Anexa nr. 22
la Documentația standard nr._____
din "____" _____ 20___

Specificaţii tehnice

Numărul procedurii de achiziție ocds-b3wdp1-MD-1658736740900 din 25.07.2022
Obiectul achiziției: Bunuri și consumabile pentru Sistemele de comunicații critice a MAI (repetat)

Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/serviciului**	**Țara de origine**	**Produ-cătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Bunuri/servicii						
Lotul III: Licențe/Echipamente/Utilaj specializat pentru sistemele de comunicații critice ale MAI						
ECHIPAMENTE RADIO BACKBONE SI BACKHAUL	Ceragon FibeAir IP-20F	Israel	Ceragon Networks Ltd	Conform Caietului de sarcini	Coincide cu caietului de sarcini. Se anexeaza datasheet	
TOTAL						

Semnat:_____ Numele, Prenumele: Cioban Alexei În calitate de: Director

Ofertantul: IT-LAB GRUP SRL Adresa: mun. Chisinau; str-la Studentilor 2/4 of 217

Digitally signed by Cioban Alexei
Date: 2022.09.12 09:53:28 EEST
Reason: MoldSign Signature
Location: Moldova

Anexa tehnica

Lotul III: Licențe/Echipamente/Utilaj specializat pentru sistemele de comunicații critice ale MAI	
Specificarea tehnică deplină solicitată de către autoritatea contractantă	**Specificarea tehnică deplină propusă de către ofertant**
-Echipamentul de transport de tip radioreleu solicitat este în configurație 2+0 XPIC, cu modemuri de tip nativ Ethernet, ce poate asigura transportul unui trafic Ethernet agregat cu viteze de minim 1000 Mbps. Arhitectură de tip split-mount în sensul în care fiecare modul modem radio instalat în unitatea de interior (IDU) va fi conectată cu unitatea radio de exterior (ODU) utilizând un cablu coaxial RG8 cu diametrul de 10mm sau alte soluții de interconectare (FO, FPTP, alimentare, etc.), pentru transportul datelor intermediare și pentru alimentarea unității radio. Sistemul trebuie să permită efectuarea de bucle soft local și distant la nivelul unitații radio de exterior (ODU) cu posibilitatea de monitorizare, control și diagnosticare defect. Sistemul trebuie să permită efectuarea de bucle soft local și distant la nivelul frecvenței intermediare (IF) cu posibilitatea de monitorizare, control și diagnosticare defect. Distribuirea traficului de date pe cele două polarizări V și H se va face la nivel fizic (L1 Link Aggregation), în mod egal, astfel încât încărcarea să fie simetrică. Echipamentul va fi instalat/montat și configurat de către Furnizor și transmis Beneficiarului cu toată documentația aferentă. Garanția și suportul tehnic vor fi de minim 36 luni din momentul primirii în exploatare de către Beneficiar. În sensul respectării condițiilor de garanție, furnizorul va anexa autorizarea din partea producătorului de echipamente care ar demonstra expertiza și dreptul de a monta, configura echipamentele în cauză. **-Constructia echipamentului:** Tip "Split mount" (suport orice conditii de mediu) în banda frecvență de lucru de 7GHz și 15 GHz. Caracteristici de frecventa, modulatie şi lăţime de canal radio: • Banda de frecvențe: 7GHz, 15 GHz; • Ecart Rx/Tx conform ETSI. • Echipamentul trebuie sa suporte configurarea latimii canalului radio de 28MHz si preferential 56 MHz Pentru atingerea unui throughput agregat de 1000 Mbps trebuie ca fiecare canal sa suporte o capacitate minim de 500 Mbps. - Configurabilă software în trepte, în cuante de maxim 1dBm; Să dispună de reglarea puterii de emisie în mod automat prin utilizarea funcției ATPC (Automatic Transmit Power Control) sau echivalent;	-Echipamentul de transport de tip radioreleu este în configurație 2+0 XPIC, cu modemuri de tip nativ Ethernet, ce poate asigura transportul unui trafic Ethernet agregat cu viteze de minim 1000 Mbps. Arhitectură de tip split-mount în sensul în care fiecare modul modem radio instalat în unitatea de interior (IDU) va fi conectată cu unitatea radio de exterior (ODU) utilizând un cablu coaxial RG8 cu diametrul de 10mm, pentru transportul datelor intermediare și pentru alimentarea unității radio. Sistemul să permită efectuarea de bucle soft local și distant la nivelul unitații radio de exterior (ODU) cu posibilitatea de monitorizare, control și diagnosticare defect. Sistemul să permită efectuarea de bucle soft local și distant la nivelul frecvenței intermediare (IF) cu posibilitatea de monitorizare, control și diagnosticare defect. Distribuirea traficului de date pe cele două polarizări V și H se va face la nivel fizic (L1 Link Aggregation), în mod egal, astfel încât încărcarea să fie simetrică. Echipamentul va fi instalat/montat și configurat de către Furnizor și transmis Beneficiarului cu toată documentația aferentă. Garanția și suportul tehnic vor fi de 36 luni din momentul primirii în exploatare de către Beneficiar. **-Constructia echipamentului:** Tip "Split mount" (suport orice conditii de mediu) în banda frecvență de lucru de 7GHz și 15 GHz. Caracteristici de frecventa, modulatie şi lăţime de canal radio: • Banda de frecvențe: 7GHz, 15 GHz; • Ecart Rx/Tx conform ETSI. • Echipamentul trebuie sa suporte configurarea latimii canalului radio de 28MHz si preferential 56 MHz Pentru atingerea unui throughput agregat de 1000 Mbps trebuie ca fiecare canal sa suporte o capacitate minim de 500 Mbps. - Configurabilă software în trepte, în cuante de maxim 1dBm; Să dispună de reglarea puterii de emisie în mod automat prin utilizarea funcției ATPC (Automatic Transmit Power Control) sau echivalent; Să dispună și să permită funcționarea simultană a schemelor de modulație adaptivă și reglarea automată a puterii prin ATPC în vederea furnizării unui grad ridicat de disponibilitate a liniilor radio în cazul schimbărilor de condiții de propagare cauzate de condițiile de mediu.

Să dispună și să permită funcționarea simultană a schemelor de modulație adaptivă și reglarea automată a puterii prin ATPC în vederea furnizării unui grad ridicat de disponibilitate a liniilor radio în cazul schimbărilor de condiții de propagare cauzate de condițiile de mediu. Să permită o putere de transmisie de minim 24 dBm – 7GHz și 20 dBm – 15GHz în configurația de modulație ce permite echipamentului o functionare de 500 Mbps/polarizare când lațimea de canal este 56 MHz. - Sistemul trebuie să permită conectarea unităților radio la o singură antenă pe ambele polarizari H si V pentru fiecare link. - Conformitate cu versiunile curente ale standardelor aplicabile (ITU-T, ITU-R, ETSI, IEEE etc). Următoarele standarde vor fi luate în considerare, în special: • EN 301 489-4 • EN 301 489-1 • EN 60950-1 • IEC 60950-1 • UL 60950-1 • EN 60950-22 • UL 60950-22 **-ECHIPAMENTUL DE INTERIOR (IDU)** • Rack-abil pe lățimea de 19inch. • Monobloc sau structură modulară în limita fiecărei direcții de link (șasiu dedicat pentru fiecare direcție de link în configurarea 2+0). • Toate echipamentele furnizate obligatoriu vor asigura condiția de interschimbabilitatea a modulelor, ansamblurilor sau subansamblurilor. • Structura modulară va integra următoarele componente: 1. Alimentare echipament interior (IDU): a) IDU va fi prevăzut cu două module de alimentare independente cu funcție ”hot swap” sau echivalenta, conectate la două surse distincte întreruptibile ce asigură redundanță sursei de alimentare pentru fiecare IDU; b) Modulele sursă de alimentare vor fi alimentate cu -48 Vcc cu borna pozitivă la masă. 2. Module modem radio vor fi echipate cu 1(una) interfață IF. Numărul de module radio este dimensionat după următoarele criterii: a) Câte două module pentru direcție RF care pleacă dintr-un capăt de linie 2+0. b) În funcție de numărul de direcții RF se va calcula necesarul de sasiuri IDU, pentru fiecare direcție în parte.	Să permită o putere de transmisie de minim 24 dBm – 7GHz și 20 dBm – 15GHz în configurația de modulație ce permite echipamentului o functionare de 500 Mbps/polarizare când lațimea de canal este 56 MHz. - Sistemul trebuie să permită conectarea unităților radio la o singură antenă pe ambele polarizari H si V pentru fiecare link. - Conformitate cu versiunile curente ale standardelor aplicabile (ITU-T, ITU-R, ETSI, IEEE etc). Următoarele standarde vor fi luate în considerare, în special: • EN 301 489-4 • EN 301 489-1 • EN 60950-1 • IEC 60950-1 • UL 60950-1 • EN 60950-22 • UL 60950-22 **-ECHIPAMENTUL DE INTERIOR (IDU)** • Rack-abil pe lățimea de 19inch. • Monobloc sau structură modulară în limita fiecărei direcții de link (șasiu dedicat pentru fiecare direcție de link în configurarea 2+0). • Toate echipamentele furnizate obligatoriu vor asigura condiția de interschimbabilitatea a modulelor, ansamblurilor sau subansamblurilor. • Structura modulară va integra următoarele componente: 3. Alimentare echipament interior (IDU): c) IDU va fi prevăzut cu două module de alimentare independente cu funcție ”hot swap” sau echivalenta, conectate la două surse distincte întreruptibile ce asigură redundanță sursei de alimentare pentru fiecare IDU; d) Modulele sursă de alimentare vor fi alimentate cu -48 Vcc cu borna pozitivă la masă. 4. Module modem radio vor fi echipate cu 1(una) interfață IF. Numărul de module radio este dimensionat după următoarele criterii: f) Câte două module pentru direcție RF care pleacă dintr-un capăt de linie 2+0. g) În funcție de numărul de direcții RF se va calcula necesarul de sasiuri IDU, pentru fiecare direcție în parte. h) Modulele de modem radio vor asigura telealimentarea unităților radio exterioare (ODU) conform prevederilor tehnice a soluției ofertate și vor fi ofertate în set. i) În vederea utilizării CCDP, modemul radio va avea implementată tehnologia XPIC pentru filtrarea interferențelor dintre cele două polarizări V și H.

