFC 7311 Accumulated IGP Metric Attribute for BGP
- RFC 7348 Virtual eXtensible Local Area Network (VXLAN)
- 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 7490 Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)
- RFC 7510 Encapsulating MPLS in UDP
- RFC 7551 RSVP-TE Extensions for Associated Bidirectional Label Switched Paths (LSPs)
- RFC 7552 LDP Specification for IPv6
- RFC 7570 Label Switched Path (LSP) Attribute in the Explicit Route Object (ERO)
- RFC 7582 Multicast Virtual Private Network (MVPN): Using Bidirectional P-Tunnels
- RFC 7607 Codification of AS 0 Processing
- RFC 7611 BGP ACCEPT_OWN Community Attribute
- RFC 7674 Clarification of the Flowspec Redirect Extended Community
- RFC 7684 OSPFv2 Prefix/Link Attribute Advertisement
- RFC 7705 Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute
- RFC 7752 North-Bound Distribution of Link-State and Traffic Eng. (TE)

- RFC 7770 Extensions to OSPF for Advertising Optional Router Capabilities
- RFC 7775 IS-IS Route Preference for Extended IP 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 7854 BGP Monitoring Protocol (BMP)
- 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 7987 IS-IS Minimum Remaining Lifetime
- RFC 8077 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 8092 Large Community Attributes
- RFC 8093 Deprecation of BGP Path Attribute Values 30, 31, 129, 241, 242, and 243
- RFC 8097 BGP Prefix Origin Validation State Extended Community
- RFC 8186 Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)
- RFC 8202 IS-IS Multi-Instance
- RFC 8212 Default External BGP (EBGP) Route Propagation Behavior without Policies
- 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 8277 Using BGP to Bind MPLS Labels to Address Prefixes
- 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 8299 YANG Data Model for L3VPN Service Delivery
- RFC 8326 Graceful BGP Session Shutdown
- RFC 8356 Experimental Codepoint Allocation for the Path Computation Element Communication Protocol (PCEP)
- RFC 8395 Extensions to BGP-Signaled Pseudowires to Support Flow-Aware Transport Labels
- RFC 8402 Segment Routing Architecture
- RFC 8408 Conveying path setup type in PCEP messages
- RFC 8476 Signaling Maximum SID Depth (MSD) Using OSPF
- RFC 8491 Signaling MSD (Maximum SID Depth) using IS-IS
- RFC 8500 IS-IS Routing with Reverse Metric
- RFC 8510 OSPF Link-Local Signaling (LLS) Extensions for Local Interface ID Advertisement
- RFC 8570 IS-IS Traffic Engineering (TE) Metric Extensions
- RFC 8571 BGP-LS Advertisement of IGP Traffic Engineering Performance Metric Extensions
- RFC 8633 Network Time Protocol Best Current Practices
- RFC 8642 Policy Behavior for Well-Known BGP Communities
- RFC 8660 Segment Routing with MPLS data plane
- RFC 8661 Segment Routing interworking with LDP
- RFC 8664 PCEP Extensions for Segment Routing
- RFC 8665 OSPF Extensions for Segment Routing
- RFC 8667 IS-IS 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 8671 Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)
- 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 8706 Restart Signaling for IS-IS
- 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 8800 PCEP extension for signaling LSP diversity constraint
- RFC 8814 Signaling Maximum SID Depth (MSD) Using the Border Gateway Protocol - Link State
- RFC 8919 Invalid TLV Handling in IS-IS
- RFC 5310 IS-IS Generic Cryptographic authentication

4. REQUISITOS PARTICULARES E OBRIGATÓRIOS DOS EQUIPAMENTOS

Cada um dos equipamentos a fornecer deve vir equipado com, pelo menos, a seguinte quantidade de interfaces:

- 16 x 100Gbps
- 20 x 10Gbps

Caso os equipamentos a fornecer utilizem um modelo de licenciamento por funcionalidade e/ou capacidade, estes não devem possuir qualquer limitação, tanto ao nível de funcionalidades como de capacidade de até, pelo menos, 4Tbps². É também permitida a transferência de licenças entre equipamentos. Durante a vigência do contrato, caso existam novas funcionalidades ou limitações de escalabilidade que sejam melhoradas através de software, estas deverão poder ser utilizadas sem restrições (serviços disponíveis, número de instâncias de cada serviço, número de rotas, etc.).

