09:12:34

Expira em:
01:57:32

Fale Conosco

Documentos

Voltar para Disputa

Fornecedores

Clique para listar os arquivos

05.680.391/0001-56 - fsf tecnologia s.a.

Baixar Todos

Declarações

Finalizar Habilitanet

Finalizar Proposta Final

Finalizar Documentação Legal

05.680.391/0001-56 - fsf tecnologia s.a.

Lista dos Arquivos

pc_1719240200.rar
Envio: 24/06/2024 11:43:21 Downloads: 4
Proposta Final

hab_juridica_1719240476.rar
Envio: 24/06/2024 11:47:57 Downloads: 3
Proposta Final

09:12:34

Expira em:
01:57:32

Fale Conosco

Maceió/AL, 24 de junho de 2024.

Ao
TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS

Ref.: PREGÃO ELETRÔNICO Nº 005/2024

Prezado (a) Senhor (a),

FSF TECNOLOGIA S.A., sociedade anônima fechada, com sede na Rua Joaquim Nabuco, 325, Farol, Maceió, AL, CEP 57051-410, inscrita no CNPJ/MF sob o nº 05.680.391/0001-56, vem, com o objetivo de atender ao Pregão Eletrônico nº 005/2024 do TRIBUNAL DE JUSTIÇA DE ALAGOAS, apresentar, conforme segue, a proposta comercial para contratação de empresa especializada na prestação de serviços de rede de telecomunicações privada via IP, com vistas a interligar a sede do Poder Judiciário de Alagoas a suas unidades judiciais e administrativas, conforme especificações técnicas, condições e quantitativos constantes no Termo de Referência e seus anexos.

Colocamo-nos à disposição de V.S.a. para quaisquer esclarecimentos adicionais, através do fone/fax: (082) 2123-3500, e-mail: comercial@alootelecom.com.br.

Atenciosamente,

FELIPE CALHEIROS CANSANCAO:04163392475
Assinado de forma digital por FELIPE CALHEIROS CANSANCAO:04163392475
Dados: 2024.06.24 11:27:36 -03'00'

(Assinado eletronicamente)
FSF TECNOLOGIA S.A.
p. FELIPE CALHEIROS CANSANÇÃO
Diretor Presidente

Ao
TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS

REF: Edital de Pregão Eletrônico nº 005/2024

Prezados Senhores,

Após examinar todas as cláusulas e condições estipuladas no edital em referência, apresentamos nossa proposta nos termos consignados no mencionado ato convocatório e seus anexos, com os quais concordamos plenamente.
Nossa proposta é válida por 60 (sessenta) dias, contados da data prevista para entrega dela, sendo o preço ofertado firme e irreajustável durante sua validade.
Prazo de fornecimento dos serviços: Conforme item 3 do Termo de Referência – Anexo V do Edital.
Informamos que estão inclusos nos preços ofertados todos os custos e despesas, tais como: impostos, taxas, fretes e outra (o)s que incidam sobre o objeto licitado, sendo de nossa inteira responsabilidade, ainda, os que porventura venham a ser omitidos na proposta ou incorretamente cotados.

O valor global de nossa proposta é de R$ 11.756.490,63 (onze milhões, setecentos e cinquenta seis mil, quatrocentos e noventa reais e sessenta e três centavos), nos termos abaixo:

LOTE ÚNICO								
ITEM 1 - Rede privada via IP/MPLS								
ITEM	**Categoria do ponto de acesso**	**Q**	**PA**	**AE**	**VTM**	**I**	**VTI**	**VT1 (36M)**
1.1	I	86	R$ 1.790,00	R$ 100,00	R$ 162.540,00	R$ 1.000,00	R$ 86.000,00	R$ 5.937.440,00
1.2	II	23	R$ 2.490,00	R$ 100,00	R$ 59.570,00	R$ 1.000,00	R$ 23.000,00	R$ 2.167.520,00
1.3	III	1	R$ 40.000,00	R$ 100,00	R$ 40.100,00	R$38.730,63	R$ 38.730,63	R$ 1.482.330,63
VALOR GLOBAL ITEM 1								**R$ 9.587.290,63**
ITEM 2 - Rede Ponto a Ponto (LAN TO LAN)								
	Site	**Descrição do Site**	**VI**		**VMA**		**VMC**	**VT2 (36M)**
2.1	1	Tribunal de Justiça de Alagoas Sede	R$ 1.000,00		R$ 100,00		R$ 30.000,00	R$ 1.084.600,00
2.2	2	Fórum Des. Jairon Maia Fernandes	R$ 1.000,00		R$ 100,00		R$ 30.000,00	R$ 1.084.600,00
VALOR GLOBAL ITEM 2								**R$ 2.169.200,00**
VALOR GLOBAL DA PROPOSTA (ITEM 1 + ITEM 2)								**R$ 11.756.490,63**

ONDE:

SIGLAS ITEM 1:	SIGLAS ITEM 2:
*Q - Quantidade *PA - Valor unitário mensal do ponto de acesso; *AE - Valor unitário mensal de aluguel de equipamentos; *VMT - Valor mensal total = (PA+AE)*Q; *I - Valor unitário da instalação; *VTI - Valor total da instalação = I*Q; *VT1 (36M) - Valor Total em 36 meses = (VMT*36)+VTI	*VI – Valor da Instalação *VMA - Valor mensal do aluguel dos equipamentos *VMC - Valor mensal do circuito *VT2 (36M)- Valor Total em 36 meses = VI + (VMA + VMC)*36

RELAÇÃO DOS EQUIPAMENTOS

a) No Datacenter do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS:

1. Switch do fabricante HUAWEI no modelo S6730 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

b) No Datacenter do FÓRUM DES. JAIRON MAIA FERNANDES:

1. Switch do fabricante HUAWEI no modelo S6730 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

c) No concentrador do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS:

1. Roteador do fabricante JUNIPER no modelo MX204 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

d) Nos demais endereços do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS:

1. Roteador do fabricante HPE no modelo MSR1002 ou JUNIPER no modelo SSR130 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

e) No backbone da ALOO TELECOM:

1. Roteador do fabricante NOKIA no modelo Nokia 7750 SR-12e ou similar;
2. Switch do fabricante EDGECORE no modelo AS5912 ou similar;
3. Switch do fabricante HUAWEI no modelo S6730 ou similar;
4. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;
5. DIO do fabricante ROSEMBERGER no modelo DIO INTERCON I ou similar.

No mais, segue em anexo proposta técnica para atender o serviço especificado no Termo de Referência.

Maceió/AL, 24 de junho de 2024.

FELIPE CALHEIROS CANSANCAO:04163392475
Assinado de forma digital por FELIPE CALHEIROS CANSANCAO:04163392475
Dados: 2024.06.24 11:28:37 -03'00'

(Assinado eletronicamente)
FSF TECNOLOGIA S.A.
p. FELIPE CALHEIROS CANSANÇÃO
Diretor Presidente

PROPOSTA TÉCNICA

1. CONSIDERAÇÕES INICIAIS

1.1. Para elaboração dessa proposta foram consideradas as especificações contidas no Termo de Referência e seus anexos.

1.2. Informações cadastrais:

Razão Social: FSF TECNOLOGIA S.A.;
Nome fantasia: Aloo Telecom;
CNPJ/MF: 05.680.391/0001-56;
Inscrição Estadual: 241047889;
Inscrição Municipal: 900646713;
Endereço: Rua Joaquim Nabuco, 325, Farol, Maceió-AL;
Telefone/fax: (082) 2123-3500;
E-mail: comercial@alootelecom.com.br;
Endereço Eletrônico: www.aloo.com.br.

1.3. Estão inclusos nos preços propostos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, impostos, taxa de administração, materiais, serviços, encargos sociais, trabalhistas, previdenciários, seguros, lucro e outros ônus que porventura possam recair sobre o fornecimento do objeto do Edital.

2. OBJETO

2.1. A presente proposta que tem como objeto a contratação de empresa especializada na prestação de serviços de rede de telecomunicações privada via IP, com vistas a interligar a sede do Poder Judiciário de Alagoas a suas unidades judiciais e administrativas, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

3. PRAZOS

3.1. PRAZO DE VALIDADE DA PROPOSTA

3.1.1. A presente proposta tem validade de 60 (sessenta) dias, podendo ser prorrogada, através de solicitação do **TRIBUNAL DE JUSTIÇA DE ALAGOAS**.

3.2. PRAZO DE VIGÊNCIA DO CONTRATO

3.2.1. O prazo de vigência do contrato será de 36 (trinta e seis) meses consecutivos, contado a partir de sua assinatura, prorrogável na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

3.3. PRAZO DE IMPLANTAÇÃO DOS LINKS DE DADOS

3.3.1. O prazo para instalação/implantação do link de dados é de 120 (cento e vinte) dias corridos, contados do recebimento da ordem de serviço.

3.3.2. O prazo máximo de instalação dos objetos e início da prestação dos serviços contratados, contados a partir da aprovação do plano de trabalho, será gradativo, conforme priorização da ALOO TELECOM, da seguinte forma:

a) Até 30 dias: para 25% do total de circuitos contratados.
b) Até 60 dias: para 50% do total de circuitos contratados.
c) Até 90 dias: para 75% do total de circuitos contratados.
d) Até 120 dias: para 100% de circuitos contratados.

4. CARACTERÍSTICAS GERAIS DOS CIRCUITOS E SERVIÇOS

4.1. Serviço de rede privada corporativa de longa distância via IP/MPLS

4.1.1. A Aloo Telecom interligará, através da sua rede, as unidades do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS, relacionadas no ANEXO II - TABELA DE LOCALIZAÇÃO DOS ACESSOS – REDE CORPORATIVA (MPLS), ao ponto sede do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS;

4.1.2. A interligação das unidades do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS ao ponto sede será implementada através de rede VPN, com tecnologia MPLS ou superior e seguirá as velocidades mínimas garantidas dispostas na planilha de localidades, permitindo-se apenas alternativas de velocidades superiores e devendo ser entregues em cada unidade do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS, no mínimo uma porta LAN Giga Ethernet, com interface para conexão de Fibra Óptica ou UTP Cat.6a e implementando protocolo de enlace (Camada Nível 02 do Modelo de Referência OSI);

4.1.3. A taxa de transmissão ativada sempre estará disponível na totalidade do fluxo contratado e não deve incluir a taxa de overhead de protocolos até a camada 2 do modelo OSI.

4.1.4. A velocidade de todos os links será simétrica e disponível de forma simultânea, ou seja, mesma velocidade de entrada e de saída (circuitos full-duplex).

4.1.5. A sede do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS, localizada em Maceió, será considerado o ponto central da rede (concentrador), para onde os dados oriundos dos demais endereços da solução deverão convergir;

4.1.6. Permitirá o tráfego de toda a suíte de protocolos que compõe o padrão TCP/IP V4 e V6;

4.1.7. Será implementado por meio de acessos dedicados e permanentes;

4.1.8. Será utilizado na última milha dos acessos dedicados o meio físico terrestre confeccionado com fibra óptica. Apenas será permitida a conversão do meio óptico para UTP para compatibilização com as interfaces dos CPEs.

4.1.9. Não serão implantados acessos dedicados via radiofrequência devido à alta probabilidade de baixa performance no circuito, assim como devido à alta probabilidade de perda de pacotes que este meio disponibiliza.

4.1.10. Será implementado os padrões RFC 1163 - A Border Gateway Protocol, RFC 2283 – Multiprotocol Extensions for BGP-4, RFC 2547 - BGP/MPLS VPNs e RFC - 427 BGP4.

4.1.11. Incluirá mecanismo de priorização de tráfego, através de tecnologia QoS (qualidade de serviço), seguindo os padrões das RFC 2474 e 2475 - DiffServ, complementados pela RFC 2597 – Assured Forwarding PHB, pela RFC 2598 - Expedited Forwarding e pela RFC 3270 – Muti-Protocol Label Switching Support of Differentiated Services, podendo o Tribunal solicitar à ALOO TELECOM em qualquer momento prioridade para os pacotes de dados/voz que julgar necessário.

4.1.12. Todos os roteadores instalados nos sites suportarão o padrão IEEE 802.1p.

4.1.13. Incluirá instalação e fornecimento de qualquer equipamento e/ou recurso necessário, se a solução adotada impuser o uso, tais como: roteadores, modems e demais ativos de rede. Outrossim, a ALOO TELECOM se responsabilizará por eventuais adequações nas instalações físicas do CONTRATANTE, assim como na infraestrutura externa para a implantação do serviço contratado (passagem de cabos, lançamento de fibras ópticas, adaptação de tomadas, etc).

4.1.14. Todos os appliances CPE (Customer Premises Equipment) serão dimensionados para operar com carga máxima de CPU e memória de 70% (setenta por cento) quando o valor médio de utilização da banda (medido a cada cinco minutos) for menor ou igual à capacidade do canal contratado. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para a CONTRATANTE

4.1.15. Todos os appliances CPE serão dimensionados de forma que tenham capacidade de encaminhamento de pacotes IP, em pacotes por segundo, compatíveis com as velocidades dos links WAN conectados.

4.1.16. Os links irão transportar pacotes IPv4 e IPv6 com 1500 (mil e quinhentos) bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.

4.2. Sistema de gerenciamento e monitoramento de rede e de serviços

4.2.1. Gerenciamento pró-ativo da ALOO TELECOM

4.2.1.1. O sistema de gerenciamento pró-ativo possuirá:

a) Geração automática de alarmes em caso falhas do(s) elemento(s) de rede gerenciado(s);

b) Geração automática de alarmes em caso de quedas de desempenho do(s) elemento(s) de rede gerenciados (perda de pacotes, latência, aumento/queda de tráfego);

c) Informações sobre a localização física de ativos de rede (roteadores, portas, acessos);

d) Informações detalhadas sobre a configuração atual de cada um dos roteadores;

e) Disponibilidade medida (real) de todos os elementos gerenciados da rede;

f) Visão gráfica da topologia da rede com os respectivos alarmes;
g) Abertura de trouble tickets via 0800, portal web ou serviço de mensageria (“WhatsApp” ou similares).

h) Gráficos e relatórios de tendência;

i) Monitoração por classe de serviço;

j) Análise da situação atual da rede e sugestão de melhorias (capacity planning);

k) Canal de atendimento exclusivo, 24 x 7h, diferenciado e prioritário para clientes que possuam o serviço de gerência;

l) Disponibilizar comunidade RO via SNMP em todos os ativos e fornecer todas as OIDs pertinentes aos mesmos. Nome da comunidade SNMP deve ser TJAL;

m) Quando da geração automática de alarmes em casos de indisponibilidade ou queda de desempenho, e-mail será enviado automaticamente a endereço eletrônico disponibilizado pela CONTRATANTE.

n) Em caso de uso excessivo de link, a ALOO TELECOM informará qual ip ou quais IPs, portas e camada de transporte são responsáveis pelo evento;

o) Ativar suporte a Netflow ou semelhante em seus ativos para captura.

4.2.2. Monitoramento da rede

4.2.2.1. Fornecido pela ALOO TELECOM à CONTRATANTE.

4.2.2.2. Solução de monitoramento que permite:

a) Visualizar a composição do tráfego (por site/toda rede).

b) Verificar o volume de tráfego por protocolo, aplicação, IP (origem e destino), marcações ToS e classes de QoS.

c) Identificar os ofensores em cada tipo de tráfego.

4.2.2.3. A ALOO TELECOM irá disponibilizar e configurar um sistema de monitoramento de rede que será gerenciado pela Contratante, sem ação direta da ALOO TELECOM. Este sistema não irá abrir chamados pró-ativamente.

4.2.2.4. A ALOO TELECOM irá prover o treinamento in loco para o responsável pela rede da Contratante, de acordo com a configuração da ferramenta, de forma que a Contratante possa gerenciar e emitir os relatórios que achar convenientes.

4.2.2.5. O sistema possibilitará a identificação do tráfego IP passante na rede, caracterizando-o de forma qualitativa e assim classificando o seu uso, possibilitando que o TRIBUNAL DE

JUSTIÇA DE ALAGOAS conheça quais máquinas acessam mais a Internet, quais departamentos mais acessam as aplicações corporativas, qual aplicação utiliza mais um determinado link, quais as aplicações que mais oneram cada classe de serviço, matriz de tráfego entre localidades, distribuição de tráfego bem como os usuários e aplicações que mais consomem banda.

4.2.2.6. O sistema de monitoramento atenderá aos seguintes requisitos mínimos para o gerenciamento de tráfego:

a) Processos de coleta: múltiplos, intrusivo e/ou distribuídos.

b) Tecnologias de coleta: fluxos (Cisco Netflow, Huawei Netstream ou Juniper J-Flow), geração de fluxos a partir de espelhamento de portas (port mirror) e SNMP versões 1, 2 e 3.

c) O tráfego nas interfaces de rede será coletado também via SNMP através dos contadores ifInOctets e ifOutOctets (ou ifHCInOctets e IfHCOutOctets em interfaces GigabitEthernet ou mais rápidas) da IF-MIB.

d) Sumarização por objetos: criação de objeto(s) de análise de tráfego (bloco IP com máscara, endereço IP, blocos de IPs com máscaras, variações de IPs, portas UDP, portas TCP, conjunto de variações de portas UDP, conjunto de variações de portas TCP, protocolo, interface física de entrada de um equipamento, interface física de saída de um equipamento, número ASN de entrada e número ASN de saída, marcação ToS e grupo de marcação ToS).

e) Domínios: visualização de vários domínios (rede corporativa de múltiplos fornecedores, serviços e ambientes).

f) Controle de fluxos repetidos.

g) Configuração de perfis de visualização independentes por usuário.

h) Definição de aplicações: baseadas no IP/conjunto de IPs, porta (UDP ou TCP) ou um conjunto de portas e IPs.

i) Suporte a alarmes baseados em medições correntes de tráfego ou de alterações de comportamento: os alarmes devem ser configurados utilizandose de qualquer curva exibida nos gráficos do sistema. Ocorrências de alarmes devem ser enviadas através de TRAPs SNMP.

j) Detecção de tráfego suspeito: IP flood e alta taxa de transferência entre dois hosts.

k) Disponibilização das seguintes informações (on line e/ou on demand):

   i. Matriz de tráfego entre localidades, quebra de tráfego de localidades e de interfaces de rede por aplicações, protocolos e classes de QoS, quebra de tráfego de classes de QoS por aplicações e protocolos.
   ii. Distribuição do tráfego das localidades entre as suas subredes.

iii. Acesso aos fluxos exportados pelos roteadores por meios de relatórios, em que haja a sumarização pelos campos Netflow escolhidos pelo usuário. Ao sumarizar, o relatório deve mostrar os momentos da abertura do primeiro fluxo e de fechamento do último. Deve ser oferecida uma opção para exibição detalhada dos fluxos, com todos os campos disponíveis.
iv. Relatório dos objetos do sistema (subredes, protocolos, aplicações, classes de serviço, etc.) que possuem maior tráfego, distinguindo tráfego origem e destino

l) Quanto ao formato da solução:

i. Será escalável, suportando aumento da base coletada através da adição de Appliances coletores, mantendo um único portal de acesso aos dados.
ii. Exibir todos os gráficos e relatórios em ambiente web (via HTTPS), sendo necessário somente um navegador e o plugin Java.
iii. Permitir acesso a console de configuração via cabo serial ou remotamente, através de uma conexão SSH.
iv. Não é necessário estar instalado no ambiente da CONTRATANTE, contanto que isso não impeça de receber informações em tempo real.

4.3. Serviço ponto a ponto

4.3.1. Link de Transmissão de Dados ponto a ponto com garantia de banda full duplex e transparência a protocolos, com interface Ethernet.

4.3.2. Irá interligar, através da rede da LICITANTE, as unidades do TRIBUNAL DE JUSTIÇA DE ALAGOAS, relacionadas no ANEXO III - TABELA DE LOCALIZAÇÃO DOS ACESSOS – REDE PONTO A PONTO, do Edital.

a) Há a previsão de mudança do Datacenter Secundário, localizado no Fórum Des. Jairon Maia Fernandes (Fórum da Capital), para a Nova Sede Administrativa do Poder Judiciário, a ser situado no antigo prédio da Secretaria de Educação do Estado de Alagoas, na Rua Barão de Alagoas, Centro.

b) Após a mudança, será habilitado um novo ponto de acesso na Nova Sede Administrativa, que passará a trafegar dados do Serviço de Rede Ponto a Ponto, enquanto o circuito do Fórum da Capital integrará a malha da rede IP/MPLS;

c) Todos os custos envolvidos nesta transição, que ocorrerá durante a vigência do contrato, estarão incluídos no valor da instalação.

4.3.3. A tecnologia utilizada para tráfego de dados deverá ser implementada utilizando-se fibra óptica, ao longo de todo o circuito, fornecendo uma banda mínima de 40 Gbps com infraestrutura redundante tipo anel óptico.

4.3.4. O circuito utilizará o conceito de dupla abordagem.

4.3.5. O anel óptico redundante será implementado de maneira tal que garanta total continuidade do serviço na indisponibilidade de uma das fibras ópticas (Ex.: Queda de poste, vandalismo, etc.).

4.3.6. O ponto de acesso ao link será disponibilizado nos data centers, localizados no interior do prédio, das respectivas unidades.

4.3.7. O serviço entregará, em cada sala do data Center, tanto na sede quanto na unidade remota, apenas um ponto com fibra ótica preferencialmente e caso seja usado outra mídia, a Infra desta corte deverá avisada.

4.3.8. Em caso de falha na fibra principal, o anel óptico redundante assumirá de imediato, sem perdas.

4.3.9. O link será dimensionado para garantir um tempo de latência máximo, no pior caso, de 20 milissegundos de uma extremidade a outra do link de dados.

4.3.10. O serviço será compatível com os Switchs Huawei Switch Core 48 portas 1/10G L3 Model CE6881-48S6CQ com a GBIC Huawei Single-mode Model QSFP 40G-ER4 Optical Transceiver.

4.4. NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

4.4.1. Os Níveis Mínimos de Serviço (ANS) visam garantir que os serviços contratados sejam prestados pela ALOO TELECOM em grau mínimo de eficiência e qualidade exigido pela CONTRATANTE.

4.4.2. A ALOO TELECOM será responsável pelo cumprimento e medição dos índices estabelecidos neste item que serão auditados pela CONTRATANTE durante todo o prazo de vigência do contrato, e que poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados.

4.4.3. As inoperâncias e/ou indisponibilidades dos serviços, no todo ou em parte, que não sejam de responsabilidade da CONTRATANTE, bem como insuficiência no alcance dos níveis mínimos de satisfação dos requisitos técnicos, representados por indicadores, devem gerar descontos na fatura proporcionais ao tempo de desconformidade.

4.4.4. Relatório Gerencial de Serviço (RGS)

a) Até o 5° dia útil de cada mês, será emitido o Relatório Gerencial de Serviço (RGS) relativo ao mês anterior, que consolidarão os Níveis Mínimos de Serviço apurados.

b) O RGS será enviado em formato PDF pesquisável, planilha XLS ou HTML para o endereço de email a ser disponibilizado pelo CONTRATANTE ou ainda disponibilizado para acesso/download através do Portal de Acompanhamento da ALOO TELECOM.

c) Estarão incluídas no relatório, no mínimo, as seguintes informações:

   i. Enlaces contratados, incluindo designações, data de ativação, velocidades contratadas, etc.

ii. Lista de chamados abertos, classificação de severidade (em conformidade com o item 3.5), data/hora de abertura, data/hora de fechamento, tempo de solução definitiva, se o prazo de solução foi ultrapassado, cálculo de desconto por descumprimento dos NMS, descritivo da solução.

iii. Índice de disponibilidade do enlace, além dos demais indicadores de aferição da qualidade do link, incluindo totalizações de eventuais glosas por não cumprimento dos NMS.

d) Caso o CONTRATANTE julgue pertinente, poderá, a qualquer momento, solicitar que novas informações sejam incluídas no relatório gerencial.

4.5. Disponibilidade Mensal do Serviço

4.5.1. A disponibilidade operacional mensal mínima é definida como a relação entre o tempo em que o sistema apresenta as características técnicas e operacionais especificadas e o tempo total considerado.

4.5.2. Será assegurada disponibilidade operacional mensal mínima de 99,4%

4.5.3. O serviço estará disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, todos os dias do ano. Desta maneira a ALOO TELECOM estabelecerá estrutura de operação para este nível de serviço.

4.5.4. No cálculo da disponibilidade serão consideradas todas as interrupções do serviço, exceto as programadas pelo CONTRATANTE ou pela ALOO TELECOM.

4.5.5. A disponibilidade do serviço indicará o percentual de tempo, durante o período de 01 (um) mês de operação, em que o serviço permanece em condições normais de funcionamento.

4.5.6. O serviço será considerado indisponível a partir do início de uma interrupção registrada no centro de atendimento/supervisão da ALOO TELECOM ou a partir da comunicação de interrupção, feita pela CONTRATANTE, até o restabelecimento do serviço às condições normais de operação e a respectiva informação à CONTRATANTE.

4.5.7. 7 Serão excluídas desta contagem as interrupções programadas para manutenção, desde que seja feita comunicação à CONTRATANTE com pelo menos 05 (cinco) dias úteis de antecedência e que a interrupção seja programada para ser executada das 19h00 às 05h00.

4.5.8. Serão excluídas dessa contagem as interrupções causadas por falta de energia elétrica nas localidades que ocasione o desligamento dos equipamentos instalados na CONTRATANTE, hipótese que será investigada pela equipe da CONTRATANTE.

4.5.9. Caso haja interrupções não programadas nos serviços, a ALOO TELECOM fica sujeita a descontos na fatura mensal, aplicados no mês imediatamente subsequente ao mês no qual ocorreram os fatos que originaram os descontos.

4.5.10. A indisponibilidade dos equipamentos da ALOO TELECOM, utilizados na sustentação do serviço, implicará automaticamente na indisponibilidade do serviço para efeitos de penalização dos indicadores de NMS.

4.6. Métodos e Indicadores de Aferição da Qualidade do Link de Dados

4.6.1. A aferição das metas estipuladas no acordo de Níveis Mínimos de Serviço (NMS) obedecerão aos indicadores abaixo, sem que isso isente a ALOO TELECOM de cumprir todas as demais exigências do Termo de Referência, as quais também são passíveis de sanção.

4.6.2. A ALOO TELECOM irá disponibilizar, mensalmente, relatório consolidado com

4.6.3. O CONTRATANTE promoverá auditagem das aferições realizadas pela CONTRATADA através de conferência dos relatórios disponibilizados e por meio de ferramentas próprias de monitoramento de rede.

4.6.4. Indicador de Disponibilidade Mensal

INDICADOR DE DISPONIBLIDADE MENSAL	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir o pleno funcionamento de um circuito, em condições normais de operação
Início de Vigência	Data do Termo de Recebimento Definitivo (TRD)
Cálculo	IDM = [(To-ΣTi)/To]*100 Onde: IDM = índice de disponibilidade mensal do enlace em % To = período de operação (um mês) em minutos. ΣTi = somatório dos tempos de inoperância durante o período de operação (um mês) em minutos.
Limiar de Satisfação	Mínimo de 99,4%
Forma de Acompanhamento	A CONTRATADA deverá incluir no Relatório Gerencial de Serviço (RGS) o IDM apurado e totalizado no mês para cada circuito contratado. Neste relatório deverá ser apresentado (em minutos): o tempo de indisponibilidade, o tempo de interrupções programadas, o tempo de interrupções de responsabilidade do CONTRATANTE.
Glosas/sanções	Se o IDM for inferior ao limiar de satisfação (99,4%) e superior ou igual a 95%: aplica-se desconto de 0,3% sobre o valor mensal do enlace afetado a cada 0,1% abaixo do limiar de satisfação. Se o IDM for inferior a 95%: será aplicado desconto de 0,5% sobre o valor mensal do enlace afetado a cada 0,1% abaixo do limiar de satisfação, além da sanção de advertência. Caso a empresa acumule 2 advertências consecutivas, aplicadas em função desta métrica para o mesmo enlace, será aplica, cumulativamente, multa compensatória de 1% sobre o valor mensal do contrato.
Observações	No caso de inoperância reincidente num período inferior a 2 (duas) horas, contado a partir do restabelecimento do enlace da última

	inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o enlace estiver totalmente operacional. A ausência de dados coletados pela contratada poderá ser considerada indisponibilidade.

4.6.5. Indicador de Taxa de Perda de Pacotes

INDICADOR DE TAXA DE PERDA DE PACOTES (TPP)	
ITEM	**DESCRIÇÃO**
Finalidade	Representa a quantidade de pacotes perdidos fim a fim. É medida em percentual tomado como referência o volume total de pacotes que alcançaram o destino, medido em qualquer ponto dentro dos limites do backbone da ALOO TELECOM, dentre o volume total de pacotes transmitidos, medido na interface WAN do CPE (Customer Premises Equipment).
Periodicidade	Medições diárias e constantes, sobretudo em horários de maior tráfego. A ALOO TELECOM deverá realizar as medições através de sua plataforma de monitoração, em todos os períodos do dia, apresentando as em valores referentes a cada intervalo de 5 (cinco) minutos. Caso qualquer uma das medições exceda os limites estabelecidos continuamente por mais de 15 (quinze) minutos, o canal será considerado indisponível desde o início da anomalia até o restabelecimento total de sua operação normal, incluindo eventuais intermitências. O canal será considerado intermitente se a recorrência estiver dentro do intervalo de 10 (dez) minutos.
Cálculo	TPP = (NPorigem – NPdestino)/NPorigem x 100, onde: TPP = Taxa de Perda de Pacotes (em %) NPorigem = Número de pacotes na origem NPdestino = Número de pacotes no destino
Limiar de Satisfação	Menor ou igual a 2%
Forma de Acompanhamento	A CONTRATADA deverá incluir no Relatório Gerencial de Serviço o tempo apurado e totalizado no mês para cada enlance, referente aos períodos que exacerbarem o limiar de satisfação (TPP > 2%) acima do tempo tolerado (15 minutos).
Glosas/sanções	Acima do limiar de satisfação, mesmo intermitente, o serviço será considerado indisponível para efeito de descontos. Logo, o somatório de tempo em que TPP > 2% será agregado ao IDM (item 3.4.3.1, do Termo de Referência) para totalizar a glosa que será aplicada no mês referente ao enlace.
Observações	Para o cálculo deste parâmetro, serão considerados erros de interface, pacotes corrompidos pelo enlace, bem como descartes injustificados por parte do roteador. Para o cálculo deste indicador, não serão considerados pacotes descartados em função do esgotamento da capacidade do link entre a rede CONTRATANTE e o 1º roteador da ALOO TELECOM,

	situações definidas quando a utilização for superior a 90% (noventa por cento) da utilização da taxa contratada

4.6.6. Indicador de Nível de Latência

INDICADOR DE NÍVEL DE LATÊNCIA (INL)	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir que o retardo do circuito contratado esteja dentro de uma margem aceitável.
Periodicidade	Medições diárias e constantes, sobretudo em horários de maior tráfego. A ALOO TELECOM realizará as medições através de sua plataforma de monitoração, em todos os períodos do dia, apresentando-as em valores referentes a cada intervalo de 5 (cinco) minutos. Caso qualquer uma das medições exceda os limites estabelecidos continuamente por mais de 15 (quinze) minutos, o canal será considerado indisponível desde o início da anomalia até o restabelecimento total de sua operação normal, incluindo eventuais intermitências. O canal será considerado intermitente se a recorrência estiver dentro do intervalo de 10 (dez) minutos
Limiar de Satisfação	Máximo de 20 ms para pontos de acesso na capital Máximo de 30 ms para pontos de acesso no interior
Forma de Acompanhamento	A apuração da latência na rede do Tribunal será efetuada com o envio de pacotes ICMP de tamanho fixo de 32 (trinta e dois) octetos de dados, entre terminais de origem e destino localizados em sítios da rede dentro do mesmo backbone e retornando à origem onde será realizada a medição do tempo de resposta destes pacotes. A latência corresponde ao tempo de ida e volta do pacote. Para os links MPLS das Unidades Judiciais, as medições de latência devem ser feitas entre o CPE (concentrador) da Sede e o CPE da referida Unidade Judicial. Para o link MPLS da Sede, as medições de latência e perda de pacotes devem ser feitas entre o CPE (concentrador) da Sede e o centro de gerência da ALOO TELECOM. O tempo de resposta limite a ser aguardado para cada pacote será de 5 segundos. Valores superiores a este tempo serão considerados “timeout”. Cada medida deverá ser realizada através do envio de uma série de 4 pacotes ICMP por vez. Os intervalos de observação deverão ser de 5 (cinco) minutos durante o intervalo de tempo demandado pelo Tribunal. Todos os resultados obtidos através das medições deverão ser disponibilizados e considerados no indicador diário de latência. Para garantir a validade das medidas, a contratada poderá configurar os roteadores da rede (nível 3 da camada OSI) para tratarem os pacotes ICMP com prioridade, porém nunca superior ao restante do tráfego. A ALOO TELECOM deverá incluirá no Relatório Gerencial de Serviço o tempo apurado e totalizado no mês, referente aos períodos que exacerbarem o limiar de satisfação (INL > 20ms ou 30ms) acima do tempo tolerado (15 minutos).

Glosas/sanções	Acima do limiar de satisfação, mesmo intermitente, o serviço será considerado indisponível para efeito de descontos. Logo, o somatório de tempo de INL > 20ms ou 30ms será agregado ao IDM (item 3.4.3.1, do Termo de Referência) para totalizar a glosa que será aplicada no mês referente ao enlace.

4.7. Atendimento Técnico e Operacional

4.7.1 Além dos indicadores anteriores, devem ser apurados níveis de serviço dos chamados realizados pelo CONTRATANTE, ou pela ALOO TELECOM de forma proativa, referentes a incidentes e atendimentos técnicos ou operacionais.

4.7.2. Serão consideradas as seguintes métricas para os incidentes:

a) Nível de severidade: prioridade a ser atribuído a um chamado realizado pelo CONTRATANTE.

b) Prazo de atendimento: Tempo decorrido entre a abertura do chamado automático, por iniciativa da ALOO TELECOM, ou realizado pelo CONTRATANTE e a disponibilização/envio do número do protocolo de atendimento ao CONTRATANTE.

c) Prazo de solução definitiva: Tempo decorrido entre a data e hora de registro da OS e o efetivo restabelecimento do serviço ao seu pleno estado de funcionamento ou atendimento integral da demanda, isto é, até o momento da comunicação da solução definitiva do problema pela ALOO TELECOM e aceite pela equipe técnica do CONTRATANTE.

4.7.3. O limite temporal para atendimento técnico e operacional deverá obedecer à classificação de severidade, o prazo de atendimento e de solução definitiva, conforme tabela abaixo:

4.7.4. Os eventuais descontos referentes ao atendimento técnico e operacional são cumulativos com os eventuais descontos referentes à qualidade do link de dados.

4.7.5. Em caso de extrapolação do prazo de solução definitiva que corresponda ao valor total mensal do contrato, será aplicada multa por descumprimento parcial de contrato, sem prejuízo das glosas acimas estipuladas.

4.7.6. Após concluído o suporte técnico, a ALOO TELECOM comunicará o fato à equipe técnica do CONTRATANTE e solicitará autorização para o fechamento do chamado. Durante o período de conclusão do suporte até a efetiva comunicação ao CONTRATANTE, o chamado permanecerá em espera, de forma a não haver penalização indevida à ALOO TELECOM. Caso o CONTRATANTE não confirme a solução definitiva do problema, o chamado será reaberto, e os prazos de atendimento voltarão a ser considerados, até que seja efetivamente solucionado pela ALOO TELECOM.

4.7.7. O CONTRATANTE encaminhará à ALOO TELECOM, quando da reunião de alinhamento de expectativas, relação nominal da equipe técnica autorizada a abrir e fechar chamados de suporte técnico.

4.7.8. Faculta se à ALOO TELECOM substituir temporariamente o equipamento, peça ou componente defeituoso por outros que restabeleçam o serviço aos níveis de serviço acordados, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva.

5. A ALOO TELECOM APRESENTA, DOCUMENTAÇÃO TÉCNICA DA SOLUÇÃO, DESCREVENDO:

5.1. Relação dos Equipamentos Ativos

5.1.1. Serão fornecidos e instalados os seguintes equipamentos para ativar os serviços de telecomunicações bidirecionais, baseado no conceito de redes convergentes, que se referem à concentração de serviços diversos com possibilidade de aplicação de dados, voz e multimídia de forma dinâmica através de tecnologia IP/MPLS.

a) No Datacenter do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS:

1. Switch do fabricante HUAWEI no modelo S6730 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

b) No Datacenter do FÓRUM DES. JAIRON MAIA FERNANDES:

1. Switch do fabricante HUAWEI no modelo S6730 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

c) No concentrador do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS:

1. Roteador do fabricante JUNIPER no modelo MX204 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

d) Nos demais endereços do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS:

1. Roteador do fabricante HPE no modelo MSR1002 ou JUNIPER no modelo SSR130 ou similar;
2. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;

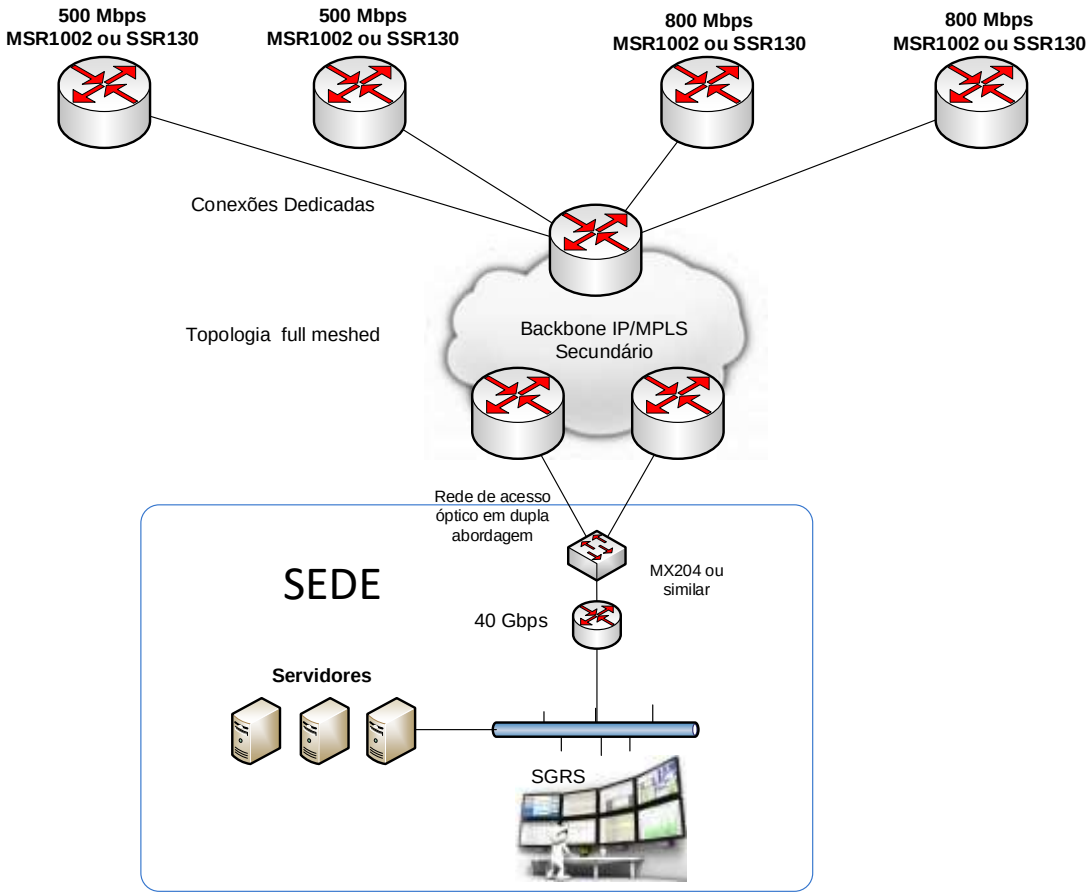
e) No backbone da ALOO TELECOM:

1. Roteador do fabricante NOKIA no modelo Nokia 7750 SR-12e ou similar;
2. Switch do fabricante EDGECORE no modelo AS5912 ou similar;
3. Switch do fabricante HUAWEI no modelo S6730 ou similar;
4. Fibra Óptica do fabricante ZTT no modelo CFOA-SM-AS80-G-12F ou similar;
5. DIO do fabricante ROSEMBERGER no modelo DIO INTERCON I ou similar.

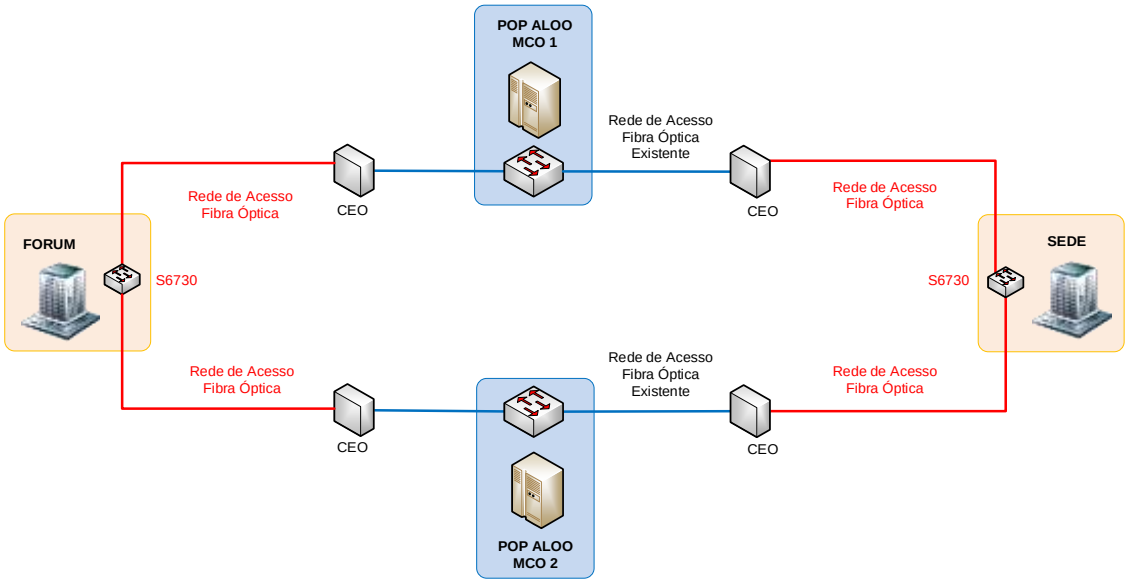
Os datasheets dos fabricantes encontram-se anexos aos documentos de habilitação.

5.2. Projeto de Encaminhamento e Implantação Inicial do Serviço no Concentrador

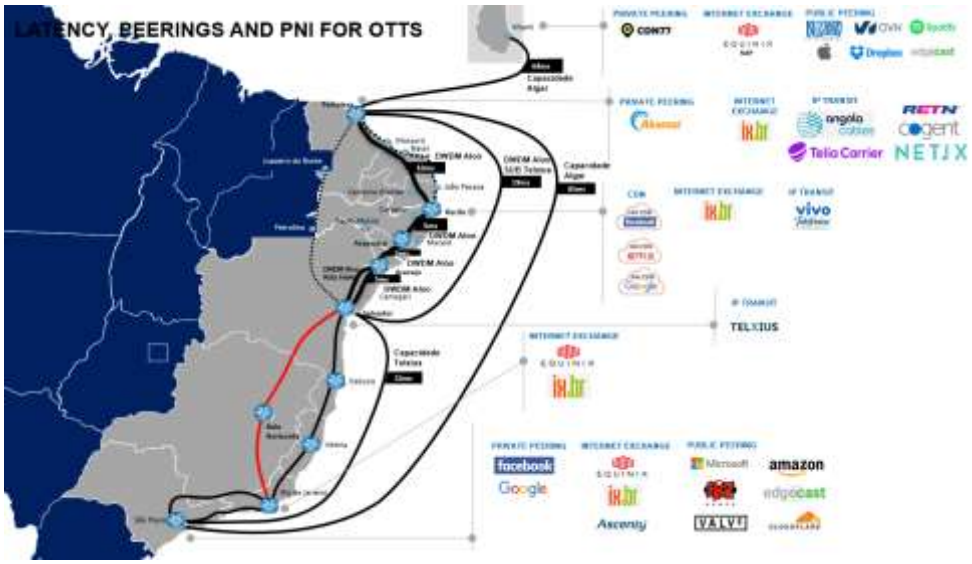
5.3. Os acessos de Fibra Óptica entre o backbone da Aloo e a Sede do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS seguirão conforme detalhado abaixo no diagrama:



5.4. Os acessos de Fibra Óptica entre a Sede do TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS e o FÓRUM DES. JAIRON MAIA FERNANDES seguirão conforme detalhado abaixo no diagrama:



5.5. Backbone da ALOO TELECOM.



5.6. Cronograma de Implantação

Projeto	Duração
TJAL	**120 dias**
Projetos	**30 dias**
Emissão de Termo de Abertura do Projeto	1 dia
Abertura de Ordens de Serviços	2 dias
Esboço do projeto de Rede Óptica	2 dias
Solicitação de materiais/equipamentos	2 dias

Suprimentos	**30 dias**
Fornecimento do cabo óptico	5 dias
Fornecimento de miscelânea	5 dias
Fornecimento de DGO	5 dias
Fornecimento de CEO	5 dias
Entrega de miscelânea no local da obra	3 dias
Entrega de DGO no local da obra	3 dias
Entrega de CEO no local da obra	3 dias
Documentação	**30 dias**
Elaboração do Projeto de Rede Óptica	5 dias
Protocolo na concessionária de energia local	5 dias
Licenciamento na Concessionária de energia local	5 dias
Licenciamento Ambiental	5 dias
Entrega de As-Built	5 dias
Entrega das Curvas OTDR	2 dias
Entrega dos testes de Potência Óptica	2 dias
Entrega do Plano de Bobina	3 dias
Entrega dos testes de Bobina	3 dias
Implantação do cabo óptico	**30 dias**
Equipamento de postes	3 dias
Lançamento de cabo óptico	3 dias
Emendas e Fusões	**4 dias**
Instalação/fusão das CEO	2 dias
Teste em Rede Optica	**15 dias**
Entrega dos Testes de OTDR	5 dias
Instalação de equipamentos	**1 dia**
Instalação de Equipamento	1 dia
Entrega do circuito	**30 dias**
Implantação de Link	30 dias
Testes de Potência Óptica	**4 dias**
Análise dos testes OTDR/Potência	4 dias
Emissão de relatório de entrega/aceitação	2 dias

6. PROPOSTA TÉCNICA DA SOLUÇÃO

6.1. Os serviços objetos do Edital serão atendidos através da utilização dos seguintes produtos da Aloo:

6.1.1. Produto VPN IP MPLS

6.1.1.1. Características

a) MPLS, ou MultiProtocol Label Switching, é uma tecnologia de encaminhamento de pacotes baseada em rótulos (labels) que funciona, basicamente, com a adição de um rótulo nos pacotes de tráfego (O MPLS é indiferente ao tipo de dados transportado, pelo que pode ser tráfego IP

ou outro qualquer) à entrada do backbone (roteadores de borda) e, a partir daí, todo o encaminhamento pelo backbone passa a ser feito com base neste rótulo. Comparativamente ao encaminhamento IP, o MPLS torna-se mais eficiente uma vez que dispensa a consulta das tabelas de routing.

b) Este protocolo permite a criação de Redes Virtuais Privadas garantindo um isolamento completo do tráfego com a criação de tabelas de "labels" (usadas para roteamento) exclusivas de cada VPN.

c) Além disso é possível realizar QoS (Quality of Service) com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN. QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo.

d) O produto baseado em MPLS que a Aloo utiliza permite agregar valor ao seus produtos, pois passam a não oferecer apenas banda, mas um tráfego diferenciado com: Multimídia (Voz, Vídeo e Dados) e aplicações críticas, com garantias aplicáveis de QoS, através das seguintes classes de serviço:

i. Multimídia: priorização de tráfego dos pacotes multimídia (ex.: vídeo conferência, etc.).
ii. Voz: priorização de tráfego dos pacotes de voz (ex.: interligação de PABX, telefonia IP, etc.).
iii. Dados Expressos: priorização de tráfego de dados de aplicações críticas (ex.: SAP, GVCollege, etc.).
iv. Dados: tráfego de dados sem priorização (Best Effort).

e) O MPLS foi concebido para satisfazer as necessidades de infraestrutura de comunicação segura e economicamente viável entre:

i. escritórios de uma mesma empresa em diferentes localidades;
ii. força de trabalho em constante deslocamento;
iii. empresa, clientes, fornecedores.

f) O produto baseado em MPLS, oferecido pela Aloo, permite que ele possa ser utilizado nas seguintes situações:
i. acesso corporativo a servidores de aplicações centralizadas como sistemas corporativos, e-mail e Intranet;
ii. formação de redes para compartilhamento de arquivos;
iii. integração de sistemas de telefonia;
iv. formação de sistemas de videoconferência;
v. acesso remoto aos sistemas corporativos.