c) Modulele de modem radio vor asigura telealimentarea unităților radio exterioare (ODU) conform prevederilor tehnice a soluției ofertate și vor fi ofertate în set.
d) În vederea utilizării CCDP, modemul radio va avea implementată tehnologia XPIC pentru filtrarea interferențelor dintre cele două polarizări V și H.
e) XPIC va fi configurabil software.

- Configurația liniilor radio 2+0 XPIC trebuie să asigure redundanța și permită funcționarea legăturii radio la cel puțin jumătate din capacitate (500Mbps) în cazul defectării unuia dintre următoarele componente:
  - Modul modem
  - Unitate radio de exterior (ODU)
  - Link de interconectare IDU/ODU

- SPECIFICATII TEHNICE FUNCTII SWITCH SI INTERFETE ETHERNET

- Modulele sau echipamentele ce asigură funcțiile de switch Ethernet și interfețele acestora trebuie să asigure minim 4 porturi Ethernet pentru trafic date (nu include portul de management și/sau acces local), din care 2 porturi de tip FastEthernet sau GigabitEthernet, conector RJ-45, soluție constructivă tip "built-in" sau tip "SFP electric/optic",
- Arhitectură non-blocking pentru matricea de switching
- Definirea a minim 8 clase de prioritate CoS, fiecare clasă având propria sa „queue".
- Ethernet Private Line/E-LINE conform definițiilor MEF 6.
- Ethernet Private LAN/E-LAN conform definițiilor MEF 6.
- 802.1Q
- Toate porturile Ethernet trebuie să permită:
  1. Configurarea în mod acces și trunk.
  2. Încapsularea traficului cu etichete de VLAN (802.1q).
  3. Identificarea priorității pachetelor în baza câmpului PCP (802.1q), DSCP (IPv4 si IPV6), EXP (MPLS).
  4. Adresarea a 4094 VLAN-uri unice.
  5. Configurarea simultană a minim 1000 VLAN-uri.
  6. Minim 4000 intrări în tabela de adrese MAC.
  7. Link Aggregation Control Protocol (LACP 802.3ad) între 2 porturi Ethernet de pe același modul și/sau de pe module diferite.
  8. Prioritizarea pachetelor pe baza câmpului PCP (CoS), DSCP (IPv4 si IPV6) sau EXP (MPLS).

j) XPIC va fi configurabil software.

- Configurația liniilor radio 2+0 XPIC trebuie să asigure redundanța și permită funcționarea legăturii radio la cel puțin jumătate din capacitate (500Mbps) în cazul defectării unuia dintre următoarele componente:
  - Modul modem
  - Unitate radio de exterior (ODU)
  - Link de interconectare IDU/ODU

- SPECIFICATII TEHNICE FUNCTII SWITCH SI INTERFETE ETHERNET

- Modulele sau echipamentele ce asigură funcțiile de switch Ethernet și interfețele acestora trebuie să asigure minim 4 porturi Ethernet pentru trafic date (nu include portul de management și/sau acces local), din care 2 porturi de tip FastEthernet sau GigabitEthernet, conector RJ-45, soluție constructivă tip "built-in" sau tip "SFP electric/optic",
- Arhitectură non-blocking pentru matricea de switching
- Definirea a minim 8 clase de prioritate CoS, fiecare clasă având propria sa „queue".
- Ethernet Private Line/E-LINE conform definițiilor MEF 6.
- Ethernet Private LAN/E-LAN conform definițiilor MEF 6.
- 802.1Q
- Toate porturile Ethernet trebuie să permită:
  9. Configurarea în mod acces și trunk.
  10. Încapsularea traficului cu etichete de VLAN (802.1q).
  11. Identificarea priorității pachetelor în baza câmpului PCP (802.1q), DSCP (IPv4 si IPV6), EXP (MPLS).
  12. Adresarea a 4094 VLAN-uri unice.
  13. Configurarea simultană a minim 1000 VLAN-uri.
  14. Minim 4000 intrări în tabela de adrese MAC.
  15. Link Aggregation Control Protocol (LACP 802.3ad) între 2 porturi Ethernet de pe același modul și/sau de pe module diferite.
  16. Prioritizarea pachetelor pe baza câmpului PCP (CoS), DSCP (IPv4 si IPV6) sau EXP (MPLS).

-ECHIPAMENTE RADIO DE EXTERIOR

- Unitatea ODU trebuie să fie prevăzută cu un punct de măsură a nivelului de recepție printr-un conector dedicat.
- Legătura între unitatea de interior și unitatea ODU se va efectua conform coluției constructive ofertate, soluția constructive trebuie dimensionată astfel încât să asigure o bună funcționare pentru lungimi de până la 200 metri.

Sistemul trebuie să permită conectarea unităților radio de exterior (ODU) la o singură antenă printr-un cuplor simetric pe ambele polarizari H si V.

-ECHIPAMENTE RADIO DE EXTERIOR

- Unitatea ODU trebuie să fie prevăzută cu un punct de măsură a nivelului de recepție printr-un conector dedicat.
- Legătura între unitatea de interior și unitatea ODU se va efectua conform coluției constructive ofertate, soluția constructive trebuie dimensionată astfel încât să asigure o bună funcționare pentru lungimi de până la 200 metri.

Sistemul trebuie să permită conectarea unităților radio de exterior (ODU) la o singură antenă printr-un cuplor simetric pe ambele polarizari H si V.

- Posibilitatea stocarii complete a configuratiei de lucru a unui terminal radioreleu sub formă de fişier, pentru replicarea acesteia în diferite locatii

Posibilitatea stocarii şi afisarii datelor statistice în conformitate cu standardul SNMP.

- Asigurarea gratuita a upgrade-ului de firmware al tuturor unitatilor indoor / outdoor, pe perioada de garantie a echipamentelor (min 36 luni). Upgrade-ul de firmware se va putea executa de către personalul tehnic al achizitorului, prin încărcarea firmware-ului pe unităţi,utilizând exclusiv aplicaţiile de management distant şi local furnizate. Ofertantul va anunţa achizitorul asupra apariţiei tuturor release-urilor majore de firmware şi va pune la dispoziţia acestuia fişierele necesare, precum şi release notes-urile elaborate de producător.

Prin upgrade de firmware se înţelege o variantă de firmware care elimină bug-uri şi disfuncţionalităţi constatate în funcţionarea echipamentelor.

Se va asigura integrarea echipamentelor in soluția de monitorizare a sistemului de comunicații a Beneficiarului (SNMP v.1,2,3 inclusiv MIB, TRAP etc.), după caz se vor include toate licențile necesare.

- **MANAGEMENT LOCAL**

Obligatoriu, radioreleele ofertate vor putea fi administrate local, cu ajutorul unei aplicaţii de management local, accesul la interfaţa acestei aplicaţii fiind restricţionat cu username şi parola, aplicaţia de management local poate fi un software dedicat (dacă acesta este cazul, această aplicaţie se va furniza fără niciun fel de restricţii de licenţionare) sau o aplicaţie de uz general, disponibilă în cadrul sistemului de operare Windows (web, telnet, tftp etc.).

- Echipament va asigura funcţionarea în regimul de lucru 2+0 folosind solutia XPIC sau echivalentă.

Configurabil software.

Interconectat la nivel fizic între două module radio ale unui capăt de link 2+0.

Se va specifica tipul de echipament ofertat (denumirea/codul produsului cf. documentaţiei de producător), avându-se în vedere îndeplinirea tuturor cerinţelor tehnice obligatorii şi a celor pentru care ofertantul îşi asumă depăşirea valorilor minime solicitate.

- Condiţii de mediu :

-Operare:ETSI 300 019-2-4 class 4.1 sau echivalent

- Posibilitatea stocarii complete a configuratiei de lucru a unui terminal radioreleu sub formă de fişier, pentru replicarea acesteia în diferite locatii

Posibilitatea stocarii şi afisarii datelor statistice în conformitate cu standardul SNMP.