Após o termo de vigência do contrato, a utilização do licenciamento não poderá retirar funcionalidades ou capacidade dos equipamentos, no entanto, poderá ser limitada a transição das licenças entre equipamentos.

Adicionalmente, cada equipamento tem de cumprir os seguintes requisitos:

- a) Estar equipado com todas as fontes de alimentação possíveis para o chassis (para AC 230v). Estas devem ter potência suficiente de forma a garantir que é possível colocar uma carta de expansão adicional no chassis e com esta carta adicional é possível uma das fontes de alimentação falhar, mantendo-se o equipamento em pleno funcionamento;
- b) Os cabos de alimentação serão fornecidos pelo adjudicante e devem, para três dos equipamentos, terem terminação adequada para ligar numa régua do tipo IEC-C13 (caso seja de 10Amp) ou IEC-C19 (caso utilize 16 Amp). Os restantes dois equipamentos devem ser fornecidos com cabos com terminação do tipo Schuko;
- c) Estar equipado com todos os sistemas de ventilação possíveis para o equipamento de forma a haver redundância das mesmas e com capacidade de utilização de uma carta de expansão adicional;
- d) Vir equipado com duas cartas Processadoras de Encaminhamento. As cartas Processadoras de Encaminhamento devem possuir RAM suficiente para acomodar 6M de rotas IPv4/IPv6;
- e) Vir equipado com quaisquer outras cartas, módulos ou interfaces necessários para cumprir os requisitos do presente caderno de encargos e que permitam futuras expansões para ligar uma carta adicional com interfaces com capacidade para, pelo menos 20 x 100G.

² O equipamento pode ser fornecido com licenciamento adicional (caso se aplique) em múltiplos de 400Gbps, sendo isso valorizado nos termos referidos no anexo II ao programa do concurso

5. MANUTENÇÃO

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

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

5.6. 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

5.7. 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 (Seramente 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.

5.8. 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.

5.9. 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.

5.10. 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.

5.11. 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.

5.12. SOFTWARE

Futuras versões do software para os equipamentos fornecidos terão de ser disponibilizadas 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.

6. COLOCAÇÃO DOS EQUIPAMENTOS NAS INSTALAÇÕES DO ADJUDICANTE

Os bens a fornecer ao abrigo do contrato devem ser colocados à disposição da FCT, I.P., para efeitos de realização dos testes de aceitação a que se refere o número seguinte no prazo de cento e setenta dias após entrada em vigor 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 dos bens ocorrerá na seguinte morada da FCT|FCCN, em Lisboa:

- FCT|FCCN, Campus do LNEC, Av. Do Brasil, 101, 1700-066 LISBOA

É da responsabilidade do adjudicatário o transporte do equipamento até à morada indicada.

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

7. TESTES DE ACEITAÇÃO

O adjudicante poderá promover a realização de testes de aceitação, destinados à verificação da conformidade dos bens fornecidos 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 nos termos referidos no ponto anterior.

Os bens consideram-se entregues na aceção do artigo 5º na data em que a FCT, I.P. disso expressamente notificar o adjudicatário 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 os bens sejam 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 conceder novo prazo de sete dias ao adjudicatário para correção das anomalias detetadas, aplicando-se com as devidas adaptações o estabelecido neste nº 7 ou, em alternativa, considerar incumprida a obrigação de fornecimento e rescindir o contrato.

8. 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 a fornecer pelo adjudicatário. O tempo máximo para formação que a FCT poderá solicitar ao adjudicatário é de três semanas e tem por destinatários 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.