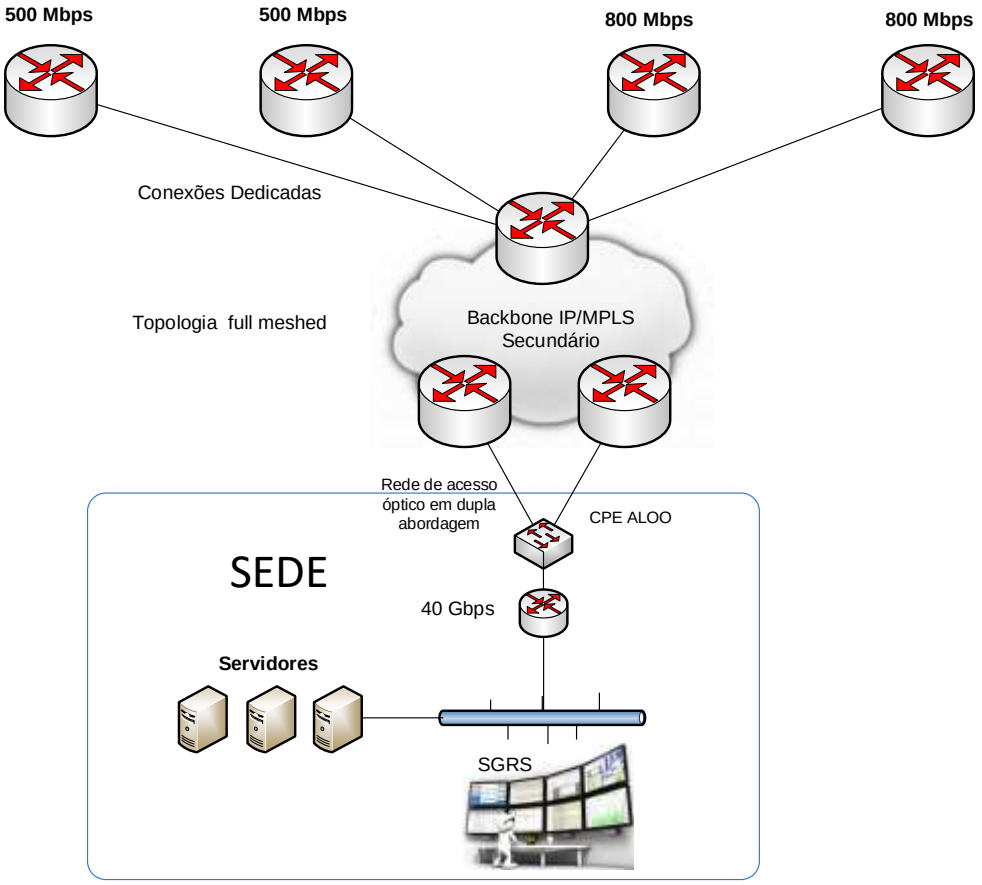
6.1.1.2. Vantagens

a) Melhor desempenho no encaminhamento de pacotes;
b) Criação de caminhos (Label Switching Paths) entre os roteadores;
c) Possibilidade de associar requisitos de QoS, baseados nos rótulos carregados pelos pacotes.

6.1.1.3. Funções de MPLS

a) Mecanismos para o tratamento de fluxos de dados entre hardware, ou mesmo aplicações, distintas.
b) Independência em relação aos protocolos das camadas OSI 2 (enlace) e 3 (rede).
c) Mapeamento entre os endereços IP e labels, para envio de pacotes.
d) Interfaces com protocolos de roteamento, como OSPF.

6.1.1.4. Diagrama da Solução VPN IP MPLS



6.1.2. Produto GERENCIAMENTO PROATIVO

6.1.2.1. Características do Gerenciamento Proativo

a) Gerenciamento de todos os circuitos e serviços, independentemente de uma eventual subcontratação;

b) Abrange todos os roteadores, circuitos, backbone e serviços, independentemente de suas tecnologias;

c) A Aloo é responsável por fornecer, dimensionar e configurar os equipamentos, sistemas e ferramentas necessárias para o provimento da solução de Gerência;

d) Qualquer inclusão ou alteração de características técnicas dos circuitos na gerência, será realizada no prazo do ANO, a partir da implementação da característica técnica ou da ativação dos novos circuitos;

e) A Gerência de Rede e Serviços atuará de forma proativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço, realizando abertura, acompanhamento e fechamento dos chamados técnicos;

f) A Gerência irá operar 24 horas por dia, 7 dias por semana, todos os dias do ano;

g) Caso haja necessidade de realizar manutenção preventiva da solução, a ALOO TELECOM formalizará via e-mail, à CONTRATANTE, com no mínimo 5 (cinco) dias úteis de antecedência;

h) A indisponibilidade dos dados de gerência será contabilizada como indisponibilidade do serviço, no período em que os dados não forem coletados ou ficaram inacessíveis, caso isto implique em perda de dados;

i) Os dados ficarão armazenados ao longo de todo o contrato. A disponibilização dos dados será realizada on-line, para dados dos últimos 180 (cento e oitenta) dias e, acesso sob demanda para dados anteriores a esse período;

j) O cliente deve fornecer todas as informações necessárias, como endereço completo, telefones e contatos em todas as unidades que farão parte do backbone, e serão gerenciadas pela Aloo;

k) Será habilitado o protocolo SNMP nos equipamentos, onde será criada a comunidade SNMP designada pela ALOO TELECOM com o acesso liberado para a Gerência do Cliente, independente do gerenciamento realizado pela Aloo.

6.1.2.2. Chamado Técnico

a) A abertura do chamado será realizada pela equipe de gerência da Aloo, imediatamente após a constatação de defeito ou falha em qualquer circuito ou serviço que esteja em funcionamento;

b) Os circuitos e serviços receberão uma identificação única tanto para o Cliente como para a Aloo, que será de conhecimento de todos os atendentes da equipe de Gerência, e será utilizada na abertura do chamado técnico pela Gerência Proativa;

c) As informações de chamados, que serão visualizadas através do Portal, irão conter:

i. Número do Chamado
ii. Data e Hora da Abertura
iii. Status (aberto/fechado)
iv. Localidade

d) As tentativas de contato com os técnicos do Cliente para aberturas de chamados, recorrências ou encerramento de chamados, que não tenham tido sucesso por ausência dos técnicos, serão

registradas no campo “Histórico” do chamado, não resultando em penalidades de SLA para a Aloo;

e) Os chamados técnicos só serão encerrados por um técnico do Cliente, em conjunto com a Central de Atendimento, que entrará em contato com o Cliente, para encerrar os chamados solucionados. Não será admitido o fechamento do chamado técnico por técnicos das unidades do Cliente;

f) Os técnicos autorizados para o encerramento dos chamados serão informados pelo Cliente, na implantação do serviço.

6.1.2.3. Portal de Gerência

a) A visualização das informações são via WEB;

b) Possibilitará definição de perfis de usuários e senhas para controle de acesso às informações de gerência, com conexão segura;

c) Terá uma interface única para o acesso independente dos equipamentos ou tecnologias empregadas para a prestação dos serviços;

d) O intervalo de coleta dos dados para exibição das informações serão de 5 minutos;

e) A visualização das informações apresentará todas as funcionalidades listadas nos itens abaixo:

i. Alertas em caso de falhas e anormalidade dos circuitos, com grau de criticidade;

ii. Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos. O agrupamento dos elementos que compõem a topologia da rede (roteadores e circuitos) será definido pelo Cliente;

iii. Visualização da utilização de banda dos circuitos, em tempo real, diário, semanal e mensal, com a opção de consulta de dados históricos;

iv. Visualização do consumo de CPU e memória dos roteadores com opção de consulta de dados históricos;

v. Visualização do tempo de resposta dos circuitos, em tempo real, com opção de consulta de dados históricos;

vi. Indicação de congestionamento nos circuitos, além dos valores de limiares excedidos e o enfileiramento e/ou descarte do tráfego nos roteadores;

vii. Visualização dos chamados registrados, abertos e encerrados, dentro do prazo contratual, por data ou circuito, permitindo acesso ao detalhamento dos chamados.

6.1.2.4. Relatórios

a) O acompanhamento da qualidade dos serviços da rede, acompanhamento dos chamados e do SLA estabelecido são feitos através de relatórios disponibilizados pela Aloo, no Portal de Gerência, para consulta diária, mensal ou sob demanda;

b) O portal conterá todas as informações necessárias;

c) A Aloo armazena todos os dados e informações coletadas durante a vigência do contrato, tais como: dados brutos coletados nos elementos gerenciados, dados sumarizados para confecção de relatórios, acompanhamento dos chamados, acompanhamento da qualidade de serviço, de faturamento, dentre outros. Esses dados serão disponibilizados ao Cliente ao final do contrato;

d) Todos os relatórios permitem o uso de diversos filtros para visualizar as informações. Os filtros também permitem a seleção de informações a serem impressas de um ou mais circuitos ou de toda rede, à critério do Cliente;

e) Todos os relatórios possibilitam a seleção de datas de início e fim do período a que se referem os dados a serem exibidos;

f) A solução de gerência permite que todos os relatórios possam ser visualizados, armazenados em meio eletrônicos e impressos. É implementada a funcionalidade de exportação dos relatórios em formatos compatíveis com MS Office, BR Office e PDF;

g) Os relatórios abaixo são visualizados on-line ou gerados sob demanda:

i. Relatórios de Tráfego: relatórios diários que apresentam o tráfego de todos os circuitos, com suas séries históricas, fornecendo subsídios para analisar o desempenho e as tendências de aproveitamento dos recursos da rede. Devem demonstrar informações da banda utilizada e do volume de tráfego;

ii. Relatório de Acompanhamento dos Chamados: relatório diário com todas as informações relativas ao chamado como data, hora, identificação do elemento (circuito ou equipamento), descrição detalhada do chamado;

iii. Relatórios de Chamados: relatório mensal de chamados abertos e encerrados;

iv. Relatórios de Reincidência: relatórios que mostram problemas reincidentes dos elementos (circuitos ou equipamentos) da rede;

v. Relatório de Acompanhamento de SLA: descritivo de SLA, contendo para cada circuito as ocorrências de falhas, caso tenham existido e os valores mensais apurados para cada indicador (Parâmetros de Qualidade dos Circuitos e Serviços);

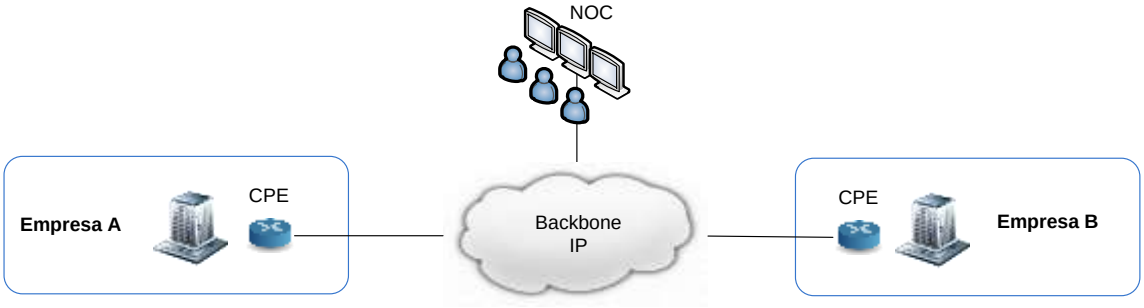
vi. Relatório Específico de SLA: relatório de acompanhamento de cada indicador a ser monitorado para o SLA. Estes relatórios serão emitidos mensalmente.

6.1.3. ALOO PONTO A PONTO

6.1.3.1. Características

a) O PONTO A PONTO é um serviço adequado para corporações que necessitam interligar localidades ou redes com segurança, alta disponibilidade (baixo atraso) e transparência de protocolos. Essas facilidades permitem tráfego de dados de forma constante, interligação de sistemas corporativos, compartilhamento de infraestrutura, flexibilidade de crescimento e centralização de custos voltados para um único fornecedor.

b) Sua empresa pode formar redes ponto-a-ponto, de acordo com a necessidade, por meio de circuitos exclusivamente dedicados. A solução PONTO A PONTO tem gestão baseada na rede IP da Aloo TELECOM, a mais completa plataforma de integração de serviços com SLA (Acordo de Nível de Serviço) estabelecido conforme contrato.



6.1.3.2. Aplicações

a) Transmissão contínua de grandes volumes de dados, notadamente para aplicações em tempo real;

b) Formação de redes corporativas próprias, suportando intranets e/ou redes privativas de voz;

c) Transporte integrado de sinais multimídia (voz, dados e imagem) e videoconferências;

d) Interligação de redes locais e soluções de comunicação remota, tais como, acesso a hosts através de terminais remotos e aplicações Clientes / Servidor.

7. REPRESENTANTE LEGAL:

a) Nome: Felipe Calheiros Cansanção;
b) Nacionalidade: Brasileira;
c) Estado Civil: Casado;
e) Profissão: Empresário;
f) Cargo: Diretor Presidente;
g) CPF: 041.633.924-75;
h) RG: 2000001100607 - SSP/AL;

8. RESPONSÁVEL TÉCNICO

8.1. Segue abaixo os dados do profissional com formação superior em uma das graduações exigidas no Art. 9 da Resolução nº 218/73 do CONFEA, que será o responsável técnico pela execução dos serviços conforme descritos nesta proposta comercial:

a) Nome: Sérgio Ferreira de Brito;
b) Profissão: Engenheiro Eletricista;
c) CREA/AL: 0205030912;
d) RG: 1419604 - SSP/AL;
e) CPF: 020.871.724-20.

9. DADOS BANCÁRIOS

9.1. Banco do Brasil (001); Agência: 1523-7; C/Corrente: 150.000-7.

10. NETWORK OPERATION CENTER - NOC

noc@alootelecom.com.br

Número principal 24/7 (24 horas por dia, 7 dias na semana, todos os dias do ano)

11. CALL CENTER 0800 725 3505 / 82.2123-3500

Se o escalonamento é necessário para questões técnicas relacionadas a um bilhete de problema em que não se consiga resolver no número principal, favor ligar imediatamente para ordem listada abaixo:

Normal	Primeiro Nível	Segundo Nível	Terceiro Nível
Tel.: 08007253505 82.2123-3500 (WhatsApp)	**Plantão Sobreaviso** Cel.: 82.99117-8606 E-mail: noc@alootelecom.com.br	**Marcos Paulo** **Supervisor CGR** Cel.: 82.99321-3092 E-mail: marcos.silva@alootelecom.com.br	**Marlos Silva** **Gerente CGR** Cel.: 82.99127-9314 E-mail: marlos@alootelecom.com.br

12. CENTRAL DE RELACIONAMENTO ALOO TELECOM

Seg a sex 08h00 – 18h00:
www.alootelecom.com.br
Atendimento Online: 09h00 – 20h00

Mônica Rollim
Coordenadora BCC/ SAC
82.2123-3536
82.99118-0495
monica.rollim@alootelecom.com.br

Ana Cláudia Lamin
Executiva de negócios
82.99122-2107
ana.lamin@alootelecom.com.br

13. FATURAMENTO E ADMINISTRATIVO ALOO TELECOM

Seg a sex 8h00 – 18h00:
Samara Lima
Coordenadora Financeira
82.2123-3514
samara.lima@alootelecom.com.br

ZTT
Your Partner in Cable

SEU PARCEIRO EM CABOS

www.zttcable.com.br

CABO ÓPTICO DIELÉTRICO AUTO-SUSTENTADO - CFOA-SM-AS-Y-S-Z NR/RC

FIBRA

Monomodo	ZTT Fiber ITU.T - G.652D - Baixo Pico d'água
Atenuação máxima da fibra no cabo dB/Km	1310nm : 0.34 & 1550nm : 0.20
PMDq	≤ 0.2 ps/ √km

UNIDADE BÁSICA

Preenchimento	Gel para impedir o ingresso de água na unidade básica
Tubo	Material termoplástico

NÚCLEO

Elemento Central Dielétrico	Elemento FRP (Fibre Reinforced Plastic) revestido com PE
Preenchimento do núcleo	Material Hidro Expansível bloqueador de água
Enchimento	Polietileno
Enfaixamento do núcleo	Fita bloqueadora de água

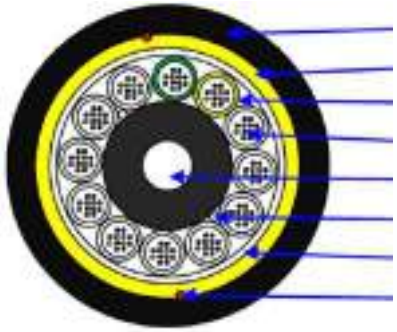
CABO

Fio de rasgamento	Fios de Poliester trançados
Elemento de Tração periférico	Fios de aramida
Revestimento externo	Polietileno preto resistente a UV

DESCRIÇÃO

Cabo óptico para aplicação aérea auto-sustentado e vão de até 200 metros.
Com 2 até 144 fibras do tipo SM G.652D
Possui o núcleo seco e simples capa (KP)

DETALHES DE CONSTRUÇÃO



1. REVESTIMENTO DE POLIETILENO PRETO
2. FIOS DE ARAMIDA
3. UNIDADE BÁSICA
4. FIBRAS E GEL
5. ELEMENTO CENTRAL FRP
6. FIOS HIDROEXPANSÍVEIS
7. FITA BLOQUEADORA DE ÁGUA
8. FIO DE RASGAMENTO

Imagem ilustrativa - fora de escala

ZTT
Your Partner in Cable

SEU PARCEIRO EM CABOS

www.zttcable.com.br

CABO ÓPTICO DIELÉTRICO AUTO-SUSTENTADO - CFOA-SM-AS-Y-S-Z NR/RC

PARÂMETROS DE PERFORMANCE

MECÂNICO

Resistência à compressão	1 x Peso/Km (>1000N , <2200N)
Resistência ao impacto	25 impactos, com carga variando c/ diâmentro cabo
Teste de torção	± 180º, 10 Ciclos
Raio mín. Curvatura na instalação	20 x diâmetro externo cabo
Raio mín. Curvatura após instalação	10 x diâmetro externo cabo
Resistência a vibração	100 milhões ciclos

AMBIENTAL

Temperatura:	
Instalação	-0ºC a +60ºC
Operação	-20ºC a +65ºC
Armazenagem	-20ºC a +65ºC
Ciclo Térmico	Conforme NBR 13510
Penetração umidade	Conforme NBR 9136
Teste escoamento	Conforme NBR 9149
Intemperismo	ASTM G155 ciclo 1

VÃO (M)	80	120	200
CARGA MÁXIMA (x peso cabo/Km)	1.5	2.0	3.0

ATENDE A TODOS OS PARÂMETROS DA NORMA ABNT NBR 14160

Certificado ANATEL: 4411-13-2878 para cabo com fibra SM G.652D

DETALHES DE IMPRESSÃO

Impressão no cabo	Fibras Ópticas ZTT Ano/Semana Produção CFOA-SM-AS-Y-S-Z-NR/RC ANATEL NR. Metragem
Cores das Fibras	Verde, amarela, branca, azul, vermelha, violeta, marrom, rosa, preta, cinza, laranja, aqua
Cores Unidades Básicas	Verde, amarela e o restante branca
Cor Revestimento Externo	Preta

Comprimentos padrões

Bobinas	4000 metros para cabos até 36 fibras 3000 metros para cabos 48 até 144 fibras
Tolerância nominal	± 3% (outras tolerâncias podem ser acordadas com o cliente)

ZTT
Your Partner in Cable

SEU PARCEIRO EM CABOS

www.zttcable.com.br

CABO ÓPTICO DIELÉTRICO AUTO-SUSTENTADO - CFOA-SM-AS-Y-S-Z NR/RC

DIMENSÕES REVESTIMENTO EXTERNO NORMAL (NR)

Número Fibras	Fibras por Unidade Básica	Diâmetro externo (mm)			Peso do cabo (Kg/Km) (+/- 10%)		
		VÃO (metros)			VÃO (metros)		
		80	120	200	80	120	200
2~12	2	10.3 +0.5	10.5 ± 0.5	11.1 ± 0.5	82	85	98
18~36	6	10.3 +0.5	10.5 ± 0.5	11.1 + 0.5	82	85	98
48~60	12	10.9 +0.5	11.0 ± 0.5	11.1 + 0.5	94	96	98
72	12	10.9 +0.5	11.0 ± 0.5	11.1 + 0.5	94	96	98
96	12	15.7 +0.8	15.8 ± 0.8	16.3 ± 0.8	185	195	210
144	12	15.7 +0.8	15.8 ± 0.8	16.3 + 0.8	185	195	210

DIMENSÕES REVESTIMENTO EXTERNO RETARDANTE A CHAMA (RC)

Número Fibras	Fibras por Unidade Básica	Diâmetro externo (mm)			Peso do cabo (Kg/Km) (+/- 10%)		
		VÃO (metros)			VÃO (metros)		
		80	120	200	80	120	200
2~12	2	11.5 +0.5	11.6 ± 0.5	12.1 ± 0.6	100	102	115
18~36	6	11.5 +0.5	11.6 ± 0.5	12.1 + 0.6	100	102	115
48~60	12	11.9 +0.6	12.0 ± 0.6	12.1 + 0.6	110	112	115
72	12	11.9 +0.6	12.0 ± 0.6	12.1 + 0.6	110	112	115
96	12	16.8 +0.8	17.0 ± 0.8	17.4 ± 0.8	210	220	240
144	12	16.8 +0.8	17.0 ± 0.8	17.4 + 0.8	210	220	240

AS5912-54X Switch

Data Center and Service Provider Edge Switch
Bare Metal Hardware

Design Contributed to OCP

Product Overview

The Edgecore AS5912-54X switch meets the high-performance, availability, and network-scaling requirements of cloud data centers and carrier access providers. The AS5912-54X provides switching at Layer 2 or Layer 3 across 48 x 10 GbE ports and 6 x 100 G uplinks. The switch can be deployed either as a Top-of-Rack switch, as part of a 100 GbE or 40 GbE distributed spine, forming a non-blocking folded-Clos data center fabric, or as a carrier access switch. The switch is rack mountable in either a standard 19 inch rack, or with an Open Rack Switch Adapter in a 21-inch Open Rack.

The AS5912-54X hardware provides high-availability features, including; redundant, hot-swappable AC or -48 VDC PSUs, or 12 VDC power input; fans with 5+1 redundant fan modules; and port-to-power or power-to-port airflow options.

Key Features and Benefits

- Cost-effective, bare-metal switch infrastructure for data center and carrier access.
- 48 x SFP+ switch ports, supporting 10 GbE (DAC, AOC, 10GBASE-SR/LR) or 1 GbE (1000BASE-T/SX/LX).
- 6 x 100G QSFP28 ports at front.
- Expandable packet buffering for carrier access.
- Layer 2 and/or Layer 3 forwarding of 800 Gbps.
- Rack mountable in standard 19" racks. Mountable in 21" Open Rack with the Open Rack Switch Adapter.
- Hot-swappable, load sharing, redundant AC or -48 VDC PSUs. 12 VDC power input option.
- Hot swappable 5+1 redundant fan modules.
- Management: Ethernet and console RJ-45 ports; USB storage port.
- Hardware switch pre-loaded with Open Network Install Environment (ONIE) for automated loading of compatible open source and commercial NOS offerings.
  Compatible with Open Network Linux (ONL), the open-source, OCP reference NOS.
  Compatible with OcNOS from IP Infusion.
  Compatible with future version of SnapRoute FlexSwitch.

Data Center Switch

onie snaproute ipinfusion™

AS5912-54X Product Specifications

www.edge-core.com

Features

Ports
Switch Ports:
- 48 x SFP+ each supporting 10 GbE or 1 GbE
- 6 x 100G QSFP28 each supporting 1 x 40/100 GbE

Management Ports on Front Panel:
- 1 x RJ-45 serial console
- 1 x RJ-45 100/1000BASE-T management port
- 1 x USB Type A storage port

Key Components
Switch Silicon:
- AS5912-54X: Broadcom Qumran-MX BCM88370

CPU Modules:
- Intel Rangeley C2538 quad-core 2.4GHz x86 processor
- DDR3 SO-DIMM 8 GB x 2
- mSATA: 32 GB

Performance
Switching Capability: 800 Gbps
Forwarding Rate: 1 Bpps
Jumbo Frame: 9 Kbytes
Packet Buffer: expandable to 6 GB
MAC Addresses: 750 K
VLAN IDs: 4 K
L3 Routes: 750 K expandable to 8 million

Supported Optics and Cables
SFP+ Ports:
- 10GBASE-CR DAC: up to 3 m passive; up to 10 m active
- 10GBASE-SRL/SR: up to 100/300 m over OM3 MMF
- 10GBASE-LR: Up to 10 km over SMF
- 1000BASE-SX, 1000BASE-LX, 100/1000BASE-T

QSFP+ Ports:
- 40GBASE-CR4 DAC; up to 3 m passive; up to 10 m active
- 40GBASE-CR4 DAC to 4 x SFP+ 10GBASE-CR DAC; up to 3 m passive; up to 10 m active
- 40GBASE-SR4: Up to 100 m over OM3 MMF, 150 m over OM4 MMF
- 40GBASE-LR4: Up to 10 km over SMF
- 100GBASE-SR4: 100 Gbps short reach transceiver
- 100GBASE-LR4: 100 Gbps long reach transceiver
- QSFP28 AOC Cable: 100 Gbps to 100 Gbps AOC cable with upto 30 M 100G QSFP28 to 100 G QSFP28

Physical and Environmental
Dimensions (WxDxH): 44 x 54.8 x 4.4 (17.32 x 21.57 x 1.73 inch)
Weight: 9.34 kg (20.59 lb), with two installed PSU modules
Fans: hot-swappable 5+1 redundant fans
Operating Temperature: 0°C to 40°C (32°F to 104°F)
Storage Temperature: -40°C to 70°C (-40°F to 158°F)
Operating Humidity: 5% to 95% non-condensing

Software
Switch is loaded with Open Network Install Environment (ONIE) software installer
Compatible with the following NOS options:
- Open Network Linux (ONL), the open-source, OCP reference NOS
- OcNOS from IP Infusion
- Future version of SnapRoute FlexSwitch

Carrier Access Features
Carrier Access switch with expandable packet buffering
Carrier feature support MPLS

Power
PSUs: 2 redundant, load-sharing, hot-swappable AC or -48 VDC
AC input range: 90 V~300 VAC (90~ 277 VAC is minimum)
DC input range: -36~-72 VDC
Power Input Option: 12 VDC
Redundant, current sharing, PG
Environmental Criteria: -5 ~ 55°C

Regulatory
EMI
- CE Mark
- EN55022 Class A
- EN55024
- EN61000-3-2
- EN61000-3-3
- FCC Part 15 Subpart B Class A
- VCCI Class A

Safety
- CB
- UL/CUL

Environmental:
- Temperature: IEC 68-2-14
- Vibration: IEC 68-2-36, IEC 68-2-6
- Shock: IEC 68-2-29
- Drop: ISTA 2A
- Acoustic Level: 62 dB@ 27°C

RoHS-6 Compliant
WEEE Standards: The switches complied with the following WEEE standards: Waste Electrical and Electronic Equipment (WEEE Directive 2002/96/EC)

Warranty
Please check www.edge-core.com for the warranty terms in your country.

TEL: +886-3-5638888 FAX: +886-3-6686111
No.1, Creation Rd. III, Hsinchu Science Park, Taiwan 30077
sales@edge-core.com www.edge-core.com

TEL: +1 (949)-336-6801
20 Mason Irvine, CA 92618

AS5912-54X Product Specifications

www.edge-core.com

Ordering Information

Base Model: AS5912-54X; 48-Port 10G QSFP+ with 6 x 100G QSFP28 uplinks; ONIE software installer

Model Number	CPU Module	PSU	Airflow	Region (power cord)
5912-54X-O-AC-F-US	Intel Rangeley C2538 processor	dual AC PSUs	port-to-power airflow	N. America
5912-54X-O-AC-B-US	Intel Rangeley C2538 processor	dual AC PSUs	power-to-port airflow	N. America
5912-54X-O-AC-F-EU	Intel Rangeley C2538 processor	dual AC PSUs	port-to-power airflow	Europe
5912-54X-O-AC-B-EU	Intel Rangeley C2538 processor	dual AC PSUs	power-to-port airflow	Europe
5912-54X-O-AC-F-UK	Intel Rangeley C2538 processor	dual AC PSUs	port-to-power airflow	UK
5912-54X-O-AC-B-UK	Intel Rangeley C2538 processor	dual AC PSUs	power-to-port airflow	UK
5912-54X-O-AC-F-JP	Intel Rangeley C2538 processor	dual AC PSUs	port-to-power airflow	Japan
5912-54X-O-AC-B-JP	Intel Rangeley C2538 processor	dual AC PSUs	power-to-port airflow	Japan

For More Information

To find out more about Edgecore Networks Corporation products and solutions, visit www.edge-core.com.

About Edgecore Networks Corporation

Edgecore Networks Corporation is in the business of providing innovative network solutions. In the service provider network, in the data center or in the cloud, Edgecore Networks Corporation delivers the software and systems that transform the way the world connects. Edgecore Networks Corporation serves customers and partners worldwide. Additional information can be found at www.edge-core.com.

Edgecore Networks Corporation is a subsidiary of Accton Technology Corporation, the leading network ODM company. The Edgecore Data Center switches are developed and manufactured by Accton.

To purchase Edgecore Networks solutions, please contact your Edgecore Networks Corporation representatives at +886 3 563 8888 (HQ) or +1 (949)-336-6801 or authorized resellers.

TEL: +886-3-5638888 FAX: +886-3-6686111
No.1, Creation Rd. III, Hsinchu Science Park, Taiwan 30077
sales@edge-core.com www.edge-core.com

TEL: +1 (949)-336-6801
20 Mason Irvine, CA 92618

Hewlett Packard Enterprise

HPE MSR1000 Router Series

Key features

- Up to 500 Kpps IP forwarding; converged high-performance routing, switching, security, voice, and mobility
- Embedded security features with hardware-based encryption, firewall, network address translation (NAT), and VPNs
- Industry-leading breadth of LAN and WAN connectivity options
- No additional licensing complexity; no cost for advanced features
- Zero-touch solution, with single-pane-of-glass management

Product overview

The HPE MSR1000 Router Series is a next generation multiservices router designed to deliver unmatched application performance for small branch offices. The MSR1000 series provides a flexible multiservice end point for small branches and remote offices that quickly adapts to changing business requirements while delivering integrated, concurrent services on a single, easy-to-manage platform.

Features and benefits

Performance

- Excellent forwarding performance
  Provides forwarding performance up to 500 Kpps; meets current and future bandwidth-intensive application demands of enterprise businesses
- Powerful encryption capacity
  Includes embedded hardware encryption accelerator to improve encryption performance

Product architecture

- SDN/OpenFlow
  OpenFlow is the communications interface defined between the control and forwarding layers of a SDN (Software-Defined Networking) architecture. OpenFlow separates the data forwarding and routing decision functions. It keeps the flow-based forwarding function and employs a separate controller to make routing decisions. OpenFlow matches packets against one or more flow tables. MSR support OpenFlow 1.3.1

- Ideal multiservice platform
  Provides WAN router, Ethernet switch, wireless LAN, 3G or 4G WAN, firewall, VPN, and SIP or voice gateway all in one box
- High-density voice interfaces
  Provide flexible analog voice interface options for easy integration within a wide range of deployments
- USB interface
  Uses USB memory disk to download and upload configuration files; supports an external USB 3G modem for a 3G WAN uplink
- Advanced hardware architecture
  Delivers Gigabit Ethernet switching and a PCIe bus

Connectivity

- VXLAN (Virtual eXtensible LAN)
  VXLAN (Virtual eXtensible LAN, scalable virtual local area network) is an IP-based network, using the "MAC in UDP" package of Layer VPN technology. VXLAN can be based on an existing ISP or enterprise IP networks for decentralized physical site provides Layer 2 communication, and can provide service isolation for different tenants
- Virtual Private LAN Service (VPLS)
  Virtual Private LAN Service (VPLS) delivers a point-to-multipoint L2VPN service over an MPLS or IP backbone. The backbone is transparent to the customer sites, which can communicate with each other as if they were on the same LAN. The following protocols support on MSRs, RFC4447, RFC4761 and RFC4762, BFD detection in VPLS, Support hierarchical HOPE(H-VPLS), MAC address recovery in H-VPLS to speed up convergence
- NEMO (Network Mobility)
  Network mobility (NEMO) enables a node to retain the same IP address and maintain application connectivity when the node travels across networks. It allows location-independent routing of IP datagrams on the Internet
- Packet storm protection
  Protects against broadcast, multicast, or unicast storms with user-defined thresholds
- Loopback
  Supports internal loopback testing for maintenance purposes and an increase in availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
- 3G/4G access support
  Provides 3G/4G LTE wireless access for primary or backup connectivity via a 3G/4G LTE SIC modules certified on various cellular networks; optional carrier 3G/4G USB modems available
- Flexible port selection
  Provides a combination of fiber and copper interface modules, 100/1000BASE-X auto-speed selection, and 10/100/1000BASE-T auto-speed detection plus auto duplex and MDI/MDI-X
- Multiple WAN interfaces
  Provide a traditional link with E1, T1, ADSL, ADSL2, ADSL2+, G.SHDSL, Serial, and ISDN backup; provide high-density Ethernet access with Fast Ethernet/Gigabit Ethernet, mobility access with IEEE 802.11b/g/n Wi-Fi, and 3G/4G LTE options
- High-density port connectivity
  Integrates four or eight Giga LAN switching ports (All switching ports can be configured as routed ports.), two or three SIC slots, and up to 30 module options

Layer 2 switching

- Spanning Tree Protocol (STP)
  Supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping
  Control and manage the flooding of multicast packets in a Layer 2 network
- Port mirroring
  Duplicates port traffic (ingress and egress) to a local or remote monitoring port
- VLANs
  Support IEEE 802.1Q-based VLANs
- sFlow
  Allows traffic sampling
- Define port as switched or routed
  Supports command switch to easily change switched ports to routed (maximum eight GE ports)

Layer 3 routing

- Static IPv4 routing
  Provides simple manually configured IPv4 routing
- Routing Information Protocol (RIP)
  Uses a distance vector algorithm with User Datagram Protocol (UDP) packets for route determination; supports RIPv1 and RIPv2 routing; includes loop protection
- Open Shortest Path First (OSPF)
  Delivers faster convergence; uses this link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery
- Border Gateway Protocol 4 (BGP-4)
  Delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks
- Intermediate system to intermediate system (IS-IS)
  Uses a path vector Interior Gateway Protocol (IGP), which is defined by the ISO organization for IS-IS routing and extended by IETF RFC 1195 to operate in both TCP/IP and the OSI reference model (Integrated IS-IS)
- Static IPv6 routing
  Provides simple manually configured IPv6 routing
- Dual IP stack
  Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
- Routing Information Protocol next generation (RIPng)
  Extends RIPv2 to support IPv6 addressing
- OSPFv3
  Provides OSPF support for IPv6
- BGP+
  Extends BGP-4 to support Multiprotocol BGP (MP-BGP), including support for IPv6 addressing
- IS-IS for IPv6
  Extends IS-IS to support IPv6 addressing

- IPv6 tunneling
  Allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6 to 4, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels; is an important element for the transition from IPv4 to IPv6

- Multiprotocol Label Switching (MPLS)
  Uses BGP to advertise routes across Label Switched Paths (LSPs), but uses simple labels to forward packets from any Layer 2 or Layer 3 protocol, which reduces complexity and increases performance; supports graceful restart for reduced failure impact; supports LSP tunneling and multilevel stacks

- Multiprotocol Label Switching (MPLS) Layer 3 VPN
  Allows Layer 3 VPNs across a provider network; uses Multiprotocol BGP (MP-BGP) to establish private routes for increased security; supports RFC 2547 multiple autonomous system VPNs for added flexibility; supports IPv6 MPLS VPN

- Multiprotocol Label Switching (MPLS) Layer 2 VPN
  Establishes simple Layer 2 point-to-point VPNs across a provider network using only MPLS Label Distribution Protocol (LDP); requires no routing and therefore decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; supports Circuit Cross Connect (CCC), Static Virtual Circuits (SVCs), Martini draft, and Kompella draft technologies

- Policy routing
  Allows custom filters for increased performance and security; supports access control lists (ACLs), IP prefix, AS paths, community lists, and aggregate policies

Layer 3 services

- NAT-PT
  Network Address Translation – Protocol Translation (NAT-PT) enables communication between IPv4 and IPv6 nodes by translating between IPv4 and IPv6 packets. It performs IP address translation, and according to different protocols, performs semantic translation for packets. This technology is only suitable for communication between a pure IPv4 node and a pure IPv6 node

- WAN Optimization
  MSR performs optimization using TFO and a combination of DRE, Lempel-Ziv (LZ) compression to provide the bandwidth optimization for file service and web applications. The policy engine module determines which traffic can be optimized and which optimization action should be taken. A pair of WAN optimization equipment can discover each other automatically and complete the negotiation to establish a TCP optimization session

- Address Resolution Protocol (ARP)
  Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network

- User Datagram Protocol (UDP) helper
  Redirects UDP broadcasts to specific IP subnets to prevent server spoofing

- Dynamic Host Configuration Protocol (DHCP)
  Simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets

Quality of service (QoS)

- Traffic policing
  Supports Committed Access Rate (CAR) and line rate

- Congestion management
  Supports FIFO, PQ, CQ, WFQ, CBQ, and RTPQ

- Weighted random early detection (WRED)/Random early detection (RED)
  Delivers congestion avoidance capabilities through the use of queue management algorithms
- Other QoS technologies
  Support traffic shaping, FR QoS, MPLS QoS, and MP QoS/LFI

Security

- IPS
  Built-in Intrusion Prevention System (IPS) detects and protects the branch office from security threats. Optional HPE integration filters for client-side, branch protection from exploits and vulnerabilities
- Zone based firewall
  Zone-Based Policy Firewall changes the firewall configuration from the older interface-based model to a more flexible, more easily understood zone-based model. Interfaces are assigned to zones, and inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface
- Enhanced stateful firewall
  Application layer protocol inspection, Transport layer protocol inspection, ICMP error message check, and TCP SYN check. Support more L4 and L7 protocols like TCP, UDP, UDP-Lite, ICMPv4/ICMPv6, SCTP, DCCP, RAWIP, HTTP, FTP, SMTP, DNS, SIP, H.323, SCCP
- Auto Discover VPN (ADVPN)
  Collects, maintains, and distributes dynamic public addresses through the VPN Address Management (VAM) protocol, making VPN establishment available between enterprise branches that use dynamic addresses to access the public network; compared to traditional VPN technologies, ADVPN technology is more flexible and has richer features, such as NAT traversal of ADVPN packets, AAA identity authentication, IPSec protection of data packets, and multiple VPN domains
- Access control list (ACL)
  Supports powerful ACLs for both IPv4 and IPv6; ACLs are used for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header; rules can be set to operate on specific dates or times
- Terminal Access Controller Access-Control System (TACACS+)
  Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security
- Network login
  Standard IEEE 802.1x allows authentication of multiple users per port
- RADIUS
  Eases security access administration by using a password authentication server
- Network address translation (NAT)
  Supports one-to-one NAT, many-to-many NAT, and NAT control, enabling NAT-PT to support multiple connections; supports blacklist in NAT/NAT-PT, and a limit on the number of connections, session logs, and multi-instances
- Secure shell (SSHv2)
  Uses external servers to securely login to a remote device or securely login to MSR from a remote location; with authentication and encryption, it protects against IP spoofing and plain text password interception; increases the security of Secure File Transfer Protocol (SFTP) transfers

- Unicast Reverse Path Forwarding (URPF)
  Allows normal packets to be forwarded correctly, but discards the attaching packet due to lack of reverse path route or incorrect inbound interface; prevents source spoofing and distributed attacks
- IPSec VPN
  Supports DES, Triple DES (3DES), and Advanced Encryption Standard (AES) 128/192/256 encryption, and MD5 and SHA-1 authentication
- Attack detection and protection
  Responding to network attacks and threats by MSR Comware, support max connection limitation, single-packet attacks protection, scanning attack protection, flood attack protection, TCP and ICMP Attack Protection and so on

Convergence

- Internet Group Management Protocol (IGMP)
  Utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3
- Protocol Independent Multicast (PIM)
  Defines modes of Internet IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM Dense Mode (DM), Sparse Mode (SM), and Source-Specific Multicast (SSM)
- Multicast Source Discovery Protocol (MSDP)
  Allows multiple PIM-SM domains to interoperate; is used for interdomain multicast applications
- Multicast Border Gateway Protocol (MBGP)
  Allows multicast traffic to be forwarded across BGP networks and kept separate from unicast traffic

Integration

- Embedded NetStream
  Improves traffic distribution using powerful scheduling algorithms, including Layer 4 to 7 services; monitors the health status of servers and firewalls
- Embedded VPN and stateful firewall
  Provide enhanced stateful packet inspection and filtering; deliver advanced VPN services with Triple DES (3DES) and Advanced Encryption Standard (AES) encryption at high performance and low latency, and application prioritization and enhancement

Resiliency and high availability

- Backup center
  Acts as a part of the management and backup function to provide backup for device interfaces; delivers reliability by switching traffic over to a backup interface when the primary one fails
- Virtual Router Redundancy Protocol (VRRP)
  Allows groups of two routers to dynamically back each other up to create highly available routed environments; supports VRRP load balancing

Management

- Ease of deployment
  Zero-touch deployment, supports TR-069, USB disk auto deployment and 3G SMS auto deployment
- Industry-standard CLI with a hierarchical structure
  Reduces training time and expenses, and increases productivity in multivendor installations
- Management security
  Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide Telnet and SNMP access; local and remote syslog capabilities allow logging of all access

- SNMPv1, v2, and v3
  Provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption
- Remote monitoring (RMON)
  Uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- FTP, TFTP, and SFTP support
  Offers different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; trivial FTP (TFTP) is a simpler method using User Datagram Protocol (UDP); Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security
- Debug and sampler utility
  Supports ping and traceroute for both IPv4 and IPv6
- Network Time Protocol (NTP)
  Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time
- Information center
  Provides a central repository for system and network information; aggregates all logs, traps, and debugging information generated by the system and maintains them in order of severity; outputs the network information to multiple channels based on user-defined rules
- Management interface control
  Provides management access through modem port and terminal interface; provides access through terminal interface, Telnet, or SSH
- Network Quality Analyzer (NQA)
  Analyzes network performance and service quality by sending test packets, and provides network performance and service quality parameters such as jitter, TCP, or FTP connection delays; allows network manager to determine overall network performance and diagnose and locate network congestion points

Additional information

- OPEX savings
  Simplifies and streamlines deployment, management, and training through the use of a common operating system, thereby cutting costs as well as reducing the risk of human errors associated with having to manage multiple operating systems across different platforms and network layers
- High reliability
  Provides a state-of-the-art unified code base
- Faster time to market
  Allows new and custom features to be brought rapidly to market through engineering efficiencies, delivering better initial and ongoing stability
- Green initiative support
  Provides support for RoHS and WEEE regulations

Warranty and support

- 1-year Warranty
  See **hpe.com/networking/warrantysummary** for warranty and support information included with your product purchase.
- Software releases
  To find software for your product, refer to **hpe.com/networking/support**; for details on the software releases available with your product purchase, refer to **hpe.com/networking/warrantysummary**

HPE MSR1000 Router Series

Specifications	 HPE MSR1002-4 AC Router (JG875A)	 HPE MSR1003-8 AC Router (JG732A) Comware V5 based	 HPE MSR1003-8S AC Router (JH060A) Comware V7 based
I/O ports and slots	2 SIC slots, or 1 DSIC slot 1 RJ-45 autosensing 10/100/1000 WAN port 1 SFP fixed Gigabit Ethernet SFP port 4 RJ-45 autosensing 10/100/1000 LAN ports 1 Serial port	3 SIC slots, or 1 DSIC slot, and 1 SIC slot 2 RJ-45 autosensing 10/100/1000 WAN ports 8 RJ-45 autosensing 10/100/1000 LAN ports	3 SIC slots, or 1 DSIC slot, and 1 SIC slot 2 RJ-45 autosensing 10/100/1000 WAN ports 8 RJ-45 autosensing 10/100/1000 LAN ports
Additional ports and slots	1 USB 2.0 1 RJ-45 console port to access limited CLI port	1 USB 2.0 1 RJ-45 console port to access limited CLI port	1 USB 2.0 1 RJ-45 console port to access limited CLI port
AP characteristics			
Radios (via optional modules)	3G, 4G LTE	3G, 4G LTE	3G, 4G LTE
Physical characteristics			
Dimensions	14.17(w) x 11.81(d) x 1.74(h) in (36 x 30 x 4.42 cm) (1U height)	14.17(w) x 11.81(d) x 17.4(h)in (36 x 30 x 44.2 cm)	14.17(w) x 11.81(d) x 17.4(h) in (36 x 30 x 44.2 cm)
Weight	6.83 lb (3.10 kg)	6.94 lb (3.15 kg)	6.94 lb (3.15 kg)
Memory and processor	RISC @ 667 MHz, 1 GB DDR3 SDRAM, 256 MB flash	RISC @ 667 MHz, 512 MB DDR3 SDRAM, 256 MB flash	RISC @ 667 MHz, 1 GB DDR3 SDRAM, 256 MB flash
Mounting and enclosure	Desktop or can be mounted in a EIA standard 19-inch telco rack when used with the rack-mount kit in the package.	Desktop or can be mounted in a EIA standard 19-inch telco rack when used with the rack-mount kit in the package.	Desktop or can be mounted in a EIA standard 19-inch telco rack when used with the rack-mount kit in the package.
Performance			
Throughput	Up to 500 Kpps (64-byte packets)	Up to 500 Kpps (64-byte packets)	Up to 500 Kpps (64-byte packets)
Routing table size	200000 entries (IPv4), 200000 entries (IPv6)	30000 entries (IPv4), 30000 entries (IPv6)	200000 entries (IPv4), 200000 entries (IPv6)
Forwarding table size	200000 entries (IPv4), 200000 entries (IPv6)	30000 entries (IPv4), 30000 entries (IPv6)	200000 entries (IPv4), 200000 entries (IPv6)
Environment			
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing	5% to 95%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing	5% to 95%, noncondensing
Altitude	Up to 16,404 ft (5 km)	Up to 16,404 ft (5 km)	Up to 16,404 ft (5 km)
Electrical characteristics			
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
Maximum heat dissipation	92 BTU/hr (97.06 kJ/hr)	65 BTU/hr (68.58 kJ/hr)	65 BTU/hr (68.58 kJ/hr)
AC voltage	100—240 VAC, rated (depending on power supply chosen)	100—240 VAC, rated (depending on power supply chosen)	100—240 VAC, rated (depending on power supply chosen)
Maximum power rating	30 W	30 W	30 W
	Notes Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.