- Asigurarea gratuita a upgrade-ului de firmware al tuturor unitatilor indoor / outdoor, pe perioada de garantie a echipamentelor (min 36 luni). Upgrade-ul de firmware se va putea executa de către personalul tehnic al achizitorului, prin încărcarea firmware-ului pe unităţi,utilizând exclusiv aplicaţiile de management distant şi local furnizate. Ofertantul va anunţa achizitorul asupra apariţiei tuturor release-urilor majore de firmware şi va pune la dispoziţia acestuia fişierele necesare, precum şi release notes-urile elaborate de producător.

Prin upgrade de firmware se înţelege o variantă de firmware care elimină bug-uri şi disfuncţionalităţi constatate în funcţionarea echipamentelor.

Se va asigura integrarea echipamentelor in soluția de monitorizare a sistemului de comunicații a Beneficiarului (SNMP v.1,2,3 inclusiv MIB, TRAP etc.), după caz se vor include toate licențile necesare.

- **MANAGEMENT LOCAL**

Obligatoriu, radioreleele ofertate vor putea fi administrate local, cu ajutorul unei aplicaţii de management local, accesul la interfaţa acestei aplicaţii fiind restricţionat cu username şi parola, aplicaţia de management local poate fi un software dedicat (dacă acesta este cazul, această aplicaţie se va furniza fără niciun fel de restricţii de licenţionare) sau o aplicaţie de uz general, disponibilă în cadrul sistemului de operare Windows (web, telnet, tftp etc.).

- Echipament va asigura funcţionarea în regimul de lucru 2+0 folosind solutia XPIC sau echivalentă.

Configurabil software.

Interconectat la nivel fizic între două module radio ale unui capăt de link 2+0.

Se va specifica tipul de echipament ofertat (denumirea/codul produsului cf. documentaţiei de producător), avându-se în vedere îndeplinirea tuturor cerinţelor tehnice obligatorii şi a celor pentru care ofertantul îşi asumă depăşirea valorilor minime solicitate.

- Condiţii de mediu :

-Operare:ETSI 300 019-2-4 class 4.1 sau echivalent

-Depozitare :ETSI 300 019-1-1 class 1.2 sau echivalent

-Transport: ETSI 300 019-1-2 class 2.3 sau echivalent

- Consum maxim 160 W per terminal/directie (configuraţie 2+0 XPIC) in regim standart power.

- Conectarea (ODU) se va face prin intermediul unui cablu coaxial.

- Echipamentele vor implementa un mecanism de modulaţie adaptivă, care să permită transmiterea fără erori a traficului, în cazul înrăutăţirii condiţiilor de propagare.

- Forward Error Correction (FEC) pentru îmbunătăţirea performanţelor BER.

- **INTERFEŢE DE MANAGEMENT ŞI SUPERVIZARE**

-Depozitare :ETSI 300 019-1-1 class 1.2 sau echivalent
-Transport: ETSI 300 019-1-2 class 2.3 sau echivalent
- Consum maxim 160 W per terminal/directie (configuraţie 2+0 XPIC) in regim standart power.
- Conectarea (ODU) se va face prin intermediul unui cablu coaxial.
- Echipamentele vor implementa un mecanism de modulaţie adaptivă, care să permită transmiterea fără erori a traficului, în cazul înrăutăţirii condiţiilor de propagare.
- Forward Error Correction (FEC) pentru îmbunătăţirea performanţelor BER.
- **INTERFEŢE DE MANAGEMENT ŞI SUPERVIZARE**
- Managamentul local se va putea face pe un port dedicat (serial RS 232, sau USB, sau Ethernet 10/100 BaseT conector RJ 45) sau inband pe unul din porturile de trafic Ethernet.
- Managamentul distant se va putea face pe un port dedicat (Ethernet 10/100 BaseT conector RJ 45) sau inband pe canalul de trafic Ethernet. În acest din urmă cazul, traficul de management va fi tagat 802.1q şi se va putea prioritiza VLAN-ul de management.
Se vor detalia modurile de configurare a managementului distant.
Sistemul de OAM va fi conform cu standardele 802.1ag, G.8013/Y.1731, MEF-17, MEF-20, MEF-30, MEF-31 sau echivalent.
- Pentru legăturile în banda de 7 GHz şi 15 GHz, echipamentele ofertate şi livrate trebuie să acopere toate frecvenţele de lucru utilizate de achizitor, frecvenţa de lucru putând fi setată cu ajutorul aplicaţiei software de management local şi a celei de management distant.
Se va oferta acelasi model/varianta constructiva de echipamente pentru ambele benzi de frecventa solicitate, pentru toate legaturile radio din scopul acestui proiect.
Conexiunea echipamentului fiind facuta catre un Generic Ethernet Device ce poate fi un switch/router.
Unitatea ODU trebuie să fie prevăzută cu un punct de măsură a nivelului de recepție printr-un conector dedicat. Sistemul trebuie să permită conectarea unităților radio de exterior (ODU) la o singură antenă pe ambele polarizari H si V.
- Standarde suportate sau echivalentul acestora cu cerinte minime integrate sub:
- Frecvente radio: ETSI EN 302 217,
- Gama temperaturilor de lucru,
- cu garantarea păstrării caracteristicilor funcţionale: conform ETSI EN 300 019-2-4 Class 4.1
- Conditii continue:-$30^0 \div +40^0$C (fara radiatie solara)
- Conditii continue extinse:- 45°C la +55°C (fara radiatie solara)
- Umiditate relativa: maximum 100%
- Etanseitate : EN60529, IP cod IP65

- Managamentul local se va putea face pe un port dedicat (serial RS 232, sau USB, sau Ethernet 10/100 BaseT conector RJ 45) sau inband pe unul din porturile de trafic Ethernet.
- Managamentul distant se va putea face pe un port dedicat (Ethernet 10/100 BaseT conector RJ 45) sau inband pe canalul de trafic Ethernet. În acest din urmă cazul, traficul de management va fi tagat 802.1q şi se va putea prioritiza VLAN-ul de management.
Se vor detalia modurile de configurare a managementului distant.
Sistemul de OAM va fi conform cu standardele 802.1ag, G.8013/Y.1731, MEF-17, MEF-20, MEF-30, MEF-31 sau echivalent.
- Pentru legăturile în banda de 7 GHz şi 15 GHz, echipamentele ofertate şi livrate trebuie să acopere toate frecvenţele de lucru utilizate de achizitor, frecvenţa de lucru putând fi setată cu ajutorul aplicaţiei software de management local şi a celei de management distant.
Se va oferta acelasi model/varianta constructiva de echipamente pentru ambele benzi de frecventa solicitate, pentru toate legaturile radio din scopul acestui proiect.
Conexiunea echipamentului fiind facuta catre un Generic Ethernet Device ce poate fi un switch/router.
Unitatea ODU trebuie să fie prevăzută cu un punct de măsură a nivelului de recepție printr-un conector dedicat. Sistemul trebuie să permită conectarea unităților radio de exterior (ODU) la o singură antenă pe ambele polarizari H si V.
- Standarde suportate sau echivalentul acestora cu cerinte minime integrate sub:
- Frecvente radio: ETSI EN 302 217,
- Gama temperaturilor de lucru,
- cu garantarea păstrării caracteristicilor funcţionale: conform ETSI EN 300 019-2-4 Class 4.1
- Conditii continue:-$30^0 \div +40^0$C (fara radiatie solara)
- Conditii continue extinse:- 45°C la +55°C (fara radiatie solara)
- Umiditate relativa: maximum 100%
- Etanseitate : EN60529, IP cod IP65
- Depozitare : EN 300 019-01-01, Clasa 1.2
- Transport:EN 300 019-01-02, Clasa 2.3
- Vibratii si socuri: EN 300 019-2-4 Test 4.1 CLASA 4M5
- EMC / EMI : EN 300330, EN 303413, EN 301 489-1 si EN 301 489-4
- Putere de emisie la ieşirea ODU pentru canalizaţie de 56 MHz vor suporta minim:

Frecvența	Banda canal radio 56 MHz	Putere emisie [dB]	Prag pentru BER 10-6	Castig sistem [dB]
7 GHz	4QAM	28 - 30	-(78 - 84)	106 - 114
	16QAM	27 - 30	-(76 - 77)	103 - 107
	64QAM	26 - 30	-(69 - 70)	98 - 100
	128QAM	26 - 30	-(67 - 68)	93 - 98

- Depozitare : EN 300 019-01-01, Clasa 1.2
- Transport:EN 300 019-01-02, Clasa 2.3
- Vibratii si socuri: EN 300 019-2-4 Test 4.1 CLASA 4M5
- EMC / EMI : EN 300330, EN 303413, EN 301 489-1 si EN 301 489-4
- Putere de emisie la ieşirea ODU pentru canalizaţie de 56 MHz vor suporta minim:

Frecvența	Banda canal radio 56 MHz	Putere emisie [dB]	Prag pentru BER 10-6	Castig sistem [dB]
7 GHz	4QAM	28 - 30	-(78 - 84)	106 - 114
	16QAM	27 - 30	-(76 - 77)	103 - 107
	64QAM	26 - 30	-(69 - 70)	98 - 100
	128QAM	26 - 30	-(67 - 68)	93 - 98
	256QAM	26 - 29	-(64 - 65)	90 - 94
	512QAM	25 – 29	-(61 - 62)	86 - 91
	1024QAM	24 – 28	-(58 - 62)	82 - 90
	2048QAM	23 – 28	-(54 - 58)	76 - 86
	4096QAM	21 - 27	-(51 - 55)	72 - 82
15GHZ	4QAM	24 - 27	-(78 - 83)	102 - 110
	16QAM	24 - 26	-(75 - 77)	99 - 103
	64QAM	24 - 25	-(68 - 71)	92 - 96
	128QAM	24 - 25	-(66 - 68)	90 - 93
	256QAM	22 - 24	-(62 - 65)	84 - 89
	512QAM	22 - 24	-(60 - 62)	82 - 86
	1024QAM	20 - 23	-(57 - 59)	77 - 82
	2048QAM	20 - 23	-(53 - 57)	73 - 80
	4096QAM	18 - 22	-(50 - 53)	68 - 75

Se vor specifica valorile puterii de emisie pentru toate modulaţiile permise de echipament şi pentru toate canalizaţiile.
- Porturi de conectare ODU:
se vor specifica conform soluţiei constructive ofertate
- **ANTENE**
- Antenele ofertate vor fi din clasa „high performance” de ultimă generaţie recomandate de producător pentru construirea reţelelor de transport şi vor respecta minim următoarele specificaţii tehnice:
Minim ETSI class 3, cu posibilitatea de lucru în mediu cu interferențe radio foarte ridicate.
Dublă polarizare V&H indiferent de banda de frecvență și de dimensiunea antenei.
- Antenele vor fi prevăzute cu un sistem de reducere al radiaților secundare.

	256QAM	26 - 29	-(64 - 65)	90 - 94
	512QAM	25 – 29	-(61 - 62)	86 - 91
	1024QAM	24 – 28	-(58 - 62)	82 - 90
	2048QAM	23 – 28	-(54 - 58)	76 - 86
	4096QAM	21 - 27	-(51 - 55)	72 - 82
15GHZ	4QAM	24 - 27	-(78 - 83)	102 - 110
	16QAM	24 - 26	-(75 - 77)	99 - 103
	64QAM	24 - 25	-(68 - 71)	92 - 96
	128QAM	24 - 25	-(66 - 68)	90 - 93
	256QAM	22 - 24	-(62 - 65)	84 - 89
	512QAM	22 - 24	-(60 - 62)	82 - 86
	1024QAM	20 - 23	-(57 - 59)	77 - 82
	2048QAM	20 - 23	-(53 - 57)	73 - 80
	4096QAM	18 - 22	-(50 - 53)	68 - 75

Se vor specifica valorile puterii de emisie pentru toate modulaţiile permise de echipament şi pentru toate canalizaţiile.
- Porturi de conectare ODU:
se vor specifica conform soluţiei constructive ofertate
- **ANTENE**
- Antenele ofertate vor fi din clasa „high performance” de ultimă generaţie recomandate de producător pentru construirea reţelelor de transport şi vor respecta minim următoarele specificaţii tehnice:
Minim ETSI class 3, cu posibilitatea de lucru în mediu cu interferențe radio foarte ridicate.
Dublă polarizare V&H indiferent de banda de frecvență și de dimensiunea antenei.
- Antenele vor fi prevăzute cu un sistem de reducere al radiaților secundare.

- Antenele vor fi complet echipate pentru prindere pe suport cilindric între ø60mm și ø120mm.
Antenele mai mari de 1,2m exclusiv vor fi prevăzute cu sistem de rigidizare a poziției în plan orizontal (contravintuire).
- Conformitate Electrica ETSI 302 217 Class 2-3
- Frecventa de Operare : 7GHz and 15GHz
-Condiţii de supravieţuire a antenei :
Operationala:
-0.3m min: 110 km/h
-0.6m min: 110 km/h
-0.9m min: 110 km/h
-1.2m min: 110 km/h
Supravietuire:

- Antenele vor fi complet echipate pentru prindere pe suport cilindric între ø60mm și ø120mm. Antenele mai mari de 1,2m exclusiv vor fi prevăzute cu sistem de rigidizare a poziției în plan orizontal (contravintuire). - Conformitate Electrica ETSI 302 217 Class 2-3 - Frecventa de Operare : 7GHz and 15GHz -Condiţii de supravieţuire a antenei : Operationala: -0.3m min: 110 km/h -0.6m min: 110 km/h -0.9m min: 110 km/h -1.2m min: 110 km/h Supravietuire: -0.3m min: 200 km/h -0.6m min: 200 km/h -0.9m min: 200 km/h -1.2m min: 200 km/h conform standardului ETSI EN 300 833/ Anexa A - depuneri de gheaţă (densitatea de 7 kN/m3): 25 mm radiale. - Tip antenă: cu radom solid. - Câştigul antenei (midband): -0.3m min 32 dBi -0.6m min 31 dBi -0.9m min 35 dBi -1.2m min 37 dBi Atenuarea cross-polarizare: min. 30 dB Raport faţă/spate: ± 1 dB -0.3m min: 54 dB -0.6m min: 57 dB -0.9m min: 62 dB -1.2m min: 63 dB VSWR max. 1.4 ± 0,2 Diametru Antene : 0.3-1.8m Sistem de reglaj fin (azimut/elevaţie): min. ±15º	-0.3m min: 200 km/h -0.6m min: 200 km/h -0.9m min: 200 km/h -1.2m min: 200 km/h conform standardului ETSI EN 300 833/ Anexa A - depuneri de gheaţă (densitatea de 7 kN/m3): 25 mm radiale. - Tip antenă: cu radom solid. - Câştigul antenei (midband): -0.3m min 32 dBi -0.6m min 31 dBi -0.9m min 35 dBi -1.2m min 37 dBi Atenuarea cross-polarizare: min. 30 dB Raport faţă/spate: ± 1 dB -0.3m min: 54 dB -0.6m min: 57 dB -0.9m min: 62 dB -1.2m min: 63 dB VSWR max. 1.4 ± 0,2 Diametru Antene : 0.3-1.8m Sistem de reglaj fin (azimut/elevaţie): min. ±15º

Technical Description

FibeAir® IP-20F

April 2019 | ANSI Version

CeraOS: 10.7 | Rev A.01

Notice

Trademarks

Statement of Conditions

The information contained in this document is subject to change without notice. Ceragon Networks Ltd. shall not be liable for errors contained herein or for damage in connection with the furnishing, performance, or use of this document or equipment supplied with it.

Open Source Statement

The Product may use open source software, among them O/S software released under the GPL or GPL alike license ("Open Source License"). Inasmuch that such software is being used, it is released under the Open Source License, accordingly. The complete list of the software being used in this product including their respective license and the aforementioned public available changes is accessible at:

Network element site: ftp://ne-open-source.license-system.com

NMS site: ftp://nms-open-source.license-system.com/

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

Intended Use/Limitation

Fixed point-to-point radio links for private networks.

Authorized to Use

Only entities with individual authorization from the National Regulator to operate the mentioned radio equipment.

The equipment can be used in the following EU countries:

Austria (AT) - Belgium (BE) - Bulgaria (BG) - Switzerland/Liechtenstein (CH) - Cyprus (CY) - Czech Republic (CZ) - Germany (DE) – Denmark (DK) - Estonia (EE) - Finland (FI) - France (FR) -Greece (GR) - Hungary (HU) - Ireland (IE) – Iceland (IS) – Italy (IT) – Lithuania (LT) - Luxembourg (LU) – Latvia (LV) - Malta (MT) - Netherlands (NL) - Norway (NO) - Portugal (PT) - Romania (RO) - Sweden (SE) - Slovenia (SI) - Slovak Republic (SK) – United Kingdom (UK) – Spain (SP) – Poland (PL)

Table of Contents

List of Figures

List of Tables

About This Guide

This document describes the main features, components, and specifications of the FibeAir IP-20F. This document applies to CeraOS version 10.7.

What You Should Know

This document describes applicable ANSI standards and specifications. An ETSI version of this document is also available.

Target Audience

This manual is intended for use by Ceragon customers, potential customers, and business partners. The purpose of this manual is to provide basic information about the FibeAir IP-20F for use in system planning, and determining which FibeAir IP-20F configuration is best suited for a specific network.

1. Synonyms and Acronyms

Acronym	Equivalent Term
ACM	Adaptive Coding and Modulation
ACR	Adaptive Clock Recovery
AES	Advanced Encryption Standard
AIS	Alarm Indication Signal
ATPC	Automatic Tx Power Control
BBC	Baseband Combining
BER	Bit Error Ratio
BLSR	Bidirectional Line Switch Ring
BMCA	Best Master Clock Algorithm
BPDU	Bridge Protocol Data Units
BWA	Broadband Wireless Access
CBS	Committed Burst Size
CCDP	Co-channel dual polarization
CE	Customer Equipment
CET	Carrier-Ethernet Transport
CFM	Connectivity Fault Management
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
DA	Destination Address
DSCP	Differentiated Service Code Point
EBS	Excess Burst Size
EIR	Excess Information Rate
EPL	Ethernet Private Line
EVPL	Ethernet Virtual Private Line
EVC	Ethernet Virtual Connection
FEC	Forward Error Correction
FTP (SFTP)	File Transfer Protocol (Secured File Transfer Protocol)
GbE	Gigabit Ethernet
HSB	Hot Standby

Acronym	Equivalent Term
HSO	Hot Switchover
HTTP (HTTPS)	Hypertext Transfer Protocol (Secured HTTP)
IDC	Indoor Controller
IDU	Indoor unit
LACP	Link Aggregation Control Protocol
LANs	Local area networks
LLF	Link Loss Forwarding
LOC	Loss of Carrier
LOF	Loss of Frame
LoS	Line of Sight
LOS	Loss of Signal
LTE	Long-Term Evolution
LTE-TDD	LTE Time-Division Duplex
MAID	Maintenance Association (MA) Identifier (ID)
MEN	Metro Ethernet Network
MPLS	Multiprotocol Label Switching
MRU	Maximum Receive Unit
MSP	Multiplex Section Protection
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmit Capability
NMS	Network Management System
NTP	Network Time Protocol
OAM	Operation Administration & Maintenance (Protocols)
OFDMA	Orthogonal Frequency-Division Multiple Access
OOF	Out-of-Frame
PCM	Pulse Code Modulation
PDV	Packed Delay Variation
PIR	Peak Information Rate
PM	Performance Monitoring
PN	Provider Network (Port)
PSN	Packet Switched Network
PTP	Precision Timing-Protocol
PW	Pseudowire

Acronym	Equivalent Term
QoE	Quality of-Experience
QoS	Quality of Service
RBAC	Role-Based Access Control
RDI	Remote Defect Indication
RFU	Radio Frequency Unit
RMON	Ethernet Statistics
RSL	Received Signal Level
RSTP	Rapid Spanning Tree Protocol
SAP	Service Access Point
SD	Space Diversity
SFTP	Secure FTP
SLA	Service level agreements
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNTP	Simple Network Time Protocol
SP	Service Point
STP	Spanning Tree Protocol
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Messages
SyncE	Synchronous Ethernet
TC	Traffic Class
TDD	Time-Division Duplex
ToD	Time of Day
TOS	Type of Service
UE	User Equipment
UNI	User Network Interface
UTC	Coordinated Universal Time
VC	Virtual Containers
Web EMS	Web-Based Element Management System
WG	Wave guide
WFQ	Weighted Fair Queue
WRED	Weighted Random Early Detection
XPIC	Cross Polarization Interference Cancellation

2. Introduction

This chapter provides an overview of the IP-20F, Ceragon's high capacity, split-mount edge node. IP-20F is specially designed for edge/tail sites, and features a small footprint, high density, and a high degree of availability. IP-20F supports up to five carriers per node, in up to three directions.

IP-20F is an integral part of the FibeAir IP-20 family of high-capacity wireless backhaul products. Together, the FibeAir IP-20 family of products provides a wide variety of backhaul solutions that can be used separately or combined to form integrated backhaul networks or network segments.

This enables operators to utilize a combination of FibeAir IP-20 IDUs and radio units (RFUs) to build networks in which the most appropriate FibeAir product can be utilized for each node in the network to provide the feature support, capacity support, frequency range, density, and footprint that is optimized to meet the needs of that node.

FibeAir IP-20F enables operators to continuously increase operational efficiency and provide better quality of experience to their customers. Highlights include:

- Provides the highest radio capacity and spectral efficiency in any condition and any frequency channel size (up to 80 MHz in microwave bands and up to 500 MHz in E-band).
- Doubles wireless backhaul capacity via remote activation of another radio carrier with no site visits required – the fastest transmission network setup from planning to fulfillment.
- Reduces tower or roof-top equipment footprint by 50% in dual carrier configurations.
- Enables operators to deploy sites where needed, removing wireless backhaul constraints by doubling the reuse of microwave frequency channels, using Advanced Frequency Reuse technology embedded in the multicore technology.
- Optimizes E-Band aggregation sites, supporting TDM over E-Band and enhancing existing microwave links with E-Band.

The diverse portfolio of FibeAir RFUs enables operators to utilize a large variety of radio capabilities in a single IP-20F node or in multiple nodes, depending on the network requirements. This includes MultiCore functionality, XPIC, wide-channel support (up to 80 MHz in microwave bands and up to 500 MHz in E-band), modulations of up to 4096 QAM, and high-power and ultra-high-power options.

This chapter includes:

- Product Overview
- Solution Overview
- New Features in CeraOS 10.7

2.1 Product Overview

FibeAir IP-20F is a split-mount edge node that delivers multi-Gbps radio capacity to the transport network. It provides operators with the simplicity that comes with deploying a very compact, fixed configuration node, helping operators to meet their operational efficiency targets. The IP-20F's fixed configuration simplifies installation, spare part management and maintenance. What's more, its passive cooling design suits harsh environments, increases reliability and minimizes ambient noise.

FibeAir IP-20F can use any mix of FibeAir RFUs to provide a wide variety of radio features and functionality, tailored to the needs of the operator. FibeAir RFUs such as single-carrier RFU-S and MultiCore RFU-D support wide channels of up to 80 MHz in microwave bands and up to 500 MHz in E-band, and modulations of up to 4096 QAM. In the same IP-20F node, operators can use standard, high-power, and ultra-high-power radios, and MultiCore or single core radios.

The MultiCore RFU-D and RFU-D-HP radios enable operators to start with a single core with the option of enabling the second core remotely when network capacity requirements increase. MultiCore radios also enable IP-20F to support advanced features such as 2+0 Multi-Carrier ABC configurations, utilizing a single RFU and a single RFU interface on the IDU.

IP-20F enables operators to maximize QoE with an improved customer experience by providing TCP-friendly backhaul. The system provides support for emerging services, standards, and networking protocols (future proof). It also enables operators to reduce TCO by supporting rich, revenue-generating services, simplified management for reduced OPEX, and improved service availability and time-to-revenue. IP-20F features an advanced feature set for Carrier Ethernet Transport, including a sophisticated Ethernet services engine, cutting-edge header de-duplication techniques, frame cut-through, and more.

IP-20F provides an innovative TDM and packet backhaul services solution that is designed to meet the challenges faced by operators building next-generation wireless backhaul networks for delivery of packet-based services. Meeting these challenges requires the ability to maintain services with strict SLA by enforcing a services policy that guarantees and monitors service performance. It also requires the ability to manage the explosion of data by ensuring capacity allocation and traffic management under wireless link congestion scenarios.

IP-20F maintains high capacity at the aggregation network, with up to 4096 QAM modulation. The IP-20F aggregation solution is based upon rich backhaul services and simplified management that are supported using advanced QoS, service OAM, and carrier-grade service resiliency (G.8032, MSTP).

2.1.1 IP-20F Radio Options

An IP-20F system consists of an IP-20F indoor unit (IDU) and one or more of the following radio frequency units (RFUs).

- FibeAir RFU-D – MultiCore RFU that operates in the 6-42 GHz frequency range, supporting channel bandwidth of 20-80 MHz and modulations of BSPK to 4096 QAM.
- FibeAir RFU-D-HP – High-Power MultiCore RFU that operates in the 4-11 GHz frequency range, supporting channel bandwidth of 20-80 MHz and modulations of BSPK to 4096 QAM.
- FibeAir RFU-E –Operates in the E-band frequency range, supporting 71-76 GHz and 81-86 GHz frequencies, channel bandwidth of 62.5, 125, 250, and 500 MHz, and modulations of BSPK to 1024 QAM.
- FibeAir RFU-S – Operates in the 6-42 GHz frequency range, supporting channel bandwidth of 20-80 MHz and modulations of BSPK to 4096 QAM.

2.1.2 FibeAir IP-20F Interoperability with other Ceragon Products

FibeAir IP-20F interoperable with other FibeAir IP-20 IDUs and FibeAir RFUs as described in Table 1.

Notes:	For specific software version requirements, refer to the Release Notes for the version you are using.

Table 1: Interoperability with Other Ceragon Products

Site 1		**Site 2**		**Link Configuration**
IDU	**RFU**	**IDU**	**RFU**	
IP-20F	RFU-S	IP-20A	RFU-S	1+0
IP-20F	RFU-D	IP-20A	RFU-D	1+0, 2+0 MC-ABC
IP-20F	RFU-S	IP-20A, IP-20GX	RFU-C[1]	1+0
IP-20F	RFU-D-HP	IP-20A	RFU-D-HP	1+0, 2+0 MC-ABC
IP-20F	RFU-E	IP-20A	RFU-E	1+0
IP-20F	RFU-E	IP-20E		1+0 (up to 250 MHz)

[1] Planned for future release.