Specifications	HPE MSR1002-4 AC Router (JG875A)	HPE MSR1003-8 AC Router (JG732A) Comware V5 based	HPE MSR1003-8S AC Router (JH060A) Comware V7 based
Reliability Availability	137.5	137.5	137.5
Safety	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; AS/NZS 60950-1; GB 4943.1	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; AS/NZS 60950-1; GB 4943.1	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; AS/NZS 60950-1; GB 4943.1
Emissions	VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; ICES-003 Class A; EN 300 386; CISPR 24; AS/NZS CISPR 22 Class A; EN 61000-3-2; EN 61000-3-3; FCC (CFR 47, Part 15) Class A	VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; ICES-003 Class A; EN 300 386; CISPR 24; AS/NZS CISPR 22 Class A; EN 61000-3-2; EN 61000-3-3; FCC (CFR 47, Part 15) Class A	VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; ICES-003 Class A; EN 300 386; CISPR 24; AS/NZS CISPR 22 Class A; EN 61000-3-2; EN 61000-3-3; FCC (CFR 47, Part 15) Class A
Telecom	FCC part 68; CS-03	FCC part 68; CS-03	FCC part 68; CS-03
Management	IMC—Intelligent Management Center; command-line interface; Web browser; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); SNMP Manager; Telnet; RMON1; FTP; IEEE 802.3 Ethernet MIB	IMC—Intelligent Management Center; command-line interface; Web browser; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); SNMP Manager; Telnet; RMON1; FTP; IEEE 802.3 Ethernet MIB	IMC—Intelligent Management Center; command-line interface; Web browser; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); SNMP Manager; Telnet; RMON1; FTP; IEEE 802.3 Ethernet MIB
Services	Refer to the Hewlett Packard Enterprise website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at **hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

Standards and Protocols
(applies to JG875A and JH060A models)

BGP	RFC 1163 Border Gateway Protocol (BGP) RFC 1267 Border Gateway Protocol 3 (BGP-3) RFC 1657 Definitions of Managed Objects for BGPv4 RFC 1771 BGPv4 RFC 1772 Application of the BGP RFC 1773 Experience with the BGP-4 Protocol RFC 1774 BGP-4 Protocol Analysis RFC 1965 BGP-4 confederations RFC 1997 BGP Communities Attribute RFC 2439 BGP Route Flap Damping RFC 2547 BGP/MPLS VPNs RFC 2796 BGP Route Reflection	RFC 2842 Capability Advertisement with BGP-4 RFC 2858 BGP-4 Multi-Protocol Extensions RFC 2918 Route Refresh Capability RFC 3065 Autonomous System Confederations for BGP RFC 3107 Support BGP carry Label for MPLS RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4) RFC 4273 Definitions of Managed Objects for BGP-4 RFC 4274 BGP-4 Protocol Analysis	RFC 4275 BGP-4 MIB Implementation Survey RFC 4276 BGP-4 Implementation Report RFC 4277 Experience with the BGP-4 Protocol RFC 4360 BGP Extended Communities Attribute RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) RFC 4724 Graceful Restart Mechanism for BGP RFC 4760 Multiprotocol Extensions for BGP-4 RFC1998 An Application of the BGP Community Attribute in Multi-home Routing
Denial of service protection	CPU DoS Protection	Rate Limiting by ACLs	

Standards and Protocols
(applies to JG875A and JH060A models)

Device management	RFC 1155 Structure and Mgmt Information (SMIv1) RFC 1157 SNMPv1/v2c RFC 1305 NTPv3 RFC 1591 DNS (client) RFC 1902 (SNMPv2)	RFC 1908 (SNMP v1/2 Coexistence) RFC 1945 Hypertext Transfer Protocol—HTTP/1.0 RFC 2271 Framework RFC 2573 (SNMPv3 Applications) RFC 2576 (Coexistence between SNMP V1, V2, V3)	RFC 2578-2580 SMIv2 RFC 2579 (SMIv2 Text Conventions) RFC 2580 (SMIv2 Conformance) RFC 3416 (SNMP Protocol Operations v2) RFC 3417 (SNMP Transport Mappings)
General protocols	RFC 768 UDP RFC 760 DoD standard Internet Protocol RFC 764 Telnet Protocol specification RFC 777 Internet Control Message Protocol RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 813 Window and Acknowledgement Strategy in TCP RFC 815 IP datagram reassembly algorithms RFC 826 ARP RFC 854 Telnet Protocol Specification RFC 855 Telnet Option Specifications RFC 856 Telnet Binary Transmission RFC 857 Telnet Echo Option RFC 858 Telnet Suppress Go Ahead Option RFC 862 Echo Service (TCP Echo) RFC 879 TCP maximum segment size and related topics RFC 882 Domain names: Concepts and facilities RFC 883 Domain names: Implementation specification 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 (Trivial File Transfer Protocol) RFC 917 Internet Subnets RFC 919 Broadcasting Internet Datagrams	RFC 922 Broadcasting Internet Datagrams in the Presence of Subnets (IP_BROAD) RFC 925 Multi-LAN Address Resolution RFC 926 Protocol for providing the connectionless mode network services RFC 950 Internet Standard Subnetting Procedure RFC 951 BOOTP RFC 958 Network Time Protocol (NTP) RFC 959 File Transfer Protocol (FTP) RFC 973 Domain system changes and observations RFC 988 Host extensions for IP multicasting RFC 1027 Proxy ARP RFC 1034 Domain names—concepts and facilities RFC 1035 Domain names—implementation and specification RFC 1048 BOOTP (Bootstrap Protocol) vendor information extensions RFC 1054 Host extensions for IP multicasting RFC 1058 RIPv1 RFC 1059 Network Time Protocol (version 1) specification and implementation RFC 1060 Assigned numbers RFC 1063 IP MTU (Maximum Transmission Unit) discovery options RFC 1071 Computing the Internet checksum RFC 1072 TCP extensions for long-delay paths RFC 1079 Telnet terminal speed option RFC 1084 BOOTP (Bootstrap Protocol) vendor information extensions	RFC 1091 Telnet Terminal-Type Option RFC 1093 NSFNET routing architecture RFC 1101 DNS encoding of network names and other types RFC 1119 Network Time Protocol (version 2) specification and implementation RFC 1122 Requirements for Internet Hosts—Communication Layers RFC 1141 Incremental updating of the Internet checksum RFC 1142 OSI IS-IS Intra-domain Routing Protocol RFC 1164 Application of the Border Gateway Protocol in the Internet RFC 1166 Internet address used by Internet Protocol (IP) RFC 1171 Point-to-Point Protocol for the transmission of multi-protocol datagrams over Point-to-Point links RFC 1172 Point-to-Point Protocol (PPP) initial configuration options RFC 1185 TCP Extension for High-Speed Paths RFC 1191 Path MTU discovery RFC 1195 OSI ISIS for IP and Dual Environments RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPF v2) RFC 1265 BGP Protocol Analysis RFC 1266 Experience with the BGP Protocol RFC 1268 Application of the Border Gateway Protocol in the Internet RFC 1271 Remote Network Monitoring Management Information Base

Standards and Protocols
(applies to JG875A and JH060A models)

General protocols

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 (IPv4 only)
RFC 1321 The MD5 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 1333 PPP Link Quality Monitoring
RFC 1334 PPP Authentication Protocols
RFC 1349 Type of Service
RFC 1350 TFTP Protocol (revision 2)
RFC 1364 BGP OSPF Interaction
RFC 1370 Applicability Statement for OSPF
RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)
RFC 1393 Traceroute Using an IP Option
RFC 1395 BOOTP (Bootstrap Protocol) Vendor Information Extensions
RFC 1398 Definitions of Managed Objects for the Ethernet-Like Interface Types
RFC 1403 BGP OSPF Interaction
RFC 1444 Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1449 Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC 1473 The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
RFC 1483 Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1490 Multiprotocol Interconnect over Frame Relay
RFC 1497 BOOTP (Bootstrap Protocol) Vendor Information Extensions
RFC 1519 CIDR
RFC 1531 Dynamic Host Configuration Protocol
RFC 1532 Clarifications and Extensions for the Bootstrap Protocol
RFC 1533 DHCP Options and BOOTP Vendor Extensions
RFC 1534 Interoperation Between DHCP and BOOTP
RFC 1541 Dynamic Host Configuration Protocol
RFC 1542 BOOTP Extensions
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1548 The Point-to-Point Protocol (PPP)
RFC 1549 PPP in HDLC Framing
RFC 1570 PPP LCP (Point-to-Point Protocol Link Control Protocol) Extensions
RFC 1577 Classical IP and ARP over ATM
RFC 1597 Address Allocation for Private Internets
RFC 1618 PPP over ISDN
RFC 1619 PPP over SONET/SDH (Synchronous Optical Network/ Synchronous Digital Hierarchy)
RFC 1624 Incremental Internet Checksum
RFC 1631 NAT
RFC 1650 Definitions of Managed Objects for the Ethernet-like Interface Types 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
RFC 1702 Generic Routing Encapsulation over IPv4 networks
RFC 1717 The PPP Multilink Protocol (MP)
RFC 1721 RIP-2 Analysis
RFC 1722 RIP-2 Applicability
RFC 1723 RIP v2
RFC 1724 RIP Version 2 MIB Extension
RFC 1757 Remote Network Monitoring Management Information Base
RFC 1777 Lightweight Directory Access Protocol
RFC 1812 IPv4 Routing
RFC 1825 Security Architecture for the Internet Protocol
RFC 1826 IP Authentication Header
RFC 1827 IP Encapsulating Security Payload (ESP)
RFC 1829 The ESP DES-CBC Transform
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1884 IP Version 6 Addressing Architecture
RFC 1885 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 1886 DNS Extensions to support IP version 6 RFC 1889 RTP (Real-Time Protocol): A Transport Protocol for Real-Time Applications. Audio-Video Transport Working Group
RFC 1933 Transition Mechanisms for IPv6 Hosts and Routers
RFC 1945 Hypertext Transfer Protocol—HTTP/1.0
RFC 1962 The PPP Compression Control Protocol (CCP)
RFC 1966 BGP Route Reflection An alternative to full mesh IBGP
RFC 1970 Neighbor Discovery for IP Version 6 (IPv6)
RFC 1971 IPv6 Stateless Address Autoconfiguration
RFC 1972 A Method for the Transmission of IPv6 Packets over Ethernet Networks
RFC 1981 Path MTU Discovery for IP version 6 RFC 1982 Serial Number Arithmetic
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2001 TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms
RFC 2002 IP Mobility Support
RFC 2003 IP Encapsulation within IP
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 Acknowledgement Options
RFC 2021 Remote Network Monitoring Management Information Base Version 2 using SMIv2
RFC 2073 An IPv6 Provider-Based Unicast Address Format
RFC 2082 RIP-2 MD5 Authentication
RFC 2091 Triggered Extensions to RIP to Support Demand Circuits
RFC 2104 HMAC: Keyed-Hashing for Message Authentication
RFC 2131 DHCP
RFC 2132 DHCP Options and BOOTP Vendor Extensions
RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC 2138 Remote Authentication Dial In User Service (RADIUS)
RFC 2205 Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification
RFC 2209 Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules
RFC 2210 Use of RSVP (Resource Reservation Protocol) in Integrated Services
RFC 2225 Classical IP and ARP over ATM
RFC 2236 IGMP Snooping
RFC 2246 The TLS Protocol Version 1.0
RFC 2251 Lightweight Directory Access Protocol (v3)
RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2283 MBGP
RFC 2292 Advanced Sockets API for IPv6

Standards and Protocols
(applies to JG875A and JH060A models)

General protocols

RFC 2309 Recommendations on queue management and congestion avoidance in the Internet
RFC 2327 SDP: Session Description Protocol
RFC 2338 VRRP
RFC 2344 Reverse Tunneling for Mobile IP
RFC 2358 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 2364 PPP Over AAL5
RFC 2365 Administratively Scoped IP Multicast
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 2427 Multiprotocol Interconnect over Frame Relay
RFC 2428 FTP Extensions for IPv6 and NATs
RFC 2433 Microsoft PPP CHAP (Challenge Handshake Authentication Protocol) Extensions
RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2452 IP Version 6 Management Information Base for the Transmission Control Protocol
RFC 2453 RIPv2
RFC 2454 IP Version 6 Management Information Base for the User Datagram Protocol
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 IP Version 6: Textual Conventions and General Group
RFC 2466 Management Information Base for IP Version 6: ICMPv6 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 2507 IP Header Compression
RFC 2508 Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
RFC 2509 IP Header Compression over PPP
RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2519 A Framework for Inter-Domain Route Aggregation
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2543 SIP: Session Initiation Protocol
RFC 2548 (MS-RAS-Vendor only)
RFC 2553 Basic Socket Interface Extensions for IPv6
RFC 2570 Introduction to Version 3 of the Internet-standard Network Management Framework
RFC 2581 TCP Congestion Control
RFC 2597 Assured Forwarding PHB Group
RFC 2598 An Expedited Forwarding PHB
RFC 2615 PPP over SONET/SDH (Synchronous Optical Network/ Synchronous Digital Hierarchy)
RFC 2616 HTTP Compatibility v1.1
RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
RFC 2618 RADIUS Authentication Client MIB
RFC 2620 RADIUS Accounting Client MIB
RFC 2644 Changing the Default for Directed Broadcasts in Routers
RFC 2661 L2TP
RFC 2663 NAT Terminology and Considerations
RFC 2665 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 2668 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 2675 IPv6 Jumbograms
RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2685 Virtual Private Networks Identifier
RFC 2686 The Multi-Class Extension to Multi-Link PPP
RFC 2694 DNS extensions to Network Address Translators (DNS_ALG)
RFC 2698 A Two Rate Three Color Marker
RFC 2702 Requirements for Traffic Engineering Over MPLS
RFC 2711 IPv6 Router Alert Option
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2747 RSVP Cryptographic Authentication
RFC 2763 Dynamic Name-to-System ID mapping
RFC 2784 Generic Routing Encapsulation (GRE)
RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing
RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2866 RADIUS Accounting
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 2884 Performance Evaluation of Explicit Congestion Notification (ECN) in IP Networks.
RFC 2894 Router Renumbering for IPv6
RFC 2917 A Core MPLS IP VPN Architecture
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2963 A Rate Adaptive Shaper for Differentiated Services
RFC 2965 HTTP State Management Mechanism
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 2976 The SIP INFO Method
RFC 2993 Architectural Implications of NAT
RFC 3011 The IPv4 Subnet Selection Option for DHCP
RFC 3022 Traditional IP Network Address Translator (Traditional NAT)
RFC 3024 Reverse Tunneling for Mobile IP, revised
RFC 3025 Mobile IP Vendor/ Organization-Specific Extensions
RFC 3027 Protocol Complications with the IP Network Address Translator
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3036 LDP Specification
RFC 3037 LDP (Label Distribution Protocol) Applicability
RFC 3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 3046 DHCP Relay Agent Information Option
RFC 3063 MPLS Loop Prevention Mechanism
RFC 3097 RSVP (Resource Reservation Protocol) Cryptographic Authentication—Updated Message Type Value
RFC 3115 Mobile IP Vendor/ Organization-Specific Extensions
RFC 3137 OSPF Stub Router Advertisement
RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP
RFC 3176 InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks
RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP-Tunnels

Standards and Protocols
(applies to JG875A and JH060A models)

General protocols

RFC 3215 LDP State Machine
RFC 3220 IP Mobility Support for IPv4
RFC 3246 Expedited Forwarding PHB
RFC 3261 SIP: Session Initiation Protocol
RFC 3262 Reliability of Provisional Responses in Session Initiation Protocol (SIP)
RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3270 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
RFC 3273 Remote Network Monitoring Management Information Base for High Capacity Networks
RFC 3277 IS-IS Transient Blackhole Avoidance
RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses
RFC 3311 The Session Initiation Protocol (SIP) UPDATE Method
RFC 3319 Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
RFC 3344 IP Mobility Support for IPv4
RFC 3345 Border Gateway Protocol (BGP) Persistent Route Oscillation Condition
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 3392 Support BGP capabilities advertisement
RFC 3410 Introduction to Version 3 of the Internet-standard Network Management Framework
RFC 3442 The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4
RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
RFC 3446 Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP)
RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
RFC 3493 Basic Socket Interface Extensions for IPv6
RFC 3495 Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration
RFC 3509 OSPF ABR Behavior
RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC 3515 The Session Initiation Protocol (SIP) Refer Method
RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3527 Link Selection sub-option for the Relay Agent Information Option for DHCPv4
RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6
RFC 3547 The Group Domain of Interpretation
RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC 3569 An Overview of Source-Specific Multicast (SSM)
RFC 3584 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 3587 IPv6 Global Unicast Address Format
RFC 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC 3596 DNS Extensions to Support IP Version 6
RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec
RFC 3612 Applicability Statement for Restart Mechanisms for the Label Distribution Protocol (LDP)
RFC 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3621 Power Ethernet MIB
RFC 3623 Graceful OSPF Restart
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 3636 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
RFC 3704 Unicast Reverse Path Forwarding (URPF)
RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3711 The Secure Real-time Transport Protocol (SRTP)
RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3737 IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB (Management Information Base) modules
RFC 3768 Virtual Router Redundancy Protocol (VRRP)
RFC 3782 The NewReno Modification to TCP's Fast Recovery Algorithm
RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3809 Generic Requirements for Provider Provisioned Virtual Private Networks (VPNs)
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 3814 Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)
RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC 3847 Restart signaling for IS-IS
RFC 3879 Deprecating Site Local Addresses
RFC 3898 Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

Standards and Protocols
(applies to JG875A and JH060A models)

General protocols

RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 3917 Requirements for IP Flow Information Export (IPFIX)
RFC 3942 Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options
RFC 3948 UDP Encapsulation of IPsec ESP Packets
RFC 3954 Cisco Systems NetFlow Services Export Version 9
RFC 3973 Protocol Independent Multicast—Dense Mode (PIM-DM): Protocol Specification (Revised)
RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
RFC 4022 Management Information Base for the Transmission Control Protocol (TCP)
RFC 4023 Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
RFC 4026 Provider Provisioned VPN terminology
RFC 4061 Benchmarking Basic OSPF Single Router Control Plane Convergence
RFC 4062 OSPF Benchmarking Terminology and Concepts
RFC 4063 Considerations When Using Basic OSPF Convergence Benchmarks
RFC 4075 Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
RFC 4105 Requirements for Inter-Area MPLS Traffic Engineering
RFC 4109 Algorithms for Internet Key Exchange version 1 (IKEv1)
RFC 4113 Management Information Base for the User Datagram Protocol (UDP)
RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering
RFC 4125 Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
RFC 4127 Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
RFC 4133 Entity MIB (Version 3)
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4221 Multiprotocol Label Switching (MPLS) Management Overview
RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance
RFC 4242 Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 4244 An Extension to the Session Initiation Protocol (SIP) for Request History Information
RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers
RFC 4251 The Secure Shell (SSH) Protocol Architecture
RFC 4252 The Secure Shell (SSH) Authentication Protocol
RFC 4253 The Secure Shell (SSH) Transport Layer Protocol
RFC 4254 The Secure Shell (SSH) Connection Protocol
RFC 4272 BGP Security Vulnerabilities Analysis
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 4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4306 Internet Key Exchange (IKEv2) Protocol
RFC 4308 Cryptographic Suites for IPsec
RFC 4361 Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4365 Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4377 Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks
RFC 4381 Analyses of the Security of BGP/MPLS IP VPNs
RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base
RFC 4384 BGP Communities for Data Collection
RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 4419 Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
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 4451 BGP MULTI_EXIT_DISC (MED) Considerations
RFC 4486 Subcodes for BGP Cease Notification Message
RFC 4502 Remote Network Monitoring Management Information Base Version 2
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 4561 Definition of a Record Route Object (RRO) Node-Id sub-Objects
RFC 4562 MAC-Forced Forwarding: A Method for Subscriber Separation on an Ethernet Access Network
RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams
RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4594 Configuration Guidelines for DiffServ Service Classes
RFC 4601 Protocol Independent Multicast—Sparse Mode (PIM-SM): Protocol Specification (Revised)
RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC 4605 Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")
RFC 4607 Source-Specific Multicast for IP RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
RFC 4618 Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks
RFC 4619 Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks
RFC 4632 Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan

Standards and Protocols
(applies to JG875A and JH060A models)

General protocols	RFC 4649 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN RFC 4664 Framework for Layer 2 Virtual Private Networks (L2VPNs) RFC 4665 Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks RFC 4741 NETCONF Configuration Protocol RFC 4742 Using the NETCONF Configuration Protocol over Secure SHell (SSH) RFC 4743 Using NETCONF over the Simple Object Access Protocol (SOAP) RFC 4750 OSPF Version 2 Management Information Base RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling RFC 4765 Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks RFC 4781 Graceful Restart Mechanism for BGP with MPLS RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP 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 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 4816 Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service RFC 4818 RADIUS Delegated-IPv6-Prefix Attribute RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) RFC 4861 Neighbor Discovery for IP version 6 (IPv6) RFC 4862 IPv6 Stateless Address Autoconfiguration RFC 4878 Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on RFC 4893 BGP Support for Four-octet AS Number Space RFC 4940 IANA Considerations for OSPF	RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6 RFC 5004 Avoid BGP Best Path Transitions from One External to Another RFC 5007 DHCPv6 Leasequery RFC 5015 Bidirectional Protocol Independent Multicast (BIDIR-PIM) RFC 5036 LDP Specification RFC 5060 Protocol Independent Multicast MIB RFC 5065 Autonomous System Confederations for BGP RFC 5072 IP Version 6 over PPP 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 5095 Deprecation of Type 0 Routing Headers in IPv6 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 Administrative Tags RFC 5132 IP Multicast MIB RFC 5187 OSPFv3 Graceful Restart RFC 5214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) RFC 5240 Protocol Independent Multicast (PIM) Bootstrap Router MIB RFC 5254 Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3) RFC 5277 NETCONF Event Notifications RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 5281 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) 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 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 Intermediate System to Intermediate System (IS-IS) Cryptographic 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 5310 IS-IS Generic Cryptographic Authentication RFC 5359 Session Initiation Protocol Service Examples RFC 5381 Experience of Implementing NETCONF over SOAP RFC 5382 The IP Network Address Translator (NAT) RFC 5398 Autonomous System (AS) Number Reservation for Documentation Use RFC 5415 Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification RFC 5416 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11 RFC 5443 LDP IGP Synchronization RFC 5492 Capabilities Advertisement with BGP-4 RFC 5496 The Reverse Path Forwarding (RPF) Vector TLV RFC 5508 NAT Behavioral Requirements for ICMP RFC 5539 NETCONF over Transport Layer Security (TLS) RFC 5601 Pseudowire (PW) Management Information Base (MIB) RFC 5602 Pseudowire (PW) over MPLS PSN Management Information Base (MIB) RFC 5613 OSPF Link-Local Signaling RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge RFC 5681 TCP Congestion Control RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 RFC 5833 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Base MIB RFC 5834 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding MIB for IEEE 802.11 RFC 5880 Bidirectional Forwarding Detection RFC 5881 BFD for IPv4 and IPv6 (Single Hop) RFC 5881 Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) RFC 5882 Generic Application of BFD RFC 5883 BFD for Multihop Paths RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification RFC 5969 IPv6 Rapid Deployment on IPv4 Infrastructures (6RD)—Protocol Specification RFC 6037 Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs RFC 6085 Address Mapping of IPv6 Multicast Packets on Ethernet
IP multicast	RFC 1112 IGMP RFC 2362 PIM Sparse Mode RFC 2710 Multicast Listener Discovery (MLD) for IPv6	RFC 2934 Protocol Independent Multicast MIB for IPv4 RFC 3376 IGMPv3 RFC 3376 IGMPv3 (host joins only)	RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

Standards and Protocols
(applies to JG875A and JH060A models)

IPv6	RFC 2080 RIPng for IPv6 RFC 2460 IPv6 Specification RFC 2473 Generic Packet Tunneling in IPv6 RFC 2475 IPv6 DiffServ Architecture RFC 2529 Transmission of IPv6 Packets over IPv4	RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2740 OSPFv3 for IPv6 RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers	RFC 3056 Connection of IPv6 Domains via IPv4 Clouds RFC 3162 RADIUS and IPv6 RFC 3315 DHCPv6 (client and relay) RFC 5340 OSPF for IPv6
MIBs	RFC 1213 MIB II RFC 1493 Bridge MIB RFC 1724 RIPv2 MIB RFC 1850 OSPFv2 MIB RFC 1907 SNMPv2 MIB RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP	RFC 2013 SNMPv2 MIB for UDP RFC 2096 IP Forwarding Table MIB RFC 2233 Interfaces MIB RFC 2273 SNMP-NOTIFICATION-MIB RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB	RFC 2573 SNMP-Notification MIB RFC 2574 SNMP USM MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2737 Entity MIB (Version 2) RFC 2863 The Interfaces Group MIB RFC 3813 MPLS LSR MIB
Network management	IEEE 802.1D (STP) RFC 1098 Simple Network Management Protocol (SNMP) RFC 1158 Management Information Base for network management of TCP/IP-based internets: MIB-II RFC 1212 Concise MIB definitions RFC 1215 Convention for defining traps for use with the SNMP RFC 1389 RIPv2 MIB Extension RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1450 Management Information Base (MIB) for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1902 Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1903 SNMPv2 Textual Conventions RFC 1904 SNMPv2 Conformance	RFC 1905 SNMPv2 Protocol Operations RFC 1906 SNMPv2 Transport Mappings RFC 1908 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC 1918 Private Internet Address Allocation RFC 2037 Entity MIB using SMIv2 RFC 2261 An Architecture for Describing SNMP Management Frameworks RFC 2262 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) RFC 2263 SNMPv3 Applications RFC 2264 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 2265 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) RFC 2272 SNMPv3 Management Protocol RFC 2273 SNMPv3 Applications	RFC 2274 USM for SNMPv3 RFC 2275 VACM for SNMPv3 RFC 2575 SNMPv3 View-based Access Control Model (VACM) RFC 3164 BSD syslog Protocol 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 SNMPv3 User-based Security Model (USM) RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
OSPF	RFC 1245 OSPF protocol analysis RFC 1246 Experience with OSPF RFC 1583 OSPFv2 RFC 1587 OSPF NSSA	RFC 1765 OSPF Database Overflow RFC 1850 OSPFv2 Management Information Base (MIB), traps	RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option RFC 3101 OSPF NSSA
QoS/CoS	IEEE 802.1P (CoS) RFC 2474 DS Field in the IPv4 and IPv6 Headers RFC 2475 DiffServ Architecture RFC 2597 DiffServ Assured Forwarding (AF)	RFC 2598 DiffServ Expedited Forwarding (EF) RFC 2697 A Single Rate Three Color Marker RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP	RFC 3247 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior) RFC 3260 New Terminology and Clarifications for DiffServ
Security	IEEE 802.1X Port Based Network Access Control RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication RFC 2138 RADIUS Authentication RFC 2139 RADIUS Accounting	RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 The Internet Key Exchange (IKE) RFC 2412 The OAKLEY Key Determination Protocol RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile	RFC 2818 HTTP Over TLS RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP) RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
VPN	RFC 1828 IP Authentication using Keyed MD5 RFC 1853 IP in IP Tunneling 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 2410 The NULL Encryption Algorithm and Its Use With IPSec RFC 2411 IP Security Document Roadmap	RFC 3948—UDP Encapsulation of IPSec ESP Packets RFC 4301—Security Architecture for the Internet Protocol RFC 4302—IP Authentication Header (AH) RFC 4303—IP Encapsulating Security Payload (ESP) RFC 4305—Cryptographic Algorithm Implementation Requirements for ESP and AH

Standards and Protocols
(applies to JG732A model)

BGP	RFC 1163 Border Gateway Protocol (BGP) RFC 1267 Border Gateway Protocol 3 (BGP-3) RFC 1657 Definitions of Managed Objects for BGPv4 RFC 1771 BGPv4	RFC 1772 Application of the BGP RFC 1773 Experience with the BGP-4 Protocol RFC 1774 BGP-4 Protocol Analysis RFC 1997 BGP Communities Attribute	RFC 1998 An Application of the BGP Community Attribute in Multi-home Routing RFC 2385 BGP Session Protection via TCP MD5 RFC 2439 BGP Route Flap Damping
Denial of service protection	CPU DoS Protection	Rate Limiting by ACLs	
Device management	RFC 1305 NTPv3	RFC 1945 Hypertext Transfer Protocol—HTTP/1.0	RFC 2452 MIB for TCP6 RFC 2454 MIB for UDP6
General protocols	IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1w Rapid Reconfiguration of Spanning Tree RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 855 Telnet Option Specification RFC 856 TELNET RFC 858 Telnet Suppress Go Ahead Option RFC 894 IP over Ethernet RFC 925 Multi-LAN Address Resolution RFC 950 Internet Standard Subnetting Procedure RFC 959 File Transfer Protocol (FTP) RFC 1006 ISO transport services on top of the TCP: Version 3 RFC 1027 Proxy ARP RFC 1034 Domain Concepts and Facilities RFC 1035 Domain Implementation and Specification RFC 1042 IP Datagrams RFC 1058 RIPv1 RFC 1071 Computing the Internet Checksum RFC 1091 Telnet Terminal-Type Option RFC 1122 Host Requirements RFC 1141 Incremental updating of the Internet checksum RFC 1142 OSI IS-IS Intra-domain Routing Protocol RFC 1144 Compressing TCP/IP headers for low-speed serial links RFC 1195 OSI ISIS for IP and Dual Environments RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1293 Inverse Address Resolution Protocol RFC 1315 Management Information Base for Frame Relay DTEs RFC 1332 The PPP Internet Protocol Control Protocol (IPCP) RFC 1333 PPP Link Quality Monitoring RFC 1334 PPP Authentication Protocols (PAP) RFC 1349 Type of Service RFC 1350 TFTP Protocol (revision 2) RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)	RFC 1695 Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2 RFC 1701 Generic Routing Encapsulation RFC 1702 Generic Routing Encapsulation over IPv4 networks RFC 1721 RIP-2 Analysis RFC 1722 RIP-2 Applicability RFC 1723 RIP v2 RFC 1795 Data Link Switching: Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Standard Version 1 RFC 1812 IPv4 Routing RFC 1829 The ESP DES-CBC Transform RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses RFC 1944 Benchmarking Methodology for Network Interconnect Devices RFC 1973 PPP in Frame Relay RFC 1974 PPP Stac LZS Compression Protocol RFC 1990 The PPP Multilink Protocol (MP) RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2091 Trigger RIP RFC 2131 DHCP RFC 2132 DHCP Options and BOOTP Vendor Extensions RFC 2166 APPN Implementer's Workshop Closed Pages Document DLSw v2.0 Enhancements RFC 2205 Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification RFC 2280 Routing Policy Specification Language (RPSL) RFC 2284 EAP over LAN RFC 2338 VRRP RFC 2364 PPP Over AAL5 RFC 2374 An Aggregatable Global Unicast Address Format RFC 2451 The ESP CBC-Mode Cipher Algorithms RFC 2453 RIPv2 RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols RFC 2511 Internet X.509 Certificate Request Message Format RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE) RFC 2644 Directed Broadcast Control RFC 2661 L2TP RFC 2663 NAT Terminology and Considerations	RFC 3022 Traditional IP Network Address Translator (Traditional NAT) RFC 3027 Protocol Complications with the IP Network Address Translator RFC 3031 Multiprotocol Label Switching Architecture RFC 3032 MPLS Label Stack Encoding RFC 3036 LDP Specification RFC 3046 DHCP Relay Agent Information Option RFC 3063 MPLS Loop Prevention Mechanism RFC 3065 Support AS confederation RFC 3137 OSPF Stub Router Advertisement RFC 3209 RSVP-TE Extensions to RSVP for LSP Tunnels RFC 3210 Applicability Statement for Extensions to RSVP for LSP-Tunnels RFC 3212 Constraint-Based LSP setup using LDP (CR-LDP) RFC 3214 LSP Modification Using CR-LDP RFC 3215 LDP State Machine RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) RFC 3277 IS-IS Transient Blackhole Avoidance RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 3392 Support BGP capabilities advertisement RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP) RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers RFC 3784 ISIS TE support RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit 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)

Standards and Protocols
(applies to JG732A model)

General protocols	RFC 1381 SNMP MIB Extension for X.25 LAPB RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol RFC 1472 The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol RFC 1490 Multiprotocol Interconnect over Frame Relay RFC 1519 CIDR RFC 1534 DHCP/BOOTP Interoperation RFC 1542 Clarifications and Extensions for the Bootstrap Protocol RFC 1552 The PPP Internetworking Packet Exchange Control Protocol (IPXCP) RFC 1577 Classical IP and ARP over ATM RFC 1613 Cisco Systems X.25 over TCP (XOT) RFC 1624 Incremental Internet Checksum RFC 1631 NAT RFC 1638 PPP Bridging Control Protocol (BCP) RFC 1661 The Point-to-Point Protocol (PPP) RFC 1662 PPP in HDLC-like Framing	RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 RFC 2694 DNS extensions to Network Address Translators (DNS_ALG) RFC 2702 Requirements for Traffic Engineering Over MPLS RFC 2747 RSVP Cryptographic Authentication RFC 2763 Dynamic Name-to-System ID mapping support RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT) RFC 2766 Network Address Translation—Protocol Translation (NAT-PT) RFC 2784 Generic Routing Encapsulation (GRE) RFC 2787 Definitions of Managed Objects for VRRP 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 2993 Architectural Implications of NAT	RFC 3847 Restart signaling for IS-IS FRF.1.2 PVC User-to-Network Interface (UNI) Implementation Agreement—July 2000 FRF.11.1 Voice over Frame Relay Implementation Agreement—May 1997—Annex J added March 1999 FRF.12 Frame Relay Fragmentation Implementation Agreement—December 1997 FRF.16.1 Multilink Frame Relay UNI/NNI Implementation Agreement—May 2002 FRF.2.2 Frame Relay Network-to-Network Interface (NNI) Implementation Agreement—March 2002 FRF.20 Frame Relay IP Header Compression Implementation Agreement—June 2001 FRF.3.2 Frame Relay Multiprotocol Encapsulation Implementation Agreement—April 2000 FRF.7 Frame Relay PVC Multicast Service and Protocol Description—October 1994 FRF.9 Data Compression Over Frame Relay Implementation Agreement—January 1996
IP multicast	RFC 1112 IGMP RFC 2236 IGMPv2 RFC 2283 Multiprotocol Extensions for BGP-4	RFC 2362 PIM Sparse Mode RFC 2365 Administratively Scoped IP Multicast RFC 2710 Multicast Listener Discovery (MLD) for IPv6	RFC 2934 Protocol Independent Multicast MIB for IPv4 RFC 3376 IGMPv3
IPv6	RFC 1981 IPv6 Path MTU Discovery RFC 2080 RIPng for IPv6 RFC 2292 Advanced Sockets API for IPv6 RFC 2373 IPv6 Addressing Architecture RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2462 IPv6 Stateless Address Auto-configuration	RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2472 IP Version 6 over PPP RFC 2473 Generic Packet Tunneling in IPv6 RFC 2475 IPv6 DiffServ Architecture RFC 2529 Transmission of IPv6 Packets over IPv4 RFC 2545 Use of MP-BGP-4 for IPv6	RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2740 OSPFv3 for IPv6 RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers RFC 3056 Connection of IPv6 Domains via IPv4 Clouds RFC 3513 IPv6 Addressing Architecture RFC 3596 DNS Extension for IPv6
MIBs	RFC 1213 MIB II RFC 1229 Interface MIB Extensions RFC 1286 Bridge MIB RFC 1493 Bridge MIB RFC 1573 SNMP MIB II RFC 1724 RIPv2 MIB RFC 1757 Remote Network Monitoring MIB	RFC 1850 OSPFv2 MIB RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP RFC 2013 SNMPv2 MIB for UDP RFC 2233 Interfaces MIB RFC 2454 IPV6-UDP-MIB RFC 2465 IPv6 MIB	RFC 2466 ICMPv6 MIB RFC 2618 RADIUS Client MIB RFC 2620 RADIUS Accounting MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2737 Entity MIB (Version 2) RFC 2863 The Interfaces Group MIB RFC 2933 IGMP MIB RFC 3813 MPLS LSR MIB
Network management	IEEE 802.1D (STP) RFC 1155 Structure of Management Information RFC 1157 SNMPv1 RFC 1905 SNMPv2 Protocol Operations	RFC 2272 SNMPv3 Management Protocol RFC 2273 SNMPv3 Applications RFC 2274 USM for SNMPv3 RFC 2275 VACM for SNMPv3	RFC 2575 SNMPv3 View-based Access Control Model (VACM) RFC 3164 BSD syslog Protocol
OSPF	RFC 1245 OSPF protocol analysis RFC 1246 Experience with OSPF RFC 1587 OSPF NSSA	RFC 1765 OSPF Database Overflow RFC 1850 OSPFv2 Management Information Base (MIB), traps	RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option RFC 3101 OSPF NSSA
QoS/CoS	IEEE 802.1P (CoS) RFC 2474 DS Field in the IPv4 and IPv6 Headers	RFC 2475 DiffServ Architecture RFC 2597 DiffServ Assured Forwarding (AF)	RFC 2598 DiffServ Expedited Forwarding (EF) RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP

Standards and Protocols
(applies to JG732A model)

Security	IEEE 802.1X Port Based Network Access Control RFC 1321 The MD5 Message-Digest Algorithm RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication	RFC 2138 RADIUS Authentication RFC 2209 RSVP-Message Processing RFC 2246 Transport Layer Security (TLS) RFC 2716 PPP EAP TLS Authentication Protocol	RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 3567 Intermediate System (IS) to IS Cryptographic Authentication
VPN	RFC 2403—HMAC-MD5-96 RFC 2404—HMAC-SHA1-96 RFC 2405—DES-CBC Cipher algorithm RFC 2547 BGP/MPLS VPNs	RFC 2796 BGP Route Reflection—An Alternative to Full Mesh IBGP RFC 2842 Capabilities Advertisement with BGP-4 RFC 2858 Multiprotocol Extensions for BGP-4	RFC 2918 Route Refresh Capability for BGP-4 RFC 3107 Carrying Label Information in BGP-4
IPSec	RFC 1828 IP Authentication using Keyed MD5 RFC 2401 IP Security Architecture RFC 2402 IP Authentication Header RFC 2406 IP Encapsulating Security Payload	RFC 2407—Domain of interpretation RFC 2410—The NULL Encryption Algorithm and its use with IPSec RFC 2411 IP Security Document Roadmap	RFC 2412—OAKLEY RFC 2865—Remote Authentication Dial In User Service (RADIUS)
IKEv1		RFC 2865—Remote Authentication Dial In User Service (RADIUS)	RFC 3748—Extensible Authentication Protocol (EAP)

HPE MSR1000 Router Series accessories

Transceivers	HPE X110 100M SFP LC FX Transceiver (JD102B) HPE X110 100M SFP LC LX Transceiver (JD120B) HPE X110 100M SFP LC LH40 Transceiver (JD090A) HPE X110 100M SFP LC LH80 Transceiver (JD091A) HPE X120 1G SFP LC SX Transceiver (JD118B) HPE X120 1G SFP LC LX Transceiver (JD119B) HPE X125 1G SFP LC LH40 1310nm Transceiver (JD061A) HPE X120 1G SFP LC LH40 1550nm Transceiver (JD062A) HPE X125 1G SFP LC LH70 Transceiver (JD063B) HPE X120 1G SFP LC LH100 Transceiver (JD103A) HPE X120 1G SFP LC BX 10-U Transceiver (JD098B) HPE X120 1G SFP LC BX 10-D Transceiver (JD099B)
Cables	HPE X200 V.24 DTE 3m Serial Port Cable (JD519A) HPE X200 V.24 DCE 3m Serial Port Cable (JD521A) HPE X200 V.35 DTE 3m Serial Port Cable (JD523A) HPE X200 V.35 DCE 3m Serial Port Cable (JD525A) HPE X260 RS449 3m DTE Serial Port Cable (JF825A) HPE X260 RS449 3m DCE Serial Port Cable (JF826A) HPE X260 RS530 3m DTE Serial Port Cable (JF827A) HPE X260 RS530 3m DCE Serial Port Cable (JF828A) HPE X260 Auxiliary Router Cable (JD508A) HPE X260 E1 RJ45 3m Router Cable (JD509A) HPE X260 E1 (2) BNC 75 ohm 3m Router Cable (JD175A) HPE X260 E1 BNC 20m Router Cable (JD514A) HPE X260 E1 RJ45 BNC 75-120 ohm Conversion Router Cable (JD511A) HPE X260 2E1 BNC 3m Router Cable (JD643A) HPE X260 T1 Router Cable (JD518A) HPE X260 SIC-8AS RJ45 0.28m Router Cable (JD642A) HPE X260 E1 RJ45 20m Router Cable (JD517A) HPE X260 mini D-28 to 4-RJ45 0.3m Router Cable (JG263A)
Mounting Kit	HPE 3100/4210-16/-8 PoE Rack Mount Kit (JD323A)

HPE MSR1000 Router Series accessories (continued)

Router Modules	HPE MSR 9-port 10/100Base-T Switch DSIC Module (JD574B) HPE MSR 4-port 10/100Base-T Switch SIC Module (JD573B) HPE MSR 4-port Gig-T Switch SIC Module (JG739A) HPE MSR 1-port GbE Combo SIC Module (JG738A) HPE MSR 1-port 10/100Base-T SIC Module (JD545B) HPE MSR 1-port 100Base-X SIC Module (JF280A) HPE MSR 2-port FXO SIC Module (JD558A) HPE MSR 2-port FXS SIC Module (JD560A) HPE MSR 2-port FXS/1-port FXO SIC Module (JD632A) HPE MSR 1-port 8-wire G.SHDSL (RJ45) DSIC Module (JG191A) HPE MSR 1-port E1/Fractional E1 (75ohm) SIC Module (JD634B) HPE MSR 2-port E1/Fractional E1 (75ohm) SIC Module (JF842A) HPE MSR 1-port T1/Fractional T1 SIC Module (JD538A) HPE MSR 1-port Enhanced Serial SIC Module (JD557A) HPE MSR 2-port Enhanced Sync/Async Serial SIC Module (JG736A) HPE MSR 4-port Enhanced Sync/Async Serial SIC Module (JG737A) HPE MSR 1-port ISDN-S/T SIC Module (JD571A) HPE MSR 16-port Async Serial SIC Module (JG186A) HPE MSR 8-port Async Serial SIC Module (JF281A) HPE MSR 1-port E1/CE1/PRI SIC Module (JG604A) HPE MSR 4-port FXS/1-port FXO DSIC Module (JG189A) HPE Flex Network MSR 4G LTE SIC Module for LTE 700/1700/2100 MHz CDMA UMTS/HSPA+/HSPA/EDGE/GPRS/GSM (JG742B) HPE MSR 4G LTE SIC Module for ATT/LTE 700/1700/2100 MHz and UMTS/HSPA+/HSPA/EDGE/GRPS/GSM (JG743A) HPE MSR 4G LTE SIC Module for Global/LTE 800/900/1800/2100/2600MHz UMTS/HSPA+/HSPA/EDGE/GRPS/GSM (JG744B) HPE MSR HSPA+/WCDMA SIC Module (JG929A) HPE MSR 1-port E1/T1 Voice SIC Module (JH240A)
License	HPE IPS Activation for MSR1000 E-LTU (JH226AAE) HPE DV Essential IPS Filter Service for MSR1000 1yr E-LTU (JH230AAE)

Learn more at
hpe.com/networking

Sign up for updates

4AA5-0754ENW, September 2016, Rev. 5

Hewlett Packard Enterprise

MX 204/240/480/960 SERIES UNIVERSAL ROUTING PLATFORMS DATASHEET

Product Overview

Unrelenting traffic growth is straining traditional service provider and enterprise networks.To accommodate this reality, Juniper's Secure Automated Distributed Cloud solution helps service providers react to changing market conditions and accelerate service delivery requirements. The MX Series, an integral part of this solution:

— is powered by Junos OS and programmable Trio 5 silicon chipset

— delivers powerful routing, switching, security, and services features

— helps operators successfully transform their networks—and their businesses

— in today's hyper-connected world

Product Description

The continuous expansion of mobile, video, and cloud-based services is disrupting traditional networks and impacting the businesses that rely on them. While annual double-digit traffic growth requires massive resource investments to prevent congestion and accommodate unpredictable traffic spikes, capturing return on that investment can be elusive. Emerging trends such as 5G mobility, Internet of Things (IoT) communications, and the continued growth of cloud networking promise even greater network challenges in the near future. The Juniper Networks® MX Series Universal Routing Platform delivers the industry's first end-to-end infrastructure security solution for enterprises as they look to move business-critical applications to public clouds. Delivering features, functionality, and secure services at scale in the 5G era with no compromises, the MX Series is a critical part of the network evolution happening now.

At the same time, traditional operations environments are increasingly challenged to meet consumer and business requirements for rapid service delivery and cloud-like network experiences. Issues related to monitoring and management are placing additional stress on already strained budgets and personnel, and promising technologies like Network Functions Virtualization (NFV) and SDN introduce an entirely new set of operational challenges.

Our hyper-connected world demands more agile, automated, and scalable networks. Now more than ever, network operators need to transform their networks—and their operations environments—to accommodate this reality.

Utilizing state-of-the-art software and hardware innovations, MX Series Universal Routing Platforms are helping network operators worldwide successfully transform their networks and services. Powered by the Juniper Networks Junos® operating system and the programmable Trio chipset, MX Series platforms support a broad set of automation tools and telemetry capabilities that enable a rich set of business- and consumer-oriented services with predictable low latency and wire-rate forwarding at scale, while providing the reliability needed to meet strict service-level agreements (SLAs).

An Agile Family of Cloud-Era Universal Routing Platforms

The MX Series portfolio was designed for agility and built from the ground up to support a universal set of edge applications, helping Juniper customers rapidly respond to evolving business and technical requirements while simplifying operations without sacrificing their current infrastructure investments.

With its massive scale and efficiency, the MX Series is ideal for space- and power-constrained environments. It redefines per-slot economics, enabling customers to do more with less while simplifying network design, reducing OpEx. It also enables the profitable delivery of a broad range of business, residential, mobile, cable, data center, and cloud services while seamlessly supporting traditional and emerging network architectures with adaptive software and pervasive security. The flexibility of the MX Series is enabled by the programmable Trio chipset, which allows MX Series platforms to add support for new features, such as telemetry, without costly hardware upgrades. Additionally, support for the Junos Automation Toolkit and the Juniper Extension Toolkit provide modern programming languages that reduce costs and increase profitability by improving productivity and customization.

This agility is evident in the wide variety of MX Series use cases that have been proven in the world's largest and most demanding networks, including:

- **Business Edge**: MX Series platforms support the broadest range of L2/L2.5/L3 VPN services which, in combination with multilayer, multiprotocol resiliency, ensure that customer SLAs are met under all network conditions.
- **Internet/Peering Gateway**: MX Series platforms support the high performance, reliability, scale, and density needed to efficiently peer with Internet and other service provider networks.
- **Broadband Network Gateway (BNG)**: MX Series platforms offer the highest subscriber density and most sophisticated broadband edge features available in the industry.
- **Universal SDN Gateway**: The MX Series offers a comprehensive solution for interconnecting virtual and physical networks—as well as between virtual networks operating with different technologies—via support for Multiprotocol BGP (MBGP), dynamic tunnels using MPLSoGRE or Virtual Extensible LAN (VXLAN) encapsulation, virtual routing and forwarding (VRF) tables, E-VPNs, and Network Configuration Protocol (NETCONF), along with the ability to send traffic between VRF and global routing tables based on configuration and policy.
- **Data Center and Cloud Edge**: The MX Series is ideal for data center/cloud edge applications, with support for multiple overlay encapsulation methods, including VXLAN, Network Virtualization using Generic Routing Encapsulation (NVGRE), MPLSoUDP, MPLSoGRE, 802.1BR, SR-MPLS, and SR-V6. The MX Series also incorporates data plane security with inline MACsec in the MPC-10E line cards, making it a perfect fit for data center and cloud deployments.
- **Enterprise WAN**: Enterprises and government agencies worldwide use MX Series platforms to build their own overlay network on top of a service provider's Layer 2 or MPLS network, using encapsulation technologies such as MPLSoGRE, VXLAN, and IPsec for secure transport.
- **Universal Metro/Aggregation**: MX Series platforms offer a full suite of routing and switching features, allowing you to choose a deployment model that best fits your business and technical needs. The MX Series can be deployed as IP/IP VPN edge routers, Ethernet VPN (EVPN) and virtual private LAN service (VPLS) provider edge (VPLS-PE) routers, MPLS label-switching (LSR) routers, and as Layer 2 Ethernet switches or Layer 3 IP routers.
- **Mobile Backhaul**: In addition to switching, routing, and security features, MX Series platforms support highly scalable and reliable hardware-based timing that meets the strictest LTE requirements, including Synchronous Ethernet for frequency and the Precision Time Protocol (PTP) for frequency and phase synchronization.

At-a-Glance: MX Series Universal Routing Platforms Comparison

The MX Series portfolio includes a wide range of physical and virtual platforms that share a common architecture and feature set. This enables Juniper customers to select the platform that best addresses their unique business goals and satisfies their scale, density, resiliency, space, power, and value-added service requirements without compromising on quality or features.

Modular MX Series Platforms

MX960, MX480, and MX240 Universal Routing Platforms are modular, chassis-based platforms.

- The MX960 has been proven in the world's largest service provider, cable, mobile, and data center networks, offering 12 Tbps of system capacity in support of business and residential broadband services as well as peering and provider edge applications.

- The MX480 is a modular, 7.5 Tbps-capable router that supports a wide range of cloud, campus, enterprise, data center, service provider, cable, and mobile service core applications.
- The MX240 is a compact, 3 Tbps-capable router ideal for space-constrained cloud, enterprise, data center, service provider, cable, and mobile service core deployments.

The latest generation of line card hardware for the MX960, MX480, and MX240 platforms delivers multi-terabit crypto capabilities with 256-bit encryption complying with AES-GCM encapsulation per RFC4303; AES-GCM encapsulation per RFC4106; AES-GMAC encapsulation per RFC4543; and AES-GMAC (IPv4/v6) encapsulation per RFCs 4302 and 4543. Along with multi-terabit routing, the latest MPC also delivers integrated Layer 2 MACsec features at flexible interface rates of 10GbE, 40GbE, and 100GbE.

Fixed-Configuration MX Series Platforms

The MX204 Universal Routing Platforms is fixed-configuration platforms that supports modular interfaces.

- The MX204 is a space- and power-optimized router delivering ultra-high port density and throughput while consuming just 0.9 W/Gb. It addresses the emerging edge and metro Ethernet networking needs of service providers, mobile, web-scale operators, and MSOs by delivering 400 Gbps of throughput in support of high-density 100GbE, 40GbE, and discrete and breakout 10GbE and 1GbE interfaces—all in a single rack unit.

The following table provides a comparison between the various MX Series modular and fixed-configuration platforms.

Architecture and Key Components

Modular Components for Chassis-Based MX Series Platforms

The modular, chassis-based MX960, MX480, and MX240 share the following components:

- Modular Port Concentrators (MPCs) provide routing, MPLS, switching, inline services, subscriber management, and hierarchical quality of service (HQoS) among many other features. MPCs may also host interfaces directly or via Modular Interface Cards (MICs) that allow users to "mix and match" interface types. Powered by the programmable Trio chipset, MPCs collect and stream telemetry that identifies resource utilization, loss and delay, and other metrics.

Table 1. MX Series Universal Routing Platforms at a Glance

	MX960	MX480	MX240	MX204
Rack units	16	8	5	1
Systems per rack	3	6	9	48
Slots	11 MPCs	6 MPCs	2 MPCs	8 10GbE, 4 100GbE
Per slot capacity	1.5 Tbps	1.5 Tbps	1.5 Tbps	NA
Maximum system throughput[1]	12 Tbps	7.5 Tbps	3 Tbps	400 Gbps
PDH	Yes	Yes	Yes	NA
Sonet/SDH	Yes	Yes	Yes	NA
Maximum 1GbE	440	240	80	24
Maximum 10GbE	528	300	120	24
Maximum 40GbE	132	75	30	4
Maximum 100GbE	120	75	30	4
Maximum 400GbE	24	15	6	NA
10GbE DWDM	88	48	16	8
100GbE DWDM	22	40	4	4

[1]Full duplex maximum system throughput values (to determine half-duplex values, double system throughput)

- Switch Control Boards (SCBs) feature an integrated switch fabric that connects to all slots in the chassis in a nonblocking architecture. The SCBs house the Routing Engine, control power to MPCs, monitor and control system functions such as fan speed and the system front panel, and manage clocking, resets, and boots.
- The Routing Engine (RE) provides the control plane, runs Juniper Networks Junos® operating system, and handles all routing protocol processes as well as the software processes that control MPCs, chassis components, system management, and user access to the router. In addition, unique cryptographic digital identity has been added to the Trusted Platform Module (TPM 2.0), which is embedded in the latest generation of REs. This addition enables device attestation and enhances security. REs communicate with MPCs via dedicated out-of-band management channels.