2.1.3 IP-20F Highlights

- Optimized tail/edge solution supporting seamless integration of radio (L1) and end-to-end Carrier Ethernet transport/services (L2) functionality.
- Rich packet processing feature set for support of engineered end-to-end Carrier Ethernet services with strict SLA.
- Integrated support for multi-operator and converged backhaul business models, such as wholesale services and RAN-sharing.
- Highest capacity, scalability and spectral efficiency.
- High precision, flexible packet synchronization solution combining SyncE and IEEE-1588v2.[2]
- Best-in-class integrated TDM migration solution.
- Specifically built to support resilient and adaptive multi-carrier radio links, scaling to GbE capacity.
- Future-proof with maximal investment protection.
- Supports modulations up to 4096 QAM with RFU-D, RFU-D-HP, and RFU-S.

2.1.4 Supported IP-20F Radio Configurations

Table 2 lists the radio configurations supported by FibeAir IP-20F.

Table 2: Supported IP-20F Radio Configurations

Configuration	Directions	RFUs
1+0	1	RFU-D, RFU-D-HP, RFU-E, RFU-S
3x 1+0	3	3 x RFU-S
2+0	1	RFU-D, RFU-D-HP
2x 2+0	2	2 x RFU-D/RFU-D-HP
2x 2+0 + 1+0	3	1 x RFU-S and 2 x RFU-D/RFU-D-HP
1+1 HSB[3]	1	2 x RFU-S
2+2 HSB[3]	1	2 x RFU-D/RFU-D-HP

[2] IEEE-1588v2 is planned for future release.

[3] Planned for future release.

2.2 Solution Overview

FibeAir IP-20F is part of the FibeAir IP-20 family of integrated wireless backhaul devices. The IP-20 family constitutes a single platform serving all radio transport technologies. The IP-20 platform consists of a variety of product types built around a powerful software-defined engine and operated by a common operating system (CeraOS).

The IP-20 platform provides:

- Ultra-high capacities
- Support for any radio transmission technology in any topology and any installation configuration.
- High service granularity and rich- service-centric features.

2.3 New Features in CeraOS 10.7

The following table lists the features that have been added in CeraOS version 10.7, and indicates where further information can be found on the new features in this manual and where configuration instructions can be found in the User Guide.

Table 3: New Features in CeraOS 10.7

Feature	Further Information	Configuration Instructions in the User's Guide
Multi-Carrier ABC Minimum Bandwidth Override Option	*Multi-Carrier ABC Minimum Bandwidth Override Option* on page 102	Section 3.4.2.3, *Configuring the Multi-Carrier ABC Minimum Bandwidth Override Option*
500 MHz Channels with RFU-E	*Specifications* on page 262	n/a
Web Support for Queue-Level PMs	*Egress PMs and Statistics* on page 186	Section 7.8, *Configuring and Displaying Queue-Level PMs*
Web EMS Support for Voltage PMs	*Power Interface* on page 33	Section 12.5, *Configuring Voltage Alarm Thresholds, Masking Undervoltage Alarms, and Displaying Voltage PMs*
Stricter HTTPS Cipher Hardening	*HTTPS (Hypertext Transfer Protocol Secure)* on page 253	Section 23.6, *Configuring HTTPS Cipher Hardening (CLI)*
Login Banner	n/a	Section 14.4, *Defining a Login Banner*

3. IDU Hardware Description

This chapter describes the FibeAir IP-20F indoor unit and its interfaces, including a description of the available hardware assembly options.

This chapter includes:

- Hardware Architecture
- Front Panel Description
- Ethernet Traffic Interfaces
- Ethernet Management Interfaces
- DS1 Interface
- OC-3 Interfaces
- Radio Interfaces
- Power Interface
- Synchronization Interface
- Terminal Interface
- Unit/ACT LED
- External Alarms
- Storage Memory Card
- FibeAir IP-20F Unit Redundancy

3.1 Hardware Architecture

FibeAir IP-20F is a compact unit that fits in a single rack unit, with a passive cooling system that eliminates the need for fans. An IP-20F system consists of an IP-20F indoor unit (IDU) and up to three radio frequency units (RFUs).

The IDU is connected to each RFU via CAT-5e or CAT-6/6a cables or optical fibers. Power can be provided to the RFUs via PoE over the CAT-5e or CAT-6/6a cables, or via an external DC power source when using optical fibers and in all cases for RFU-D-HP. For details, see *IDU-RFU Cable Connection* on page 328.

An IP-20F IDU contains:

- 4 x 1 GbE combo interfaces (GbE 1-4/SFP 1-4)
- 1 x 2.5/1 GbE combo interface (2.5GE6/SFP6)
- Two combo (RJ-45 or SFP) radio interfaces (RFU1 and RFU 2)
- 1 x radio or 2.5/1 GbE combo interface (RFU3/SFP5, RFU3/2.5GE5)

For TDM traffic, an IP-20F IDU includes a 16 x DS1 interface and two OC-3 interfaces that require the addition of an optional rear-mounted OC-3 module. The OC-3 interfaces can be used in a 1+1 OC-3 protection configuration.

Note: OC-3 is planned for future release.

The IDU also includes two FE management interfaces, a DB9 dry contact external alarms interface, and an RJ-45 terminal console interface for connection to a local craft terminal. Optionally, one of the FE management interfaces can be used as an RJ-45 synchronization interface.

IP-20F receives an external supply of -48V, with a dual-feed option for power redundancy.

3.2 Front Panel Description

This section describes the IP-20F's front panel. The following sections provide detailed descriptions of the IP-20F interfaces and LEDs.

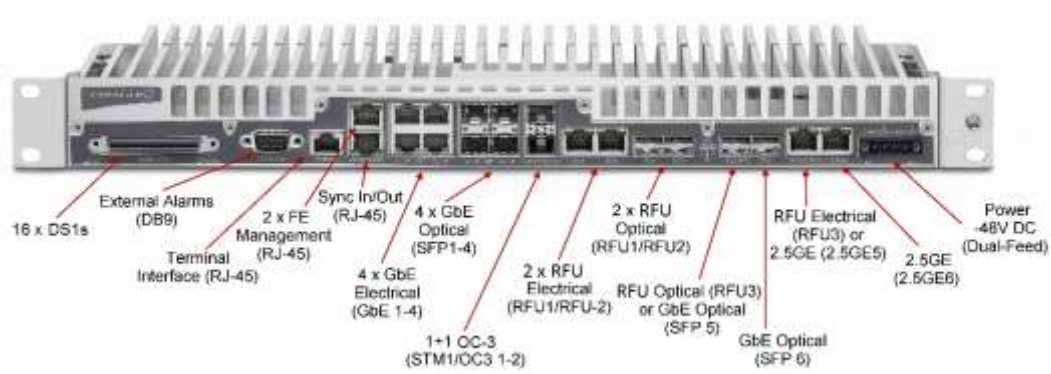


Figure 1: IP-20F Front Panel and Interfaces

Table 4: IP-20F Interfaces

Interface	For Further Information
16 x DS1s	*DS1 Interface*
External Alarms (DB9)	*External Alarms*
Terminal Interface (RJ-45)	*Terminal Interface*
2 x FE Management Interfaces (RJ-45)	*Ethernet Management Interfaces*
Sync Interface In/Out (RJ-45)	*Synchronization Interface*
4 x 1 GbE Combo Interfaces (GbE 1-4/SFP 1-4)	*Ethernet Traffic Interfaces*
1 x 2.5/1 GbE Combo Interface (2.5GE6/SFP6)	*Ethernet Traffic Interfaces*
1+1 OC-3 Interface (STM1/OC3 1-2)[4]	*OC-3 Interfaces*
2 x Electrical/Optical RFU Interfaces (RFU1/RFU2)	*Radio Interfaces*
1 x Optional RFU or 2.5/1 GbE Combo Interface (RFU3/SFP5, RFU3/2.5GE5)	*Ethernet Traffic Interfaces*
Power Interface -48V	*Power Interface*

[4] OC-3 requires the addition of an optional rear-mounted OC-3 module, which is planned for future release.

3.3 Ethernet Traffic Interfaces

Related Topics:

- Ethernet Specifications

The front panel of the FibeAir IP-20F contains 4 x GbE combo interfaces (electrical or optical) for Ethernet traffic. These interfaces are numbered as shown in Figure 2.

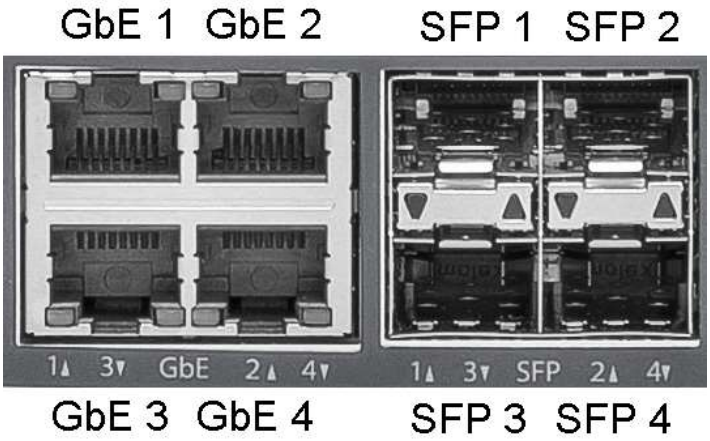


Figure 2: GbE Combo Interface Numbering

GbE 1/SFP 1 and GbE 2/SFP 2 can be configured as normal Ethernet traffic interfaces or as cascading interfaces. When operating in cascading mode, these interfaces can handle hybrid Ethernet and Native TDM traffic, enabling operators to create links among multiple IP-20 units in a node for multi-directional applications based on hybrid Ethernet and Native or pseudowire TDM services..