MPC-10E Line Card

The MPC-10E line card is a key contributor to the service provider transformation in the cloud era when deployed with MX960, MX480, and MX240 platforms in a Juniper Secure Automated Distributed Cloud environment. By providing the underlying network infrastructure with scale, agility, routing innovation, and pervasive security while incorporating universal (10/40/100/400GbE) ports, the MPC-10E protects existing investments with disaggregated software innovation and infinite programmability. Built-in automation enables rapid deployment without disrupting the existing MX960/MX480/MX240 footprint. The MPC-10E line card is powered by Juniper Trio 5 silicon, which enables the benefits highlighted in Table 2.

Table 2. MPC-10E Line Card Benefits at a Glance

Attribute	Benefit
Performance	Triples MX960/MX480/MX240 chassis performance to 1/1.5 Tbps per slot with new SCBE3 fabric, enabling up to 12 Tbps throughput
Universal Interfaces	Reduces interface sparing with multi-rate 10/40/100GbE interfaces
Power Efficiency	Consumes ~0.5 W per gigabit per system level
Inline Data Plane Security	Features AES-256 MACsec line-side encryption
Investment Protection	Backward compatible with existing MPCs and REs: MPC3E/MPC4E/MPC5E/MPC7E, MX-SPC3, MPC2E/3E-NG, and 16x10G MPCs; RE-S-1800 and RE-S-X6 Routing Engine modules
Seamless Deployment	Reuse deployed MX960/MX480/MX240 chassis, power modules, and fan trays

Junos OS

Junos OS is a reliable, high-performance, modular network operating system that is supported across all of Juniper's physical and virtual routing, switching, and security platforms. Junos OS improves network operations and increases service availability, performance, and security with features like low-latency multicast, comprehensive quality of service (QoS), unified in-service software upgrade (unified ISSU), and Junos Continuity, which eliminates the risk and complexity of OS upgrades. With secure programming interfaces, versatile scripting support, and integration with popular orchestration frameworks, Junos OS offers flexible options for DevOps style management that can unlock more value from the network.

The Programmable Trio Chipset

The programmable Trio chipset is Juniper-developed breakthrough silicon technology that is implemented across the MX Series portfolio. Its innovative design improves business economics by enabling a truly converged platform with maximum performance, service agility, and exceptional power and thermal efficiency.

Trio has a programmable forwarding data structure that allows fast microcode changes in the hardware itself, as well as a programmable lookup engine that allows inline service processing. Furthermore, Trio's programmable QoS engine supports coarse and fine-grained queuing to efficiently address the diverse requirements of core, edge, and aggregation use cases.

With its proven extensibility and agility, the programmable Trio chipset helps network operators worldwide successfully address their most complex technical and market challenges, and promises to meet the requirements of emerging applications for many years to come.

Network Edge Services

MX Series platforms can host optionally licensed Junos OS-based network edge services at scale, both inline on MPCs as well as on dedicated service cards. Hosting network edge services on MX Series platforms reduces network cost and complexity by eliminating numerous elements, operating systems, and interconnections.

- MPCs support inline services using the programmable Trio chipset; supported services include flow monitoring, 1:1 Network Address Translation (NAT), port mirroring, generic routing encapsulation (GRE), IP tunneling, logical tunnels, lawful intercept, flow monitoring, and video monitoring.
- The MS-MPC and the MS-MIC provide dedicated processing for compute-intensive services such as carrier-grade NAT (CGNAT), IPsec, stateful firewall, deep packet inspection, flow monitoring, and load balancing.
- The MX-SPC3 provides security services such as carrier-grade NAT (CGNAT), IPsec, stateful firewall, deep packet inspection, IDS, traffic load balancing, Web filtering, and DNS sinkhole.

MX Series Platform/Feature Matrix

		MX960	MX480	MX240	MX204
Security	Firewall filters/ACLs	✓	✓	✓	✓
	DDoS—control plane	✓	✓	✓	✓
	DDoS—FlowSpec	✓	✓	✓	✓
	Stateless filters L2-L4	✓	✓	✓	✓
	Stateful services	✓	✓	✓	✓

		MX960	MX480	MX240	MX204
Inline Services	GRE reassembly	✓	✓	✓	✓
	1:1 NAT	✓	✓	✓	✓
	Flow monitoring	✓	✓	✓	✓
	Video monitoring	✓	✓	✓	✓
	Lawful intercept	✓	✓	✓	✓
	Mirroring	✓	✓	✓	✓
	Corero SmartWall Threat Defense Director	✓	✓	✓	✓
	SecIntel Threat Intelligence	✓	✓	✓	No
Service Card Supported Services[6]	Deep packet inspection	✓	✓	✓	No
	CGNAT	✓	✓	✓	No
	Flow monitoring	✓	✓	✓	No
	Server traffic load balancing[7]	✓	✓	✓	No
	IPsec	✓	✓	✓	No
	Stateful firewall	✓	✓	✓	No
	HTTP header manipulation	✓	✓	✓	No
	Web filtering	✓	✓	✓	No
	DNS sinkhole	✓	✓	✓	No
	Intrusion detection system	✓	✓	✓	✓
Resiliency	Redundant RE	✓	✓	✓	No
	Unified ISSU	✓	✓	✓	No
	Nonstop active routing (NSR)	✓	✓	✓	No
	Fast restoration	✓	✓	✓	✓
	Operation, Administration, and Maintenance (OAM)	✓	✓	✓	✓
System Virtualization	Enhanced SLA and queuing	✓	✓	✓	✓
	Junos Fusion Edge (AD)	✓	✓	✓	✓
	Logical systems	✓	✓	✓	✓
	Virtual router/switch	✓	✓	✓	✓
	Path Computation Element Protocol (PCEP)	✓	✓	✓	✓
	OpenConfig	✓	✓	✓	✓
	YANG data modeling	✓	✓	✓	✓
	Juniper Extension Toolkit	✓	✓	✓	✓

[6]Service Card supported services are available via optional software license and require an MX-SPC3, MS-MPC, or MS-MIC.
[7]For more information, see https://www.juniper.net/documentation/en_US/junos/topics/concept/tdf-tlb-overview.html
[8]Features are supported as part of the Broadband Gateway (BNG) solution
[9]Flow Monitoring leverages the MS-MPC and MS-MIC service cards. The MX-SPC3 is not required to support Flow Monitoring as it runs inline on the MPC's

Key Features and Benefits

Unmatched Network Availability

MX Series platforms ensure network and service availability with a broad set of multilayered physical, logical, and protocol-level resiliency features, including Juniper's Virtual Chassis technology, which supports chassis-level redundancy while enabling users to manage two routers as a single element. Additionally, a multichassis link aggregation group (MC-LAG) implementation supports stateful chassis, card, and port redundancy, as well as subscriber and session persistence.

Application Aware Networking

MX Series platforms use deep packet inspection to detect applications, and they consult with user-defined policies to determine traffic treatment on a per-application basis, enabling highly customized and differentiated services at scale. Working in conjunction with Juniper Networks Contrail® Cloud Platform ™, MX Series routers can also steer into complex service chains and stream granular data to analytics engines and back-office systems to permit real-time charging and end-user engagement at the application and content level.

Junos Continuity and Unified In-Service Software Upgrade (Unified ISSU)

Junos Continuity and unified ISSU features remove the downtime risks associated with implementing new hardware or upgrading operating systems.

- Junos Continuity eliminates OS upgrades and system reboots when adding new hardware to MX Series platforms; a plug-in package provides the drivers and support files needed to bring the hardware online.

- Unified ISSU reduces the risks associated with OS upgrades by enabling upgrades between two different Junos OS releases (major or minor) with no control plane disruption and minimal traffic disruption on the forwarding plane.

Junos Telemetry Interface

The Junos Telemetry Interface feature streams component-level data to monitoring, analytics, performance management, and visualization tools as well as to Path Computation Elements such as Juniper Networks NorthStar Controller. Analytics derived from this streaming telemetry can identify current and trending congestion, resource utilization, traffic volume, and buffer occupancy, which can be used to make informed decisions on network design and investments.

Integrated Timing

MX Series platforms support highly scalable and reliable hardware-based timing that meets the strictest LTE requirements, including Synchronous Ethernet for frequency, and the Precision Time Protocol (PTP) for frequency and phase synchronization. Synchronous Ethernet and PTP can be combined in a "hybrid" mode to achieve the highest level of frequency (10 ppb) and phase (< 1.5 uS) accuracy required for LTE-Advanced, eliminating the need for external clocks.

Junos Fusion Provider Edge

Junos Fusion Provider Edge enables MX Series platforms to act as aggregation devices for the Juniper Networks EX4300 Ethernet Switch and QFX5100 line of data center switching platforms acting as satellite devices while appearing to management as a single, port-dense device managed by a single IP address. Junos Fusion Provider Edge significantly expands the number of network interfaces on the MX Series router while keeping operations simple.

Automated Support and Prevention

Juniper's Automated Support and Prevention consists of an ecosystem of tools, applications, and systems that simplify and streamline operations, delivering operational efficiency, reducing downtime, and increasing your network's ROI running Junos OS. Automated Support and Prevention brings operational efficiency by automating several time-consuming tasks such as incident management, inventory management, proactive bug notification, and on-demand End-of-Life/End-of-Support/End-of-Engineering (EOL/EOS/EOE) reports. The Junos Space® Service Now and Service Insight service automation tools are standard entitlements of all Juniper Care contracts.

Junos Automation Toolkit and Juniper Extension Toolkit

Included in Junos OS software, the Junos Automation Toolkit is a suite of tools supported on all Juniper Networks switches, routers, and security devices. These tools, which leverage the native XML capabilities of Junos OS, include commit scripts, op scripts, event policies and event scripts, and macros that help automate operational and configuration tasks. Additionally, the platform-independent Juniper Extension Toolkit provides a modern programming tool kit that includes support for:

- OpenConfig/YANG
- gRPC, Thrift, NETCONF
- JSON/XML
- API support for all modern programming languages
- Rich on-box scripting support using Python
- REST APIs

Together, Junos OS automation and programmability features simplify complex configurations and reduce the potential for configuration errors. They also save time by automating operational and configuration tasks, speed troubleshooting, and maximize network uptime by warning operators of potential problems and automatically responding to system events.

Security Intelligence for the Edge

The MX960, MX480, and MX240 can be used for advanced threat prevention when deployed as edge routers, further extending security coverage to applications and infrastructure.

Using Juniper's SecIntel capabilities, these MX Series routers offer another layer of network security by identifying and blocking command and control traffic discovered by Juniper Threat Labs and other industry-leading threat feeds, as well as by utilizing custom blacklists and whitelists at a network hardware level. This feature makes your MX Series router an information security enforcement point without having to invest in additional hardware.


MX960


MX480


MX204


MX240

Specifications

		MX960	MX480	MX240	MX204
Layout	System capacity	12 Tbps	7.5 Tbps	3 Tbps	400 Gbps
	Slot orientation	Vertical	Horizontal	Horizontal	NA
	Mounting	Front or center	Front or center	Front or center	Front or center
Physical Specification	Dimensions (W x H x D)	17.37 x 27.75 x 23 in (44.11 x 70.49 x 58.42 cm)	17.45 x 14 x 24.5 in (44.3 x 35.6 x 62.2 cm)	17.45 x 8.71 x 24.5 (44.3 x 22.1 x 62.2 cm)	17.6 x 1.75 x 18.7 in (44.7 x 4.45 x 47.5 cm)
	Weight fully loaded	334 lb/151.6 kg	180 lbs/81.6 kg	130 lb/59 kg	23.15 lb/10.5 kg
	Weight unloaded	150 lbs/68.1 kg	65.5 lbs/29.7 kg	52 lbs/23.6 kg	17 lb/7.71 kg
Routing Engine	Default memory	2x16 MB NOR flash storage; 64 GB of DDR4 RAM; 2x50 GB SSD	2x16 MB NOR flash storage; 64 GB of DDR4 RAM; 2x50 GB SSD	2x16 MB NOR flash storage; 64 GB of DDR4 RAM; 2x50 GB SSD	32GB DDR4; 2x100 GB SSD
	Number of cores	6 cores	6 cores	6 cores	8 cores
Redundancy	Components	Power supplies, REs, fans	Power supplies, REs, fans	Power supplies, REs, fans	Power supplies and fans
Environmental	Air flow	Front to back	Side to side	Side to side	Front to back
	Operating temperature	32° to 115° F (0° to 46° C) at sea level	32° to 115° F (0° to 46° C) at sea level	32° to 115° F (0° to 46° C) at sea level	32° to 115° F (0° to 46° C)
	Operating humidity	5% to 90%	5% to 90%	5% to 90%	5% to 90%
	Operating altitude	10,000 ft (3048 m)	10,000 ft (3048 m)	10,000 ft (3048 m)	6,000 ft (1900 m)
Certifications	NEBS	- GR-1089-Core EMC and Electrical Safety - Common Bonding Network (CBN) - National Electrical Code (NEC) - GR-63-Core Physical Protection	- GR-1089-Core EMC and Electrical Safety - Common Bonding Network (CBN) - National Electrical Code (NEC) - GR-63-Core Physical Protection	- GR-1089-Core EMC and Electrical Safety - Common Bonding Network (CBN) - National Electrical Code (NEC) - GR-63-Core Physical Protection	- GR-1089-Core EMC and Electrical Safety - Common Bonding Network (CBN) - National Electrical Code (NEC) - GR-63-Core Physical Protection

Ordering Information

MX204 Base Product Bundles

Product	Product Number	Description
MX204	MX204-HW-BASE	MX204 chassis with 3 fan trays and 2 power supplies. MX204 integrated SKU with base HW + standard Junos SW, Perpetual
	MX204-HWBASE-AC-FS	MX204 chassis with 3 fan trays and 2 power supplies, R mode MX204 Fixed AC System - HW and standard Junos; feature right to use must be ordered separately
	MX204-HWBASE-DC-FS	MX204 chassis with 3 fan trays and 2 power supplies, IR mode. MX204 Fixed DC System - HW and standard Junos; feature right to use must be ordered separately

MX204 Chassis

Product	Product Number	Description
MX204	JNP204-CHAS	MX204 chassis, spare

MX204 Power Supply

Product	Product Number	Description
MX204	JPSU-650W-AC-AO	MX204 AC power supply, spare
	JPSU-650W-DC-AFO	MX204 DC power supply, spare

MX204 Fan Trays

Product	Product Number	Description
MX204	JNP-FAN-1RU	MX204 fan tray

MX240, MX480, and MX960 Base Bundles

Product	Product Number	Description
MX240	MX240BASE-AC-HIGH	4 slot MX240 base chassis with 1 AC power supply, 1 SCB
	MX240BASE-AC-LOW	4 slot MX240 base chassis with 2 AC power supplies, 1 SCB
	MX240BASE3-DC	4 slot MX240 base 3 chassis, DC power
	MX240BASE-DC	4 slot MX240 base chassis with 1 fan tray, 1 DC power supply, 1 SCB
	MX240BASE3-ACH	4 slot MX240 base 3 chassis, highline AC power
	MX240BASE3-ACL	4 slot MX240 base chassis, lowline AC power
MX480	MX480BASE3-AC	8 slot MX480 base bundle, AC power
	MX480BASE-AC	8 slot MX480 AC base chassis, 1 fan tray, 3 AC power supplies, 1 SCB, 1 RE
	MX480BASE3-DC	8 slot MX480 base 3 chassis, DC power
	MX480BASE-DC	8 slot MX480 base chassis with 1 fan tray, 2 DC power supplies, 1 SCB, 1 RE
MX960	MX960BASE3-AC	14 slot MX960 base 3 chassis, AC power
	MX960BASE-AC	14 slot MX960 base chassis with 2 fan trays, 3 AC power supplies, 2 SCBs, 1 RE
	MX960BASE3-AC-ECM	14 slot MX960 base 3 chassis with AC power and extended cable manager
	MX960BASE-AC-ECM	14 slot MX960 base chassis with AC power and extended cable manager
	MX960BASE3-DC	14 slot MX960 base 3 chassis, DC power
	MX960BASE-DC	14 slot MX960 base chassis with 2 fan trays, 2 DC power supplies, 2 SCBs, 1 RE
	MX960BASE3-DC-ECM	14 slot MX960 base 3 chassis with DC power and extended cable manager
	MX960BASE-DC-ECM	14 slot MX960 base chassis with DC power extended cable manager

MX240, MX480 and MX960 Premium Bundles

Product	Product Number	Description
MX240	MX240-PREMIUM2-AC-HIGH	4 slot MX240 premium 2 chassis with midplane, redundant RE, SCBEs, highline AC power
	MX240-PREMIUM2-AC-LOW	4 slot MX240 premium 2 chassis with midplane, redundant RE, SCBEs, lowline AC powe
	MX240-PREMIUM2-DC	4 slot MX240 premium 2 chassis with midplane, redundant RE, SCBEs, DC power
	MX240-PREMIUM3-ACH	4 slot MX240 premium 3 chassis with enhanced midplane, redundant RE, SCBEs, highline AC power
	MX240-PREMIUM3-ACL	4 slot MX240 premium 3 chassis with enhanced midplane, redundant RE, SCBEs, lowline AC power
	MX240-PREMIUM3-DC	4 slot MX240 premium 3 chassis with enhanced midplane, redundant RE, SCBEs, DC power
MX480	MX480-PREMIUM2-AC	8 slot MX480 premium 2 chassis with midplane, redundant RE, SCBEs, AC power
	MX480-PREMIUM2-DC	8 slot MX480 premium 2 chassis with midplane, redundant RE, SCBEs, DC power
	MX480-PREMIUM3-AC	8 slot MX480 premium 3 chassis with enhanced midplane, redundant RE, SCBEs, AC power
	MX480-PREMIUM3-DC	8 slot MX480 premium 3 chassis with enhanced midplane, redundant RE, SCBEs, DC power
MX960	MX960-PREMIUM2-AC-ECM	14 slot MX960 premium 2 chassis with midplane, redundant Routing Engine, SCBEs, AC power, and extended cable manager
	MX960-PREMIUM2-DC-ECM	14 slot MX960 premium2 chassis with midplane, redundant Routing Engine, SCBEs, DC power, and extended cable manager
	MX960-PREMIUM3-AC-ECM	14 slot MX960 premium 3 chassis with enhanced midplane, redundant Routing Engine, SCBEs, AC power, and extended cable manager
	MX960-PREMIUM3-DC-ECM	14 slot MX960 premium 3 chassis with enhanced midplane, redundant Routing Engine, SCBEs, DC power, and extended cable manager
	MX960-PREMIUM2-AC	14 slot MX960 premium 2 chassis with midplane, redundant Routing Engine, SCBEs, AC power
	MX960-PREMIUM2-DC	14 slot MX960 premium 2 chassis with midplane, redundant Routing Engine, SCBEs, DC power
	MX960-PREMIUM3-AC	14 slot MX960 premium 3 chassis with enhanced midplane, redundant Routing Engine, SCBEs, AC
	MX960-PREMIUM3-DC	14 slot MX960 premium 3 chassis with enhanced midplane, redundant Routing Engine, SCBEs, DC power

MX240, MX480, and MX960 Chassis

Base Unit	MX240	MX480	MX960
DC Chassis	MX240BASE-DC, MX240BASE3-DC	MX480BASE-DC, MX480BASE3- DC	MX960BASE3-DC; MX960BASE-DC
AC Chassis	MX240BASE-AC, MX240BASE3- ACH, MX240BASE3-ACL	MX480BASE-AC, MX480BASE3-AC	MX960BASE3-AC; MX960BASE-AC

MX240, MX480, and MX960 Power Supplies

Product	Product Number	Description
MX240 MX480	PWR-MX480-2400-DC-BB	MX480/MX240 2400W DC P/S, base bundle
	PWR-MX480-2400-DC-R	MX480/MX240 2400W DC P/S, redundant
	PWR-MX480-2400-DC-S	MX480/MX240 2400W DC P/S, spare
	PWR-MX480-2520-AC-BB	MX480/MX240 2520W AC P/S, base bundle
	PWR-MX480-2520-AC-R	MX480/MX240 2520W AC P/S, redundant
	PWR-MX480-2520-AC-S	MX480/MX240 2520W AC P/S, spare

Product	Product Number	Description
MX960	MX960-PSM-5K-AC-BB	MX960 5000W AC power supply, base bundle
	MX960-PSM-5K-AC-R	MX960 5000W AC power supply, redundant
	MX960-PSM_5K-AC-S	MX960 5000W AC power supply, spare
	MX960-PSM-HV-BB	MX960 High Voltage Power, base bundle
	MX960-PSM-HV-R	MX960 High Voltage Power, redundant
	MX960-PSM-HV-S	MX960 High Voltage Power, spare
	PWR-MX960-4100-AC-BB	MX960 4100W AC power supply, base bundle
	PWR-MX960-4100-AC-R	MX960 4100W AC power supply, redundant
	PWR-MX960-4100-AC-S	MX960 4100W AC power supply, spare
	PWR-MX960-4100-DC-BB	MX960 4100W DC power supply, base bundle
	PWR-MX960-4100-DC-R	MX960 4100W DC power supply, redundant
	PWR-MX960-4100-DC-S	MX960 4100W DC power supply, spare

MPCs

Product Number	Description
MPC10E-10C-P-BASE	Fixed 8xQSFP28 multirate ports (10/40/100GbE) plus 2xQSFP56-DD multirate ports (10/40/100/400GbE) line card bundle with standard Junos software, perpetual
MPC10E-15C-P-BASE	Fixed 12xQSFP28 multirate ports (10/40/100GbE) plus 3xQSFP56-DD multirate ports (10/40/100/400GbE) line card bundle with standard Junos software, perpetual
MPC7E-10G	Fixed 40x10GbE line card bundle with full-scale L2/L2.5 and reduced scale L3 features; optional license permits up to 32,000 queues with HQoS
MPC7E-10G-RB	Fixed 40x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3, and L3VPN features
MPC7E-10G-I-RB	Fixed 40x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3 features, and up to 16 L3VPN instances
MPC7E-MRATE	Fixed 12xQSFP line card bundle for the MPC7-MRATE only; all ports support 4x10GbE and 40GbE, and 4 ports support 100GbE (QSFP 28), with full-scale L2/L2.5 and reduced scale L3 features; optional license permits up to 32,000 queues with HQoS
MPC7E-MRATE-RB	Fixed 12xQSFP line card bundle for the MPC7-MRATE only; all ports support 4x10GbE and 40GbE, and 4 ports support 100GbE (QSFP 28); includes full-scale L2/L2.5, L3, and L3VPN features
MPC7E-MRATE-I-RB	Fixed 12xQSFP line card bundle for the MPC7-MRATE only; all ports support 4x10GbE and 40GbE, and 4 ports support 100GbE (QSFP 28); includes full-scale L2/L2.5 and L3 features and up to 16 L3VPN instances
MPC7E-MRATE-Q	Fixed 12xQSFP line card for the MPC7-MRATE only; all ports support 4x10GbE and 40GbE, and 4 ports support 100GbE (QSFP 28) with HQoS; supports 1 million queues and 128,000 sessions; with full-scale L2/L2.5 and reduced scale L3 features
MPC7E-MRATE-Q-RB	Fixed 12xQSFP line card bundle; all ports support 4x10GbE and 40GbE, and 4 ports support 100GbE (QSFP 28) with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3, and L3VPN features
MPC7E-MRATE-Q-I-RB	Fixed 12xQSFP line card bundle for the MPC7-MRATE only; all ports support 4x10GbE and 40GbE, and 4 ports support 100GbE (QSFP 28) with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3 features, and up to 16 L3VPN instances
MPC5E-100G10G	Fixed 2x100GbE and 4x10GbE line card bundle with full-scale L2/L2.5 and reduced scale L3 features; optional license permits up to 32,000 queues with HQoS
MPC5E-100G10G-IRB	Fixed 2x100GbE and 4x10GbE line card bundle with full-scale L2/L2.5, L3 features and up to 16 L3VPN instances; optional license permits up to 32,000 queues with HQoS
MPC5E-100G10G-RB	Fixed 2x100GbE and 4x10GbE line card bundle with full-scale L2/L2.5, L3, and L3VPN features; optional license permits up to 32,000 queues with HQoS
MPC5E-40G10G	Fixed 6x40GbE or 24x10GbE line card bundle with full-scale L2/L2.5 and reduced scale L3 features; optional license permits up to 32,000 queues with HQoS
MPC5E-40G10G-IRB	Fixed 6x40GbE or 24x10GbE line card bundle with full-scale L2/L2.5, L3 features and up to 16 L3VPN instances; optional license permits up to 32,000 queues with HQoS
MPC5E-40G10G-RB	Fixed 6x40GbE or 24x10GbE line card bundle with full-scale L2/L2.5, L3, and L3VPN features; optional license permits up to 32,000 queues with HQoS
MPC5EQ-100G10G	Fixed 2x100GbE and 4x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5 and reduced scale L3 features
MPC5EQ-100G10G-IRB	Fixed 2x100GbE and 4x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3 features, and up to 16 L3VPN instances
MPC5EQ-100G10G-RB	Fixed 2x100GbE and 4x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3, and L3VPN features
MPC5EQ-40G10G	Fixed 6x40GbE or 24x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5 and reduced scale L3 features
MPC5EQ-40G10G-IRB	Fixed 6x40GbE or 24x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3 features, and up to 16 L3VPN instances
MPC5EQ-40G10G-RB	Fixed 6x40GbE or 24x10GbE line card bundle with HQoS; supports 1 million queues and 128,000 sessions; includes full-scale L2/L2.5, L3, and L3VPN features
MPC4E-3D-2GE	Fixed 2x100GbE and 8x10GbE line card bundle with full-scale L2/L2.5 and reduced scale L3 feature
MPC4E-3D-32XGE-SFPP	Fixed 32x10GbE line card bundle with full-scale L2/L2.5 and reduced scale L3 features
MPC4E-3D-2CGE-8XGE-IRB	Fixed 2x100GbE and 8x10GbE line card bundle with full-scale L2/L2.5, L3 features; up to 16 L3VPNs per MPC
MPC4E-3D-32XGE-IRB	Fixed 32x10GbE SFPP line card bundle with full-scale L2/L2.5, L3 features; up to 16 L3VPNs per MPC
MPC4E-3D-2CGE8XGE-RB	Fixed 2x100GbE and 8x10GbE line card bundle with full-scale L2/L2.5, L3, and L3VPN features
MPC4E-3D-32XGE-RB	Fixed 32XGbE small form-factor pluggable transceiver (SFP) line card bundle with full-scale L2/L2.5, L3, and L3VPN features
MX-MPC3E-3D	MPC3 with support for 100GbE, 40GbE, and 10GbE interfaces, L2.5 features, optics sold separately
MX-MPC3E-3D-R-B	MPC3E with support for 100GbE, 40GbE, and 10GbE interfaces; includes full-scale L2, L3, L3VPN features; optics sold separately
MPC3E-3D-NG	Next-generation MPC3E with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 and reduced scale L3 features; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by MPC1E, MPC2E, and MPC3E
MPC3E-3D-NG-IR-B	Next-generation MPC3E line card bundle with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 and L3 features and up to 16 L3VPNs per MPC; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by the MPC1E, MPC2E, and MPC3E
MX-MPC3E-3D-R-B	MPC3E with support for 100GbE, 40GbE, and 10GbE interfaces; includes full-scale L2, L3, L3VPN features; optics sold separately

Product Number	Description
MPC3E-3D-NG	Next-generation MPC3E with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 and reduced scale L3 features; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by MPC1E, MPC2E, and MPC3E
MPC3E-3D-NG-IR-B	Next-generation MPC3E line card bundle with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 and L3 features and up to 16 L3VPNs per MPC; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by the MPC1E, MPC2E, and MPC3E
MPC3E-3D-NG-R-B	Next-generation MPC3E line card bundle with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3, and L3VPN features; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by the MPC1E, MPC2E, and MPC3E
MPC3E-3D-NG-Q	Next-generation MPC3E with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 features, reduced scale L3 features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by the MPC1E, MPC2E, and MPC3E
MPC3E-3D-NG-Q-IR-B	Next-generation MPC3E line card bundle with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3, and up to 16 L3VPN features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by the MPC1E, MPC2E, and MPC3E
MPC3E-3D-NG-Q-R-B	Next-generation MPC3E line card bundle with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 features, L3 features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by the MPC1E, MPC2E, and MPC3E
MPC-3D-16XGE-SFPP	Fixed 16x10GbE line card bundle with L2.5 features
MPC-3D-16XGE-SFPP-R-B	Fixed 16x10GbE line card bundle with full-scale L2/L2.5 and L3 features
MPC2E-3D-NG	Next-generation MPC2E with upgraded CPU and memory; offers full feature parity with the MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5 and reduced scale L3 features; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-IR-B	Next-generation MPC2E line card bundle with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3 features, and up to 16 L3VPNs per MPC; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-R-B	Next-generation MPC2E line card bundle with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3, and L3VPN features; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-Q	Next-generation MPC2E with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, reduced scale L3 features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-Q-IR-B	Next-generation MPC2E line card bundle with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3, and up to 16 L3VPN features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-R-B	Next-generation MPC2E line card bundle with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3, and L3VPN features; flexible queuing option enables HQoS support with up to 32,000 total queues; supports all MICs supported by MPC1E and MPC2E

Product Number	Description
MPC2E-3D-NG-Q	Next-generation MPC2E with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, reduced scale L3 features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-Q-IR-B	Next-generation MPC2E line card bundle with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3, up to 16 L3VPN features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by MPC1E and MPC2E
MPC2E-3D-NG-Q-R-B	Next-generation MPC2E line card bundle with upgraded CPU and memory; offers full feature parity with MPC1E, MPC2E, and MPC3E; includes full-scale L2/L2.5, L3 features, and HQoS with up to 512,000 queues per slot; supports all MICs supported by MPC1E and MPC2E
MX-MPC2-3D	MPC2 with port queuing; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2-3D-EQ	MPC2 line card bundle with per-IFL HQoS, 512,000 queues; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2-3D-EQ-R-B	MPC2 line card bundle with per-IFL HQoS, 512,000 queues; includes full-scale L3, L2, and L2.5 features
MX-MPC2-3D-Q	MPC2 line card bundle with per-IFL HQoS, 256,000 queues (max 128,000 egress); includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2-3D-Q-R-B	MPC2 line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC2-3D-R-B	MPC2 line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC2E-3D-R-B	Enhanced MPC2 line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC2E-3D	Enhanced MPC2 with port queuing; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-EQ	Enhanced MPC2 with per-IFL HQoS, 512,000 queues; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-EQ-R-B	Enhanced MPC2 line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC2E-3D-P	Enhanced MPC2 with 1588v2, port queuing; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-P-Q-B	Enhanced MPC2 line card bundle; includes 1588v2, per-IFL HQoS, 256,000 queues (maximum 128,000 egress), full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-P	Enhanced MPC2 with 1588v2, port queuing; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-P-Q-B	Enhanced MPC2 line card bundle; includes 1588v2, per-IFL HQoS, 256,000 queues (maximum 128,000 egress), full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-Q	Enhanced MPC2 line card bundle; includes per-IFL HQoS, 256,000 queues (maximum 128,000 egress); includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC2E-3D-Q-R-B	Enhanced MPC2E line card bundle; includes per-IFL HQoS, 256,000 queues (maximum 128,000 egress); includes full-scale L3, L2, and L2.5 features
MX-MPC1-3D	MPC1 with port queuing; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC1-3D-Q	MPC1 with per-IFL HQoS, 128,000 queues (maximum 64,000 egress); includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC1-3D-Q-R-B	MPC1 line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC1-3D-R-B	MPC1 line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC1E-3D	Enhanced MPC1 with port queuing; includes full-scale L2/L2.5 and reduced scale L3 features
MX-MPC1E-3D-Q	Enhanced MPC1 with per-IFL HQoS, 128,000 queues (maximum 64,000 egress); includes full-scale L2/L2.5 and reduced scale L3 features

Product Number	Description
MX-MPC1E-3D-Q-R-B	Enhanced MPC1 with per-IFL HQoS, 128,000 queues (maximum 64,000 egress) line card bundle; includes full-scale L3, L2, and L2.5 features
MX-MPC1E-3D-R-B	Enhanced MPC1 line card bundle; includes full-scale L3, L2, and L2.5 features
MS-MPC-128	Multiservices MPC supports a variety of optionally licensed applications, including stateful firewall, carrier-grade NAT, IPsec, and deep packet inspection (DPI; each purchased separately
MX-SPC3	Security services card supports a variety of optionally licensed applications, including stateful firewall, carrier-grade NAT, IPsec, deep packet inspection (DPI), IDS, traffic load balancing, Web filtering, and DNS sinkhole

Modular Interface Cards

Product Number	Description
MIC3-3D-10XGE-SFPP	MIC with 10x10GbE small form-factor pluggable plus transceiver (SFP+) interface; optics sold separately
MIC3-3D-1X100GE-CFP	MIC with 1x100GbE C form-factor pluggable transceiver (CFP) interface; optics sold separately
MIC3-3D-1X100GE-CXP	MIC with 1x100GbE 100-gigabit small form-factor pluggable transceiver (CXP) interface; optics sold separately
MIC3-100G-DWDM	MIC with 1x100GbE OTU4 dense wavelength-division multiplexing (DWDM) PIC, DP-QPSK, full C-band tunable, GFEC, HGFEC, SDFEC; requires MPC3E or MPC3E-NG; optics sold separately
MIC3-3D-2X40GE-QSFPP	MIC with 2x40GbE quad small form-factor pluggable plus transceiver (QSFP+) interface; optics sold separately
MIC-3D-1CHOC48	1 port channelized OC48/channelized STM16 (down to DS0) MIC
MIC-3D-1OC192-XFP	1 port OC192/STM64 MIC
MIC-3D-20GE-SFP	20x10/100/1000 MIC for MX Series; requires optics sold separately
MIC-3D-2XGE-XFP	2x10GbE MIC for MX Series; requires optics sold separately
MIC-3D-40GE-TX	40x10/100/1000 RJ-45 full height MIC (fixed optics)
MIC-3D-4CHOC3-2CHOC12	4 port channelized OC3/2 port channelized OC12 (down to DS0) MIC
MIC-3D-4COC3-1COC12-CE	Multi-rate circuit emulation MIC; 4 port channelized OC3/STM1 (to DS0) or 1 port channelized OC12/STM4 (to DS0)
MIC-MACSEC-20GE	2x10GbE/20x10GbE MACsec MIC for MX104/ MX240/ MX480/MX960, supports both 128b AES and 256b AES MACsec
MS-MIC-16	Multiservices MIC supports a variety of optionally licensed applications, including stateful firewall, carrier-grade NAT, IPsec, and deep packet inspection (DPI); ; each purchased separately

Routing Engines

Product Number	Description
RE-S-X6-64G-BB	6 Core 2.0 GHz CPU and 64 GB memory, base bundle
RE-S-X6-64G-S	6 Core 2.0 GHz CPU and 64 GB memory, spare
RE-S-X6-64G-R	6 Core 2.0 GHz CPU and 64 GB memory, redundant RE
RE-S-X6-64G-LT-S	6 Core 2.0 GHz CPU with 64 GB memory, limited encryption version, spare
RE-S-X6-64G-LT-BB	6 Core 2.0 GHz CPU with 64 GB memory, limited encryption version, base bundle
RE-S-X6-64G-LT-R	6 Core 2.0 GHz CPU with 64 GB memory, limited encryption version, redundant
RE-S-X6-128G-S-BB	6 Core 2.0 GHz CPU with 128 GB memory, base bundle
RE-S-X6-128G-S-S	6 Core 2.0 GHz CPU with 128 GB memory, spare
RE-S-X6-128G-S-R	6 Core 2.0 GHz CPU with 128 GB memory, redundant
RE-S-1300-2048-BB	1.3 GHz CPU and 2 GB memory, base bundle
RE-S-2000-4096-UPG-BB	2 GHz CPU and 4 GB memory, base bundle
RE-S-1300-2048-R	1.3 GHz CPU and 2 GB memory, redundant
RE-S-2000-4096-R	2 GHz CPU and 4 GB memory, redundant
RE-S-1800X2-8G-R	Dual-core 1.8 GHz CPU and 8 GB memory, redundant
RE-S-1800X2-16G-R	Dual-core 1.8 GHz CPU and 16 GB memory, redundant
RE-S-1800X4-8G-R	Quad-core 1.8 GHz CPU and 8 GB memory, redundant
RE-S-1800X4-16G-R	Quad-core 1.8 GHz CPU and 16 GB memory, redundant
RE-S-1800X2-8G-UPG-BB	Dual-core 1.8 GHz CPU and 8 GB memory, upgrade for base bundle
RE-S-1800X2-16G-UPG-BB	Dual-core 1.8 GHz CPU and 16 GB memory, upgrade for base bundle
RE-S-1800X4-8G-UPG-BB	Quad-core 1.8 GHz CPU and 8 GB memory, upgrade for base bundle
RE-S-1800X4-16G-UPG-BB	Quad-core 1.8 GHz CPU and 16 GB memory, upgrade for base bundle
RE-S-1800X4-32G-BB	Quad core 1.8GHz CPU with 32 GB memory, base bundle
RE-S-1800X4-32G-R	Quad core 1.8GHz CPU with 32 GB memory, redundant
RE-S-1800X4-32G-S	Quad core 1.8GHz CPU with 32 GB memory, spare
RE-S-1800X4-32G-UB	Quad core 1.8GHz CPU with 32 GB memory, upgrade for base bundle
RE-S-1800X4-32G-WS	Quad core 1.8GHz CPU with 32 GB memory, worldwide version

Switch Control Board

Product Number	Description
SCB-MX960-BB	SCB for MX240, MX480, and MX960
SCBE-MX-BB	Enhanced Switch Control Board (SCBE) for MX240, MX480, and MX960
SCBE2-MX-BB	SCBE for MX240, MX480, and MX960
SCBE3-MX-BB	1.5 T fabric card for MX240, MX480, and MX960

Broadband Network Gateway (BNG) Licensing

Subscriber Access Feature Pack Licenses

One Subscriber Access (SA) license is required per chassis, and provides:

- Per-subscriber RADIUS accounting (time- and volume-based)
- RADIUS-based authentication and authorization
- Subscriber configuration via client profiles at subscriber login
- RADIUS and/or SDX-based address (pool) management
- Static and dynamic IP management
- Dynamic auto-sensed VLANs

Product Number	Description
S-SA-FP2	Subscriber Access feature pack license for MX240, MX480, MX960, MX2010, and MX2020

Subscriber Services Management Feature Pack Licenses

Subscriber Services Management licenses are optional additions to Subscriber Access licenses that offer:

- Per-service RADIUS accounting (time- and volume-based)
- Service profile activation/deactivation at subscriber login via RADIUS grants/access accepts (services activation/deactivation VSAs); or change existing sessions via RADIUS COA/RID or Session and Resource Control (SRC)
- Parameterization of service profiles
- ANCP QoS adjustment based on sync rate via Access Node Control Protocol (ANCP)

Product Number	Description
S-SSM-FP	Subscriber Service Management feature pack license (RADIUS/SRC-based service activation/deactivation); per-service accounting features for subscribers, for MX240, MX480, MX960, MX2010, and MX2020
S-SSP-FP	Subscriber Traffic Lawful Intercept feature pack License, for MX240, MX480, MX960, MX2010, and MX2020
S-BB-NASREQ	Junos Broadband Policy Enforcement feature license for dynamic subscriber authentication and authorization using NASREQ, for MX240, MX480, MX960, MX2010, and MX2020

Additional Subscriber Services Management licenses are available to support Inline L2TP LNS Tunneling, Subscriber-Based Lawful Intercept, Virtual Chassis, and interface with policy management systems, as indicated in the table below.

Product Number	Description
S-BB-GX	Junos Broadband Policy Enforcement feature license for PCRF communications using 3GPP Gx and Gx+, for MX240, MX480, MX960, MX2010, and MX2020
S-BB-GY	Junos Broadband Policy Enforcement feature license for online charging using 3GPP Gy interface, for MX240, MX480, MX960, MX2010, and MX2020
S-LNS-IN	Software license for Inline L2TP LNS, for MX240, MX480, MX960, MX2010, and MX2020
S-VCR	Software license for single member of an MX Series Virtual Chassis

Subscriber Access Scale Licenses

These tiered licenses support from 4000 to 256,000 sessions and are bound to one chassis.

Product Number	Description
S-SA-4K	Subscriber scale license, up to 4000 subscribers
S-SA-8K	Subscriber scale license, up to 8000 subscribers
S-SA-16K	Subscriber scale license, up to 16,000 subscribers
S-SA-32K	Subscriber scale license, up to 32,000 subscribers
S-SA-64K	Subscriber scale license, up to 64,000 subscribers
S-SA-128K	Subscriber scale license, up to 128,000 subscribers
S-SA-256K	Subscriber scale license, up to 256,000 subscribers

Subscriber Access Scale Upgrade Licenses

These tiered licenses support from 4000 to 256,000 sessions and are bound to one chassis.

Product Number	Description
S-SA-UP-8K	Subscriber scale upgrade, from 4000 to 8000 subscribers
S-SA-UP-16K	Subscriber scale upgrade, from 8000 to 16,000 subscribers
S-SA-UP-32K	Subscriber scale upgrade, from 16,000 to 32,000 subscribers
S-SA-UP-64K	Subscriber scale upgrade, from 32,000 to 64,000 subscribers
S-SA-UP-96K	Subscriber scale upgrade, from 64,000 to 96,000 subscribers
S-SA-UP-128K	Subscriber scale upgrade, from 96,0000 to 128,000 subscribers
S-SA-UP-256K	Subscriber scale upgrade, from 128,000 to 256,000 subscribers

Flex Licensing

MX204

Product Number	Description
Base Hardware	
MX204-HW-BASE	MX204-HW-BASE integrated SKU with base hardware and standard Junos software, perpetual
Software	
S-MX-4C-A1-C1-1*	MX Series Advanced software feature subscription license for 1-year term; 4x100GbE software support included; valid for subscription renewals only
S-MX-4C-A1-C1-3	MX Series Advanced software feature subscription license for 3-year term; 4x100GbE software support included
S-MX-4C-A1-C1-5	MX Series Advanced software feature subscription license for 5-year term; 4x100GbE software support included
S-MX-4C-A1-C1-P	MX Series Advanced software feature perpetual license; 4x100GbE; software support not included
S-MX-4C-P1-C1-1*	MX Series Premium software feature subscription license for 1-year term; 4x100GbE software support included; valid for subscription renewals only
S-MX-4C-P1-C1-3	MX Series Premium software feature subscription license for 3-year term; 4x100GbE software support included
S-MX-4C-P1-C1-5	MX Series Premium software feature subscription license for 5-year term; 4x100GbE software support included
S-MX-4C-P1-C1-P	MX Series Premium software feature perpetual license; 4x100GbE; software support not included

MX240, MX480, MX960

Product Number	Description
MPC10E-10C Base Hardware	
MPC10E-10C-P-BASE	Fixed 8xQSFP28 multirate ports (10/40/100GbE) plus 2xQSFP56-DD multirate ports (10/40/100/400GbE) line card bundle with standard Junos software, perpetual
MPC10E-10C Software	
S-MX-10C-A1-1*	MX Series Advanced software feature subscription license for 1-year term; 10x100GbE software support included; valid for subscription renewals only
S-MX-10C-A1-3	MX Series Advanced software feature subscription license for 3-year term; 10x100GbE software support included
S-MX-10C-A1-5	MX Series Advanced software feature subscription license for 5-year term; 10x100GbE software support included
S-MX-10C-A1-P	MX Series Premium software feature perpetual license; 10 x100GbE; software support not included
S-MX-10C-P1-1*	MX Series Premium software feature subscription license for 1-year term; 10x100GbE software support included; valid for subscription renewals only

Product Number	Description
S-MX-10C-P1-3	MX Series Premium software feature subscription license for 3-year term; 10x100GbE software support included
S-MX-10C-P1-5	MX Series Premium software feature subscription license for 5-year term; 10x100GbE software support included
S-MX-10C-P1-P	MX Series Premium software feature perpetual license; 10 x100GbE; software support not included
MPC10E-15C Base Hardware	
MPC10E-15C-P-BASE	Fixed 12xQSFP28 multirate ports (10/40/100GbE) plus 3xQSFP56-DD multirate ports (10/40/100/400GbE) line card bundle with standard Junos software, perpetual
MPC10E-15C Software	
S-MX-15C-A1-1*	MX Series Advanced software feature subscription license for 1-year term; 15x100GbE software support included; valid for subscription renewals only
S-MX-15C-A1-3	MX Series Advanced software feature subscription license for 3-year term; 15x100GbE software support included
S-MX-15C-A1-5	MX Series Advanced software feature subscription license for 5-year term; 15x100GbE software support included
S-MX-15C-A1-P	MX Series Premium software feature perpetual license; 15 x100GbE; software support not included
S-MX-15C-P1-1*	MX Series Premium software feature subscription license for 1-year term; 15x100GbE software support included; valid for subscription renewals only
S-MX-15C-P1-3	MX Series Premium software feature subscription license for 3-year term; 15x100GbE; software support included
S-MX-15C-P1-5	MX Series Premium software feature subscription license for 5-year term; 15x100GbE software support included
S-MX-15C-P1-P	MX Series Premium software feature perpetual license; 15 x100GbE; software support not included

*1-year term license for Advanced and Premium tier are renewal only

Junos OS

- USA: Junos OS
- Worldwide: Junos-WW

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Juniper Networks | Driven by Experience™

Nokia 7750 Service Router

Release 15

The Nokia 7750 Service Router (SR) series of IP edge routers enables the delivery of advanced residential, enterprise, and mobile services. For enterprises, the 7750 SR series provides high-performance networking for cloud, data center, and branch office applications. Designed to stay ahead of evolving service demands driven by the cloud, 5G, and the Internet of Things, the 7750 SR product family consists of the 7750 SR series, the 7750 SR-e series, and the 7750 SR-a series.

High-performance IP edge

The Nokia 7750 SR series delivers high-performance routing and an extensive range of IP applications for service provider and enterprise networks. The 7750 SR scales system capacity from 2 Tb/s (half duplex) to 9.6 Tb/s (half duplex) and is equipped with high-density Gigabit Ethernet (GE), 10GE, 40GE and 100GE interfaces. At the heart of the 7750 SR is the highly programmable Nokia FP3 network processing silicon, an essential element in the quest for no compromise, high-speed, intelligent services and applications that can adapt to evolving customer requirements.

7750 SR-12e

7750 SR-12

7750 SR-7

NOKIA

Service richness

With Nokia's feature-rich Service Router Operating System (SR OS) and extensive QoS capabilities, the Nokia 7750 SR has the service richness and tools to define and deliver the most stringent SLAs for high-value, differentiated services. With specialized application processing, the 7750 SR leverages embedded subscriber, service and application intelligence to enable deeper levels of integrated service capabilities. The 7750 SR supports tens of thousands of service flows for the delivery of residential mobile and enterprise internet access, Carrier Ethernet and IP VPN services, and more—all without compromising performance.

Full array of IP edge functions

The MEF Carrier Ethernet (CE) 2.0-certified 7750 SR supports a full array of IP network functions and applications, including:

- Broadband Network Gateway (BNG) for residential subscriber management
- Provider edge (PE) router for MPLS-enabled enterprise VPN, internet access, and cloud and data center interconnect services
- Mobile aggregation router for 3G, LTE, and LTE-A mobile backhaul applications
- Mobile packet core gateway supports 2G/3G/4G SGW/PGW functions and ePDG/TWAG for Wi-Fi® access
- WLAN gateway for Wi-Fi network aggregation
- Security gateway for securing mobile backhaul networks
- High-performance IP routing for enterprise WANs, including connectivity to the data center, internet and branch offices.

High availability

For always-on service delivery, the Nokia 7750 SR sets the benchmark for high availability. Moving beyond full system redundancy, the robust SR OS supports numerous features to maximize network stability, ensuring IP/MPLS protocols and services run without interruption. These features include innovative nonstop routing, nonstop services, in-service software upgrades (ISSUs) and multi-chassis resiliency mechanisms.

Carrier SDN integration

The 7750 SR and SR OS enable multivendor software defined networking (SDN) control integration is enabled through OpenFlow, Path Computation Element Protocol (PCEP), Border Gateway Protocol with Link State (BGP-LS) and NETCONF/YANG interfaces. In combination with the Nokia Network Services Platform (NSP), the 7750 SR can be deployed as part of a Carrier SDN solution, supporting unified service automation and network optimization across IP, MPLS, Ethernet and optical transport layers.

IP/optical integration

Tunable 10G and integrated 100G coherent PM-QPSK tunable DWDM optics enable the 7750 SR to interface directly with the photonic transport layer without requiring optical transponders. A standards-based GMPLS user-network interface (UNI) enables the 7750 SR to efficiently coordinate IP routing and transport requirements across administrative boundaries and dynamically provision optical segments and end-to-end transport connections.

Network management

The Nokia 7750 SR is fully managed by the Nokia NSP, resulting in integrated network management across the access, aggregation, edge, and core network.

Hardware overview

The Nokia 7750 SR series is available in three chassis variants—the 7750 SR-12e, 7750 SR-12 and 7750 SR-7—and supports a wide range of interfaces, integrated service adapters (ISAs) and common system modules that are optimized to address various network and application requirements. For details on the Nokia 7750 SR-e series and 7750 SR-a series, refer to the 7750 SR-e and 7750 SR-a data sheets.

Switch Fabric Module (SFM5-12e) – The SFM5-12e enables 400 Gb/s line rate connectivity between all slots of the 7750 SR-12e chassis. The fabric cards are 3+1 redundant with active-active load-sharing design and are hot-swappable. The SFM5-12e is a full-height card that is modular in design and houses the pluggable CPM5 for investment protection.

Switch Fabric Module (SFM5-12, SFM5-7) – The SFM5-12 and SFM5-7 enable 200-Gb/s (redundant) line rate connectivity between all slots of the 7750 SR-12 and SR-7 chassis. The fabric cards are 1+1 redundant with active-active load-sharing design and are hot-swappable. The SFM-12 and SFM5-7 are full-height cards that are modular in design and house the pluggable CPM5 for investment protection.

Control Processor Module (CPM5) – The CPM5 is a pluggable, hot-swappable module housed within the SFM5-12e, SFM5-12 and SFM5-7. The CPM5 provides the management, security and control plane processing for the Nokia 7750 SR-12e, SR-12, and SR-7. Redundant CPMs operate in a hitless, stateful, failover mode. Central processing and memory are intentionally separated from the forwarding function on the interface modules to ensure utmost system resiliency. Face plate interfaces include an RJ-45 BITS port and a 1PPS port and a 10/100/1000BASE (RJ-45) management interface port.

* Some features are not supported on all MDA-e variants.

Switch Fabric/Control Processor Module (SF/CPM) – The SF/CPM provides data plane and control plane functionality in a full-height, hot-swappable module. The SF/CPM is 1+1 redundant with an active-active load-sharing design and is housed in an SR-12e, SR-12, and SR-7. Redundant SF/CPMs operate in a hitless, stateful, failover mode.Central processing and memory are intentionally separated from the forwarding function on the inter face modules to ensure utmost system resiliency. Face plate interfaces include an RJ-45 BITS port and a 1PPS port and a 10/100/1000BASE (RJ-45) management interface port.

Integrated Media Module (IMM) – IMMs are line cards providing integrated processing and physical interfaces on a single module. IMMs are hot-swappable and provide high-capacity Ethernet interfaces, including variants with integrated tunable DWDM optics, and deliver up to 400 Gb/s (full duplex) per slot performance. For synchronization requirements, they also support ITU-T Synchronous Ethernet (Sync-E) and IEEE 1588v2.

Input/Output Module (IOM) – IOMs are optimized for versatility in deploying a variety of multiservice and Ethernet-based applications. Each IOM supports up to two MDA and ISA module types. IOMs are hot-swappable. The IOM4-e delivers up to 200 Gb/s (full duplex) per slot performance and the IOM3-XP supports up to 50 Gb/s (full duplex) per slot performance.

Media Dependent Adapter-e (MDA-e) – MDA-e's, common with the 7750 SR-12e, SR-12, and SR-7 and the 7750 SR-e series, support up to 100 Gb/s (full duplex) and provide physical Ethernet interface connectivity. They are available in a variety of interface and density configurations and are hot-swappable. They are supported with the IOM4-e in the SR-12e, SR-12, and SR-7 and with the IOM-e in the SR-e. For synchronization requirements, they support ITU-T Sync-E and IEEE 1588v2. They also support a wide range of Optical Transport Networking (OTN) signals: OTU1e, OTU2, OTU2e, OTU4; ITU-T G.709 and Forward Error Correction (FEC)*.

Media Dependent Adapter (MDA) – MDAs, available in two hot-swappable types, provide modular physical interface connectivity and are available in a variety of interface and density configurations. MDA-XPs and MDAs support Ethernet and multiservice interfaces and support up to 25 Gb/s and 10 Gb/s respectively. For synchronization requirements, they also support ITU-T Sync-E and IEEE 1588v2.

Multiservice Integrated Service Module (MS-ISM) – MS-ISMs are hot-swappable, full-height resource modules. They provide specialized processing and buffering for deeper levels of integrated services and advanced applications. They leverage two embedded ISA2 general purpose multi-core processors and support up to 80 Gb/s of processing. Combination IMMs support Ethernet and an embedded ISA2, which supports up to 40 Gb/s of processing.

Multiservice Integrated Service Adapter 2 (MS-ISA2) – MS-ISA2s, common with the SR-12e, SR-12, and SR-7 and the SR-e series, are hot-swappable, half-height resource adapters. They provide specialized processing and buffering for deeper levels of integrated services and advanced applications. They support up to 40 Gb/s of processing and insert into an IOM4-e.

Integrated Service Module - Mobile Gateway (ISM-MG) – ISM-MGs are hot-swappable, full-height modules that fit into any 7750 SR I/O slot and provide the bearer functions for 2G/3G/4G and Wi-Fi access networks.

Advanced Power Equalization Modules (APEQs) – APEQs provide power for the 7750 SR-12e. The low voltage DC APEQs deliver up to 2800W each. The high voltage DC APEQs take 260-400 V and provide 3000W each. AC APEQs take 200-240 V single phase and deliver 3000W each. APEQs support cost-effective modular expansion as required.

Power Entry Modules (PEMs) – PEMs provide low voltage DC power for the 7750 SR-12 and 7750 SR-7 and support cost-effective modular expansion as required.

NOKIA

Technical specifications

Table 1. Technical specifications for the 7750 SR series

	7750 SR-12e	7750 SR-12	7750 SR-7
System throughput	• Switching capacity: 9.6 Tb/s (half duplex, non-redundant) or 7.2 Tb/s (half duplex, redundant) • Per-slot throughput: 400 Gb/s (full duplex, redundant)	• Switching capacity: 4 Tb/s (half duplex, redundant) • Per-slot throughput: 200 Gb/s (full duplex, redundant)	• Switching capacity: 2 Tb/s (half duplex, redundant) • Per-slot throughput: 200 Gb/s (full duplex, redundant)
Number of MDA-e's/MDAs/ISA2s per chassis	18	20	10
Number of IOMs/IMMs/ISMs per chassis	9	10	5
Common equipment redundancy	SFM5-12e, CPM5, SF/CPM, Mini-SFM, advanced power equalizers (APEQs), fans	SFM5-12, CPM5, SF/CPM, Power Entry Modules (PEMs), fans	SFM5-7, CPM5, SF/CPM, PEMs, fans
Hot-swappable modules	SFM5-12e, CPM5, SFM/CPM-12e, Mini-SFM-12e, IOMs, MDA-e's, MDAs, IMMs, ISMs, ISA2s, VSMs, APEQs, Enhanced Fan Trays (EFTs)	SFM5-12, CPM5, SF/CPM, IOMs, IMMs, ISMs, MDA-e's, MDAs, ISA2s, PEMs, VSMs, EFTs	SFM5-7, CPM5, SF/CPM, IOMs, MDA-e's, MDAs, IMMs, ISMs, ISA2s, VSMs, EFTs
Dimensions*	• Height: 97.8 cm (38.5 in), 22 RU • Width: 44.5 cm (17.5 in) • Depth: 76.2 cm (30 in)	• Height: 62.2 cm (24.5 in), 14 RU • Width: 44.5 cm (17.5 in) • Depth (without cable management): 64.5 cm (25.4 in) • Depth (with cable management): 76.5 cm (30.1 in)	• Height: 35.6 cm (14 in), 8 RU • Width: 44.5 cm (17.5 in) • Depth: 64.8 cm (25.5 in)
Weight*	• Empty: 79.4 kg (175 lb) • Loaded: 249.5 kg (550 lb)	• Empty: 56.4 kg (124.3 lb) • Loaded: 155.7 kg (343.3 lb)	• Empty: 41 kg (90.4 lb) chassis weight with factory installed fan tray and air filter • Loaded: 70.5 kg (155.4 lb)
Power	DC power: • DC-40 V to -72 V, 60A or 80A per feed or • DC 260 to 400 V, 13A per feed • 4+1 redundancy External AC power (option): • Input voltage: 200V AC -240V AC, 16A, 50/60Hz per feed • Output voltage: 42 V DC to 56 V DC • Current: 50 A	DC power: • DC-40 to -72 V, 162 A max, 6480 W or • DC-46 to -72V, 175 A max, 8050 W or • DC-49 to -55 V, 175 A max, 8575 W or • DC-50.5 to -72 V, 175 A max, 8837.5 W • 1+1 redundancy External AC power (option): • Input voltage: 200 V AC to 240 V AC • Output voltage:42 V DC to 56 V DC • Current: 50 A	DC power: • DC-40 to -72V, 100A, 4000W max or • DC-46 to -72V, 100A, 4600W max • 1+1 redundancy External AC power (option): • Input voltage: 200 V AC to 240 V AC • Output voltage: 42 V DC to 56 V DC • Current: 50 A
Cooling	Front-to-back air flow	Front-to-back air flow	Side-to-back air flow

* Dimensions and weights are approximate and subject to change. Refer to the appropriate installation guide for the current dimensions and weights.

NOKIA

Table 2. Nokia 7750 SR IMM summary

IMM type	Ports	Connector type	Maximum density		
			7750 SR-12e	7750 SR-12	7750 SR-7
10/100/1000BASE	160 or 80	CSFP or SFP	1440 or 720	1600 or 800	800 or 400
10/100/1000BASE	48	SFP	432	480	240
10GBASE	40	SFP+	360	—	—
10GBASE/100/100BASE (combination)	10/20	SFP+/SFP	90/180	100/200	50/100
10GBASE + 7x50 ISA2 (combination)	10	SFP+	90	100	50
10GBASE	12, 20	SFP+	108, 180	120, 200	60, 100
40GBASE	6	QSFP+	54	60	30
40GBASE/100/100BASE (combination)	3/20	QSFP+/SFP	27/180	30/200	15/100
100GBASE	4	CXP and CFP4	36	—	—
100GBASE	1, 2	CFP	9, 18	10, 20	5, 10
100GBASE/10GBASE (combination)	1/10	CFP/SFP+	9/90	10/100	5/50
100GBASE + 7x50 ISA2 (combination)	1	CFP	9	10	5
100GBASE IMM (DWDM tunable optics)	1	LC	9	10	5

Table 3. Nokia 7750 SR MDA-e summary

MDA-e type	Ports	Connector type	Maximum density		
			7750 SR-12e	7750 SR-12	7750 SR-7
1000BASE	40 or 20	CSFP or SFP	720 or 360	800 or 400	400 or 200
10GBASE/1000BASE (MACsec*)	12	SFP+/SFP	216	240	120
10GBASE	10, 6	SFP+	180, 108	200, 120	100, 60
100GBASE/40GBASE	2	QSFP28/QSFP+	36	40	20
100GBASE	1, 2	CFP2, CFP4	18, 36	20, 40	10, 20

* MACsec support is planned for a future SR OS release.

Table 4. Nokia 7750 SR MDA-XP and MDA summary

MDA type	Ports per MDA	Connector type	Maximum density		
			SR-12e	SR-12	SR-7
Ethernet MDA-XP					
10/100/1000BASE-TX	48	8 x mini RJ-21	864	960	480
1000BASE	10, 12, 20	SFP	180, 216, 360	200, 240, 400	100, 120, 200
10GBASE/1000BASE (LAN/WAN PHY) (combination)	2/12	XFP/SFP	36/216	40/240	20/120
10GBASE (LAN/WAN PHY)	1, 2, 4	XFP	18, 36, 72	20, 40, 80	10, 20, 40
Any Service Any Port (ASAP) MDA					
Channelized DS3/E3 ASAP	4, 12	1.0/2.3 connectors	72, 216	80, 240	40, 120
Channelized OC-3/STM-1 ASAP	4	SFP	72	80	40
Channelized OC-12/STM-4 ASAP	1	SFP	18	20	10
Other					
Versatile Service Module-XP	N/A	N/A	√	√	√

NOKIA

Table 5. Nokia 7750 SR ISA support summary

ISA type	SR-12e	SR-12	SR-7
Multiservice Integrated Service Adapter 2 (MS-ISA2)	√	√	√
Multiservice Integrated Service Module (MS-ISM)	√	√	√
Integrated Service Module - Mobile Gateway (ISM-MG)*	—	√	√

* Consult the ISM-MG data sheet for details. Support requires SR-OS-MG.

Feature and protocol support highlights

Feature and protocol support within the Nokia 7750 SR series includes (but is not limited to):

IP and MPLS routing features

- IP unicast routing: Routing Information Protocol (RIP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Multiprotocol Border Gateway Protocol (MBGP), Unicast Reverse Path Forwarding (uRPF), comprehensive control plane protection features for security, and IPv4 and IPv6 feature parity
- IP multicast routing: Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), Multicast Source Discovery Protocol (MSDP), and IPv4 and IPv6 feature parity
- MPLS: Label edge router (LER) and label switch router (LSR) functions with support for seamless MPLS designs, MPLS-Transport Profile (MPLS-TP), Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP) for MPLS signaling and traffic engineering, Point-to-Point (P2P) and Point-to-Multipoint (P2MP) label switched paths (LSPs) with Multicast LDP (MLDP), P2MP RSVP and weighted Equal-Cost Multi-Path (ECMP)
- Segment routing: Support in multiple instances of IS-IS and OSPF with shortest path tunnel and Segment Routing - Traffic Engineering (SR-TE) LSP. The implementation provides Loop-Free Alternate (LFA), remote LFA and Topology-Independent LFA (TI-LFA) protection for both types of tunnels. PCEP allows the delegation of the SR-TE LSP to the Nokia NSP or a third-party PCE function

Layer 2 features

- Ethernet LAN (ELAN): BGP-VPLS (Virtual Private LAN Service), Provider Backbone Bridging for VPLS (PBB-VPLS), Ethernet VPN (EVPN) and PBB-EVPN
- E-Line: BGP-VPWS (Virtual Private Wire Service), EVPN-VPWS and PBB-EVPN
- E-Tree: EVPN and PBB
- EVPN: EVPN-VXLAN (Virtual eXtensible LAN) to VPLS/EVPN-MPLS gateway functions

Layer 3 features

- IP-VPN, enhanced internet services, EVPN for Layer 3 services with integrated routing and bridging (EVPN-IRB), and Multicast VPN (MVPN), which includes Inter-AS MVPN and Next Generation MVPN (NG-MVPN)

Platform features

- Ethernet satellites: Port expansion through local or remote Nokia 7210 Service Access Switch (SAS)-S series GE, 10GE, 100GE and SONET/SDH satellite variants, offering 24/48xGE ports, 64xGE/10GE ports or legacy SONET/SDH ports over GE, 10GE and 100GE uplinks*
- OAM: Extensive fault and performance operations, administration and maintenance (OAM) includes Ethernet Connectivity Fault Management (CFM) (IEEE 802.1ag, ITU-T Y.1731), Ethernet in the First Mile (EFM) (IEEE 802.3ah), Bi-Directional Fault Detection (BFD), Cflowd, Two-Way Active Measurement Protocol (TWAMP), and a full suite of MPLS OAM tools, including GMPLS UNI

* Requires CPM5, an appropriate chassis mode, and an uplink via an FP2-based IMM/IOM at a minimum for 7750 SR system and requires CPM5, the chassis set to mixed mode, and an uplink via an FP2-based IMM/IOM at a minimum for 7450 ESS systems.

- Timing: ITU-T Synchronous Ethernet (SyncE), IEEE 1588v2, Network Time Protocol (NTP), BITS ports (T1, E1, 2M), and 1PPS
- QoS: Flexible intelligent packet classification; ingress and egress hierarchical QoS with multitiered shaping and two-tiered, class fair hierarchical policing; advanced, scalable network and service QoS, and end-to-end consistent QoS regardless of oversubscription or congestion
- High availability: Nonstop routing, nonstop services, in-service software upgrade (ISSU), fast reroute for IP, RSVP, LDP and segment routing, pseudowire redundancy, ITU-T G.8031 and G.8032, weighted ECMP, and weighted, mixed-speed link aggregation

Management features

- Management via CLI, SNMP, NETCONF/YANG and telemetry; comprehensive network and node management through the Nokia NSP
- Multivendor SDN control integration through OpenFlow, PCEP and BGP-LS interface support

Environmental specifications

- Operating temperature: 5°C to 40°C (41°F to 104°F)
- Operating relative humidity: 5% to 85%
- Operating altitude: Up to 4000 m (13,123 ft) at 30°C (86°F)

Safety standards and compliance agency certifications

Safety

- IEC/EN/UL/CSA60950-1 Ed2 Am2
- FDA CDRH 21-CFR 1040
- IEC/EN 60825-1
- IEC/EN 60825-2

EMC emission

- ICES-003 Class A
- FCC Part 15 Class A
- AS/NZS CISPR 32 Class A
- VCCI Class A
- EN 55032 Class A
- IEC CISPR 32 Class A
- KN 32 Class A

EMC immunity

- EN 300 386
- EN 55024
- KN 35

Ethernet standards

- EEE 802.1AB, Station and Media Access Control Connectivity Discovery
- IEEE 802.1ad, Provider Bridges
- IEEE 802.1ag, Connectivity Fault Management
- IEEE 802.1ah, Provider Backbone Bridges
- IEEE 802.1ak, Multiple Registration Protocol
- IEEE 802.1aq, Shortest Path Bridging
- IEEE 802.1ax, Link Aggregation
- IEEE 802.1D, MAC Bridges
- IEEE 802.1p, Traffic Class Expediting
- IEEE 802.1Q, Virtual LANs
- IEEE 802.1s, Multiple Spanning Trees
- IEEE 802.1w, Rapid Reconfiguration of Spanning Tree
- IEEE 802.1X, Port Based Network Access Control
- IEEE 802.3ab, 1000BASE-T
- IEEE 802.3ac, VLAN Tag
- IEEE 802.3ad, Link Aggregation
- IEEE 802.3ae, 10 Gb/s Ethernet
- IEEE 802.3ah, Ethernet in the First Mile
- IEEE 802.3ba, 40 Gb/s and 100 Gb/s Ethernet
- IEEE 802.3i, Ethernet
- IEEE 802.3u, Fast Ethernet

- IEEE 802.3x, Ethernet Flow Control
- IEEE 802.3z, Gigabit Ethernet
- ITU-T G.8031, Ethernet Linear Protection Switching
- ITU-T G.8032, Ethernet Ring Protection Switching
- ITU-T Y.1731, OAM functions and mechanisms for Ethernet based networks

Telecom standards*

- ANSI T1.105.03
- ANSI T1.105.06
- ANSI T1.105.09
- ANSI T1.403 (DS1)
- ANSI T1.404 (DS3)
- ITU-T G.703
- ITU-T G.707
- ITU-T G.813
- ITU-T G.823
- ITU-T G.824
- ITU-T G.825
- ITU-T G.957
- Telcordia GR-253-CORE

Environmental

- ETS 300 019-2-1 Storage Tests, Class 1.2
- ETS 300 019-2-2 Transportation Tests, Class 2.3
- ETS 300 019-2-3 Operational Tests, Class 3.2
- ETS 300 019-2-4, pr A 1 Seismic
- ETSI EN 300 132-2 Power Supply Interface
- WEEE
- RoHS
- China RoHS

Network Equipment Building System (NEBS)

- NEBS Level 3
- RBOC requirements:
  - ATIS-0600020
  - ATIS-0600019
  - ATIS-0600010.03
  - ATIS-0600015
  - ATIS-0600015.03
  - ATT-TP-76200
  - VZ.TPR.9205 TEEER
  - VZ.TPR.9305
  - VZ-TPR-9307

MEF certifications

- CE 2.0
  - Certified (on E-LAN, E-Line, E-Tree and E-Access MEF service types)
  - 100G certified (on E-Line and E-Access MEF service types)
- CE 1.0 (MEF 9 and MEF 14)
  - Certified

* For ATM, frame relay, PPP and SONET/SDH standards, refer to the installation guide for the full set of compliance standards.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1709015723EN (September)

CloudEngine S6730-H Series 10GE Switches

Huawei CloudEngine S6730-H series 10GE switches are next-generation enterprise-class core and aggregation switches that provide 10GE downlink optical ports and 100GE uplink optical ports.

Introduction

Huawei CloudEngine S6730-H series switches are next-generation enterprise-class core and aggregation switches that offer high performance, high reliability, cloud management, and intelligent operations and maintenance (O&M). They build on an industry-leading Versatile Routing Platform (VRP) and are purpose-built with security, IoT, and cloud in mind. With these traits, CloudEngine S6730-H can be widely used in enterprise campuses, colleges/universities, data centers, and other scenarios.

CloudEngine S6730-H switches offer 10GE, 25GE, 40GE, and 100GE port types, flexibly adapting to diversified network bandwidth requirements. They also support cloud management and implement cloud-managed network services throughout the full lifecycle from planning, deployment, monitoring, experience visibility, and fault rectification, all the way to network optimization, greatly simplifying network management.

By integrating the native wireless access controller (WAC) capability, a single CloudEngine S6730-H switch can manage a vast number of wireless access points (APs). The results are simplified network architecture, fewer required devices, and lowered networking costs. Free mobility, another key differentiator of CloudEngine S6730-H, enables consistent user experience no matter the user location or IP address, fully meeting enterprises' demands for mobile offices.

CloudEngine S6730-H switches support VXLAN to implement network virtualization, achieving multi-purpose networks and multi-network convergence for greatly improved network capacity and utilization. As such, CloudEngine S6730-H switches are an ideal choice for building next-generation IoT converged networks in terms of cost, flexibility, and scalability.

The full series of CloudEngine S6730-H switches have built-in security probes to enable abnormal traffic detection, analysis of threats even in encrypted traffic, and network-wide threat deception. With such robust security features, CloudEngine S6730-H switches transform traditional passive security defense into proactive security protection, fully ensuring campus network security.

Product Overview

Models and Appearances

The following models are available in the CloudEngine S6730-H series.

Appearance	Description
 CloudEngine S6730-H48X6C	• 48 x 10 Gig SFP+, 6 x 40/100 Gig QSFP28 • Dual pluggable power modules, 1+1 power backup • Forwarding performance: 490 Mpps • Switching capacity: 2.16Tbps/2.4Tbps

Appearance	Description
 CloudEngine S6730-H24X6C	• 24 x 10 Gig SFP+, 6 x 40/100 Gig QSFP28 • Dual pluggable power modules, 1+1 power backup • Forwarding performance: 490 Mpps • Switching capacity: 1.68Tbps/2.4Tbps *Note: All ports support 40GE by default. You can purchase right-to-use (RTU) licenses to upgrade the port rate from 40GE to 100GE*

Note：The value before the slash (/) refers to the device's switching capability, while the value after the slash (/) means the system's switching capability.

Fan Module

The following table lists the fan module on the CloudEngine S6730-H series.

Fan Module	Technical Specifications	Applied Switch Model
 FAN-031A-B	• Dimensions (W x D x H): 40 mm x 100.3 mm x 40 mm • Number of fans: 1 • Weight: 0.1 kg • Maximum power consumption: 21.6 W • Maximum fan speed: 24500±10% revolutions per minute (RPM) • Maximum wind rate: 31 cubic feet per minute (CFM) • Hot swap: Supported	• CloudEngine S6730-H48X6C • CloudEngine S6730-H24X6C

Power Supply

The following table lists the power supplies on the CloudEngine S6730-H series.

Power Module	Technical Specifications	Applied Switch Model


PAC600S12-CB
	• Dimensions (H x W x D): 40 mm x 90 mm x 215 mm
	• Weight: 0.95 kg (2.09 lb)
	• Rated input voltage range:
	  – 100 V AC to 240 V AC, 50/60 Hz
	  – 240 V DC
	• Maximum input voltage range:
	  – 90 V AC to 290 V AC, 45 Hz to 65 Hz
	  – 190 V DC to 290 V DC
	• Maximum input current:
	  – 100 V AC to 240 V AC: 8 A
	  – 240 V DC: 4 A
	• Maximum output current: 50 A
	• Rated output voltage: 12 V
	• Maximum output power: 600 W
	• Hot swap: Supported
		• CloudEngine S6730-H48X6C
		• CloudEngine S6730-H24X6C

Power Module	Technical Specifications	Applied Switch Model
 PDC1000S12-DB	• Dimensions (H x W x D): 40 mm x 90 mm x 215 mm • Weight: 1.02 kg (2.25 lb) • Rated input voltage range: -48 V DC to -60 V DC • Maximum input voltage range: -38.4 V DC to -72 V DC • Maximum input current: 30 A • Maximum output current: 83.3 A • Maximum output power: 1000 W • Hot swap: Supported	• CloudEngine S6730-H48X6C • CloudEngine S6730-H24X6C

The S6730-H uses pluggable power modules. It can be configured with a single power module or double power modules for 1+1 power redundancy.

Product Features and Highlights

Abundant Convergence Feature

- This CloudEngine S6730-H provides the integrated WLAN AC function that can manage 1K APs, reducing the costs of purchasing additional WLAN AC hardware. The wireless forwarding performance breaking the forwarding performance bottleneck of an external WLAN AC. With this switch series, customers can stay ahead in the high-speed wireless era.

NOTE

The wireless forwarding performance is calculated based on 1024-byte packets.

- The S6730-H supports SVF and functions as a parent switch. With this virtualization technology, a physical network with the "Small-sized core/aggregation switches + Access switches + APs" structure can be virtualized into a "super switch", greatly simplifying network management.
- The S6730-H provides excellent QoS capabilities and supports queue scheduling and congestion control algorithms. Additionally, it adopts innovative priority queuing and multi-level scheduling mechanisms to implement fine-grained scheduling of data flows, meeting service quality requirements of different user terminals and services.

Providing Fine Granular Network Management

- The S6730-H uses the Packet Conservation Algorithm for Internet (iPCA) technology that changes the traditional method of using simulated traffic for fault location. iPCA technology can monitor network quality for any service flow anywhere, anytime, without extra costs. It can detect temporary service interruptions in a very short time and can identify faulty ports accurately. This cutting-edge fault detection technology turns "extensive management" to "fine granular management."
- The S6730-H supports Two-Way Active Measurement Protocol (TWAMP) to accurately check any IP link and obtain the entire network's IP performance. This protocol eliminates the need of using a dedicated probe or a proprietary protocol.

Flexible Ethernet Networking

- In addition to traditional Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP), the S6730-H supports Huawei-developed Smart Ethernet Protection (SEP) technology and the latest Ethernet Ring Protection Switching (ERPS) standard. SEP is a ring protection protocol specific to the Ethernet link layer, and applies to various ring network topologies, such as open ring topology, closed ring topology, and cascading ring topology. This protocol is reliable, easy to maintain, and implements fast service switching within 50 ms. ERPS is defined in ITU-T G.8032. It implements millisecond-level protection switching based on traditional Ethernet MAC and bridging functions.
- The S6730-H supports Smart Link and Virtual Router Redundancy Protocol (VRRP), which implement backup of uplinks. One S6730-H switch can connect to multiple aggregation switches through multiple links, significantly improving reliability of access devices.

Intelligent Stack (iStack)

- The S6730-H supports the iStack function that combines multiple switches into a logical switch. Member switches in a stack implement redundancy backup to improve device reliability and use inter-device link aggregation to improve link reliability. iStack provides high network scalability. You can increase a stack's ports, bandwidth, and processing capability by simply adding member switches. iStack also simplifies device configuration and management. After a stack is set up, multiple physical switches can be virtualized into one logical device. You can log in to any member switch in the stack to manage all the member switches in it.

Cloud-based Management

- The Huawei cloud management platform allows users to configure, monitor, and inspect switches on the cloud, reducing on-site deployment and O&M manpower costs and decreasing network OPEX. Huawei switches support both cloud management and on-premise management modes. These two management modes can be flexibly switched as required to achieve smooth evolution while maximizing return on investment (ROI).

VXLAN Features

- VXLAN is used to construct a Unified Virtual Fabric (UVF). As such, multiple service networks or tenant networks can be deployed on the same physical network, and service and tenant networks are isolated from each other. This capability truly achieves 'one network for multiple purposes'. The resulting benefits include enabling data transmission of different services or customers, reducing the network construction costs, and improving network resource utilization.
- This series switches are VXLAN-capable and allow centralized and distributed VXLAN gateway deployment modes. These switches also support the BGP EVPN protocol for dynamically establishing VXLAN tunnels and can be configured using NETCONF/YANG.

Clock Synchronization

- CloudEngine S6730-H48X6C and CloudEngine S6730-H24X6C models supports the IEEE 1588v2 protocol, which implements low-cost, high-precision, and high-reliability time and clock synchronization. This feature can meet strict requirements of power and transportation industry customers on time and clock synchronization.

Note: The CloudEngine S6730-H48X6C and CloudEngine S6730-H24X6C have models supportting clock synchronization and not supporting clock synchronization, configure them as required.

High-Performance VRP Software System

- Huawei S series switches build on a unified Versatile Routing Platform (VRP) software system, meeting the growing network scale and the evolving Internet technologies and guaranteeing network services and network quality.
- VRP is a network operating system developed by Huawei with independent intellectual property rights. It can run on multiple hardware platforms and provide unified network, user, and management views. VRP provides flexible application solutions for users. In addition, VRP is a future-proof platform that maximally protects customer investments.
- The VRP platform is focused on IP services and uses a component-based architecture to provide more than 300 features. Besides, VRP stands out for its application-based tailorable and scalable capabilities.

Open Programmability System(OPS)

- Open Programmability System (OPS) is an open programmable system based on the Python language. IT administrators can program the O&M functions of a switch through Python scripts to quickly innovate functions and implement intelligent O&M.

Big Data-Powered Collaborative Security

- This series of switches supports encrypted communication analytics (ECA), a traffic identification and detection technology. ECA can precisely detect malicious traffic by efficiently identifying encrypted and non-encrypted traffic, extracting the characteristics of encrypted traffic, and sending these characteristics to HiSec Insight (a big data-powered security analysis system). Furthering to this, ECA-capable switches can work with the controller iMaster NCE-Campus to automatically isolate threats, thereby ensuring campus network security.
- This series of switches also supports network deception technology. Specifically, switches functioning as sensors can detect threats (such as IP address scanning and port scanning on the network) and lure threat traffic to the honeypot for simulated interaction with attackers. In this way, it is easy to obtain attack behaviors, extract attack tools, and analyze suspicious traffic in depth to create defense policies. Switches then work with iMaster NCE-Campus to automatically isolate threats and block the spread of attack behaviors, ensuring campus network security.

Intelligent O&M

- This series switches provides telemetry technology to collect device data in real time and send the data to Huawei campus network analyzer(iMaster NCE-CampusInsight). The CampusInsight analyzes network data based on the intelligent fault identification algorithm, accurately displays the real-time network status, effectively demarcates and locates faults in a timely manner, and identifies network problems that affect user experience, accurately guaranteeing user experience.
- This series switches supports a variety of intelligent O&M features for audio and video services, including the enhanced Media Delivery Index (eMDI). With this eDMI function, the switch can function as a monitored node to periodically conduct statistics and report audio and video service indicators to the CampusInsight platform. In this way, the CampusInsight platform can quickly demarcate audio and video service quality faults based on the results of multiple monitored nodes.

Intelligent Upgrade

- Switches support the intelligent upgrade feature. Specifically, switches obtain the version upgrade path and download the newest version for upgrade from the Huawei Online Upgrade Platform (HOUP). The entire upgrade process is highly automated and achieves one-click upgrade. In addition, preloading the version is supported, which greatly shortens the upgrade time and service interruption time.
- The intelligent upgrade feature greatly simplifies device upgrade operations and makes it possible for the customer to upgrade the version independently. This greatly reduces the customer's maintenance costs. In addition, the upgrade policies on the HOUP platform standardize the upgrade operations, which greatly reduces the risk of upgrade failures.

Product Specifications

The following table describes the functions and features available on the CloudEngine S6730-H series.

Functions and Features

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
Ethernet features	Ethernet basics	Rate auto-negotiation on an interface	Yes	Yes
		Flow control on an interface	Yes	Yes
		Jumbo frames	Yes	Yes
		Link aggregation	Yes	Yes
		Load balancing among links of a trunk	Yes	Yes
		Transparent transmission of Layer 2 protocol packets	Yes	Yes
		Device Link Detection Protocol (DLDP)	Yes	Yes
		Link Layer Discovery Protocol (LLDP)	Yes	Yes
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)	Yes	Yes
		Interface isolation	Yes	Yes
		Broadcast traffic suppression on an interface	Yes	Yes
		Multicast traffic suppression on an interface	Yes	Yes
		Unknown unicast traffic suppression on an interface	Yes	Yes
		VLAN broadcast traffic suppression	Yes	Yes
		VLAN multicast traffic suppression	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
		VLAN unknown unicast traffic suppression	Yes	Yes
	VLAN	VLAN specification	4094	4094
		VLANIF interface specification	4094	4094
		Access mode	Yes	Yes
		Trunk mode	Yes	Yes
		Hybrid mode	Yes	Yes
		QinQ mode	Yes	Yes
		Default VLAN	Yes	Yes
		VLAN assignment based on interfaces	Yes	Yes
		VLAN assignment based on protocols	Yes	Yes
		VLAN assignment based on IP subnets	Yes	Yes
		VLAN assignment based on MAC addresses	Yes	Yes
		VLAN assignment based on MAC address + IP address	Yes	Yes
		VLAN assignment based on MAC address + IP address + interface number	Yes	Yes
		Adding double VLAN tags to packets based on interfaces	Yes	Yes
		Super-VLAN	Yes	Yes
		Super-VLAN specification	256	256
		Sub-VLAN	Yes	Yes
		Sub-VLAN specification	1024	1024
		VLAN mapping	Yes	Yes
		Selective QinQ	Yes	Yes
		MUX VLAN	Yes	Yes
		Voice VLAN	Yes	Yes
		Guest VLAN	Yes	Yes
	GVRP	GARP	Yes	Yes
		GVRP	Yes	Yes
	VCMP	VCMP	Yes	Yes
	MAC	MAC address	384K max	384K max
		Automatic learning of MAC addresses	Yes	Yes
		Automatic aging of MAC addresses	Yes	Yes
		Static, dynamic, and blackhole MAC address entries	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
		Interface-based MAC address learning limiting	Yes	Yes
		Sticky MAC	Yes	Yes
		MAC address flapping detection	Yes	Yes
		Configuring MAC address learning priorities for interfaces	Yes	Yes
		MAC address spoofing defense	Yes	Yes
		Port bridge	Yes	Yes
	ARP	Static ARP	Yes	Yes
		Dynamic ARP	Yes	Yes
		ARP entry	140K max (share)	140K max (share)
		ARP aging detection	Yes	Yes
		Intra-VLAN proxy ARP	Yes	Yes
		Inter-VLAN proxy ARP	Yes	Yes
		Routed proxy ARP	Yes	Yes
		Multi-egress-interface ARP	Yes	Yes
Ethernet loop protection	MSTP	STP	Yes	Yes
		RSTP	Yes	Yes
		MSTP	Yes	Yes
		VBST	Yes	Yes
		BPDU protection	Yes	Yes
		Root protection	Yes	Yes
		Loop protection	Yes	Yes
		Defense against TC BPDU attacks	Yes	Yes
	Loopback detection	Loop detection on an interface	Yes	Yes
	SEP	SEP	Yes	Yes
	Smart Link	Smart Link	Yes	Yes
		Smart Link multi-instance	Yes	Yes
		Monitor Link	Yes	Yes
	RRPP	RRPP	Yes	Yes
		Single RRPP ring	Yes	Yes
		Tangent RRPP ring	Yes	Yes
		Intersecting RRPP ring	Yes	Yes
		Hybrid networking of RRPP rings and other ring networks	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
	ERPS	G.8032 v1	Yes	Yes
		G.8032 v2	Yes	Yes
		ERPS semi-ring topology	Yes	Yes
		ERPS closed-ring topology	Yes	Yes
IPv4/IPv6 forwarding	IPv4 and unicast routing	IPv4 static routing	Yes	Yes
		VRF	Yes	Yes
		DHCP client	Yes	Yes
		DHCP snooping	Yes	Yes
		DHCP server	Yes	Yes
		DHCP relay	Yes	Yes
		DHCP policy VLAN	Yes	Yes
		URPF check	Yes	Yes
		Routing policies	Yes	Yes
		IPv4 routes	256K max (share)	256K max (share)
		RIPv1	Yes	Yes
		RIPv2	Yes	Yes
		OSPF	Yes	Yes
		BGP	Yes	Yes
		MBGP	Yes	Yes
		IS-IS	Yes	Yes
		Policy-based routing (PBR)	Yes	Yes
	Multicast routing features	IGMPv1/v2/v3	Yes	Yes
		PIM-DM	Yes	Yes
		PIM-SM	Yes	Yes
		MSDP	Yes	Yes
		IPv4 multicast routes	64K-1 max (share)	64K-1 max (share)
		IPv6 multicast routes	4K	4K
		Multicast routing policies	Yes	Yes
		RPF	Yes	Yes
	IPv6 features	IPv6 protocol stack	Yes	Yes
		ND	Yes	Yes
		ND entry	80K max (share)	80K max (share)
		ND snooping	Yes	Yes
		VRF	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
		DHCPv6 snooping	Yes	Yes
		RIPng	Yes	Yes
		DHCPv6 server	Yes	Yes
		DHCPv6 relay	Yes	Yes
		OSPFv3	Yes	Yes
		BGP4+	Yes	Yes
		IS-IS for IPv6	Yes	Yes
		IPv6 routes	80K max (share)	80K max (share)
		VRRP6	Yes	Yes
		MLDv1/v2	Yes	Yes
		PIM-DM for IPv6	Yes	Yes
		PIM-SM for IPv6	Yes	Yes
	IPv6 transition technology	IPv6 manual tunneling	Yes	Yes
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	Yes	Yes
		IGMP snooping proxy	Yes	Yes
		MLD snooping	Yes	Yes
		Multicast traffic suppression	Yes	Yes
		Inter-VLAN multicast replication	Yes	Yes
MPLS & VPN	MPLS basic functions	LDP protocol	Yes	Yes
		Double MPLS labels	Yes	Yes
		Mapping from 802.1p priorities to EXP priorities in MPLS packets	Yes	Yes
		Mapping from DSCP priorities to EXP priorities in MPLS packets	Yes	Yes
		LSP specification	16K max	16K max
	MPLS TE	MPLS-TE tunnel establishment	Yes	Yes
		MPLS-TE tunnel specification	512	512
		MPLS-TE protection group	Yes	Yes
	VPN	MCE	Yes	Yes
		GRE tunneling	Yes	Yes
		GRE tunnel specification	512	512
		VLL	Yes	Yes
		PWE3	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
		VPLS	Yes	Yes
		MPLS L3VPN	Yes	Yes
		IPSec Efficient VPN	Yes	Yes
Device reliability	BFD	Single-hop BFD	Yes	Yes
		BFD for static routes	Yes	Yes
		BFD for OSPF	Yes	Yes
		BFD for IS-IS	Yes	Yes
		BFD for BGP	Yes	Yes
		BFD for PIM	Yes	Yes
		BFD for VRRP	Yes	Yes
	Stacking	Service interface-based stacking	Yes	Yes
		Maximum number of stacked devices	9	9
		Stack bandwidth (Bidirectional)	Up to 1.36 Tbit/s	Up to 1.36 Tbit/s
	VRRP	VRRP standard protocol	Yes	Yes
Ethernet OAM	EFM (802.3ah)	Automatic discovery of links	Yes	Yes
		Link fault detection	Yes	Yes
		Link troubleshooting	Yes	Yes
		Remote loopback	Yes	Yes
	CFM (802.1ag)	Software-level CCM	Yes	Yes
		802.1ag MAC ping	Yes	Yes
		802.1ag MAC trace	Yes	Yes
	OAM association	Association between 802.1ag and 802.3ah	Yes	Yes
	Y.1731	Unidirectional delay and jitter measurement	Yes	Yes
		Bidirectional delay and jitter measurement	Yes	Yes
QoS features	Traffic classification	Traffic classification based on ACLs	Yes	Yes
		Configuring traffic classification priorities	Yes	Yes
		Matching the simple domains of packets	Yes	Yes
	Traffic behavior	Traffic filtering	Yes	Yes
		Traffic policing (CAR)	Yes	Yes
		Modifying the packet priorities	Yes	Yes
		Modifying the simple domains of packets	Yes	Yes
		Modifying the packet VLANs	Yes	Yes
	Traffic	Traffic shaping on an egress interface	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
	shaping	Traffic shaping on queues on an interface	Yes	Yes
	Congestion avoidance	Weighted Random Early Detection (WRED) on queues	Yes	Yes
		Tail drop	Yes	Yes
	Congestion management	Priority Queuing (PQ)	Yes	Yes
		Weighted Deficit Round Robin (WDRR)	Yes	Yes
		PQ+WDRR	Yes	Yes
ACL	Packet filtering at Layer 2 to Layer 4	Number of rules per IPv4 ACL	6K (Shared with IPv6)	6K (Shared with IPv6)
		Number of rules per IPv6 ACL	6K (Shared with IPv4)	6K (Shared with IPv4)
		Basic IPv4 ACL	Yes	Yes
		Advanced IPv4 ACL	Yes	Yes
		Basic IPv6 ACL	Yes	Yes
		Advanced IPv6 ACL	Yes	Yes
		Layer 2 ACL	Yes	Yes
		User group ACL	Yes	Yes
		User-defined ACL	Yes	Yes
Configuration and maintenance	Login and configuration management	Command line interface (CLI)-based configuration	Yes	Yes
		Console terminal service	Yes	Yes
		Telnet terminal service	Yes	Yes
		SSH v1.5	Yes	Yes
		SSH v2.0	Yes	Yes
		SNMP-based NMS for unified configuration	Yes	Yes
		Web page-based configuration and management	Yes	Yes
		EasyDeploy (client)	Yes	Yes
		EasyDeploy (commander)	Yes	Yes
		SVF	Yes	Yes
		Cloud management	Yes	Yes
		OPS	Yes	Yes
	File system	Directory and file management	Yes	Yes
		File upload and download	Yes	Yes
	Monitoring and maintenance	Deception	Yes	Yes
		ECA	Yes	Yes
		eMDI	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
		Hardware monitoring	Yes	Yes
		Log information output	Yes	Yes
		Alarm information output	Yes	Yes
		Debugging information output	Yes	Yes
		Port mirroring	Yes	Yes
		Flow mirroring	Yes	Yes
		Remote mirroring	Yes	Yes
		Energy saving	Yes	Yes
	Version upgrade	Version upgrade	Yes	Yes
		Version rollback	Yes	Yes
Security	ARP security	ARP packet rate limiting	Yes	Yes
		ARP anti-spoofing	Yes	Yes
		Association between ARP and STP	Yes	Yes
		ARP gateway anti-collision	Yes	Yes
		Dynamic ARP Inspection (DAI)	Yes	Yes
		Static ARP Inspection (SAI)	Yes	Yes
		Egress ARP Inspection (EAI)	Yes	Yes
	IP security	ICMP attack defense	Yes	Yes
		IPSG for IPv4	Yes	Yes
		IPSG user capacity	3K	3K
		IPSG for IPv6	Yes	Yes
		IPSGv6 user capacity	1.5K	1.5K
	Local attack defense	CPU attack defense	Yes	Yes
	MFF	MFF	Yes	Yes
	DHCP snooping	DHCP snooping	Yes	Yes
		Option 82 function	Yes	Yes
		Dynamic rate limiting for DHCP packets	Yes	Yes
	Attack defense	Defense against malformed packet attacks	Yes	Yes
		Defense against UDP flood attacks	Yes	Yes
		Defense against TCP SYN flood attacks	Yes	Yes
		Defense against ICMP flood attacks	Yes	Yes
		Defense against packet fragment attacks	Yes	Yes
		Local URPF	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
User access and authentication	AAA	Local authentication	Yes	Yes
		Local authorization	Yes	Yes
		RADIUS authentication	Yes	Yes
		RADIUS authorization	Yes	Yes
		RADIUS accounting	Yes	Yes
		HWTACACS authentication	Yes	Yes
		HWTACACS authorization	Yes	Yes
		HWTACACS accounting	Yes	Yes
	NAC	802.1X authentication	Yes	Yes
		MAC address authentication	Yes	Yes
		Portal authentication	Yes	Yes
		Hybrid authentication	Yes	Yes
	Policy association	Functioning as the control device	Yes	Yes
Network management	-	Ping	Yes	Yes
		Tracert	Yes	Yes
		NQA	Yes	Yes
		NTP	Yes	Yes
		iPCA	Yes	Yes
		NetStream	Yes	Yes
		SNMP v1	Yes	Yes
		SNMP v2	Yes	Yes
		SNMP v3	Yes	Yes
		HTTP	Yes	Yes
		HTTPS	Yes	Yes
		RMON	Yes	Yes
		RMON2	Yes	Yes
		NETCONF/YANG	Yes	Yes
WLAN	-	AP management	Yes	Yes
		Number of managed APs	1K	1K
		Radio management	Yes	Yes
		WLAN service management	Yes	Yes
		WLAN QoS	Yes	Yes
		WLAN security	Yes	Yes

Function and Feature		Description	CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
		WLAN user management	Yes	Yes
VXLAN	-	VXLAN Layer 2 gateway	Yes	Yes
		VXLAN Layer 3 gateway	Yes	Yes
		Centralized gateway	Yes	Yes
		Distributed gateway	Yes	Yes
		BGP-EVPN	Yes	Yes
		BGP-EVPN neighbor capacity	256	256
Interoperability	-	VLAN-based Spanning Tree (VBST)	Yes	Yes
		Link-type Negotiation Protocol (LNP)	Yes	Yes
		VLAN Central Management Protocol (VCMP)	Yes	Yes

NOTE

This content is applicable only to regions outside mainland China. Huawei reserves the right to interpret this content.

Hardware Specifications

The following table lists hardware specifications of the CloudEngine S6730-H series.

Item		CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
Physical specifications	Dimensions (H x W x D)	43.6 mm x 442.0 mm x 420.0 mm (1.72 in. x 17.4 in. x 16.5 in.)	43.6 mm x 442.0 mm x 420.0 mm (1.72 in. x 17.4 in. x 16.5 in.)
	Chassis height	1 U	1 U
	Chassis weight (full configuration weight, including weight of packaging materials)	8.9 kg (19.62 lb)	9.2 kg (20.28 lb)
Fixed port	10GE port	24	48
	25GE port	-	-
	40GE port	6 (40GE and 100GE auto-sensing)	6 (40GE and 100GE auto-sensing.)
	100GE port	6	6
Management port	ETH management port	Supported	Supported
	Console port (RJ45)	Supported	Supported
	USB port	USB 2.0	USB 2.0
CPU	Frequency	1.4 GHz	1.4 GHz
	Cores	4	4
Memory	Memory (RAM)	4GB	4GB
	Flash	Hardware: 2 GB	Hardware: 2 GB
Power supply system	Power supply type	• 600 W AC (pluggable) • 1000 W DC (pluggable)	• 600 W AC (pluggable) • 1000 W DC (pluggable)

Item		CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
	Rated voltage range	• AC input: 100 V AC to 240 V AC, 50/60 Hz • High-Voltage DC input: 240 V DC • DC input: -48 V DC to -60 V DC	• AC input: 100 V AC to 240 V AC, 50/60 Hz • High-Voltage DC input: 240 V DC • DC input: -48 V DC to -60 V DC
	Maximum voltage range	• AC input: 90 V AC to 290 V AC, 45 Hz to 65 Hz • High-Voltage DC input: 190 V DC to 290 V DC • DC input: -38.4 V DC to -72 V DC	• AC input: 90 V AC to 290 V AC, 45 Hz to 65 Hz • High-Voltage DC input: 190 V DC to 290 V DC • DC input: -38.4 V DC to -72 V DC
	Maximum input current	• AC 600W：8A • DC 1000W：30A	• AC 600W：8A • DC 1000W：30A
	Typical power consumption (30% of traffic load, tested according to ATIS standard)	149 W	165 W
	Maximum power consumption (100% throughput, full speed of fans)	254 W	291 W
Heat dissipation system	Heat dissipation mode	Air-cooled heat dissipation and intelligent fan speed adjustment	Air-cooled heat dissipation and intelligent fan speed adjustment
	Number of fan modules	4, Fan modules are pluggable	4, Fan modules are pluggable
	Airflow	Air flows in from the front side and exhausts from the rear panel	Air flows in from the front side and exhausts from the rear panel
Environment parameters	Long-term operating temperature	• 0-1800 m: -5°C to 45°C • 1800-5000 m: The operating temperature decreases 1°C for every 220 m increase in altitude.	• 0-1800 m: -5°C to 45°C • 1800-5000 m: The operating temperature decreases 1°C for every 220 m increase in altitude.
	Storage temperature	-40°C to +70°C	-40°C to +70°C
	Relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing
	Operating altitude	0-5000 m	0-5000 m
	Noise under normal temperature (sound power)	< 65 dB(A)	< 65 dB(A)
	Noise under high temperature (sound power)	< 88 dB(A)	< 88 dB(A)
	Noise under normal temperature (sound pressure)	< 52 dB(A)	< 52 dB(A)
	Surge protection specification (power port)	• Using AC power modules: ±6 kV in differential mode, ±6 kV in common mode • Using DC power modules: ±2 kV in differential mode, ±4 kV in common mode	• Using AC power modules: ±6 kV in differential mode, ±6 kV in common mode • Using DC power modules: ±2 kV in differential mode, ±4 kV in common mode

Item		CloudEngine S6730-H24X6C	CloudEngine S6730-H48X6C
Reliability	MTBF (year)[2]	62.27	56.87
	MTTR (hour)	2	2
	Availability	> 0.99999	> 0.99999
Certification		• EMC certification • Safety certification • Manufacturing certification **NOTE** For details about certifications, see the section Safety and Regulatory Compliance.	• EMC certification • Safety certification • Manufacturing certification **NOTE** For details about certifications, see the section Safety and Regulatory Compliance.

NOTE

1: The power consumption under different load conditions is calculated according to the ATIS standard. Additionally.

2: The reliability parameter values are calculated based on the typical configuration of the device. The parameter values vary according to the modules configured by the customer.

Licensing

This series switches supports both the traditional feature-based licensing mode and the latest Huawei IDN One Software (N1 mode for short) licensing mode. The N1 mode is ideal for deploying Huawei CloudCampus Solution in the on-premises scenario, as it greatly enhances the customer experiences in purchasing and upgrading software services with simplicity.