In addition, two pairs of electrical and optical interfaces towards the right of the front panel can be used to provide either two Ethernet interfaces or one Ethernet interface and one radio interface:

- RFU3/SFP5 and RFU3/2.5GE5 – A combo interface that can be used as either an SFP or RJ-45 RFU interface or an SFP or RJ-45 Ethernet interface.
- SFP6/2.5GE6 – A combo interface (SFP or RJ-45) for Ethernet.

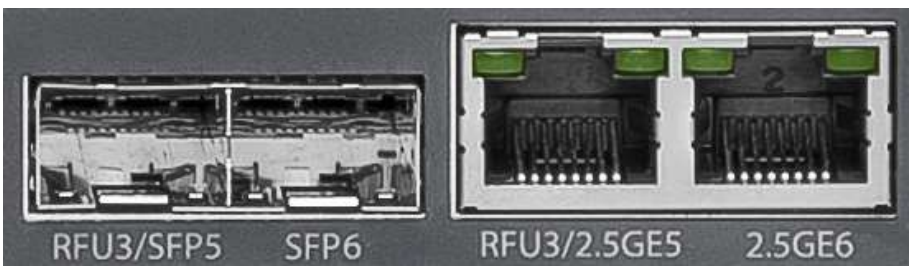


Figure 3: RFU3/SFP5-6 Interfaces

3.4 Ethernet Management Interfaces

FibeAir IP-20F contains two FE management interfaces, which connect to a single RJ-45 physical connector on the front panel. The RJ-45 connector is the upper RJ-45 interface in a pair of interfaces labeled MGMT/SYNC.

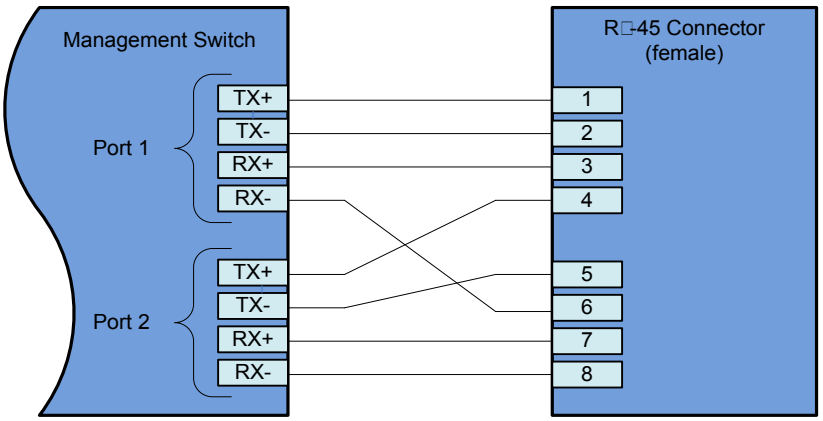


Figure 4: Management Interface Pin Connections

If the user only needs to use a single management interface, a standard Cat5 RJ-45 cable (straight or cross) can be connected to the MGMT interface.

To access both management interfaces, a special 2 x FE splitter cable can be ordered from Ceragon.

2 x FE Splitter Cable Marketing Model

Marketing Model	Marketing Description	Part Number
SPL-ETH-CBL	Ethernet split cable rohs	WA-0245-0

3.5 DS1 Interface

Related Topics:

- DS1 Interface Specifications

FibeAir IP-20F includes an MDR69 connector in which 16 DS1 interfaces are available (ports 1 through 16).

3.6 OC-3 Interfaces

Related Topics:

- OC-3 Interfaces

The IP-20F includes two ch-OC-3 ports, which can be used as a 1+1 OC-3 protection configuration. The OC-3 port provides an interface for up to 63 DS1 lines inside a standard channelized OC-3 signal. Each DS1 line is transported by a VC-12 container, which behaves like a regular line interface.

Note: OC-3 requires the addition of an optional rear-mounted OC-3 module, which is planned for future release.

For additional information:

- TDM Interface Protection

3.7 Radio Interfaces

FibeAir IP-20F includes two combo radio interfaces (electrical or optical, RFU1 and RFU2). A third interface can also be used as a combo radio interface (electrical or optical, RFU3). See *Ethernet Traffic Interfaces* on page 30.

The RFU1 and RFU2 interfaces can be used with any RFU supported by IP-20F: RFU-D, RFU-D-HP, RFU-E, and RFU-S. The MultiCore RFUs, RFU-D and RFU-D-HP, can be used in either 1+0 or 2+0 Multi-Carrier ABC configurations.

The RFU3 interface can be used with single-core RFUs, RFU-E and RFU-S.

Note: For some RFUs, PoE power can be supplied directly from the IDU via an RJ-45 radio interface. See *IDU-RFU Cable Connection* on page 328.

3.8 Power Interface

FibeAir IP-20F receives an external supply of -48V current via a dual-feed power interface, which can be connected to two separate power sources for power redundancy. The IP-20F monitors the power supply for undervoltage and overvoltage and includes reverse polarity protection, so that if the positive (+) and negative (-) inputs are mixed up, the system remains shut down.

The allowed power input range for the IP-20F is -40V to -60V. An undervoltage alarm is triggered if the power goes below a defined threshold, and an overvoltage alarm is triggered if the power goes above a defined threshold. The default thresholds are:

- Undervoltage Raise Threshold: 40V
- Undervoltage Clear Threshold: 42V
- Overvoltage Raise Threshold: 60V
- Overvoltage Clear Threshold: 58V

These thresholds are configurable.

For IP-20F units with two power inputs, overvoltage and undervoltage alarms are raised specifically for the specific power input. A power input that is not in use can be masked in order to prevent unnecessary alarms.

In addition, IP-20F provides PMs that indicate, per 15-minute and 24-hour periods:

- The number of seconds the unit was in an undervoltage state during the measured period.
- The number of seconds the unit was in an overvoltage state during the measured period.
- The lowest voltage during the measured period.
- The highest voltage during the measured period.

For devices with two power inputs, the PMs are displayed for both inputs.

3.9 Synchronization Interface

FibeAir IP-20F includes an RJ-45 synchronization interface for T3 clock input and T4 clock output. The interface is the lower RJ-45 interface in a pair of interfaces labeled MGMT/SYNC.

3.10 Terminal Interface

FibeAir IP-20F includes an RJ-45 terminal interface (RS-232). A local craft terminal can be connected to the terminal interface for local CLI management of the unit.

3.11 Unit/ACT LED

A general ACT LED for the unit is located on the lower left of the IP-20F front panel. This LED is labeled UNIT/ACT, and indicates the general status of the unit, as follows:

- **Off** – Power is off.
- **Green** – Power is on, and no alarms are present on the unit.
- **Yellow** – Power is on, and there are minor alarms or warnings on the unit.
- **Red** – Power is on, and there are major or critical alarms on the unit.

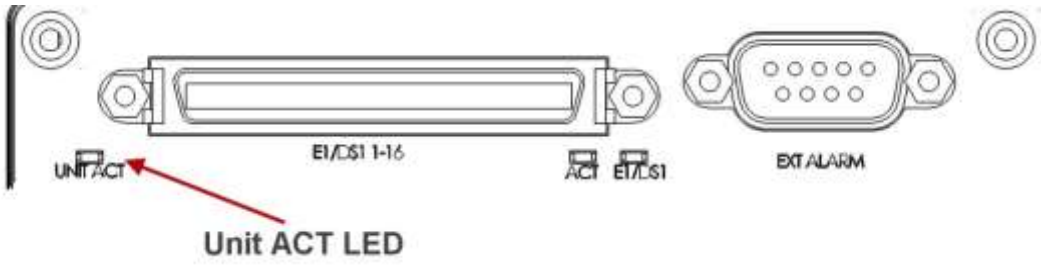


Figure 5: Unit/ACT LED

3.12 External Alarms

IP-20F includes a DB9 dry contact external alarms interface. The external alarms interface supports five input alarms and a single output alarm.

The input alarms are configurable according to:

1 Intermediate
2 Critical
3 Major
4 Minor
5 Warning

The output alarm is configured according to predefined categories.

3.13 Storage Memory Card

Each FibeAir IP-20F unit includes a Storage Memory card (SM card). The SM card holds the configuration and software for the IDU. The SM card is embedded in the SM card cover. In the event of IDU replacement, re-using the existing SM card cover is necessary to ensure that the unit's software and configuration is maintained.

An SM card is pre-installed inside each IP-20F unit. It can also be ordered as a separate item (e.g., as a spare unit).