Software Package Features in N1 Mode

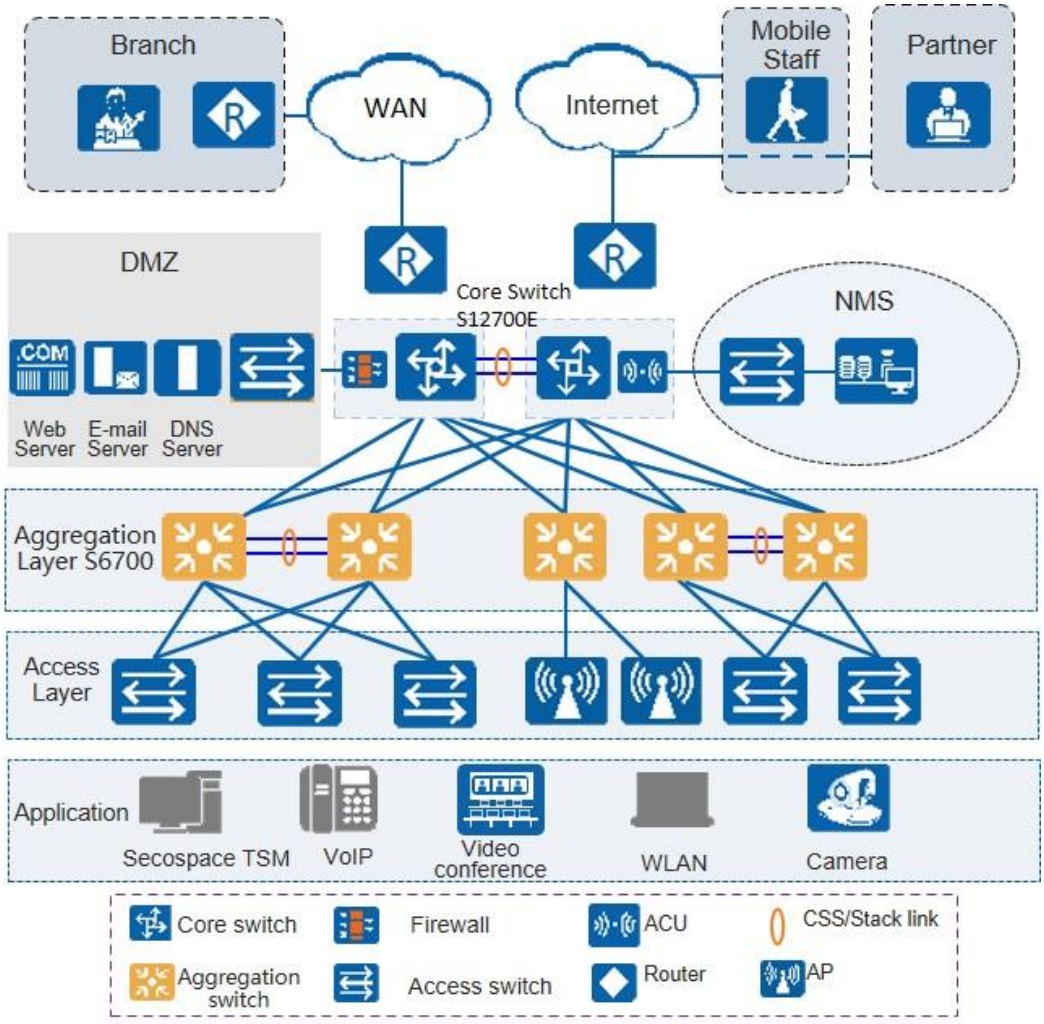
Switch Functions	N1 Basic Software	N1 Foundation Software Package	N1 Advanced Software Package
Basic network functions: Layer 2 functions, IPv4, IPv6, MPLS, SVF, and others Note: For details, see the Service Features	√	√	√
Basic network automation based on the iMaster NCE-Campus: • Basic automation: Plug-and-play, SSID, and AP group management • Basic monitoring: Application visualization • NE management: Image and topology management and discovery • WLAN enhancement: Roaming and optimization for up to 128 APs • User access authentication	×	√	√
Advanced network automation and intelligent O&M: VXLAN, free mobility, and CampusInsight basic functions	×	×	√

Note: Only V200R019C00 and later versions can support N1 mode

Networking and Applications

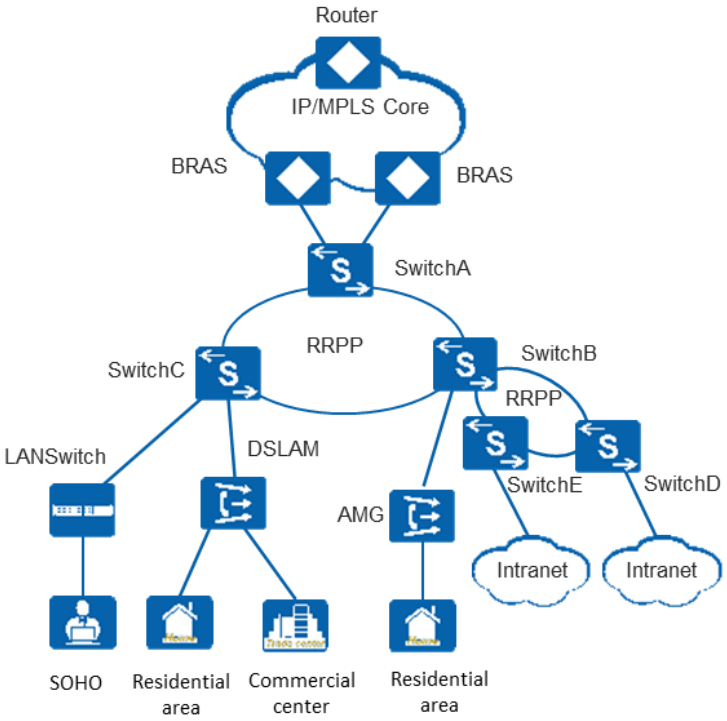
Large-scale Enterprise Campus Network

CloudEngine S6730-H series switches can be deployed at the aggregation layer of a large-scale enterprise campus network, creating a highly reliable, scalable, and manageable enterprise campus network.



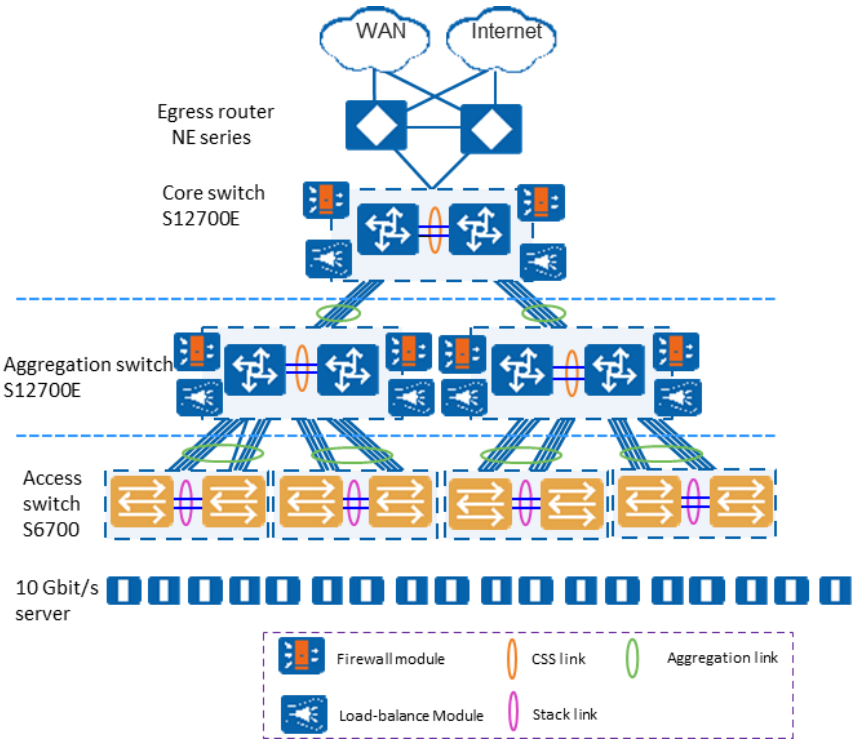
Application on a MAN

CloudEngine S6730-H series switches can be deployed at the access layer of a MAN(Metropolitan Area Network) to build a high-performance, multi-service, and highly reliable ISP MAN network.



Data Center

CloudEngine S6730-H switches can be deployed at the access layer build a virtualized, highly reliable, non-blocking, and energy conservative data center network.



Product Accessories

Optical Modules and Fibers

10GE SFP+ ports support optical modules and cables

- GE optical module

- GE-CWDM optical module
- GE-DWDM optical module
- GE copper module
- 10GE SFP+ optical module (OSXD22N00 not supported)
- 10GE-CWDM optical module
- 10GE-DWDM optical module
- 1 m, 3 m, 5 m, and 10 m SFP+ high-speed copper cables
- 3 m and 10 m SFP+ AOC cables
- 0.5 m and 1.5 m SFP+ dedicated stack cables (supported by the last 16 SFP+ ports and used only for zero-configuration stacking)

25GE SFP28 ports support optical modules and cables

- GE eSFP optical module
- GE SFP optical module
- GE-CWDM optical module
- GE-DWDM optical module
- 10GE SFP+ optical module (OSXD22N00 not supported)
- 10GE-CWDM optical module
- 10GE-DWDM optical module
- 25GE SFP28 optical module
- 1 m, 3 m, 5 m, and 10 m SFP+ high-speed cables
- 3 m and 10 m SFP+ AOC cables
- 1 m, 3 m, 5 m SFP28 high-speed cables
- 3 m, 5 m, 7 m, and 10 m SFP28 AOC cables

40GE/100GE QSFP28 ports support optical modules and cables

- QSFP+ optical module
- QSFP28 optical module
- 1 m, 3 m, and 5 m QSFP+ to QSFP+ high-speed copper cables
- 10 m QSFP+ to QSFP+ AOC cable
- 1 m QSFP28 to QSFP28 high-speed copper cable
- 10 m QSFP28 to QSFP28 AOC cable

NOTE

- A QSFP28 optical port cannot be split into four 10GE ports, regardless of whether the port uses a QSFP28 or QSFP+ optical module.
- By default, the S6730-H48X6C (part number: 02352FSF) does not have the license loaded, and QSFP28 ports on the switch are 40GE ports. The QSFP28 ports can work as 100GE ports after you activate the license, run the **assign port-speed 100GE** command, and restart the switch.
- On the S6730-H48X6C (part number: 02353FWL), the license has been activated and QSFP28 ports on these switches work as 100GE ports. To change the rate of QSFP28 ports from 100GE to 40GE, run the **undo assign port-speed 100GE** command and restart the switch.

Stack Cables

The CloudEngine S6730-H Series switches support service port stacking. The applicable stack cables are as follows:

Port Supporting Stacking	Stack Cable	Rate of a Single Port
10GE ports on the front panel	• 1 m, 3 m, and 5 m SFP+ passive high-speed cables • 10 m SFP+ active high-speed copper cables	10 Gbit/s

Port Supporting Stacking	Stack Cable	Rate of a Single Port
	• 3 m and 10 m AOC cables • 10GE SFP+ optical module and optical fiber • 0.5 m and 1.5 m SFP+ dedicated stack cable	
40GE/100GE ports on the front panel	• 1 m QSFP28 high-speed copper cables • 10 m QSFP28 AOC cables • QSFP28 optical module and optical fiber	100Gbit/s

Safety and Regulatory Compliance

The following table lists the safety and regulatory compliance of the CloudEngine S6730-H.

Certification Category	Description
Safety	• IEC 60950-1 and all country deviations • EN 60950-1 • UL 60950-1 • CAN/CSA 22.2 No.60950-1 • GB 4943
Electromagnetic Compatibility (EMC)	• EMI • FCC CFR47 Part 15 Class A • EN55022 Class A • CISPR 22 Class A • EN61000-3-2/IEC-1000-3-2, Power line harmonics • EN61000-4-3/IEC-1000-4-3, Radiated immunity • EN61000-4-2/IEC-1000-4-2, ESD • EN61000-4-4/IEC-1000-4-4, EFT • EN61000-4-5/IEC-1000-4-5, Surge Signal Port • EN61000-4-6/IEC-1000-4-6, Low frequency conducted immunity • EN61000-4-11/IEC-1000-4-11, Voltage dips and sags • EN61000-4-29/IEC61000-4-29, Voltage dips and sags • EMC Directive 89/336/EEC • EMC Directive 2004/108/EC • VCCI V-3 Class A • ICES-003 Class A • AS/NZS CISPR 22 Class A • CNS 13438 Class A • GB9254 Class A

NOTE

- EMC: electromagnetic compatibility
- CISPR: International Special Committee on Radio Interference
- EN: European Standard
- ETSI: European Telecommunications Standards Institute
- CFR: Code of Federal Regulations
- FCC: Federal Communication Commission

- IEC: International Electrotechnical Commission
- AS/NZS: Australian/New Zealand Standard
- VCCI: Voluntary Control Council for Interference
- UL: Underwriters Laboratories
- CSA: Canadian Standards Association
- IEEE: Institute of Electrical and Electronics Engineers

MIB and Standards Compliance

Supported MIBs

Category	MIB
Public MIB	• BRIDGE-MIB • DISMAN-NSLOOKUP-MIB • DISMAN-PING-MIB • DISMAN-TRACEROUTE-MIB • ENTITY-MIB • EtherLike-MIB • IF-MIB • IP-FORWARD-MIB • IPv6-MIB • LAG-MIB • LLDP-EXT-DOT1-MIB • LLDP-EXT-DOT3-MIB • LLDP-MIB • NOTIFICATION-LOG-MIB • NQA-MIB • OSPF-TRAP-MIB • P-BRIDGE-MIB • Q-BRIDGE-MIB • RFC1213-MIB • RIPv2-MIB • RMON2-MIB • RMON-MIB • SAVI-MIB • SNMP-FRAMEWORK-MIB • SNMP-MPD-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMP-USER-BASED-SM-MIB • SNMPv2-MIB • TCP-MIB • UDP-MIB
Huawei-proprietary MIB	• HUAWEI-AAA-MIB • HUAWEI-ACL-MIB • HUAWEI-ALARM-MIB

Category	MIB
	• HUAWEI-ALARM-RELIABILITY-MIB • HUAWEI-BASE-TRAP-MIB • HUAWEI-BRAS-RADIUS-MIB • HUAWEI-BRAS-SRVCFG-EAP-MIB • HUAWEI-BRAS-SRVCFG-STATICUSER-MIB • HUAWEI-CBQOS-MIB • HUAWEI-CDP-COMPLIANCE-MIB • HUAWEI-CONFIG-MAN-MIB • HUAWEI-CPU-MIB • HUAWEI-DAD-TRAP-MIB • HUAWEI-DC-MIB • HUAWEI-DATASYNC-MIB • HUAWEI-DEVICE-MIB • HUAWEI-DHCPR-MIB • HUAWEI-DHCPS-MIB • HUAWEI-DHCP-SNOOPING-MIB • HUAWEI-DIE-MIB • HUAWEI-DNS-MIB • HUAWEI-DLDP-MIB • HUAWEI-ELMI-MIB • HUAWEI-ERPS-MIB • HUAWEI-ERRORDOWN-MIB • HUAWEI-ENERGYMNGT-MIB • HUAWEI-EASY-OPERATION-MIB • HUAWEI-ENTITY-EXTENT-MIB • HUAWEI-ENTITY-TRAP-MIB • HUAWEI-ETHARP-MIB • HUAWEI-ETHOAM-MIB • HUAWEI-FLASH-MAN-MIB • HUAWEI-FWD-RES-TRAP-MIB • HUAWEI-GARP-APP-MIB • HUAWEI-GTSM-MIB • HUAWEI-HGMP-MIB • HUAWEI-HWTACACS-MIB • HUAWEI-IF-EXT-MIB • HUAWEI-INFOCENTER-MIB • HUAWEI-IPPOOL-MIB • HUAWEI-IPV6-MIB • HUAWEI-ISOLATE-MIB • HUAWEI-L2IF-MIB • HUAWEI-L2MAM-MIB • HUAWEI-L2VLAN-MIB • HUAWEI_LDT-MIB • HUAWEI-LLDP-MIB • HUAWEI-MAC-AUTHEN-MIB

Category	MIB
	• HUAWEI-MEMORY-MIB • HUAWEI-MFF-MIB • HUAWEI-MFLP-MIB • HUAWEI-MSTP-MIB • HUAWEI-MULTICAST-MIB • HUAWEI-NAP-MIB • HUAWEI-NTPV3-MIB • HUAWEI-PERFORMANCE-MIB • HUAWEI-PORT-MIB • HUAWEI-PORTAL-MIB • HUAWEI-QINQ-MIB • HUAWEI-RIPv2-EXT-MIB • HUAWEI-RM-EXT-MIB • HUAWEI-RRPP-MIB • HUAWEI-SECURITY-MIB • HUAWEI-SEP-MIB • HUAWEI-SNMP-EXT-MIB • HUAWEI-SSH-MIB • HUAWEI-STACK-MIB • HUAWEI-SWITCH-L2MAM-EXT-MIB • HUAWEI-SWITCH-SRV-TRAP-MIB • HUAWEI-SYS-MAN-MIB • HUAWEI-TCP-MIB • HUAWEI-TFTPC-MIB • HUAWEI-TRNG-MIB • HUAWEI-XQOS-MIB

NOTE

For more information about MIBs supported by the CloudEngine S6730-H series, visit:
https://support.huawei.com/enterprise/en/switches/s6700-pid-6691593?category=reference-guides

Standards Compliance

The following table lists the standards that the CloudEngine S6730-H series complies with.

Standard Organization	Standard or Protocol
IETF	• RFC 768 User Datagram Protocol (UDP) • RFC 792 Internet Control Message Protocol (ICMP) • RFC 793 Transmission Control Protocol (TCP) • RFC 826 Ethernet Address Resolution Protocol (ARP) • RFC 854 Telnet Protocol Specification • RFC 951 Bootstrap Protocol (BOOTP) • RFC 959 File Transfer Protocol (FTP) • RFC 1058 Routing Information Protocol (RIP) • RFC 1112 Host extensions for IP multicasting • RFC 1157 A Simple Network Management Protocol (SNMP)

Standard Organization	Standard or Protocol
	• RFC 1256 ICMP Router Discovery • RFC 1305 Network Time Protocol Version 3 (NTP) • RFC 1349 Internet Protocol (IP) • RFC 1493 Definitions of Managed Objects for Bridges • RFC 1542 Clarifications and Extensions for the Bootstrap Protocol • RFC 1643 Ethernet Interface MIB • RFC 1757 Remote Network Monitoring (RMON) • RFC 1901 Introduction to Community-based SNMPv2 • RFC 1902-1907 SNMP v2 • RFC 1981 Path MTU Discovery for IP version 6 • RFC 2131 Dynamic Host Configuration Protocol (DHCP) • RFC 2328 OSPF Version 2 • RFC 2453 RIP Version 2 • RFC 2460 Internet Protocol, Version 6 Specification (IPv6) • RFC 2461 Neighbor Discovery for IP Version 6 (IPv6) • RFC 2462 IPv6 Stateless Address Auto configuration • RFC 2463 Internet Control Message Protocol for IPv6 (ICMPv6) • RFC 2474 Differentiated Services Field (DS Field) • RFC 2740 OSPF for IPv6 (OSPFv3) • RFC 2863 The Interfaces Group MIB • RFC 2597 Assured Forwarding PHB Group • RFC 2598 An Expedited Forwarding PHB • RFC 2571 SNMP Management Frameworks • RFC 2865 Remote Authentication Dial In User Service (RADIUS) • RFC 3046 DHCP Option82 • RFC 3376 Internet Group Management Protocol, Version 3 (IGMPv3) • RFC 3513 IP Version 6 Addressing Architecture • RFC 3579 RADIUS Support For EAP • RFC 4271 A Border Gateway Protocol 4 (BGP-4) • RFC 4760 Multiprotocol Extensions for BGP-4 • draft-grant-tacacs-02 TACACS+ • RFC 6241 Network Configuration Protocol (NETCONF) • RFC 6020 YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)
IEEE	• IEEE 802.1D Media Access Control (MAC) Bridges • IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering • IEEE 802.1Q Virtual Bridged Local Area Networks • IEEE 802.1ad Provider Bridges • IEEE 802.2 Logical Link Control • IEEE Std 802.3 CSMA/CD • IEEE Std 802.3ab 1000BASE-T specification • IEEE Std 802.3ad Aggregation of Multiple Link Segments • IEEE Std 802.3ae 10GE WEN/LAN Standard • IEEE Std 802.3x Full Duplex and flow control

Standard Organization	Standard or Protocol
	• IEEE Std 802.3z Gigabit Ethernet Standard • IEEE 802.1ax/IEEE802.3ad Link Aggregation • IEEE 802.3ah Ethernet in the First Mile. • IEEE 802.1ag Connectivity Fault Management • IEEE 802.1ab Link Layer Discovery Protocol • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1w Rapid Spanning Tree Protocol • IEEE 802.1s Multiple Spanning Tree Protocol • IEEE 802.1x Port based network access control protocol • IEEE 802.3az Automatic power adjustment on Ethernet interfaces
ITU	• ITU SG13 Y.17ethoam • ITU SG13 QoS control Ethernet-Based IP Access • ITU-T Y.1731 ETH OAM performance monitor
ISO	• ISO 10589 IS-IS Routing Protocol
MEF	• MEF 2 Requirements and Framework for Ethernet Service Protection • MEF 9 Abstract Test Suite for Ethernet Services at the UNI • MEF 10.2 Ethernet Services Attributes Phase 2 • MEF 11 UNI Requirements and Framework • MEF 13 UNI Type 1 Implementation Agreement • MEF 15 Requirements for Management of Metro Ethernet Phase 1 Network Elements • MEF 17 Service OAM Framework and Requirements • MEF 20 UNI Type 2 Implementation Agreement • MEF 23 Class of Service Phase 1 Implementation Agreement • Xmodem XMODEM/YMODEM Protocol Reference

NOTE

The listed standards and protocols are fully or partially supported by Huawei switches. For details, visit http://e.huawei.com/en or contact your local Huawei sales office.

Ordering Information

The following table lists ordering information of the CloudEngine S6730-H series.

Model	Product Description
CloudEngine S6730-H48X6C	S6730-H48X6C (48*10GE SFP+ ports, 6*40GE QSFP28 ports, optional license for upgrade to 6*100GE QSFP28, without power module)
CloudEngine S6730-H24X6C	S6730-H24X6C (24*10GE SFP+ ports, 6*40GE QSFP28 ports, optional license for upgrade to 6*100GE QSFP28, without power module)
CloudEngine S6730-H48X6C	S6730-H48X6C Bundle (48*10GE SFP+ ports, 6*40GE/100GE QSFP28 ports, with license, without power module)
CloudEngine S6730-H24X6C	S6730-H24X6C Bundle (24*10GE SFP+ ports, 6*40GE/100GE QSFP28 ports, with license, without power module)
PAC600S12-CB	600W AC power module (for S6730-H48X6C/S6730-H24X6C series models)

Model	Product Description
PDC1000S12-DB	1000W DC power module (for S6730-H48X6C/S6730-H24X6C series models)
FAN-031A-B	Fan Module (for S6730-H48X6C/S6730-H24X6C series models)

License	Product Description
N1-S67H-M-Lic	S67XX-H Series Basic SW,Per Device
N1-S67H-M-SnS1Y	S67XX-H Series Basic SW,SnS,Per Device,1Year
L-100GEUPG-S67H	S67XX-H Series,40GE to 100GE Electronic RTU License,Per Device
L-VxLAN-S67	S67 Series, VxLAN License, Per Device
L-1AP-S67	S67 Series, Wireless Access Controller AP Resource License-1AP
N1-S67H-F-Lic	N1-CloudCampus,Foundation,S67XX-H Series,Per Device
N1-S67H-F-SnS	N1-CloudCampus,Foundation,S67XX-H Series,SnS,Per Device
N1-S67H-A-Lic	N1-CloudCampus,Advanced,S67XX-H Series,Per Device
N1-S67H-A-SnS	N1-CloudCampus,Advanced,S67XX-H Series,SnS,Per Device
N1-S67H-FToA-Lic	N1-Upgrade-Foundation to Advanced,S67XX-H,Per Device
N1-S67H-FToA-SnS	N1-Upgrade-Foundation to Advanced,S67XX-H,SnS,Per Device
N1-AM-30-Lic	N1-CloudCampus, Add-On Package, Access Management, Per 30 Endpoints
N1-AM-30-SnS1Y	N1-CloudCampus, Add-On Package, Access Management, Software Subscription and Support, Per 30 Endpoints, 1 Year
N1-EPNP-30-Lic	N1-CloudCampus, Add-On Package, Endpoints Plug and Play, Per 30 Endpoints
N1-EPNP-30-SnS1Y	N1-CloudCampus, Add-On Package, Endpoints Plug and Play, Software Subscription and Support, Per 30 Endpoints, 1 Year
N1-APP-X7FSwitch	N1-CloudCampus, Add-On Package, Intelligent Application Analysis, X7 Series Fixed Switch, Per Device
N1-APP-X7FSwitch-SnS1Y	N1-CloudCampus, Add-On Package, Intelligent Application Analysis, X7 Series Fixed Switch, Software Subscription and Support, Per Device, 1 Year

More Information

For more information about the Huawei Campus Switches, visit http://e.huawei.com or contact us in the following ways:

- Global service hotline: http://e.huawei.com/en/service-hotline
- Logging in to the Huawei Enterprise technical support website: http://support.huawei.com/enterprise/
- Sending an email to the customer service mailbox: support_e@huawei. com

Huawei Technologies Co., Ltd.

Address:Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

Website:e.huawei.com

SSR100 LINE OF ROUTERS DATASHEET

Product Overview

SSR Series Routers enable enterprises to build service-centric fabrics for any size of distributed enterprise. Powered by Session Smart technology, the purpose-built, high-performance branch routers are preloaded with Juniper Session Smart software (subscription licenses sold separately), allowing businesses to build networking environments that deliver the agility they need to move with their customers and outpace their competitors.

Product Description

Juniper® SSR Series Routers offer purpose-built, high-performance platforms that enable enterprises to build service-centric fabrics for distributed enterprises of any size.

The Juniper SSR120 Session Smart™ Router and SSR130 Session Smart Router provide the hardware foundation for Juniper SD-WAN driven by Mist AI™. When deployed at branch offices, the SSR100 line of routers provide a service-centric control plane and service-aware data plane that offer IP routing, feature-rich policy management, improved visibility, and proactive analytics. The result is a next-generation SD-WAN solution that supports the evolving needs of cloud-enabled enterprise networks.

For features and benefits of Juniper Session Smart Routers, as well as ordering information, see the Session Smart Routing Data Sheet.

Architecture and Key Components

By combining the Mist AI in Juniper Mist™ WAN Assurance with the SSR Series routers, enterprises gain industry-leading automation and insight to ensure the best user, device, and application experiences in branch and remote locations. The Juniper WAN Assurance cloud service enables simpler operations, provides better visibility into end-user experiences, and reduces mean time to repair SD-WAN issues. For detailed features and benefits of Juniper Mist WAN Assurance, see the WAN Assurance Data Sheet.

SSR120 Session Smart Router: Small Branch Model

SSR130 Session Smart Router: Medium-Sized Branch Model

The Juniper Networks SSR100 line of routers provides a service-centric control plane and service-aware data plane that offer IP routing, feature-rich policy management, improved visibility, and proactive analytics.

The fixed configuration appliances in the SSR100 line are:

- The **SSR120** for small branches
- The **SSR130** for medium branches

These appliances run the FIPS 140-2 Level 1 compliant Session Smart Router software, which provides secure and resilient WAN connectivity.

For more detailed information on basic configuration procedures for these platforms, see:

- SSR120 Hardware Guide
- SSR130 Hardware Guide

SSR120: Small Branch Routers

The SSR120 Router is ideal for small branches

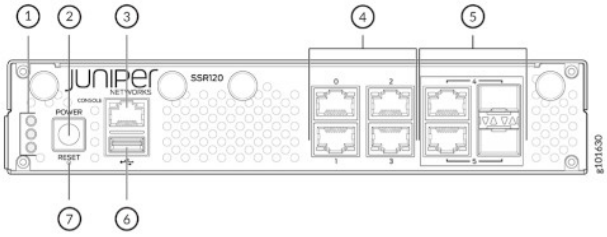


Figure 1: Front Panel Components of SSR120

SSR120 Front Panel Components

1. Chassis LEDs
2. Power button
3. Console port
4. 1 GbE Ethernet ports (0 through 3)
5. 1 GbE RJ-45/SFP ports (4 & 5)
6. USB 3.0 port
7. Reset button

The SSR120 supports:

- 4 x 1GbE RJ-45 ports
- 2 x 1GbE RJ-45/SFP ports
- Console and USB ports

SSR120 LTE Variants (SSR120-AA and SSR120-AE)

The SSR120 LTE variants (SSR120-AA and SSR130-AE) have antenna connectors for LTE.

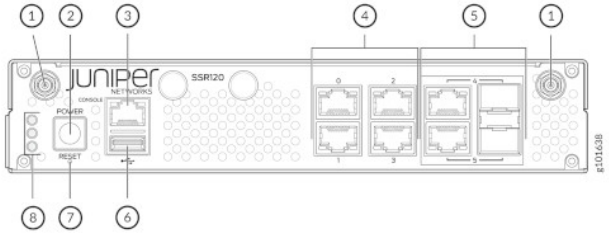


Figure 2: Front Panel Components of SSR120-AA and SSR120-AE

SSR120-AA and SSR120-AE Front Panel Components

1. Antenna connectors for LTE
2. Power button
3. Console port
4. 1 GbE Ethernet ports (0 through 3)
5. 1 GbE RJ-45/SFP ports (4 & 5)
6. USB 3.0 port
7. Reset button
8. Chassis LEDs

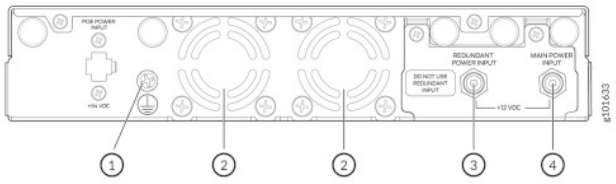


Figure 3: Real Panel Components of SSR120

SSR120 Rear Panel Components

1. Ground terminal
2. Fan
3. Redundant power input (unsupported – do not use)
4. Main power input

SSR130: Medium Branch Routers

The SSR130 Router is ideal for medium branches

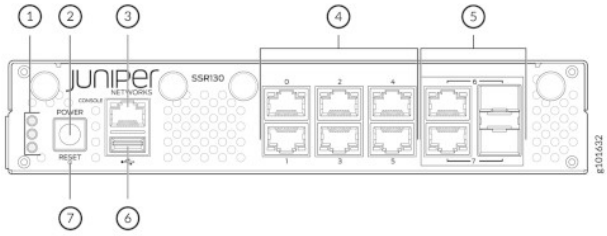


Figure 4: Front Panel Components of SSR130

SSR130 Front Panel Components

1. Chassis LEDs
2. Power button
3. Console port
4. 1 GbE Ethernet ports (0 through 5)
5. 1 GbE RJ-45/SFP ports (6 & 7)
6. USB 3.0 port
7. Reset button

The SSR130 supports:

- 6 x 1GbE RJ-45 ports
- 2 x 1GbE RJ-45/SFP ports
- Console and USB ports

SSR130 LTE Variants (SSR120-AA and SSR120-AE)

The SSR130 LTE variants (SSR130-AA and SSR130-AE) have antenna connectors for LTE.

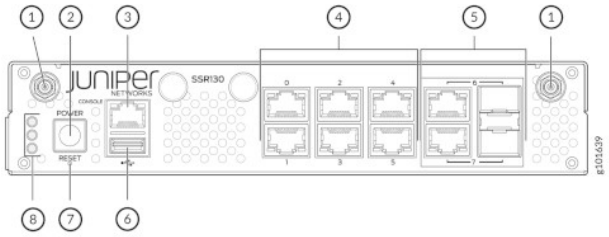


Figure 5: Front Panel Components of SSR130-AA and SSR130-AE

SSR130-AA and SSR130-AE Front Panel Components

1. Antenna connectors for LTE
2. Power button
3. Console port
4. 1 GbE Ethernet ports (0 through 5)
5. 1 GbE RJ-45/SFP ports (6 & 7)
6. USB 3.0 port
7. Reset button
8. Chassis LED

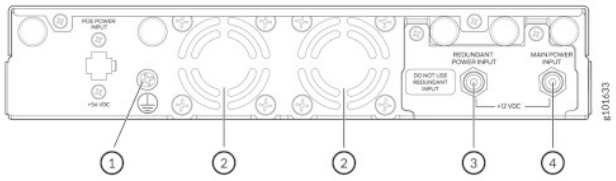


Figure 6: Rear Panel Components of an SSR130

SSR130 Rear Panel Components

1. Ground terminal
2. Fans
3. Redundant power input (unsupported – do not use)
4. Main power input

Features and Benefits

Zero Trust Security

The SSR100 line of routers ensures Zero Trust security by authenticating all routes and encrypting all session traffic. Applications, devices, and users cannot initiate any session that does not comply with the authentication policies and access rules. These appliances support Layer 2 through Layer 5 stateful firewall functions, including denial of service (DoS) and distributed denial of service (DDoS) protection, Network Address Translation (NAT), encryption, VPN, and traffic filtering.

Adaptive Encryption

The SSR100 line of routers automatically detects traffic encrypted using HTTPS or IPsec and does not re-encrypt such traffic. This capability results in improved performance and reduced overhead due to double encryption.

Simplified Onboarding and Monitoring with Juniper Mist WAN Assurance

You can quickly onboard SSR100 appliances to the Juniper Mist cloud using the claim code or QR code on the device. This helps reduce operational complexity and simplifies the deployment and configuration process. For more information regarding onboarding, configuration, and management of SSR Series devices, see the WAN Assurance Data Sheet.

Specifications

SSR120 and SSR130 Session Smart Routers Specifications

		SSR120	SSR130
Performance (as observed on Session Smart Router Software v5)			
Encrypted + HMAC (aggregate)	(IMIX)	250 Mbps	1 Gbps
	(1500 Bytes)	500 Mbps	1.8 Gbps
Encrypted only (aggregate)	(IMIX)	750 Mbps	1.8 Gbps
	(1500 Bytes)	2 Gbps (Line rate on ports)	2 Gbps (Line rate on ports)
Unencrypted (aggregate)	(IMIX)	1.5 Gbps	2 Gbps (Line rate on ports)
	(1500 Bytes)	2 Gbps (Line rate on ports)	2 Gbps (Line rate on ports)

	SSR120 for Small Branches	SSR130 for Medium-Sized Branches
Connectivity		
Onboard RJ-45 ports	4 x 1GbE RJ-45	6 x 1GbE RJ-45
Onboard RJ-45/SFP transceiver combo ports	2 x 1GbE RJ-45/SFP combo	2 x 1GbE RJ-45/SFP combo
LTE modules	Single integrated module, not field configurable. Refer to appliance SKUs below: • SSR120-AA: Appliance with LTE for APAC • SSR120-AE: Appliance with LTE for AMER/EMEA • SSR120-AE-TAA: TAA-compliant appliance with LTE for AMER/EMEA	Single integrated module, not field configurable. Refer to appliance SKUs below: • SSR130-AA: Appliance with LTE for APAC • SSR130-AE: Appliance with LTE for AMER/EMEA • SSR130-AE-TAA: TAA-compliant appliance with LTE for AMER/EMEA
Console	1 x 1GbE RJ-45	1 x 1GbE RJ-45
USB	1 x USB3.0	1 x USB3.0
PoE+ ports	Not supported	Not supported

Memory and Storage; Dimensions and Power

	SSR120 for Small Branches	SSR130 for Medium-Sized Branches
Memory and Storage		
System memory (RAM)	8 GB (ECC)	16 GB (ECC)
Storage (SSD)	120 GB	120 GB
Dimensions and Power		
Form factor	Desktop: Rackmount kit (SSR100-RMK) available and sold separately	Desktop: Rackmount kit (SSR100-RMK) available and sold separately
Size (W x D x H)	8.74 x 9.48 x 1.73 in (222 x 241 x 44 mm)	
Weight	3.68 lb (1.67 kg)	
Power supply	AC (external adapter)	AC (external adapter)
External power adapter input (AC)	100-240 V AC, 50-60 Hz, 2 A	100-240 V AC, 50-60 Hz, 2 A
External power adapter output (DC)	12V DC, 5 A	12V DC, 5 A
Maximum power draw (estimated)	32.5 W	41.5 W
Acoustic noise level	19.5 dBA (normal traffic conditions and ambient temperature 27C)	23.4 dBA (normal traffic conditions and ambient temperature 27C)
Power cord	Available for all homologated countries	Available for all homologated countries

Environmental Parameters

	SSR120 for Small Branches	SSR130 for Medium-Sized Branches
Environmental, Compliance, and Safety Certification		
Operating temperature	32° F to 104° F (0° C to 40° C)	32° F to 104° F (0°C to 40° C)
Storage temperature	-4° F to 158° F (-20° C to 70° C)	-4° F to 158° F (-20° C to 70° C)
Mean time between failures (MTBF)	192,918 hours	219,792 hours
TAA compliance	Refer to TAA-compliant appliance SKUs below: • SSR120-TAA: TAA-compliant appliance without LTE • SSR120-AE-TAA: TAA-compliant appliance with LTE for AMER/EMEA	Refer to TAA-compliant appliance SKUs below: • SSR130-TAA: TAA-compliant appliance without LTE • SSR130-AE-TAA: TAA-compliant appliance with LTE for AMER/EMEA
FIPS 140-2	Level 1 (through SSN software)	Level 1 (through SSN software)

LTE Model Specifications

	SSR1x0-AE Model	SSR1x0-AA Model
4G/LTE Capabilities		
Modem	Sierra Wireless EM7455	Sierra Wireless EM7430
Geography	AMER and EMEA	APAC (incl. ANZ)
LTE category	Cat-6	Cat-6
Carrier aggregation	Yes	Yes
SIM type	Micro-SIM	Micro-SIM
LTE bands	1, 2, 3, 4, 5, 7, 8, 12, 13, 20, 25, 26, 29, 30, 41	1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, 41
Antennas	Main and AUX (via SMA connectors)	Main and AUX (via SMA connectors)

Juniper Care Support Services Definitions

Juniper Networks includes an Enhanced Limited Lifetime Warranty (eLLW) for the SSR100 and SSR1000 line of routers by default. The offering provides next-day shipping of hardware replacements for the lifetime of the appliances and supports the entitlements offered under the previous Juniper Care Core and Juniper Care Core Plus contract service levels. For more information on eLLW, please refer to: https://support.juniper.net/support/warranty/

Juniper Care Next-Day Delivery

Juniper will deliver FRU replacements to the ship-to address in advance of receiving returned defective hardware on the next business day, provided the RMA is issued by 3:00 p.m. local time (based on ship-to address), on a business day. If the RMA is issued after 3:00 p.m., Juniper will deliver the replacement FRU on the second business day. “Next-day delivery” is subject to availability.

Juniper Care Same-Day

Juniper Networks will deliver FRU replacements to the ship-to address within four hours of issuance of RMA in advance of receipt of defective hardware. “Same-day delivery” is subject to availability.

For additional information on Juniper Care Services, refer to the Juniper Care Service Description.

SSR120 Session Smart Router Service Options

Hardware SKU	Juniper Care Next-Day Support	Juniper Care Same-Day Support
SSR120	SVC-ND-SSR120	SVC-SD-SSR120
SSR120-AE	SVC-ND-SSR120-AE (US and EMEA only)	SVC-SD-SSR120-AE (US and EMEA only)
SSR120-AA	SVC-ND-SSR120-AA (APAC only)	SVC-SD-SSR120-AA (APAC only)

SSR130 Session Smart Router Service Options

Hardware SKU	Juniper Care Next-Day Support	Juniper Care Same-Day Support
SSR130	SVC-ND-SSR130	SVC-SD-SSR130
SSR130-AE	SVC-ND-SSR130-AE (US and EMEA only)	SVC-SD-SSR130-AE (US and EMEA only)
SSR130-AA	SVC-ND-SSR130-AA (APAC only)	SVC-SD-SSR130-AA (APAC only)

SSR120-TAA Service Options

Hardware SKU	Juniper Care Next-Day Support	Juniper Care Same-Day Support
SSR120-TAA	SVC-ND-SSR120-TAA	SVC-SD-SSR120-TAA
SSR120-AE-TAA	SVC-ND-SSR120-AET (US and EMEA only)	SVC-SD-SSR120-AET (US and EMEA only)

SSR130-TAA Service Options

Hardware SKU	Juniper Care Next-Day Support	Juniper Care Same-Day Support
SSR120-TAA	SVC-ND-SSR120-TAA	SVC-SD-SSR120-TAA
SSR120-AE-TAA	SVC-ND-SSR120-AET (US and EMEA only)	SVC-SD-SSR120-AET (US and EMEA only)

Ordering Information

To order Juniper Networks SSR Series Routers and to access software licensing information, please visit the How to Buy page.

SKU	Description
SSR120 Session Smart Router: Small Branch Model	
SSR120	Small branch appliance (2x1GbE combo RJ-45/SFP, 4x1GbE RJ-45) without LTE*
SSR120-AE	Small branch appliance (2x1GbE combo RJ-45/SFP, 4x1GbE RJ-45) with LTE for Americas and EMEA*
SSR120-AA	Small branch appliance (2x1GbE combo RJ-45/SFP, 4x1GbE RJ-45) with LTE for APAC*
SSR120-TAA Session Smart Router: Small Branch Model for Federal	
SSR120-TAA	Small branch appliance (2x1GbE combo RJ-45/SFP, 4x1GbE RJ-45) without LTE*, TAA-compliant
SSR120-AE-TAA	Small branch appliance (2x1GbE combo RJ-45/SFP, 4x1GbE RJ-45) with LTE for Americas and EMEA*, TAA-compliant
SSR130 Session Smart Router: Medium-Sized Branch Model	
SSR130	Medium-sized branch appliance (2x1GbE combo RJ-45/SFP, 6x1GbE RJ-45) without LTE*
SSR130-AE	Medium-sized branch appliance (2x1GbE combo RJ-45/SFP, 6x1GbR RJ-45) with LTE for Americas and EMEA*
SSR130-AA	Medium-sized branch appliance (2x1GbE combo RJ-45/SFP, 6x1GbE RJ-45) with LTE for APAC*
SSR130-TAA Session Smart Router: Medium-Sized Branch Model for Federal	
SSR130-TAA	Medium-sized branch appliance (2x1GbE combo RJ-45/SFP, 6x1GbE RJ-45) without LTE*, TAA-compliant
SSR130-AE-TAA	Medium-sized branch appliance (2x1GbE combo RJ-45/SFP, 6x1GbE RJ-45) with LTE for Americas and EMEA*, TAA-compliant
Accessories	
SSR100-RMK	Rackmount kit for SSR100 line of Session Smart branch routers

SKU	Description
SSR100-PS	AC-DC power adapter for SSR100 line of Session Smart branch routers; excludes country-specific power cord
Optics	
EX-SFP-1GE-SX	Small form-factor pluggable 1000BASE-SX gigabit Ethernet optics
EX-SFP-1GE-LX	Small form-factor pluggable 1000BASE-LX gigabit Ethernet optics

* Session Smart networking software subscription license, optics, and rackmounts sold separately.

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver the best and most secure user experiences from the edge to the data center and cloud. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on X (Twitter), LinkedIn, and Facebook.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

ZABBIX

ENTERPRISE-CLASS MONITORING SOLUTION FOR EVERYONE

ALL-IN-ONE
OPEN-SOURCE
DISTRIBUTED MONITORING

ZABBIX

OVER
2 000 000
DOWNLOADS YEARLY

MORE THAN
18
YEARS OF EXPERIENCE

TRANSLATED IN TO
15
LANGUAGES

MONITOR OVER
100 000
DEVICES

COLLECT OVER
10 000 000
METRICS

TRUE
100%
OPEN-SOURCE

WHAT IS ZABBIX

An uncompromising mature enterprise-level platform designed for real-time monitoring of millions of metrics collected from thousands of servers, virtual machines and network devices, effortlessly scaling to even larger environments. Gather and analyze accurate statistics and performance metrics, visualize it, get notified about current and potential issues without delay, and take advantage of our time-tested professional development and support.

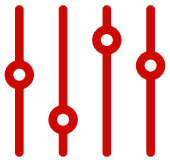
Give yourself the edge by improving the quality of your services without sacrificing operating costs.
Choose Zabbix and overcome any restrictions.

- Monitor performance and availability of networks, applications and cloud resources
- Support small to very large distributed environments
- IoT ready (Internet of Things)
- Support wide variety of architectures
- Send notifications or execute remote commands in case of current or potential problems
- Rich visualization capabilities, customizable dashboard, custom graphs and network maps
- Provide distributed monitoring options with the use of Zabbix proxies

ADVANTAGES

FEATURES

- Improve the quality of your services and reduce operating costs by avoiding downtime
- Monitor resource usage trends as your business grows and plan capacity increase in a timely manner
- Extensive documentation
- All Zabbix is open source



SCALABILITY

- Over 100,000 monitored devices
- Over 10,000,000 of metrics
- Thousands of checks per second
- Small to large distributed setups
- Easy maintenance

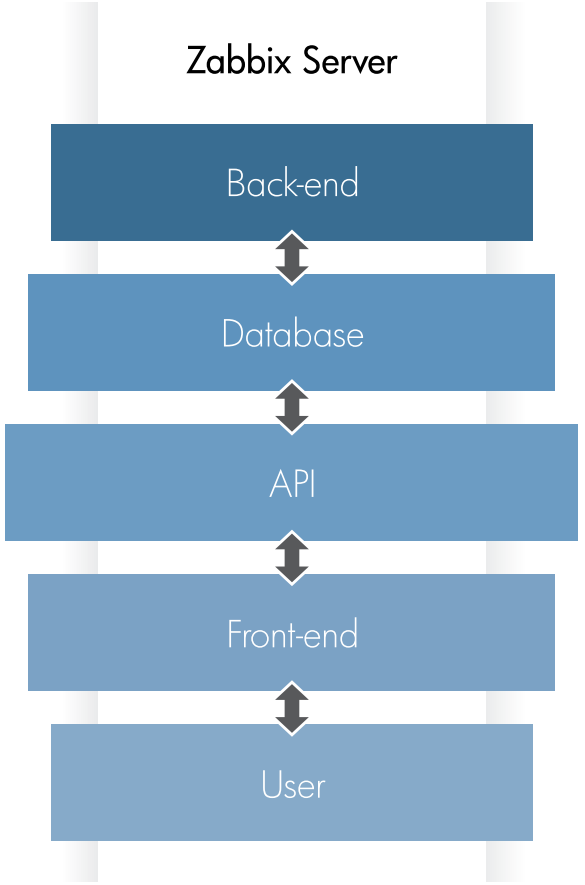
PROFESSIONAL SERVICES

- Technical Support and Training
- Trouble-free deployment
- Turn-key Solutions
- Consulting

ARCHITECTURE

Zabbix server is a central process of Zabbix software that performs monitoring, interacts with Zabbix proxies and agents, calculates triggers, sends notifications and acts as a central repository of data.

The server is the central repository in which all configuration, statistical and operational data is stored, and it is the entity in Zabbix that will actively alert administrators when problems arise in any of the monitored systems.



ZABBIX PROXY

A Zabbix proxy collects performance and availability data on behalf of the Zabbix server. This way, a proxy can take on itself some of the load of collecting tasks and offload the Zabbix server.

Also, using a proxy is the easiest way of implementing centralized and managed distributed monitoring.

ZABBIX AGENT

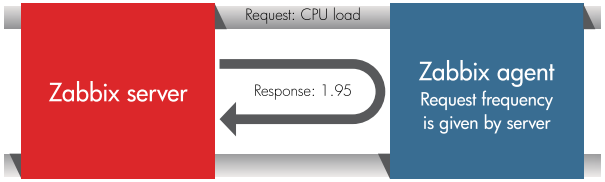
Zabbix agent is a process deployed on monitoring targets to actively monitor local resources and applications (storage drives, memory, processor statistics, network, file systems, etc).

The agent gathers operational information locally and reports data to Zabbix server for further processing.

Zabbix agents are extremely efficient because of use of native system calls for gathering information.

ZABBIX AGENT | MODES

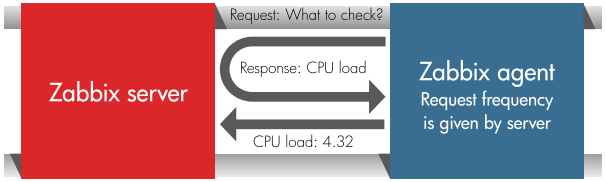
Passive Mode



Advantages of passive mode:

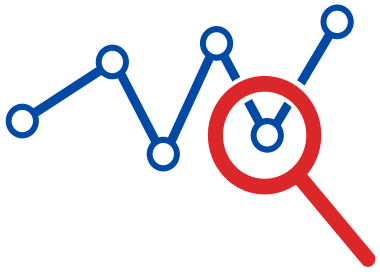
1. Ease of setup
2. Support for data collection with flexible intervals
3. Intuitiveness in communication (request <-> response).
4. Simpler troubleshooting

Active Mode



Advantages of active mode:

1. Can be used behind NAT
2. Data buffering
3. Reduce load on Zabbix server. (No load on Zabbix pollers)
4. More secure



MAIN FEATURES

A solid monitoring solution for multiple OS platforms

- Cross-platform
- Extensive customization capabilities of Zabbix allow to integrate it in any environment
- Modularity and flexibility

True open-source software

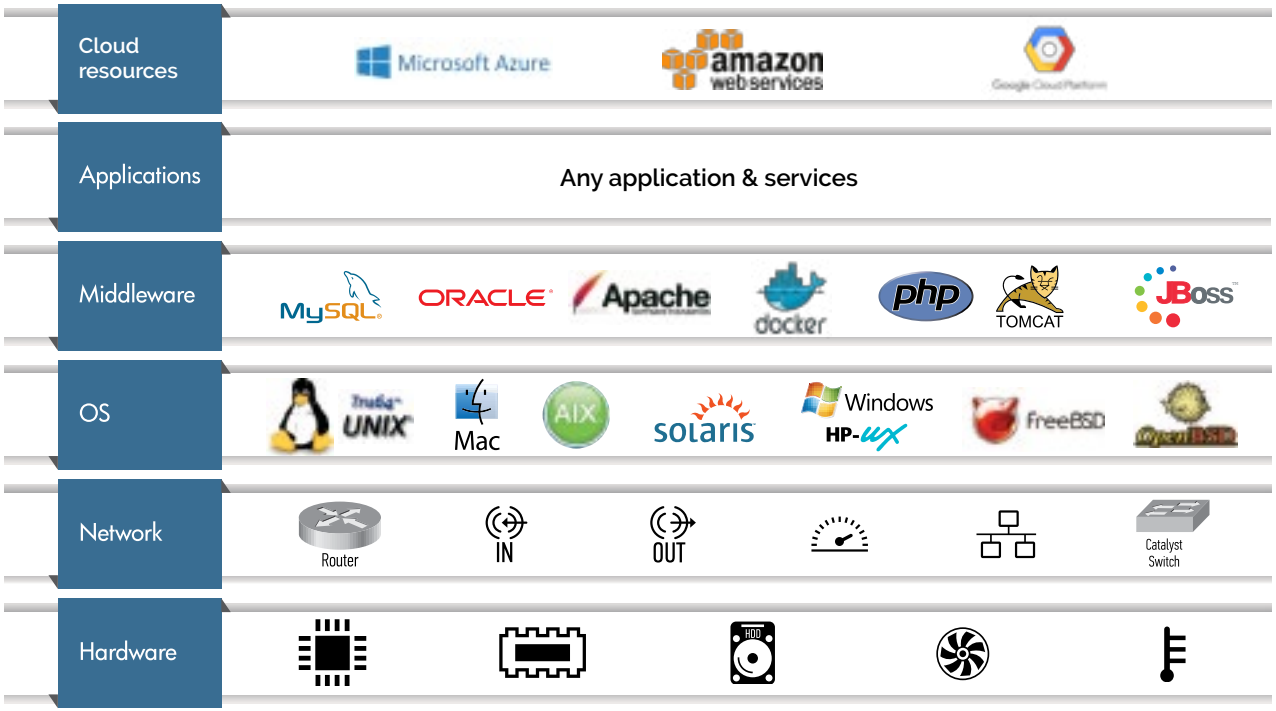
- No vendor lock-in
- Free for commercial and non-commercial use
- Phenomenal Zabbix community support from thousands of members around the world

Scaling to large environments

- Able to process more than 50,000 checks per second
- Scales up to hundreds of thousands of monitored
- devices
- Reliable commercial support

Data gathering

- Zabbix offers great performance and can be scaled to very large environments.
- Data is gathered using various methods, including Zabbix native agents and agentless options: SNMPv1, SNMPv2, SNMPv3, IPMI, WMI, trappers, SSH, Telnet, web checks.



Notification

Zabbix allows not only to collect, store and analyze information about monitored environment, but also to inform responsible personnel about occurred incidents through a variety of notification methods:

- e-mail
- SMS
- Jabber
- further notifications can be scripted and customized (depending on the context)

examples: (Skype, instant messaging, voice, etc.)

Powerful escalation module supports building of complicated workflows to assist delivering only relevant alert information to responsible personnel at the right time.

ZABBIX

PROFESSIONAL
24/7
SUPPORT

OVER
90
GLOBAL PARTNERS

SUPPORT IN OVER
15
LANGUAGES

OVER
9 500
RESOLVED
SUPPORT CASES

OVER
16 000
COMMUNITY
MEMBERS

OVER
15
BOOKS
ON ZABBIX

ZABBIX PROFESSIONAL SERVICES

Zabbix offers a wide range of professional services designed to fit customers' unique business needs, requirements and complexities. By using Zabbix Professional Services a client is guaranteed to find answers and solutions in the shortest time possible and can be confident that the solutions provided by Zabbix experts are the most appropriate in any situation.

Technical Support
We aim to provide our customers with professional on-time technical support through a web support system, by phone and e-mail.
There are 5 support tiers to choose from.

Integration
This service helps to integrate Zabbix Monitoring Solution into a customer's IT environment and with other tools and applications in accordance with corporate requirements and specifications.

Turn-key Solution
Designed to help your organization to start using Zabbix in no time. Our engineers will install and configure Zabbix Monitoring Solution remotely or on-site according to your specifications.

Upgrade
Allows companies that are using older versions of Zabbix to upgrade to the latest stable version in the shortest time without the risk of losing valuable data, trends and configuration, and with miminal to zero maintenance window.

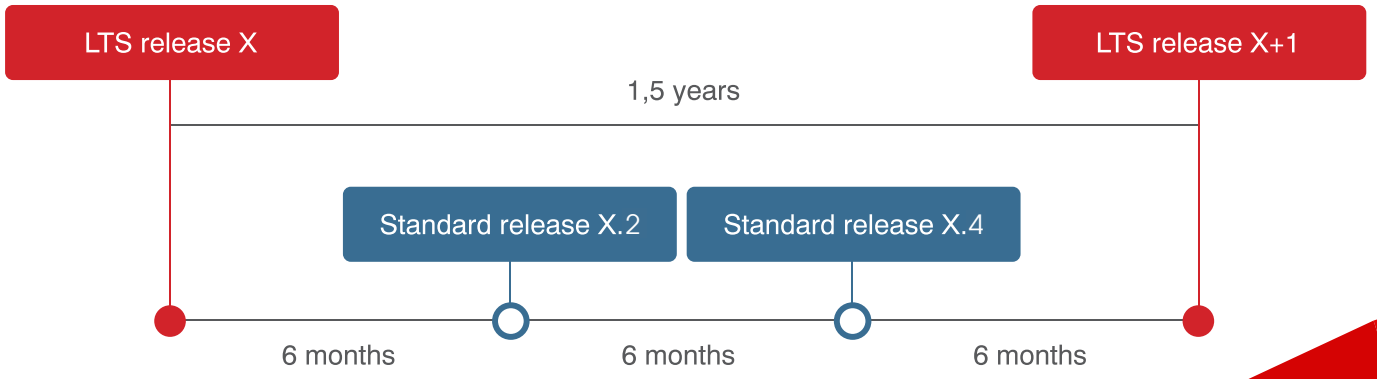
Custom Development
Achieve the most from your Zabbix implementation and address some specific requirements of the business by delivering a complete end-to-end development.

Template Building
Designed to provide customers with a comfortable, cost-efficient and secure way to start monitoring their unique or not-standard devices and systems in no time according to the specifications of the organization.

Consulting
We can assist you in better understanding the benefits and potential from using Zabbix software before and after deployment.

Remote troubleshooting
Eliminate any issues you have run into, within hours, not days or weeks, and ensure that the system is fixed correctly, accurately and without losing any valuable data.

CONTINUOUS DELIVERY OF ZABBIX RELEASES



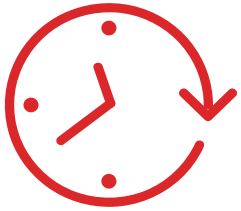
Zabbix LTS (Long Term Support) releases are supported for Zabbix customers during the next 5 years.

Standard Zabbix releases are supported for Zabbix customers during the next 6 months, plus one additional month of Limited Support (critical and security issues only).

TECHNICAL SUPPORT

While Zabbix is released under GPLv2, we understand that the key element of true enterprise-class software for a corporate customer is the availability of professional on-time technical support.

Zabbix offers to its customers 5 different support tiers, ranging from just a few tickets to unlimited 24/7 coverage, that includes remote troubleshooting, version upgrade, on-site training and on-site consulting; we believe every company will find a support level that meets its requirements.



24/7 AVAILABILITY

Support Tier Choices

BRONZE

Online based case submission

4 tickets per Year

Guaranteed response within 2 business days

SILVER

All the benefits from Bronze Tier

8 Tickets per Year

Guaranteed response within 1 business day

Phone support

GOLD

All the benefits from Silver Tier

Unlimited number of Tickets

Guaranteed response within 4 hours

Remote Troubleshooting

Distributed monitoring with Zabbix Proxy

Mon-Fri /8x5 support

PLATINUM

All the benefits from Gold Tier

Emergency response time within 90 minutes

Performance tuning

Precompiled Zabbix builds according to customers request

24/7 support

ENTERPRISE

All the benefits from Platinum Tier

One five-day business visit to customer's office by a leading Zabbix consultant

Zabbix training at customer's location for up to 5 company's employees

Upgrade service to the latest Zabbix version

Unlimited Proxies

Environment reviews

Benefits

By purchasing technical support, a customer:

- gets access to the team of Zabbix experts that know every little bit of the source code and have extensive experience in solving a variety of issues that customers are facing every day;
- receives assurance that no matter how complex the issue is, Zabbix support engineers will find a solution and deliver it according to the terms set in the contract.

ZABBIX PARTNER PROGRAM

Zabbix global partner program is designed to ensure dependable and professional support to our diverse customer community in local languages worldwide.

Key Benefits of Becoming Partner

To deliver professional services on local markets, we rely on partners for the delivery of complete solutions to the customers.

We aim to build mutually beneficial relationship that would last for many years. Becoming a Zabbix Partner provides several key benefits:

- Get recognized by potential customers and increase the visibility of your business
- Get ahead of competitors by using technical support according to professional Service Level Agreements
- Discounts on all Zabbix services (training, consulting, custom development, etc.)
- Access pre-sale consulting services
- Participation in joint marketing events

Available Partner Programs

RESELLER

Reseller is a company that engages in the promotion and re-sale of Zabbix services. Reseller's primary task is to find a lead, present and promote Zabbix product and services, consult the lead on best suited solution, and arrange signature of the contract, while Zabbix will actually provide the selected service.

CERTIFIED PARTNER

Certified Partner, besides the right to promote and re-sell Zabbix services, is officially authorized to deliver selected Zabbix services and solutions. The partner benefits from keeping a very close contact with the customers at all times and thus is able to sell other value added services to the customer along with Zabbix services and create a stronger attachment to customer.

PREMIUM PARTNER

While Premium Partner has the same authorization to promote, re-sell and deliver Zabbix services and solutions, this highest partner status is testament of special knowledge, skills and experience, as well as the capacity to participate in sophisticated projects related to Zabbix solution implementation, integration and support.

The Premium Partner status is assigned by Zabbix only to those partners that meet a special benchmark in providing Zabbix services and are able to prove high proficiency of personnel about Zabbix solution.

Zabbix has more than 90 partners located in North and South America, Europe, Asia and Australia.

This number is ever growing, and to find a local partner of Zabbix, please visit our web page: www.zabbix.com

ZABBIX TRAINING

What is Zabbix Professional Training?

Zabbix training is designed to ensure knowledge transfer between the best experts in Zabbix and trainees in a short period of time.

Training covers all aspects of Zabbix from terminology, available elements and functions, internal protocols and high availability setups to distributed monitoring. Courses are full of practical tasks, where each trainee installs and configures Zabbix on his own, sets up devices for monitoring and solves complex monitoring issues.

Zabbix Certified Specialist course is intended for those who have just begun to understand Zabbix and want to get on track fast and in the right way. During the course you will learn about the main functionality of Zabbix monitoring software, its installation, setup and further maintenance also including pro tips for advanced users..

Zabbix Certified Professional course is designed for administrators of large enterprises and companies that use Zabbix to monitor large amounts of devices located in multiple datacenters and in a distributed environments.

Target Audience

The training programs are intended for IT administrators and auditors, system integrators, and other personnel that deals with IT infrastructure monitoring. No prior knowledge of Zabbix Software is required, but all trainees should have advanced computer literacy and knowledge of Linux OS.

Even administrators with several years of experience in Zabbix software find attending these trainings beneficial, as they are still missing out on some great features and best practices that came along just recently.

Trainers

We think that quality is the key to successful development of Zabbix and the gem that we have to preserve. Therefore we take it seriously when it comes to content, the style and the outcome of our training courses.

All of our trainers have extensive theoretical and practical knowledge of Zabbix, in-depth understanding of the monitoring field, very good knowledge of the most popular hardware and software and good communication skills.

Sign-up for a Course

You can apply for Zabbix training by completing the registration form on our website. If there is no scheduled training in your region or you would like to request an On-site or Hosted training, please let us know by contacting Zabbix Sales team.

Register for upcoming scheduled training on http://www.zabbix.com/training

Courses are now delivered in English, Japanese, Russian, Portuguese, French, Italian, Latvian, German, Spanish and Dutch, constantly adding new languages.

Why Participate?

Attending Zabbix training is going to be useful for both a trainee and the company he works for. Below is just a short list of benefits.

You will

- Learn from the leading trainers and experts in a friendly and relaxed atmosphere
- Obtain both theoretical knowledge and hands-on practical experience with real-life examples
- Discover full potential of the product
- Be presented with techniques to perform everyday monitoring tasks easier and more efficiently

Your company will

- Gain confidence that your monitoring infrastructure is set up by a certified specialist according to the best practices
- Benefit from less time spent on performing
- Profit from efficient use of available IT resources regardless of the deployment scale by completing the coherent training program

Exam and Certificate

- At the end of each course there is an exam to prove your skills and knowledge of Zabbix, gained during the course.
- Certificate, signed by Zabbix Founder and CEO Alexei Vladishev, is issued at the end of each course.

APPLY FOR ZABBIX TRAINING:

On-site

Is the most convenient way to get training, as long as you have a room with a projector, screen and internet connection. You can order a session consisting of one or both courses. The main benefits of the on-site training are:

- course content can be tailored to your exact needs upon request
- company specific & security sensitive topics can be discussed that otherwise would not be possible with participants from other companies
- training at your own premises saves time and money with flexible scheduling option

Hosted

Even with one participant to attend both courses and a meeting room to accommodate up to 15 participants, you may host a training at your premises.

You provide the venue and infrastructure, Zabbix takes care of advertising the event. It's that simple. And to make things better, you get 1 free seat for both courses, or 2 free seats for one course of your choice.

Scheduled

This is the easiest way to participate in Zabbix training. Just visit Training section on the Zabbix web site and apply for any available training from the schedule. Register early to secure your seat, as the number of places is limited.

Looking for training near you?

Propose a specific venue for the next scheduled training session by filling out a training request form. Zabbix team takes this information into account when planning upcoming courses. You will get notified when training is scheduled in the region you have requested.

Extending the Reach of Zabbix Training Courses

To provide proximity to customer's location and a high frequency of coureses Zabbix Training Partner Program was introduced, enabling Zabbix training courses to be spread all around the world, with trainers speaking many different languages.

Zabbix Offices Worldwide

Europe: +371 67784742

USA: +1-877-4-ZABBIX (Toll-free)

Japan: 03-6895-7527

www.zabbix.com sales@zabbix.com twitter.com /zabbix fb.com /zabbix

ZABBIX

JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Standards Reference

Published
2024-02-01

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Standards Reference

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to identify the standards substantially supported by Junos OS.

1

PART

Overview

CHAPTER 1

Accessing Standards Documents

IN THIS CHAPTER

Accessing Standards Documents on the Internet

The following information about the location of standards on the Internet is accurate as of March 2018. It is subject to change and is provided only as a courtesy to the reader.

Information about accessing MIBs is provided in the entry for each MIB.

- ANSI standards are published by the American National Standards Institute. You can search for specific standards at http://webstore.ansi.org/.
- FRF (Frame Relay Forum) standards are published by the Broadband Forum. They can be accessed at https://www.broadband-forum.org/component/sppagebuilder/?view=page&id=185.
- GR (Generic Requirements) standards are published by Ericsson (Telcordia is now part of Ericcson). Information about them can be accessed by clicking the “Documents” link at http://telecom-info.telcordia.com/site-cgi/ido/.
- IEEE standards are published by the Institute of Electrical and Electronics Engineers. They can be accessed at http://ieeexplore.ieee.org/browse/standards/get-program/page/.
- ISO/IEC standards are published by the International Organization for Standardization/International Electrotechnical Commission. They can be accessed at https://www.iso.org/isoiec-27001-information-security.html.
- INCITS standards are published by the InterNational Committee for Information Technology Standards. They can be accessed at http://www.incits.org/standards-information/.
- Internet drafts are published by the Internet Engineering Task Force (IETF). They can be accessed at https://www.ietf.org/standards/ids/ .
- ITU–T Recommendations are published by the International Telecommunication Union. They can be accessed at http://www.itu.int/rec/T-REC.

NOTE: Junos OS supports ITU-T Y.1731 (year 2006 version) that defines Ethernet service OAM features for fault monitoring, diagnostics, and performance monitoring.

- RFCs are published by the IETF. They can be accessed at https://www.ietf.org/standards/rfcs/.

2

PART

Supported Standards

CHAPTER 2

Chassis and System Standards

IN THIS CHAPTER

Supported BFD Standards

Junos OS substantially supports the following standards for Bidirectional Forwarding Detection (BFD).

- RFC 5880, *Bidirectional Forwarding Detection*. (Partial support—Echo and Demand mode is not supported).
- RFC 5881, *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6* (Fully compliant).
- RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD).*
- RFC 5883, *Bidirectional Forwarding Detection (BFD)* (Fully compliant).
- RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*. (Partial support—Packets from egress to ingress come with singlehop port and while sending packets, the router alert option is used setting TTL to 1).
- RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. (Fully compliant)
- RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces, also called micro-BFD for sub-second failure detection*

Supported BOOTP and DHCP Standards

The Junos operating system (Junos OS) substantially supports the following RFCs, which define standards for the bootstrap protocol (BOOTP) and the Dynamic Host Control Protocol (DHCP).

- RFC 951, *BOOTSTRAP PROTOCOL (BOOTP)*
- RFC 1001, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS*
- RFC 1002, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS*
- RFC 1035, *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*
- RFC 1534, *Interoperation Between DHCP and BOOTP*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 1700, *ASSIGNED NUMBERS*
- RFC 2131, *Dynamic Host Configuration Protocol*

  DHCP over virtual LAN (VLAN)-tagged interfaces is not supported.
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3118, *Authentication for DHCP Messages*

  Only Section 4, “Configuration token,” is supported.
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*
- RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*
- RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)*
- RFC 4649, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Mobile IP Standards

Junos OS supports only static configuration of home agent addresses and IP tunnels; dynamic configuration is not supported. Junos OS does not support the Mobile IP foreign agent, accounting, QoS, policy, data path, or logical interfaces per mobile node (for a mobile subscriber).

Junos OS substantially supports the following RFCs, which define standards for Mobile IP.

- RFC 2794, *Mobile IP Network Access Identifier Extension for IPv4*
- RFC 3024, *Reverse Tunneling for Mobile IP, revised*
- RFC 3344, *IP Mobility Support for IPv4*

  Only the Mobile IP home agent is supported.
- RFC 3543, *Registration Revocation in Mobile IPv4*
- RFC 4433, *Mobile IPv4 Dynamic Home Agent (HA) Assignment*

The following RFC does not define a standard, but provides information about Mobile IP. The IETF classifies it as "Informational."

- RFC 2977, *Mobile IP Authentication, Authorization, and Accounting Requirements*

  Accounting is not supported.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Network Management Standards

Junos OS supports the majority of network management features defined in the following standards documents.

- Extended Security Options (ESO) Consortium, *ESO Consortium MIB*.

  As of February 2011, the text of this MIB is accessible at http://www.snmp.com/eso/esoConsortiumMIB.txt.
- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3ad, *Aggregation of Multiple Link Segments* (published as Clause 43 in Section 3 of the 802.3 specification)

Only the following MIB objects are supported:

- `dot3adAggPortDebugActorChangeCount`
- `dot3adAggPortDebugActorSyncTransitionCount`
- `dot3adAggPortDebugMuxState`
- `dot3adAggPortDebugPartnerChangeCount`
- `dot3adAggPortDebugPartnerSyncTransitionCount`
- `dot3adAggPortDebugRxState`
- `dot3adAggPortListTable`
- `dot3adAggPortStatsTable`
- `dot3adAggPortTable`
- `dot3adAggTable`
- `dot3adTablesLastChanged`

- Integrated Local Management Interface (ILMI) MIB in the *Integrated Local Management Interface (ILMI) Specification, Version 4.0*.

  This document is accessible at https://www.broadband-forum.org/component/sppagebuilder/?view=page&id=185 under ATM Forum Technical Specifications.

  Only the `atmfMYIPNmAddress` and `atmfPortMyIfname` objects are supported.

- Internet Assigned Numbers Authority (IANA), *IANAiftype Textual Convention MIB* (referenced by RFC 2863, *The Interfaces Group MIB*)

  As of February 2011, the text of this MIB is accessible at http://www.iana.org/assignments/ianaiftype-mib.

- RFC 1122, *Requirements for Internet Hosts -- Communication Layers*
- RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1156, *Management Information Base for Network Management of TCP/IP-based internets*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

  Only the following MIB objects are supported:

  - `isisAdjIPAddr`

- isisAreaAddr
- isisCirc
- isisCircLevel
- isisIPRA
- isisISAdj
- isisISAdjAreaAddr
- isisISAdjProtSupp
- isisMANAreaAddr
- isisPacketCount
- isisRa
- isisSysProtSupp
- isisSummAddr
- isisSystem

- RFC 1212, *Concise MIB Definitions*
- RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*

  Only the following features are supported:

  - Junos OS-specific secured access list
  - Primary configuration keywords
  - MIB II and its SNMP version 2 derivatives, including the following:
    - Interface management
    - IP (except for the ipRouteTable object, which has been replaced by the inetCidrRouteTable object, [RFC 4292, *IP Forwarding MIB*])
    - SNMP management
    - Statistics counters
  - Reconfigurations upon receipt of the SIGHUP signal
  - SNMP version 1 Get and GetNext requests and version 2 GetBulk requests

- RFC 1215, *A Convention for Defining Traps for use with the SNMP*

  Only MIB II SNMP version 1 traps and version 2 notifications are supported.

- RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types* (obsoleted by RFC 2495)

  The T1 MIB is supported.

- RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type* (obsoleted by RFC 2496)

  The T3 MIB is supported.

- RFC 1471, *The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol*

- RFC 1472, *The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol*

- RFC 1473, *The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol*

- RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*

  The `bgpBackwardTransition` and `bgpEstablished` notifications are not supported.

- RFC 1695, *Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2* (obsoleted by RFC 2515)

- RFC 1724, *RIP Version 2 MIB Extension*

- RFC 1850, *OSPF Version 2 Management Information Base*

  The following features are not supported:

  - Host Table
  - `ospfLsdbApproachingOverflow` trap
  - `ospfLsdbOverflow` trap
  - `ospfOriginateLSA` trap
  - `ospfOriginateNewLsas` MIB object
  - `ospfRxNewLsas` MIB object

- RFC 1901, *Introduction to Community-based SNMPv2.*

- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3416)
- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3418)
- 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 2024, *Definitions of Managed Objects for Data Link Switching using SMIv2*
- RFC 2068, *Hypertext Transfer Protocol -- HTTP/1.1*
- RFC 2096, *IP Forwarding Table MIB*

  The `ipCidrRouteTable` object is extended to include the tunnel name when the next hop is through an RSVP-signaled label-switched path (LSP).

  > **NOTE**: RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.

- RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

  Only the `frDlcmiTable` object is supported.

- RFC 2233, *The Interfaces Group MIB using SMIv2* (obsoleted by RFC 2863)
- RFC 2287, *Definitions of System-Level Managed Objects for Applications*

  Only the following MIB objects are supported:

  - `sysApplElmtRunTable`
  - `sysApplInstallElmtTable`
  - `sysApplInstallPkgTable`
  - `sysApplMapTable`

- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*

  IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.

- RFC 2466, *Management Information Base for IP Version 6: ICMPv6 Group*
- RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types*

  The following MIB objects are not supported:

  - `dsx1FarEndConfigTable`
  - `dsx1FarEndCurrentTable`
  - `dsx1FarEndIntervalTable`
  - `dsx1FarEndTotalTable`
  - `dsx1FracTable`
- RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type*

  The following MIB objects are not supported:

  - `dsx3FarEndConfigTable`
  - `dsx3FarEndCurrentTable`
  - `dsx3FarEndIntervalTable`
  - `dsx3FarEndTotalTable`
  - `dsx3FracTable`
- RFC 2515, *Definitions of Managed Objects for ATM Management*

  The following MIB objects are not supported:

  - `aal5VccTable`
  - `atmVcCrossConnectTable`
  - `atmVpCrossConnectTable`
- RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type* (obsoleted by RFC 3592)
- RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*

  RFC 2571, *An Architecture for Describing SNMP Management Frameworks*

  Only read-only access is supported.
- RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (obsoleted by RFC 3412)

Only read-only access is supported.

- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*
- RFC 2580, *Conformance Statements for SMIv2*
- RFC 2662, *Definitions of Managed Objects for the ADSL Lines*
- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpStatsPacketLengthErrors` MIB object
- RFC 2790, *Host Resources MIB*

  Only the following MIB objects are supported:

  - `hrStorageTable` object. The file systems `/`, `/config`, `/var`, and `/tmp` always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.
  - Objects in the `hrSystem` group.
  - Objects in the `hrSWInstalled` group.
- RFC 2819, *Remote Network Monitoring Management Information Base*

  Only the following MIB objects are supported:

  - `alarmTable`
  - `etherStatsTable` object for Ethernet interfaces
  - `eventTable`
  - `logTable`
- RFC 2863, *The Interfaces Group MIB*
- RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*
- RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*

Only the following MIB objects are supported:

- `pingCtlTable`
- `pingMaxConcurrentRequests`
- `pingProbeHistoryTable`
- `pingResultsTable`
- `traceRouteCtlTable`
- `traceRouteHopsTable`
- `traceRouteProbeHistoryTable`
- `traceRouteResultsTable`

- RFC 2932, *IPv4 Multicast Routing MIB*
- RFC 2981, *Event MIB*
- RFC 3014, *Notification Log MIB*
- RFC 3019, *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol*
- 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*

  The proxy MIB is not supported.
- 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 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

  Support is implemented under the Juniper Networks Enterprise branch.

- RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

- RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

  Supports all objects, except `dot3StatsRateControlAbility` and `dot3StatsRateControlStatus` in `dot3StatsEntry` table.

  > **NOTE**: The values of the following objects in `dot3HCStatsEntry` table will be always zero for both 32-bit counters and 64-bit counters:
  >
  > - `dot3HCStatsSymbolErrors`
  > - `dotHCStatsInternalMacTransmitErrors`

- 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)*

  Only read-only access is supported, and the following features and MIB objects are not supported:

  - MPLS tunnels as interfaces
  - `mplsTunnelCRLDPResTable` object
  - `mplsTunnelPerfTable` object
  - The following objects in the `TunnelResource` table:
    - `mplsTunnelResourceExBurstSize`
    - `mplsTunnelResourceMaxBurstSize`
    - `mplsTunnelResourceMeanBurstSize`
    - `mplsTunnelResourceMeanRate`
    - `mplsTunnelResourceWeight`

  The `mplsTunnelCHopTable` object is supported on ingress routers only.

NOTE: The branch used by the proprietary LDP MIB (`ldpmib.mib`) conflicts with RFC 3812. `ldpmib.mib` has been deprecated and replaced by `jnx-mpls-ldp.mib`.

- RFC 3813, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*

  Only read-only access is supported, and the following MIB objects are not supported:

  - `mplsInSegmentMapTable`
  - `mplsInSegmentPerfTable`
  - `mplsInterfacePerfTable`
  - `mplsOutSegmentPerfTable`
  - `mplsXCDown`
  - `mplsXCUp`

- RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*

  Only the following MIB objects are supported:

  - `mplsLdpLsrID`
  - `mplsLdpSesPeerAddrTable`

- RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

- RFC 4001, *Textual Conventions for Internet Network Addresses*

- RFC 4087, *IP Tunnel MIB*

  Supports MIB objects with `MAX-ACCESS` of read-only in the following tables:

  - `tunnelIfTable`
  - `tunnelInetConfigTable`

- RFC 4133, *Entity MIB*

  Supports tables and objects except:

  - `entityLogicalGroup` table

- entPhysicalMfgDate and entPhysicalUris objects in entityPhysical2Group table
- entLPMappingTable and entPhysicalContainsTable in entityMappingGroup table
- entityNotoficationsGroup table

> **NOTE**: Supported only on MX240, MX480, and MX960 routers.

- RFC 4188, *Definitions of Managed Objects for Bridges*
- RFC 4268, *Entity State MIB*

> **NOTE**: Supported only on MX240, MX480, and MX960 routers.

- RFC 4292, *IP Forwarding MIB*

  Supports the following table and associated MIB objects:

  - inetCidrRouteTable
  - inetCidrRouteNumber
  - inetCidrRouteDiscards

- RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB*

  Supports the following scalar objects and tables:

  - mplsL3VpnConfiguredVrfs
  - mplsL3VpnActiveVrfs
  - mplsL3VpnConnectedInterfaces
  - mplsL3VpnNotificationEnable
  - mplsL3VpnVrfConfMaxPossRts
  - mplsL3VpnVrfConfRteMxThrshTime
  - mplsL3VpnIllLblRcvThrsh
  - mplsL3VpnVrfTable
  - mplsL3VpnVrfPerfTable

  - mplsL3VpnVrfRteTable
  - mplsVpnVrfRTTable

- Internet draft draft-ietf-bfd-mib-02.txt, *Bidirectional Forwarding Detection Management Information Base*

  Only read-only access is supported, and the bfdSessDown and bfdSessUp traps are supported. Objects in the bfdSessMapTable and bfdSessPerfTable tables are not supported. The MIB that supports this draft is mib-jnx-bfd-exp.txt under the Juniper Networks Enterprise jnxExperiment branch.

- RFC 4273, *Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version*

  Only the following MIB objects are supported:

  - jnxBgpM2PrefixInPrefixes
  - jnxBgpM2PrefixInPrefixesAccepted
  - jnxBgpM2PrefixInPrefixesRejected

- RFC 4444, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

  Only the following tables are supported:

  - isisISAdjAreaAddrTable
  - isisISAdjIPAddrTable
  - isisISAdjProtSuppTable
  - isisISAdjTable

- RFC 4741, *NETCONF Configuration Protocol* (RFC 4741 is obsoleted by RFC 6241)
- RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)* (RFC 4742 is obsoleted by RFC 6242)
- RFC 5424, *The Syslog Protocol*
- RFC 5601, *Pseudowire (PW) Management Information Base (MIB)*
- RFC 5603, *Ethernet Pseudowire (PW) Management Information Base (MIB)*
- Internet draft draft-ietf-msdp-mib-08.txt, *Multicast Source Discovery protocol MIB*

  The following MIB objects are not supported:

  - msdpBackwardTransition

    - msdpEstablished
    - msdpRequestsTable

- RFC 6020, *YANG - A data modeling language for NETCONF*
- RFC 6241, *Network Configuration Protocol (NETCONF)* (RFC 6241 obsoletes RFC 4741)

  The following features are not supported:

    - Advertisement of NETCONF 1.1 capabilities during session establishment
    - :confirmed-commit:1.1 capability, which includes the <cancel-commit> operation and the <persist> and <persist-id> parameters for the <commit> operation

- RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)* (RFC 6242 obsoletes RFC 4742)

  The following feature is not supported:

    - Chunked framing

- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

  The following features are not supported:

    - Row creation
    - Set operation
    - vrrpv3StatisticsPacketLengthErrors MIB object
    - vrrpv3StatisticsRowDiscontinuityTime MIB object

- RFC 7589, *Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication*
- Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, *Management Information Base for OSPFv3*

  Only read-only access is supported, and only for the ospfv3NbrTable table. The MIB that supports this draft is mib-jnx-ospfv3mib.txt under the Juniper Networks Enterprise jnxExperiment branch; MIB object names are prefixed with jnx (for example, jnxOspfv3NbrAddressType).

- Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode*

The following RFCs do not define standards, but provide information about network management. The IETF classifies them variously as "Best Current Practice," "Experimental" or "Informational."

- RFC 1901, *Introduction to Community-based SNMPv2*

- RFC 2330, *Framework for IP Performance Metrics*
- RFC 2934, *Protocol Independent Multicast MIB for IPv4*
- RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*
- RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 5601, *PW-FRAME-MIB*

  Supported on MX Series routers with MPC/MIC interfaces that use the ATM MIC with SFP.
- RFC 5603, *PWE3 MIB*

  Supported on MX Series routers with MPC/MIC interfaces that use the ATM MIC with SFP.
- Internet draft draft-ietf-l3vpn-mvpn-mib-03.txt, *MPLS/BGP Layer 3 VPN Multicast Management Information Base*

  Implemented under the Juniper Networks enterprise branch [`jnxExperiment`]. OID for `jnxMvpnExperiment` is `.1.3.6.1.4.1.2636.5.12`. This includes `jnxMvpnNotifications` traps.

RELATED DOCUMENTATION

Network Management and Monitoring Guide

Accessing Standards Documents on the Internet | 2

Supported Port Extension Standards

Junos OS substantially supports Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1BR, *Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Bridge Port Extension*.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported RADIUS and TACACS+ Standards for User Authentication

For validation of the identity of users who attempt to access a router, Junos OS supports RADIUS authentication, TACACS+ authentication, and authentication by means of Junos OS user accounts configured on the router. Junos OS supports the configuration of Juniper Networks-specific RADIUS and TACACS+ attributes, and the creation of template accounts.

All users who can log in to the router must already be assigned to a Junos OS login class. A *login class* defines its members' access privileges during a login session, the commands they can and cannot issue, the configuration statements they can and cannot view or change, and the idle time before a member's login session is terminated.

Junos OS substantially supports the following RFCs, which define standards for RADIUS and TACACS+.

- RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*
- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 3162, *RADIUS and IPv6*
- RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

The following Internet drafts do not define standards, but provide information about RADIUS. The IETF classifies them as "Informational."

- RFC 2866, *RADIUS Accounting*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*
- RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- RFC 5176, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

RELATED DOCUMENTATION

Supported System Access Standards | 22

Accessing Standards Documents on the Internet | 2

Supported System Access Standards

Junos OS substantially supports the following protocols and applications for remote access to devices: telnet, FTP, rlogin, and finger.

Junos OS substantially supports RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*.

For jurisdictions without limits on dataplane encryption, that version of Junos OS substantially supports the following RFCs, which define standards for technologies used with Secure Sockets Layer (SSL).

- RFC 1319, *The MD2 Message-Digest Algorithm*
- RFC 1321, *The MD5 Message-Digest Algorithm*
- RFC 2246, *The TLS Protocol Version 1.0*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

Junos OS substantially supports the following RFCs and standards that apply to the SSH protocol. These are used for control plane administration on devices running Junos OS either directly using the CLI or in conjunction with NETCONF:

- RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

  You can find the assigned SSH numbers at https://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml.
- RFC 4251, *The Secure Shell (SSH) Protocol Architecture*
- RFC 4252, *The Secure Shell (SSH) Authentication Protocol*
- RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*
- RFC 4254, *The Secure Shell (SSH) Connection Protocol*
- RFC 4256, *Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*

  Also known as “keyboard-interactive” authentication.
- RFC 4335, *The Secure Shell (SSH) Session Channel Break Extension*
- RFC 4344, *The Secure Shell (SSH) Transport Layer Encryption Modes*

  The following encryption methods are supported:

  - aes128-ctr
  - aes192-ctr

  - aes256-ctr

- RFC 4419, *Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol*
- RFC 4432, *RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol*
- RFC 4819, *Secure Shell Public Key Subsystem*

  Junos OS supports SSH file transfer protocol (SFTP).

- RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer*

  The following Elliptic Curves are supported:

  - nistp256
  - nistp384
  - nistp521

  The following public keys are supported:

  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521

- RFC 6668, *SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol*

  The hmac-sha2-256 and hmac-sha2-512 integrity algorithms are supported.

- RFC 8270, *Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits*
- OpenSSH per the *openssh-portable/PROTOCOL*.

  For more information about OpenSSH, see https://github.com/openssh/openssh-portable/blob/master/PROTOCOL.

The following RFCs provide information about TFTP, which Junos OS supports as a remote access protocol. The IETF does not include the RFCs in its Standards track, instead assigning them status “Unknown (Legacy Stream.)”

- RFC 783, *THE TFTP PROTOCOL (REVISION 2)*
- RFC 906, *Bootstrap Loading using TFTP*

The following RFCs provide information about Transport Layer Security (TLS) protocol, which Junos OS supports to enable client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

- RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*
- RFC 5346, *The Transport Layer Security (TLS) Protocol Version 1.2*
- RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3*

RELATED DOCUMENTATION

Supported RADIUS and TACACS+ Standards for User Authentication | 21

Accessing Standards Documents on the Internet | 2

Supported Time Synchronization Standard

Junos OS substantially supports RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*, does not define a standard, but provides information about time synchronization technology. The IETF classifies it as "Informational."

In CLI operational mode, you can set the current date and time on the router manually or from an NTP server.

On MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP, Junos OS substantially supports RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

CHAPTER 3

Interface Standards

IN THIS CHAPTER

Supported ATM Interface Standards

Junos OS substantially supports the following standards for Asynchronous Transfer Mode (ATM) interfaces.

- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation I.432.3, *B-ISDN user-network interface - Physical layer specification: 1544 kbit/s and 2048 kbit/s operation*
- RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

  Only routed protocol data units (PDUs) are supported.
- RFC 2225, *Classical IP and ARP over ATM*

  Only responses are supported.
- RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

  Only routed PDUs and Ethernet bridged PDUs are supported.
- RFC 4717, *Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Ethernet Interface Standards

Junos OS substantially supports the following standards for Ethernet interfaces.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1ag, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management*
- IEEE Standard 802.1ah, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Amendment 7: Provider Backbone Bridges*
- IEEE Standard 802.1Q, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks*
- IEEE Standard 802.1Qaz, *IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: Enhanced Transmission Selection*
- IEEE Standard 802.1Qbb, *IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: Priority-based Flow Control*
- IEEE Standard 802.1s, *IEEE Standard for Multiple Instances of Spanning Tree Protocol (MSTP)---Virtual Bridged Local Area Networks*
- IEEE Standard 802.3, *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements, Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
- IEEE Standard 802.3ab, *1000BASE-T* (published as Clause 40 in Section 3 of the 802.3 specification)
- IEEE Standard 802.3ad, *Aggregation of Multiple Link Segments* (published as Clause 43 in Section 3 of the 802.3 specification)
- IEEE Standard 802.3ae, *10-Gigabit Ethernet* (published as Clauses 44-53 in Section 4of the 802.3 specification)
- IEEE Standard 802.3ah, *Operations, Administration, and Maintenance (OAM)* (published as Clause 57 in Section 5 of the 802.3 specification)
- IEEE Standard 802.3z, *1000BASE-X* (published as Clauses 34-39, 41-42 in Section 3 of the 802.3 specification)

- InterNational Committee for Information Technology Standards (INCITS) T11, *Fibre Channel Interfaces*
- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation Y.1731, *OAM functions and mechanisms for Ethernet based networks*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Frame Relay Interface Standards

Junos OS substantially supports the following standards for Frame Relay interfaces.

- American National Standards Institute (ANSI), *Annex D, Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames* to T1.617-1991, *Integrated Services Digital Network (ISDN)—Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1)*
- Broadband Forum standard FRF.12, *Frame Relay Fragmentation Implementation Agreement*
- FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*
- FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*
- International Telecommunication Union–Telecommunication Standardization (ITU–T), *Annex A, Additional procedures for Permanent Virtual Connection (PVC) status management (using Unnumbered Information frames)* to Recommendation Q.933, *ISDN Digital Subscriber Signalling System No. 1 (DSS1) - Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*
- RFC 1973, *PPP in Frame Relay*
- RFC 2390, *Inverse Address Resolution Protocol*
- RFC 2427, *Multiprotocol Interconnect over Frame Relay* (obsoletes RFC 1490)
- RFC 2590, *Transmission of IPv6 Packets over Frame Relay Networks Specification*
- Internet draft draft-martini-frame-encap-mpls-01.txt, *Frame Relay Encapsulation over Pseudo-Wires* (expires December 2002)

  Translation of the command/response bit and sequence numbers and padding are not supported.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported GRE and IP-IP Interface Standards

Junos OS substantially supports the following RFCs, which define standards for generic routing encapsulation (GRE) and IP-IP interfaces.

- RFC 2003, *IP Encapsulation within IP*
- RFC 2784, *Generic Routing Encapsulation (GRE)*
- RFC 2890, *Key and Sequence Number Extensions to GRE*

  The key field is supported, but the sequence number field is not.

The following RFCs do not define standards, but provide information about GRE, IP-IP, and related technologies. The IETF classifies them as "Informational."

- RFC 1701, *Generic Routing Encapsulation (GRE)*
- RFC 1702, *Generic Routing Encapsulation over IPv4 networks*
- RFC 2547, *BGP/MPLS VPNs* (over GRE tunnels)

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported PPP Interface Standards

Junos OS substantially supports the following RFCs, which define standards for Point-to-Point Protocol (PPP) interfaces.

- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1334, *PPP Authentication Protocols*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC-like Framing*

- RFC 1989, *PPP Link Quality Monitoring*
- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 2364, *PPP Over AAL5*
- RFC 2615, *PPP over SONET/SDH*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

  The following features are not supported:

  - Negotiation of address field compression and protocol field compression PPP NCP options; instead, a full 4-byte PPP header is always sent
  - Prefix elision
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

The following RFCs do not define standards, but provide information about PPP. The IETF classifies them as "Informational."

- RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 2153, *PPP Vendor Extensions*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported SDH and SONET Interface Standards

Junos OS substantially supports the following standards for SDH and SONET interfaces.

- American National Standards Institute (ANSI) standard T1.105-2001, *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*
- ANSI standard T1.105.02-2001, *Synchronous Optical Network (SONET) – Payload Mappings*
- ANSI standard T1.105.06-2002, *Synchronous Optical Network (SONET): Physical Layer Specifications*
- GR-253-CORE (Telcordia Generic Requirements standard), *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* (replaces GR-1377-CORE, *SONET OC-192 Transport System Generic Criteria*)

- GR-499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements*
- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation G.691, *Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers*
- ITU–T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.783 (1994), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*
- ITU–T Recommendation G.813 (1996), *Timing characteristics of SDH equipment client clocks (SEC)*
- ITU–T Recommendation G.825 (1993), *The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.826 (1999), *Error performance parameters and objectives for international, constant bit-rate digital paths at or above the primary rate*
- ITU–T Recommendation G.831 (1993), *Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.957 (1995), *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*
- ITU–T Recommendation G.958 (1994), *Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables*
- ITU–T Recommendation I.432 (1993), *B-ISDN user-network interface – Physical layer specification*
- RFC 1619, *PPP over SONET/SDH*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Serial Interface Standards

Junos OS substantially supports the following standards for serial interfaces.

- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation V.35, *Data transmission at 48 kilobits per second using 60-108 kHz group band circuits*

- ITU–T Recommendation X.21 (1992), *Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported T3 Interface Standard

Junos OS substantially supports International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation G.703, *Physical/electrical characteristics of hierarchical digital interfaces*.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

CHAPTER 4

Layer 2 Standards

IN THIS CHAPTER

Supported Layer 2 Networking Standards

Junos OS substantially supports the following standards for Layer 2 networking.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1ab, *IEEE Standard for Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery* (Link Layer Discovery Protocol (LLDP))
- IEEE Standard 802.1D, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*

  This document includes the standard for Rapid Spanning Tree Protocol (RSTP), which is often referred to as 802.1w. It also discusses Quality of Service (QoS) at the MAC level, often referred to as 802.1p.
- IEEE Standard 802.1X, *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*

  IEEE 802.1X Port-Based Network Access Control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.

RELATED DOCUMENTATION

Supported L2TP Standards | 33

Supported VPWS Standards | 33

Supported Layer 2 VPN Standards | 34

Accessing Standards Documents on the Internet | 2

Supported L2TP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFC, which defines the standard for Layer 2 Tunneling Protocol (L2TP).

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

The following RFC does not define a standard, but provides information about technology related to L2TP. The IETF classifies it as "Informational."

- RFC 2866, *RADIUS Accounting*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

  Junos OS does not support Section 5.3, "The Generalized PWid FEC Element."

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as "Historic."

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 (zero) is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

Supported Layer 2 VPN Standards

Junos OS substantially supports the following standards and Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- RFC 7348, *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

RELATED DOCUMENTATION

- *Supported Carrier-of-Carriers and Interprovider VPN Standards*
- *Supported VPWS Standards*
- *Supported Layer 3 VPN Standards*
- *Supported Multicast VPN Standards*
- *Supported VPLS Standards*
- Accessing Standards Documents on the Internet

Supported Security Standards

Junos OS substantially supports the following standard for security.

- IEEE Standard 802.1AE, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*

  This document will facilitate standard secure communication between two security devices through secure chassis cluster control and fabric ports.

  SRX340 and SRX345 supports only 802.1AE-2006 standard.

RELATED DOCUMENTATION

- Accessing Standards Documents on the Internet | 2

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

  Junos OS does not support Section 5.3, “The Generalized PWid FEC Element.”

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as “Historic.”

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 (zero) is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

CHAPTER 5

MPLS Applications Standards

IN THIS CHAPTER

Supported GMPLS Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for Generalized MPLS (GMPLS).

- RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

  Only the following features are supported:

  - Bidirectional LSPs (upstream label only)
  - Control channel separation
  - Generalized label (suggested label only)
  - Generalized label request (bandwidth encoding only)

- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

  Only Section 9, “Fault Handling,” is supported.

- RFC 4202, *Routing Extensions in Support of Generalized Multi-Protocol Label Switching*

  Only interface switching is supported.

- RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, *Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON)* (expires January 2005)
- Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control*

  Only S,U,K,L,M-format labels and SONET traffic parameters are supported.
- Internet draft draft-ietf-ccamp-lmp-10.txt, *Link Management Protocol (LMP)*
- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching*

  The following sub-TLV types for the Link type, link, value (TLV) are not supported:

  - Link Local/Remote Identifiers (type 11)
  - Link Protection Type (type 14)
  - Shared Risk Link Group (SRLG) (type 16)

  The features described in Section 2 of the draft, “Implications on Graceful Restart,” are also not supported.

  The Interface Switching Capability Descriptor (type 15) sub-TLV type is implemented, but only for packet switching.
- Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

Supported LDP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for LDP.

- RFC 3212, *Constraint-Based LSP Setup using LDP*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*
- RFC 7060, *Using LDP Multipoint Extensions on Targeted LDP Sessions*
- RFC 8661, *Segment Routing MPLS Interworking with LDP*
- RFC 8077, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

- Internet draft draft-napierala-mpls-targeted-mldp-01.txt, *Using LDP Multipoint Extensions on Targeted LDP Sessions*

The following RFCs do not define standards, but provide information about LDP. The IETF classifies them as “Informational.”

- RFC 3215, *LDP State Machine*
- RFC 5036, *LDP Specification*

  For the following features described in the indicated sections of the RFC, Junos OS supports one of the possible modes but not the others:

  - Label distribution control (section 2.6.1): Ordered mode is supported, but not Independent mode.
  - Label retention (section 2.6.2): Liberal mode is supported, but not Conservative mode.
  - Label advertisement (section 2.6.3): Both Downstream Unsolicited mode and Downstream on Demand mode are supported.
- RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*
- RFC 5443, *LDP IGP Synchronization*
- RFC 5561, *LDP Capabilities*
- RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

  Junos OS support limited to point-to-multipoint extensions for LDP.

Supported MPLS Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for MPLS and traffic engineering.

- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3032, *MPLS Label Stack Encoding*
- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*

  Only E-LSPs are supported.

- RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*
- RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

  Node protection in facility backup is not supported.
- RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*
- RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*
- RFC 4385, *Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*.

  Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*
- RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*
- RFC 5317, *Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile*
- RFC 5586, *MPLS Generic Associated Channel*
- RFC 5654, *Requirements of an MPLS Transport Profile*

  The following capabilities are supported in the Junos OS implementation of MPLS Transport Profile (MPLS-TP):

  - MPLS-TP OAM can send and receive packets with GAL and G-Ach, without IP encapsulation.
  - Two unidirectional RSVP LSPs between a pair of routers can be associated with each other to create an associated bidirectional LSP for binding a path for the GAL and G-Ach OAM messages. A single Bidirectional Forwarding Detection (BFD) session is established for the associated bidirectional LSP.
- RFC 5712, *MPLS Traffic Engineering Soft Preemption*
- RFC 5718, *An In-Band Data Communication Network For the MPLS Transport Profile*
- RFC 5860, *Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks*

- RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*
- RFC 5921, *A Framework for MPLS in Transport Networks*
- RFC 5950, *Network Management Framework for MPLS-based Transport Networks*
- RFC 5951, *Network Management Requirements for MPLS-based Transport Networks*
- RFC 5960, *MPLS Transport Profile Data Plane Architecture*
- RFC 6215, *MPLS Transport Profile User-to-Network and Network-to-Network Interfaces*
- RFC 6291, *Guidelines for the Use of the "OAM" Acronym in the IETF*.
- RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*
- RFC 6371, *Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks*.
- RFC 6372, *MPLS Transport Profile (MPLS-TP) Survivability Framework*
- RFC 6373, *MPLS-TP Control Plane Framework*
- RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

  Only Point-to-Multipoint LSPs are supported.
- RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*
- RFC 6425, *Detecting Data-Plane Failures in Point-to-Multipoint MPLS - Extensions to LSP Ping*
- RFC 6426, *MPLS On-Demand Connectivity Verification and Route Tracing*
- RFC 6428, *Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile*
- RFC 6510, *Resource Reservation Protocol (RSVP) Message Formats for Label Switched Path (LSP) Attributes Objects*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*
- RFC 7746, *Label Switched Path (LSP) Self-Ping*
- Internet draft draft-ietf-mpls-rsvp-te-no-php-oob-mapping-01.txt, *Non PHP behavior and Out-of-Band Mapping for RSVP-TE LSPs*

The following RFCs and Internet drafts do not define standards, but provide information about MPLS, traffic engineering, and related technologies. The IETF classifies them variously as "Experimental," "Historic," or "Informational."

- RFC 2547, *BGP/MPLS VPNs*
- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 2917, *A Core MPLS IP VPN Architecture*
- RFC 3063, *MPLS Loop Prevention Mechanism*
- RFC 3208, *PGM Reliable Transport Protocol Specification*

  Only the network element is supported.
- RFC 3469, *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*
- RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*
- RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) (Support one path per S2L mode of signaling)*

Supported PCEP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for PCEP.

- RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)—Stateful PCE*
- RFC 8231, *Path Computation Element Communication Protocol (PCEP)—Extensions for Stateful PCE*

- RFC 8281, *Path Computation Element Communication Protocol (PCEP)—Extensions PCE-Initiated LSP Setup in a Stateful PCE Model*
- Internet draft-ietf-pce-stateful-pce-07.txt, *PCEP Extensions for Stateful PCE*
- Internet draft-crabbe-pce-pce-initiated-lsp-03.txt, *PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model*
- Internet draft-ietf-pce-segment-routing-06.txt, *PCEP Extensions for Segment Routing*
- Internet draft-ietf-pce-stateful-pce-p2mp-02.txt, *Path Computation Element (PCE) Protocol Extensions for Stateful PCE usage for Point-to-Multipoint Traffic Engineering Label Switched Paths*
- Internet draft draft-cbrt-pce-stateful-local-protection-01, *PCEP Extensions for RSVP-TE Local-Protection with PCE-Stateful* (excluding support for bypass LSP mapping)
- Internet draft draft-ietf-pce-pcep-flowspec-05, *PCEP Extension for Flow Specification*

  The current implementation of this feature does not implement the following sections of the draft:

  - Section 3.1.2—Advertising PCE capabilties in IGP
  - Section 3.2—PCReq and PCRep message
  - Section 7—Most of the flow specifications, except route distinguisher and IPv4 Multicast Flow specifications, are not supported.

Supported RSVP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for RSVP.

- RFC 2205, *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2745, *RSVP Diagnostic Messages*
- RFC 2747, *RSVP Cryptographic Authentication* (updated by RFC 3097)

- RFC 2750, *RSVP Extensions for Policy Control* (RFC is not supported. Fully compliant with devices that support this RFC).
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*
- RFC 3097, *RSVP Cryptographic Authentication—Updated Message Type Value*
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

  The Null Service Object for maximum transmission unit (MTU) signaling in RSVP is not supported.
- RFC 3210, *Applicability Statement for Extensions to RSVP for LSP-Tunnels*
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

  Only Section 9, "Fault Handling," is supported.
- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

  (OSPF extensions can carry traffic engineering information over unnumbered links.)
- 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*

  The RRO node ID subobject is for use in inter-AS link and node protection configurations.
- RFC 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*
- RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*
- RFC 5420, *Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)*

  Only the LSP_ATTRIBUTES object is supported.
- RFC 6437, *IPv6 Flow Label Specification*
- RFC 6510, *Resource Reservation Protocol (RSVP) Message Formats for Label Switched Path (LSP) Attributes Objects*
- RFC 7570, *Label Switched Path (LSP) Attribute in the Explicit Route Object (ERO)*

- RFC 8370, *Techniques to Improve the Scalability of RSVP-TE Deployments*
- RFC 8577, *Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane*
- RFC 8796, *RSVP-TE Summary Fast Reroute Extensions for Label Switched Path (LSP) Tunnels*
- draft-ietf-mpls-ri-rsvp-frr-05, *Refresh Interval Independent FRR Facility Protection*

The following RFCs do not define standards, but provide information about RSVP and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 2209, *Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules*
- RFC 2216, *Network Element Service Specification Template*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 8577, *Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane (Fully compliant)*

CHAPTER 6

Open Standards

IN THIS CHAPTER

Supported Open Standards

Junos OS substantially supports the following open standards:

- *OpenFlow Switch Specification, Version 1.0.0*

  For a detailed list of supported messages and fields, match conditions, wild cards, flow actions, statistics, and features, see *OpenFlow v1.0 Compliance Matrix for Devices Running Junos OS*.

  The Junos OS implementation of OpenFlow v1.0 differs from the specification in the following ways:

  (The sections of the OpenFlow specification are indicated in the parentheses.)

  - Junos OS supports only the following flow action types (section 5.2.4):
    - OFPAT_OUTPUT—supports OFPP_NORMAL, OFPP_FLOOD, OFPP_ALL, and OFPP_CONTROLLER for normal flow actions, and OFPP_FLOOD and OFPP_ALL for Send Packet flow actions.
    - OFPAT_SET_VLAN_VID—support varies by platform.
    - OFPAT_STRIP_VLAN—support varies by platform
  - Flow priority is supported according to OpenFlow Switch Specification v1.3.0 in which there is no prioritization of exact match entries over wildcard entries.
  - Emergency mode as defined in OpenFlow v1.0 is not supported. If the controller connection is lost and cannot be reestablished, the switch maintains all flow states in the control and data planes.

  The following features are not supported:

  - Encryption through TLS connection (section 4.4)

- 802.1D Spanning Tree Protocol (sections 4.5 and 5.2.1)
- OFPP_LOCAL virtual port (section 5.2.1)
- Physical port features OFPPF_PAUSE and OFPPF_PAUSE_ASYM (section 5.2.1)
- Queue structures and queue configuration messages (section 5.2.2 and 5.3.4)
- Flow action types: OFPAT_SET_VLAN_PCP, OFPAT_SET_DL_SRC/DST, OFPAT_SET_NW_SRC/DST/TOS, OFPAT_SET_TP_SRC/DST and OFPAT_ENQUEUE (section 5.2.4)
- buffer_id for Modify Flow Entry Message, Send Packet Message, and Packet-In Message (sections 5.3.3, 5.3.6, and 5.4.1)
- Port Modification Message (section 5.3.3)
- Vendor Statistics (section 5.3.5)
- Vendor message (section 5.5.4)

- *OpenFlow Switch Specification, Version 1.3.1*

  For a detailed list of supported messages and fields, port structure flags and numbering, match conditions, flow actions, multipart messages, flow instructions, and group types, see *OpenFlow v1.3.1 Compliance Matrix for Devices Running Junos OS*.

  The Junos OS implementation of OpenFlow v1.3.1 differs from the specification in the following ways:

  (The sections of the OpenFlow specification are indicated in the parentheses.)

  - Junos OS supports only the following flow action types (section 5.12):
    - OFPAT_SET_VLAN_VID
    - OFPAT_POP_VLAN
    - OFPAT_GROUP
  - Junos OS supports only the following group types (section 5.6.1):
    - OFPGT_ALL
    - OFPGT_INDIRECT
  - Junos OS supports only one flow instruction per flow entry. Further, only the following flow instructions (section A.2.4) are supported:
    - OFPIT_WRITE_ACTIONS

    - OFPIT_APPLY_ACTIONS

- For OFPT_SET_CONFIG (section A.3.2), Junos OS supports only the OFPC_FRAG_NORMAL configuration flag, and the OFPCML_NO_BUFFER setting for the miss_send_len field.
- On MX Series routers, Junos OS supports only the following IPv6-related match conditions (A.2.3.7):
    - OFPXMT_OFB_IPV6_SRC
    - OFPXMT_OFB_IPV6_DST

The following features are not supported:

- Multiple flow tables (section 5)
- Table metadata (section 2)
- Action sets (section 5.10)
- Meter (section 5.7)
- MPLS fields (section 5.12.1)
- MPLS actions (section 5.10 and 5.12)
- Encryption through TLS connection (section 6.3.3)
- Per-port queues (section A.2.2)
- Auxiliary connections (section 6.3.5)
- Multiple virtual switches (section A.3.1)
- IPv6-related set-field actions (5.12)

RELATED DOCUMENTATION

OpenFlow v1.0 Compliance Matrix for Devices Running Junos OS

OpenFlow v1.0 Compliance Matrix for QFX5100 and EX4600 Switches

OpenFlow v1.3.1 Compliance Matrix for Devices Running Junos OS

Understanding OpenFlow Operation and Forwarding Actions on Devices Running Junos OS

CHAPTER 7

Packet Processing Standards

IN THIS CHAPTER

Supported CoS Standards

Junos OS substantially supports the following standards for class of service (CoS).

- IEEE Standard 802.1D, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*

  This document discusses Quality of Service (QoS) at the MAC level, often referred to as 802.1p.

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behaviour)*
- RFC: 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*

The following RFCs do not define standards, but provide information about CoS and related technologies. The IETF classifies them as “Informational.”

- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*
- RFC 2983, *Differentiated Services and Tunnels*

- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 3260, *New Terminology and Clarifications for Diffserv*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Packet Filtering Standards

Junos OS provides a packet filtering language that enables you to control the flow of packets being forwarded to a network destination, as well as packets destined for and sent by the router. It substantially supports the following RFCs, which define standards for packet filtering.

- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

The following RFCs do not define standards, but provide information about packet filtering and related technologies. The IETF classifies them as “Informational.”

- RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2983, *Differentiated Services and Tunnels*
- RFC 3260, *New Terminology and Clarifications for Diffserv*

RELATED DOCUMENTATION

- Routing Policies, Firewall Filters, and Traffic Policers User Guide
- Accessing Standards Documents on the Internet | 2

Supported Policing Standard

Junos OS supports policing, or rate limiting, to limit the amount of traffic that passes through an interface. For information about rate limiting, see RFC 2698, *A Two Rate Three Color Marker*.

The Junos OS implementation of policing uses a token-bucket algorithm and supports the following features:

- Adaptive shaping for Frame Relay traffic
- Virtual channels

RELATED DOCUMENTATION

- Accessing Standards Documents on the Internet | 2

CHAPTER 8

Routing Protocol Standards

IN THIS CHAPTER

Supported Standards for BGP

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP version 4 (IPv4) BGP.

For a list of supported IP version 6 (IPv6) BGP standards, see *Supported IPv6 Standards*.

Junos OS BGP supports authentication for protocol exchanges (MD5 authentication).

- RFC 1745, *BGP4/IDRP for IP—OSPF Interaction*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1997, *BGP Communities Attribute*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

- RFC 2439, *BGP Route Flap Damping*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2796, *BGP Route Reflection – An Alternative to Full Mesh IBGP*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 2918, *Route Refresh Capability for BGP-4*
- RFC 3065, *Autonomous System Confederations for BGP*
- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3345, *Border Gateway Protocol (BGP) Persistent Route Oscillation Condition*
- RFC 3392, *Capabilities Advertisement with BGP-4*
- RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 4273, *Definitions of Managed Objects for BGP-4*
- RFC 4360, *BGP Extended Communities Attribute*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*
- RFC 4486, *Subcodes for BGP Cease Notification Message*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*
- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*
- RFC 4724, *Graceful Restart Mechanism for BGP*
- RFC 4760, *Multiprotocol Extensions for BGP-4*
- RFC 4781, *Graceful Restart Mechanism for BGP with MPLS*
- RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

  Option 4b (eBGP redistribution of labeled IPv6 routes from AS to neighboring AS) is not supported.

- RFC 4893, *BGP Support for Four-octet AS Number Space*
- RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*
- RFC 5065, *Autonomous System Confederations for BGP*
- RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*
- RFC 5291, *Outbound Route Filtering Capability for BGP-4 (partial support)*
- RFC 5292, *Address-Prefix-Based Outbound Route Filter for BGP-4 (partial support)*

  Devices running Junos OS can receive prefix-based ORF messages.
- RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*
- RFC 5492, *Capabilities Advertisement with BGP-4*
- RFC 5512, *The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute*
- RFC 5549, *Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop*
- RFC 5575, *Dissemination of flow specification rules*
- RFC 5668, *4-Octet AS Specific BGP Extended Community*
- RFC 5701, *IPv6 Address Specific BGP Extended Community Attribute*
- RFC 5925, *The TCP Authentication Option*
- RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4- fully compliant*
- RFC 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 6774, *Distribution of Diverse BGP Paths*
- RFC 6793, *BGP Support for Four-Octet Autonomous System (AS) Number Space*
- RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*
- RFC 6811, *BGP Prefix Origin Validation*
- RFC 6996, *Autonomous System (AS) Reservation for Private Use*
- RFC 7300, *Reservation of Last Autonomous System (AS) Numbers*
- RFC 7311, *The Accumulated IGP Metric Attribute for BGP*
- RFC 7404, *Using Only Link-Local Addressing inside an IPv6 Network*

- RFC 7432, *BGP MPLS-Based Ethernet VPN (eVPN)*
- RFC 7606, *Revised Error Handling for BGP UPDATE Messages*
- RFC 7611, *BGP ACCEPT_OWN Community Attribute*

  We support the RFC by enabling Juniper routers to accept routes received from a route reflector with the `accept-own` community value.
- RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*
- RFC 7854, *BGP Monitoring Protocol (BMP)*
- RFC 7911, *Advertisement of Multiple Paths in BGP*
- RFC 8097, *BGP Prefix Origin Validation State Extended Community*
- RFC 8210, *The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1*
- RFC 8212, *Default External BGP (EBGP) Route Propagation Behavior without Policies- fully compliant*

  Exceptions:

  The behaviors in RFC 8212 are not implemented by default in order to avoid disruption of existing customer configuration. The default behavior is still kept to accept and advertise all routes with regard to EBGP peers.
- RFC 8277, *Using BGP to Bind MPLS Labels to Address Prefixes*
- RFC 8326, *Graceful BGP session Shutdown*
- RFC 8481, *Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)*
- RFC 8538, *Notification Message Support for BGP Graceful Restart*
- RFC 8571, *BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions*
- RFC 8584, *Framework for Ethernet VPN Designated Forwarder Election Extensibility*
- RFC 8642, *Policy Behavior for Well-Known BGP Communities*
- RFC 8669, *Segment Routing Prefix Segment Identifier Extensions for BGP*
- RFC 8810, *Revision to Capability Codes Registration Procedures*
- RFC 8814 *Signaling Maximum SID Depth (MSD) Using the Border Gateway Protocol - Link State (partial support)*

- RFC 8950, *Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop*
- RFC 9003, *Extended BGP Administrative Shutdown Communication*
- RFC 9012, *The BGP Tunnel Encapsulation Attribute*
- RFC 9029, *Updates to the Allocation Policy for the Border Gateway Protocol - Link State (BGP-LS) Parameters Registries*
- RFC 9069, *Support for Local RIB in the BGP Monitoring Protocol (BMP)*
- RFC 9085, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing*
- RFC 9384, *A BGP Cease NOTIFICATION Subcode for Bidirectional Forwarding Detection (BFD)*
- Internet draft draft-idr-rfc8203bis-00, *BGP Administrative Shutdown Communication* (expires October 2018)
- Internet draft draft-ietf-grow-bmp-adj-rib-out-01, *Support for Adj-RIB-Out in BGP Monitoring Protocol (BMP)* (expires September 3, 2018)
- Internet draft draft-ietf-idr-aigp-06, *The Accumulated IGP Metric Attribute for BGP* (expires December 2011)
- Internet draft draft-ietf-idr-as0-06, *Codification of AS 0 processing* (expires February 2013)
- Internet draft draft-ietf-idr-link-bandwidth-06.txt, *BGP Link Bandwidth Extended Community* (expires July 2013)
- Internet draft draft-ietf-sidr-origin-validation-signaling-00, *BGP Prefix Origin Validation State Extended Community (partial support)* (expires May 2011)

  The extended community (origin validation state) is supported in Junos OS routing policy. The specified change in the route selection procedure is not supported.
- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

The following RFCs and Internet draft do not define standards, but provide information about BGP and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 1965, *Autonomous System Confederations for BGP*
- RFC 1966, *BGP Route Reflection—An alternative to full mesh IBGP*
- RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*
- RFC 3345, *Border Gateway Protocol (BGP) Persistent Route Oscillation Condition*
- RFC 3562, *Key Management Considerations for the TCP MD5 Signature Option*

- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (expires July 2002)

RELATED DOCUMENTATION

Supported IPv6 Standards

Accessing Standards Documents on the Internet | 2

Supported ES-IS Standards

Junos OS substantially supports the following standards for End System–to–Intermediate System (ES-IS).

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard 8473, *Information technology — Protocol for providing the connectionless-mode network service*
- ISO/IEC standard 9542, *Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*

RELATED DOCUMENTATION

Supported Standards for IS-IS | 69

IS-IS Overview

Accessing Standards Documents on the Internet | 2

Supported ICMP Router Discovery and IPv6 Neighbor Discovery Standards

Junos OS substantially supports the following RFCs, which define standards for the Internet Control Message Protocol (ICMP for IP version 4 [IPv4]) and neighbor discovery (for IP version 6 [IPv6]).

- RFC 1256, *ICMP Router Discovery Messages*
- RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
-
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 8335, *PROBE: A Utility for Probing Interfaces*

Supported IP Multicast Protocol Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP multicast protocols, including the Distance Vector Multicast Routing Protocol (DVMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multicast Source Discovery Protocol (MSDP), Pragmatic General Multicast (PGM), Protocol Independent Multicast (PIM), Session Announcement Protocol (SAP), and Session Description Protocol (SDP).

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3376, *Internet Group Management Protocol, Version 3*
- RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*
- RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
- RFC 7761, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification*
- RFC 4604, *Using IGMPv3 and MLDv2 for Source-Specific Multicast*
- RFC 4607, *Source-Specific Multicast for IP*
- RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*
- RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*

- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

  The scoping mechanism is not supported.

- RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*

- RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

  Starting in Release 17.3R1, Junos OS provides support for Protocol Independent Multicast (PIM) resolve type-length-value (TLV) for multicast in seamless MPLS. This support allows PIM in environments where the core routers do not maintain external routes.

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*

- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*

- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*

- Internet draft draft-rosen-l3vpn-spmsi-joins-mldp-03.txt, *MVPN: S-PMSI Join Extensions for mLDP-Created Tunnels*

The following RFCs and Internet drafts do not define standards, but provide information about multicast protocols and related technologies. The IETF classifies them variously as “Best Current Practice,” “Experimental,” or “Informational.”

- RFC 1075, *Distance Vector Multicast Routing Protocol*

- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*

- RFC 2365, *Administratively Scoped IP Multicast*

- RFC 2547, *BGP/MPLS VPNs*

- RFC 2974, *Session Announcement Protocol*

- RFC 3208, *PGM Reliable Transport Protocol Specification*

- RFC 3446, *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

- RFC 3569, *An Overview of Source-Specific Multicast (SSM)*

- RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

- RFC 3973, *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)*

- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, *Distance Vector Multicast Routing Protocol*
- Internet draft draft-ietf-mboned-ssm232-08.txt, *Source-Specific Protocol Independent Multicast in 232/8*
- Internet draft draft-ietf-mmusic-sap-00.txt, *SAP: Session Announcement Protocol*
- Internet draft draft-rosen-vpn-mcast-07.txt, *Multicast in MPLS/BGP VPNs*

  Only section 7, "Data MDT: Optimizing flooding," is supported.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet

Supported IPv4, TCP, and UDP Standards

Junos OS substantially supports the following RFCs, which define standards for IP version 4 (IPv4), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

- RFC 768, *User Datagram Protocol*
- RFC 791, *INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 793, *TRANSMISSION CONTROL PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 826, *Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*
- RFC 854, *TELNET PROTOCOL SPECIFICATION*
- RFC 855, *TELNET OPTION SPECIFICATIONS*
- RFC 856, *TELNET BINARY TRANSMISSION*

  To transmit using an 8-bit binary path, use the `telnet` *`host`* `8bit` command, where *host* is the name or address of the remote system.

- 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 903, *A Reverse Address Resolution Protocol*
- RFC 919, *BROADCASTING INTERNET DATAGRAMS*
- RFC 922, *BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS*
- RFC 950, *Internet Standard Subnetting Procedure*
- RFC 959, *FILE TRANSFER PROTOCOL (FTP)*
- RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*
- RFC 1042, *A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*
- RFC 1157, A *Simple Network Management Protocol (SNMP)*
- RFC 1166, *INTERNET NUMBERS*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1256, *ICMP Router Discovery Messages*
- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*
- RFC 1812, *Requirements for IP Version 4 Routers*
- RFC 2338, *Virtual Router Redundancy Protocol* (obsoleted by RFC 3768 in April 2004)
- RFC 2873, *TCP Processing of the IPv4 Precedence Field*
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 4884 *Extended ICMP to Support Multi-Part Messages*

  NOTE: In Junos OS, support not available for setting the length attribute.

- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*

- RFC 5925, *The TCP Authentication Option*

  TCP-based features are fully supported. Master Key Tuple/ key management is Junos specific. The CLI/application uses Junos keychain infrastructure for MKT configuration.

- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpv3StatisticsRowDiscontinuityTime` MIB object
  - `vrrpv3StatisticsPacketLengthErrors` MIB object

- RFC 8335, *PROBE: A Utility for Probing Interfaces*

The following RFCs do not define standards, but provide information about IP, TCP, UDP, and related technologies. The IETF classifies them as "Informational."

- RFC 1878, *Variable Length Subnet Table For IPv4*
- RFC 1948, *Defending Against Sequence Number Attacks*

RELATED DOCUMENTATION

Supported IPv6 Standards | 62

Accessing Standards Documents on the Internet | 2

Supported IPv6 Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP version 6 (IPv6):

- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2373, *IP Version 6 Addressing Architecture*

- RFC 2375, *Multicast Address Assignments*
- 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 IP Version 6: Textual Conventions and General Group*

  IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.
- RFC 2472, *IP Version 6 over PPP*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2491, *IPv6 Over Non-Broadcast Multiple Access (NBMA) networks*
- RFC 2492, *IPv6 over ATM Networks*
- RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2675, *IPv6 Jumbograms*
- RFC 2711, *IPv6 Router Alert Option*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*
- RFC 2784, *Generic Routing Encapsulation*
- RFC 2878, *PPP Bridging Control Protocol (BCP)*
- RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds.*
- RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*
- RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

  Address assignment is supported with IP version 4 (IPv4) but not IP version 6 (IPv6).
- RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*

- RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*
- RFC 3590, *Source Address Selection for the Multicast Listener D* (Supported for SSM include mode only)
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
- RFC 3879, *Deprecating Site Local Addresses*
- RFC 3971, *Secure Neighbor Discovery for IPv6* (No support for certification paths, anchored on trusted parties)
- RFC 3972, *Cryptographically Generated Addresses*
- RFC 4007, *IPv6 Scoped Address Architecture*
- RFC 4087, *IP Tunnel MIB*
- RFC 4193, *Unique Local IPv6 Unicast Addresses*
- RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

  RFC 4213 supersedes RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*.

  NOTE: On EX Series switches, except for the EX9200 Series, only dual IP layer is supported. On EX9200 Series switches, both dual IP layer and configured tunneling of IPv6 over IPv4 are supported.

- 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* (Partial support)
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

Option 4b (eBGP redistribution of labeled IPv6 routes from AS to neighboring AS) is not supported.

- RFC 4861 *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 4884, *Extended ICMP to Support Multi-Part Messages*
- RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*
- RFC 4942, *IPv6 Transition/Coexistence Security Considerations*
- RFC 5072, *IP Version 6 over PPP*
- RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*
- RFC 5308, *Routing IPv6 with IS-IS*
- RFC 5340, *OSPF for IPv6* (RFC 2740 is obsoleted by RFC 5340)
- RFC 5575, *Dissemination of Flow Specification Rules*
- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 5905, *Network Time Protocol Version 4 (for IPv6)*
- RFC 5952, *A Recommendation for IPv6 Address Text Representation*
- RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*
- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpv3StatisticsPacketLengthErrors` MIB object
  - `vrrpv3StatisticsRowDiscontinuityTime` MIB object
- RFC 6583, *Operational Neighbor Discovery Problems*

  Only Prioritize NDP Activities, Tuning of the NDP Queue Rate Limit, and Queue Tuning are supported.
- RFC 6724, *Default Address Selection for Internet Protocol version 6 (IPv6)*
- RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

- RFC 8201, *Path MTU Discovery for IP version 6*
- RFC 8335, *PROBE: A Utility for Probing Interfaces*
- Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, *BGP-MPLS IP VPN extension for IPv6 VPN*
- Internet draft draft-ietf-lsr-flex-algo-20.txt, *IGP Flexible Algorithm* to allow IGPs to compute constraint-based paths over the network.
- Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
- Internet draft draft-ietf-softwire-dual-stack-lite-04.txt, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*
- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

The following RFCs and Internet draft do not define standards, but provide information about IPv6 and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*
- RFC 3587, *IPv6 Global Unicast Address Format*
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP*

  Only MP-BGP over IP version 4 (IPv4) approach is supported.

RELATED DOCUMENTATION

Supported IPv4, TCP, and UDP Standards | 60

Accessing Standards Documents on the Internet | 2

Supported OSPF and OSPFv3 Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for OSPF and OSPF version 3 (OSPFv3).

- RFC 1583, *OSPF Version 2*
- RFC 1765, *OSPF Database Overflow*

- RFC 1793, *Extending OSPF to Support Demand Circuits*
- RFC 1850, *OSPF Version 2 Management Information Base*
- RFC 2154, *OSPF with Digital Signatures*
- RFC 2328, *OSPF Version 2*
- RFC 2370, *The OSPF Opaque LSA Option*

  Support is provided by the `update-threshold` configuration statement at the `[edit protocols rsvp interface` *`interface-name`* `]` hierarchy level.
- RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 3623, *Graceful OSPF Restart*
- RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*
- RFC 4136, *OSPF Refresh and Flooding Reduction in Stable Topologies*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

  Only interface switching is supported.
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*
- RFC 4812, *OSPF Restart Signaling*
- RFC 4813, *OSPF Link-Local Signaling*
- RFC 4915, *Multi-Topology (MT) Routing in OSPF*
- RFC 5185, *OSPF Multi-Area Adjacency*
- RFC 5187, *OSPFv3 Graceful Restart*
- RFC 5250, *The OSPF Opaque LSA Option*

> **NOTE**: RFC 4750, mentioned in this RFC as a "should" requirement is not supported. However, RFC 1850, the predecessor to RFC 4750 is supported.

- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 5340, *OSPF for IPv6* (RFC 2740 is obsoleted by RFC 5340)
- RFC 5838, *Support of Address Families in OSPFv3*
- Internet draft draft-ietf-ospf-af-alt-10.txt, *Support of address families in OSPFv3*
- Internet draft draft-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection*

  Transmission of echo packets is not supported.
- RFC 8665, *OSPF Extensions for Segment Routing*
- Internet draft draft-ietf-lsr-flex-algo-07.txt, *IGP Flexible Algorithm*

The following RFCs do not define standards, but provide information about OSPF and related technologies. The IETF classifies them as “Informational.”

- RFC 3137, *OSPF Stub Router Advertisement*
- RFC 3509, *Alternative Implementations of OSPF Area Border Routers*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*
- RFC 8920, *OSPF Application-Specific Link Attributes*
- RFC 8920, *OSPFv2 Prefix/Link Attribute Advertisement*

RELATED DOCUMENTATION

Supported IPv6 Standards

Accessing Standards Documents on the Internet

Supported Standards for RIFT

Junos OS substantially supports the following Internet drafts for Routing in Fat Tree (RIFT) protocol.

- draft draft-ietf-rift-rift-09, *RIFT: Routing in Fat Trees*

RELATED DOCUMENTATION

Supported Standards for IS-IS | 69

Supported RIP and RIPng Standards

Junos OS substantially supports the following RFCs, which define standards for RIP (for IP version 4 [IPv4]) and RIP next generation (RIPng, for IP version 6 [IPv6]).

Junos OS supports authentication for all RIP protocol exchanges (MD5 or simple authentication).

- RFC 1058, *Routing Information Protocol*
- RFC 2080, *RIPng for IPv6*
- RFC 2082, *RIP-2 MD5 Authentication*

  Multiple keys using distinct key IDs are not supported.
- RFC 2453, *RIP Version 2*

The following RFC does not define a standard, but provides information about RIPng. The IETF classifies it as "Informational."

- RFC 2081, *RIPng Protocol Applicability Statement*

RELATED DOCUMENTATION

Supported IPv4, TCP, and UDP Standards
Supported IPv6 Standards
Accessing Standards Documents on the Internet

Supported Standards for IS-IS

Junos OS substantially supports the following standards for IS-IS.

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 8473, *Information technology — Protocol for providing the connectionless-mode network service*
- ISO 9542, *End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for the Provision of the Connectionless-mode Network Service*

- ISO/IEC 10589, *Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- 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 Administrative Tags*
- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- 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 5310, *IS-IS Generic Cryptographic Authentication*
- RFC 5880, *Bidirectional Forwarding Detection (BFD)*
- RFC 6119, *IPv6 Traffic Engineering in IS-IS*
- RFC 6232, *Purge Originator Identification TLV for IS-IS*
- RFC 6233, *IS-IS Registry Extension for Purges*
- 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 7981, *IS-IS Extensions for Advertising Router Information*
- RFC 8202, *IS-IS Multi-Instance*
- RFC 8518, *Selection of Loop-Free Alternates for Multi-Homed Prefixes*

- RFC 8570, *IS-IS Traffic Engineering (TE) Metric Extensions*
- RFC 8667, *IS-IS Extensions for Segment Routing*
- RFC 8706, *Restart Signaling for IS-IS*
- RFC 8919, *IS-IS Application-Specific Link Attributes*
- RFC 9352, *IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane*

The following RFCs do not define standards, but provide information about IS-IS and related technologies. The IETF classifies them as "Informational."

- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2973, *IS-IS Mesh Groups*
- RFC 3277, *Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance*
- RFC 3358, *Optional Checksums in Intermediate System to Intermediate System (ISIS)*
- 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 3567, *Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication*
- RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 3847, *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*
- RFC 6151, *updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*
- Internet draft draft-ietf-isis-wg-255adj-02.txt, *Maintaining more than 255 circuits in IS-IS*
- Internet draft draft-przygienda-flood-reflector-00, *Flood Reflectors*
- Internet draft draft-przygienda-lsr-flood-reflection-01, *IS-IS Flood Reflection*

RELATED DOCUMENTATION

IS-IS Overview

Supported ES-IS Standards | 57

Accessing Standards Documents on the Internet | 2

Supported Standards for Segment Routing

Junos OS substantially supports the following RFCs and Internet drafts for Segment Routing.

- draft-agrawal-spring-srv6-mpls-interworking-06, *SRv6 and MPLS interworking*

  Supports service interworking.

- draft-ali-spring-sr-traffic-accounting, *SR traffic matrix accounting (Partial support)*

  Supports counter only.

- draft-bashandy-rtgwg-segment-routing-ti-lfa, *Topology Independent Fast Reroute using Segment Routing*

- draft-bashandy-rtgwg-segment-routing-uloop, *Microloop Avoidance using Segment Routing*

- draft-barth-pce-segment-routing-policy-cp-05, *PCEP extension to support Segment Routing Policy Candidate Paths*

- draft-filsfils-rtgwg-segment-routing-use-cases-02, *Segment Routing Use Cases*

- draft-filsfils-spring-sr-policy-considerations-05, *SR Policy Implementation and Deployment Considerations*

- draft-filsfils-spring-sr-traffic-counters, *SR traffic counters*

- draft-ginsberg-isis-prefix-attributes, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability (Partial support)*

- draft-ietf-bess-srv6-services-07, *SRv6 BGP based Overlay Services*

- draft-ietf-idr-bgp-prefix-sid, *Advertise BGP segment for a BGP Prefix*

- draft-ietf-idr-bgpls-segment-routing-epe, *BGP-LS extensions for Egress peer traffic engineering using SR*

- draft-ietf-idr-segment-routing-te-policy, *Advertise SR-TE policies via BGP*

- draft-ietf-idr-segment-routing-te-policy-09, *Advertising Segment Routing Policies in BGP*

- draft-ietf-lsr-flex-algo-11.txt, *IGP Flexible Algorithm (Partial support)*

  Supports IS-IS only.

- draft-ietf-lsr-isis-srv6-extensions, *IS-IS Extensions to Support Segment Routing over IPv6 Dataplane*
- draft-ietf-ospf-segment-routing-extensions, *OSPF extensions to distribute SR segments*
- draft-ietf-pce-segment-routing, *PCE extensions to setup a SR-TE path from the controller (south bound)*
- draft-ietf-isis-segment-routing-extensions, *ISIS extensions to distribute SR segments*
- draft-ietf-rtgwg-segment-routing-ti-lfa-04, *Topology Independent Fast Reroute using Segment Routing*
- draft-ietf-spring-conflict-resolution, *Segment Routing MPLS Conflict Resolution*
- draft-ietf-spring-ipv6-use-cases, *Use Cases for IPv6 Source Packet Routing in Networking (Partial support)*
- draft-ietf-spring-resiliency-use-cases, *Resiliency use cases in SPRING networks*
- draft-ietf-spring-segment-routing-msdc, *BGP-Prefix Segment in Large Scale data centers (Partial support)*
- draft-ietf-spring-segment-routing-central-epe, *SR Centralized BGP Egress Peer Engineering*
- draft-ietf-spring-segment-routing-mpls, *Segment Routing details with MPLS forwarding*
- draft-ietf-spring-segment-routing-policy, *SR policy for TE (Partial support)*
- draft-ietf-spring-segment-routing-policy-07.txt, *Segment Routing Policy Architecture*
- draft-kaliraj-idr-bgp-classful-transport-planes-12, *BGP Classful Transport Planes*
- RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information (Partial support)*

  Supports counter only.

- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 7471, *OSPF Traffic Engineering (TE) Metric Extensions*
- RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*
- RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*

- RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*
- RFC 7855, *Source Packet Routing in Networking (SPRING) Problem Statement and Requirements*
- RFC 8102, *Remote-LFA Node Protection and Manageability*
- RFC 8277, *Using BGP to Bind MPLS Labels to Address Prefixes*
- RFC 8287, *LSP Ping/Traceroute for Segment Routing*
- RFC 8402, *Segment Routing Architecture (Partial support)*
- RFC 8403, *A Scalable and Topology-Aware MPLS Data-Plane Monitoring System*
- RFC 8426, *RSVP-SR coexistence*
- RFC 8570, *IS-IS Traffic Engineering (TE) Metric Extensions (Partial support)*

  Supports link delay related parameters.
- RFC 8571, *BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions*
- RFC 8604, *Interconnecting Millions of Endpoints with Segment Routing*
- RFC 8660, *Segment Routing with the MPLS Data Plane*
- RFC 8661, *Segment Routing MPLS Interworking with LDP*
- RFC 8663, *MPLS Segment Routing over IP (Partial support)*
- RFC 8665, *OSPF Extensions for Segment Routing*
- RFC 8690, *Clarification of Segment ID Sub-TLV Length for RFC 8287*
- draft-xu-mpls-sr-over-ip, *MPLS Segment Routing over IP (Partial support)*
- RFC 8919, *IS-IS Application-Specific Link Attributes (Partial support)*
- RFC 8986, *Segment Routing over IPv6 (SRv6) Network Programming*
- RFC 9085, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing*
- RFC 9086, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing BGP Egress Peer Engineering*
- RFC 9256, *Segment Routing Policy Architecture*

The following RFCs do not define standards, but provide information about Segment Routing and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 6571, *Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks*
- RFC 9087, *Segment Routing Centralized BGP Egress Peer Engineering*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

CHAPTER 9

Services PIC and DPC Standards

IN THIS CHAPTER

Supported DTCP Standard

Junos OS substantially supports Internet draft draft-cavuto-dtcp-03.txt, *DTCP: Dynamic Tasking Control Protocol*.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Flow Monitoring and Discard Accounting Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions), Monitoring Services PICs, or Dense Port Concentrators (DPCs), Junos OS substantially supports the standards for cflowd version 5 and version 8 formats that are maintained by CAIDA and accessible at http://www.caida.org.

RFC 3954, *Cisco Systems NetFlow Services Export Version 9* does not define a standard but provides information about flow monitoring. The IETF classifies it as “Informational.”

Internet draft *draft-kumar-ippm-ifa-02.txt, Inband Flow Analyzer* does not define standards but provides information about Inband Flow Analyzer (IFA). You use this feature to record flow-specific information from an end station or switches across a network.

On MX Series routers, Junos OS partially supports the following RFCs:

- RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*
- RFC 5102, *Information Model for IP Flow Information Export*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported IPsec and IKE Standards

On routers equipped with one or more MS-MPCs, MS-MICs, or DPCs, the Canada and U.S. version of Junos OS substantially supports the following RFCs, which define standards for IP Security (IPsec) and Internet Key Exchange (IKE).

- RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2401, *Security Architecture for the Internet Protocol* (obsoleted by RFC 4301)
- RFC 2402, *IP Authentication Header* (obsoleted by RFC 4302)
- 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* (obsoleted by RFC 4305)
- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulating Security Payload (ESP)* (obsoleted by RFC 4303 and RFC 4305)
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP* (obsoleted by RFC 4306)
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)* (obsoleted by RFC 4306)

- RFC 2409, *The Internet Key Exchange (IKE)* (obsoleted by RFC 4306)
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 2451, *The ESP CBC-Mode Cipher Algorithms*
- RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*
- RFC 3193, *Securing L2TP using IPsec*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- RFC 3948, *UDP Encapsulation of IPsec ESP Packets*
- RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*
- RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*
- RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*
- RFC 4301, *Security Architecture for the Internet Protocol*
- RFC 4302, *IP Authentication Header*
- RFC 4303, *IP Encapsulating Security Payload (ESP)*
- RFC 4305, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 4308, *Cryptographic Suites for IPsec*

  Only Suite VPN-A is supported in Junos OS.
- RFC 4754, *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*
- RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)* (obsoleted by RFC 7296)
- RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*

- RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

Junos OS partially supports the following RFCs for IPsec and IKE:

- RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*
- RFC 5114, *Additional Diffie-Hellman Groups for Use with IETF Standards*
- RFC 5903, *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*

The following RFCs and Internet draft do not define standards, but provide information about IPsec, IKE, and related technologies. The IETF classifies them as "Informational."

- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- Internet draft draft-eastlake-sha2-02.txt, *US Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006)

RELATED DOCUMENTATION

> Services Interfaces Overview for Routing Devices
>
> MX Series 5G Universal Routing Platform Interface Module Reference
>
> Accessing Standards Documents on the Internet

Supported L2TP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFC, which defines the standard for Layer 2 Tunneling Protocol (L2TP).

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

The following RFC does not define a standard, but provides information about technology related to L2TP. The IETF classifies it as "Informational."

- RFC 2866, *RADIUS Accounting*

RELATED DOCUMENTATION

- Services Interfaces Overview for Routing Devices
- MX Series 5G Universal Routing Platform Interface Module Reference
- Accessing Standards Documents on the Internet | 2

Supported Link Services Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or DPCs, Junos OS substantially supports the following RFCs, which define standards for link services.

- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 2364, *PPP Over AAL5*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

  The following features are not supported:

  - Negotiation of address field compression and protocol field compression PPP NCP options; instead, a full 4-byte PPP header is always sent
  - Prefix elision

RELATED DOCUMENTATION

- Services Interfaces Overview for Routing Devices
- MX Series 5G Universal Routing Platform Interface Module Reference
- Accessing Standards Documents on the Internet | 2

Supported NAT and SIP Standards

The Junos OS substantially supports the following Network Address Translation (NAT) and Session Initiaion Protocol (SIP) standards. NAT supports SIP dialogs and UDP/IP version 4 (IPv4) transport of SIP messages.

NOTE: This is applied to Junos routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions), Multiservices PICs or DPCs, and services cards (SPC) of a security device (i.e. SRX).

Junos OS substantially supports the following RFC and Internet draft.

- RFC 3261, *SIP: Session Initiation Protocol*
- Internet draft draft-mrw-behave-nat66-01.txt, *IPv6-to-IPv6 Network Address Translation (NAT66)*

The following RFCs do not define standards, but provide information about NAT. The IETF classifies them variously as “Best Current Practice,” “Historic,” or “Informational.”

- RFC 1631, *The IP Network Address Translator (NAT)*
- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 2766, *Network Address Translation - Protocol Translation (NAT-PT)*
- RFC 2993, *Architectural Implications of NAT*
- RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*
- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*
- RFC 5382, *NAT Behavioral Requirements for TCP*
- RFC 5508, *NAT Behavioral Requirements for ICMP*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported RPM, TWAMP, STAMP, and Benchmarking Test Standards

IN THIS SECTION

Real-Time Performance Monitoring (RPM) Standard

On routers and switches equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or DPCs, Junos OS substantially supports the Juniper-proprietary feature known as real-time performance monitoring (RPM), and provides MIB support with extensions in substantial support of RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*. Junos OS Evolved supports Packet-Forwarding-Engine-based or Routing-Engine-based RPM, and provides MIB support with extensions in substantial support of RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

Two-Way Active Measurement Protocol (TWAMP) and Simple Two-Way Active Measurement Protocol (STAMP) Standards

The Two-Way Active Management Protocol (TWAMP), described in RFC 5357 *Two-Way Active Measurement Protocol* , is an extension of the One-Way Active Management Protocol (OWAMP) that supplies two-way or round-trip measurements instead of unidirectional capabilities. Both Junos OS and Junos OS Evolved support RFC 5357, including Appendix I, which documents a simpler operational mode known as TWAMP Light. The Simple Two-Way Active Measurement Protocol (STAMP) is defined in RFC 8762 *Simple Two-Way Active Measurement Protocol* . RFC 8762 standardizes and extends this TWAMP Light operational mode. Junos OS Evolved supports RFC 8762.

Benchmarking Test Standard

RFC 2544 defines a series of tests that can be used to describe the performance characteristics of a network-interconnecting device, such as a router, and outlines specific formats to report the results of the tests. These tests can be used to benchmark interconnected network devices and devise a guideline or a measurement pattern to analyze the health and efficiency of the network devices. These tests are the standard benchmarking tests for Ethernet networks and are known as RFC 2544-based

benchmarking tests. Junos OS and Junos OS Evolved support RFC 2544, *Benchmarking Methodology for Network Interconnect Devices*.

RELATED DOCUMENTATION

- Understanding Using Probes for Real-Time Performance Monitoring on M, T, ACX, MX, and PTX Series Routers, EX and QFX Switches
- Accessing Standards Documents on the Internet | 2

Supported Voice Services Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or DPCs, Junos OS substantially supports the following RFCs, which define standards for technologies used with voice services.

- RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
- RFC 2509, *IP Header Compression over PPP*

RELATED DOCUMENTATION

- Services Interfaces Overview for Routing Devices
- MX Series 5G Universal Routing Platform Interface Module Reference

CHAPTER 10

VPLS and VPN Standards

IN THIS CHAPTER

Supported Carrier-of-Carriers and Interprovider VPN Standards

Junos OS substantially supports the following RFCs, which define standards for carrier-of-carriers and interprovider virtual private networks (VPNs).

- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*

  Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*

  Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- *RFC 5601, Pseudowire (PW) Management Information Base (MIB)*
- *RFC 5603, Ethernet Pseudowire (PW) Management Information Base (MIB)*

- RFC 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

RELATED DOCUMENTATION

Supported VPWS Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Supported Standards for BGP

Accessing Standards Documents on the Internet

Supported EVPN Standards

RFCs and Internet drafts that define standards for EVPNs:

- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 7209, *Requirements for Ethernet VPN (EVPN)*
- RFC 7432, *BGP MPLS-Based Ethernet VPN*

  The following features are not supported:

  - Automatic derivation of Ethernet segment (ES) values. Only static ES configurations are supported.
  - Host proxy ARP.
- RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*
- RFC 8214, *Virtual Private Wire Service Support in Ethernet VPN*
- RFC 8317, *Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN)*
- RFC 8365, *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*

- RFC 8560, *Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents*
- RFC 8667, *IS-IS Extensions for Segment Routing*
- RFC 9047, *Propagation of ARP/ND Flags in an Ethernet Virtual Private Network (EVPN)*
- RFC 9135, *Integrated Routing and Bridging in Ethernet VPN (EVPN)*
- RFC 9136, *IP Prefix Advertisement in Ethernet VPN (EVPN)*
- RFC 9161, *Operational Aspects of Proxy-ARP/ND in Ethernet Virtual Private Networks*
- RFC 9251, *Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Proxies for Ethernet VPN (EVPN)*
- Internet draft draft-ietf-bess-evpn-oam-req-frmwk, *EVPN Operations, Administration and Maintenance Requirements and Framework*
- Internet draft draft-ietf-bess-evpn-optimized-ir, *Optimized Ingress Replication solution for EVPN*
- Internet draft draft-ietf-bess-evpn-pref-df, *Preference-based EVPN DF Election*
- Internet draft draft-ietf-bess-evpn-virtual-eth-segment, *EVPN Virtual Ethernet Segment*
- Internet draft draft-ietf-bess-evpn-vpws-fxc, *EVPN VPWS Flexible Cross-Connect Service*
- Internet draft draft-ietf-bess-evpn-yang, *Yang Data Model for EVPN*
- Internet draft draft-ietf-spring-segment-routing-13, *Segment Routing Architecture*
- Internet draft draft-ietf-spring-segment-routing-mpls-11, *Segment Routing with MPLS data plane*
- Internet draft draft-wsv-bess-extended-evpn-optimized-ir, *Extended Procedures for EVPN Optimized Ingress Replication*
- Internet draft draft-lin-bess-evpn-irb-mcast, *EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding*

RELATED DOCUMENTATION

EVPN Overview

Accessing Standards Documents on the Internet

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

  Junos OS does not support Section 5.3, "The Generalized PWid FEC Element."

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as "Historic."

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 (zero) is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

Supported Layer 2 VPN Standards

Junos OS substantially supports the following standards and Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- RFC 7348, *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

Supported Layer 3 VPN Standards

Junos OS substantially supports the following RFCs, which define standards for Layer 3 virtual private networks (VPNs).

- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2685, *Virtual Private Networks Identifier*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*

  The traceroute functionality is supported only on transit routers.

- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*

- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- 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) Virtual Private Networks (VPNs)*

The following RFCs do not define a standard, but provide information about technology related to Layer 3 VPNs. The IETF classifies them as a "Best Current Practice" or "Informational."

- RFC 1918, *Address Allocation for Private Internets*
- RFC 2917, *A Core MPLS IP VPN Architecture*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 2 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Supported MPLS Standards

Supported Standards for BGP

Accessing Standards Documents on the Internet

Supported Multicast VPN Standards

Junos OS substantially supports the following RFCs and Internet draft, which define standards for multicast virtual private networks (VPNs).

- 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 6625, *Wildcards in Multicast VPN Auto-Discovery Routes*
- Internet draft draft-morin-l3vpn-mvpn-fast-failover-06.txt, *Multicast VPN Fast Upstream Failover*

- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*
- RFC 7900, *Extranet Multicast in BGP/IP MPLS VPNs (partial support)*
- RFC 8534, *Explicit Tracking with Wildcard Routes in Multicast VPN (partial support)*
- RFC 9081, *Interoperation between Multicast Virtual Private Network (MVPN) and Multicast Source Directory Protocol (MSDP) Source-Active Routes*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported VPLS Standards

Supported MPLS Standards

Supported Standards for BGP

Accessing Standards Documents on the Internet

Supported VPLS Standards

Junos OS substantially supports the following Internet RFCs and draft, which define standards for virtual private LAN service (VPLS).

- 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*

  FEC 128, FEC 129, control bit `0`, the Ethernet pseudowire type `0x0005`, and the Ethernet tagged mode pseudowire type `0x0004` are supported.
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*

RELATED DOCUMENTATION

- *Supported Carrier-of-Carriers and Interprovider VPN Standards*
- *Supported VPWS Standards*
- *Supported Layer 2 VPN Standards*
- *Supported Layer 3 VPN Standards*
- *Supported Multicast VPN Standards*
- Accessing Standards Documents on the Internet

DIO Intercon I

DIO Intercon I

Características Construtivas

Altura	43mm / 1U
Largura	483mm / 19"
Profundidade	343mm
Cor	Bege (RAL 7032) Cinza (RAL 7035) Preta (RAL 9005)
Peso	2,8 kg
Composição	Aço Minimizado / Alumínio
Capacidade - Adaptador	Até 24FO - E2000/SX, LC/SX, LC/DX e SC/SX
Tipo de Conexão	Fusão / Espelhamento
Aplicação	Telecomunicações / Automação Industrial
Instalação	Racks e Bastidores de 19" e 23" (21" Sob encomenda)

Propriedades

1 - Abertura de 220mm da gaveta de emenda através de trilho telescópico destacável.
2 - Painel interno angular dispõe de até 24 adaptadores com identificação numérica.
3 - Armazenamento da sobra de tubo loose na parte inferior da bandeja.
4 - "L" de fixação com regulagem de profundidade.
5 - Acessórios traseiro para entrada e fixação de cabos ópticos e junções.
6 - Cassete para emenda de fibra óptica através de fusão.
7 - Guia de rota frontal.

Detalhes

A - Disposição dos adaptadores com a bandeja de emendas totalmente aberta

D - Visão traseira do sistema montado no rack

B - Saída dos cordões pela abertura lateral do DIO

E - Preenchimento do Mapa de Rotas

C - Visão frontal do sistema montado no rack

Rosenberger Domex