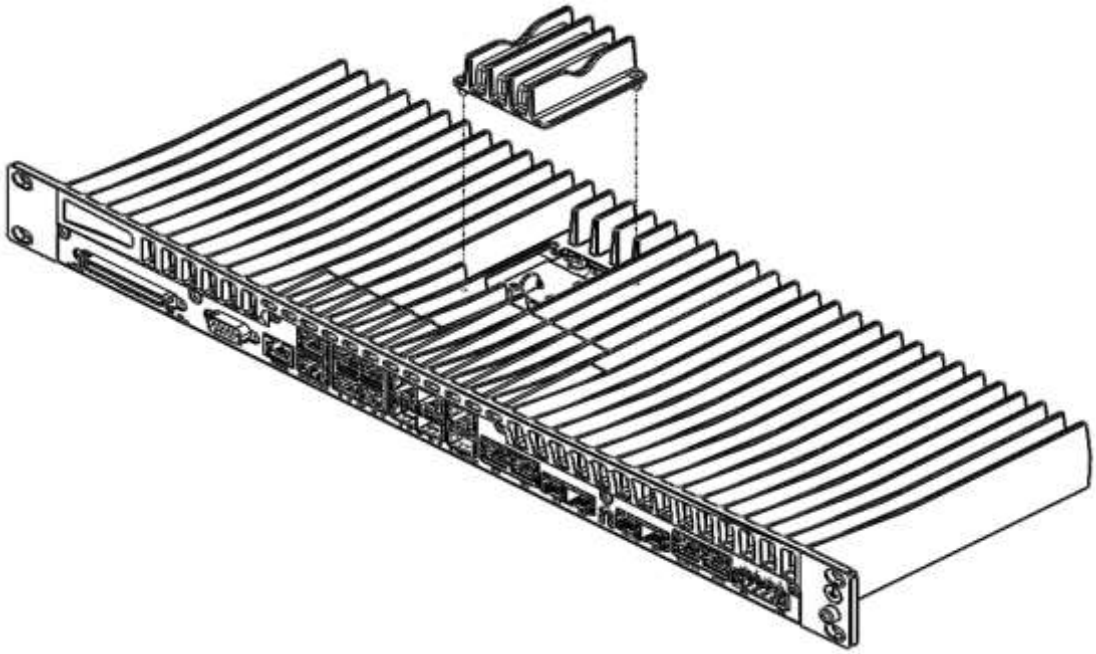


Figure 6: SM Card and Cover

3.14 FibeAir IP-20F Unit Redundancy

Notes: IP-20F unit redundancy is planned for future release.

Unit redundancy utilizes two IP-20F units, with a single antenna, to provide hardware protection for the IP-20F IDU and RFU, including protection for Ethernet, radio, and TDM interfaces. One IP-20F operates in active mode and the other operates in standby mode. If a protection switchover occurs, the roles are switched. The standby unit is managed by the active unit. The standby unit's transmitter is muted, but the standby unit's receiver is kept on in order to monitor the link. However, the received signal is terminated at the switch level.

3.14.1 Ethernet Interface Protection with IP-20F Unit Redundancy

There are three modes for Ethernet interface protection with IP-20F unit redundancy:

- Line Protection Mode – Traffic is routed to the Ethernet interfaces via two interfaces on an external switch. LACP protocol is used to determine which IP-20F port is active and which port is standby, and traffic is only forwarded to the active port. Line Protection mode can be used with optical and electrical Ethernet interfaces.

Note: The external switch must support LACP.

- Optical Splitter Mode – An optical splitter cable is used to connect both the active and the standby Ethernet ports. Optical Splitter mode can be used with optical Ethernet interfaces only.
- Electrical Splitter Mode – A Y-cable is used to connect to both the active and the standby Ethernet ports. With Electrical Splitter mode, interface protection is only supported for speeds up to 100 Mbps (Fast Ethernet). Electrical Splitter Mode can be used with electrical Ethernet interfaces only.

For Splitter Mode, the following Y-cable must be connected to the relevant interfaces on the active and standby units:

Table 5: Y-Cable for Electrical Splitter Mode FE Traffic Interface Protection

Part Number	Marketing Model	Description
WA-0244-0	15P-PROT-CBL	CABLE,RJ45F TO 2XRJ45, 1.34M,CAT-5E,

3.14.2 Supported Radio Configurations with Unit Redundancy

IP-20F unit redundancy can be used with the following radio configurations:

- 2 x 1+0 – IP-20F unit with a 1+0 configuration protecting another IP-20F unit with a 1+0 configuration.
- 2 x 2+0 – IP-20F unit with a 2+0 configuration protecting another IP-20F unit with a 2+0 configuration.

A 2 x 1+0 IP-20F configuration is interoperable with FibeAir IP-20A using a 1+1 HSB configuration. However, a 2 x 2+0 IP-20F configuration is not interoperable with FibeAir IP-20A using a 2+2 HSB configuration.

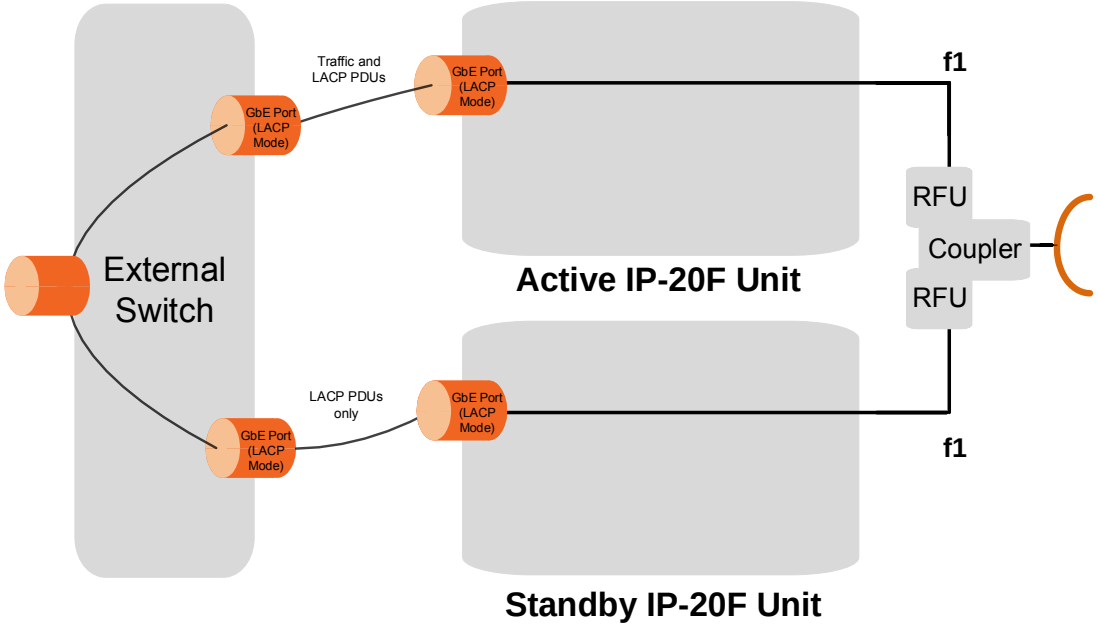


Figure 7: Unit Redundancy – 2 x 1+0 – Ethernet Line Protection Mode

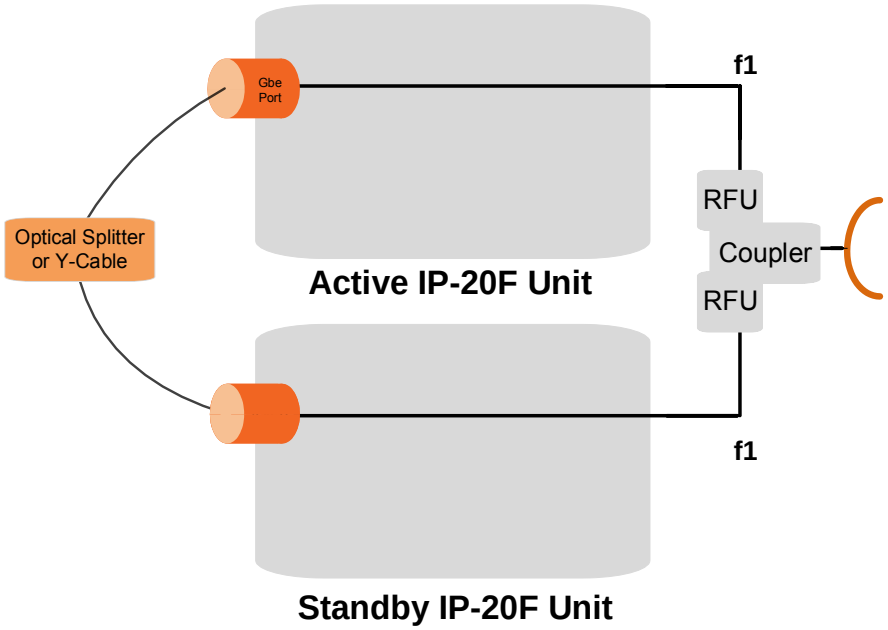


Figure 8: Unit Redundancy – 2 x 1+0 – Splitter Mode

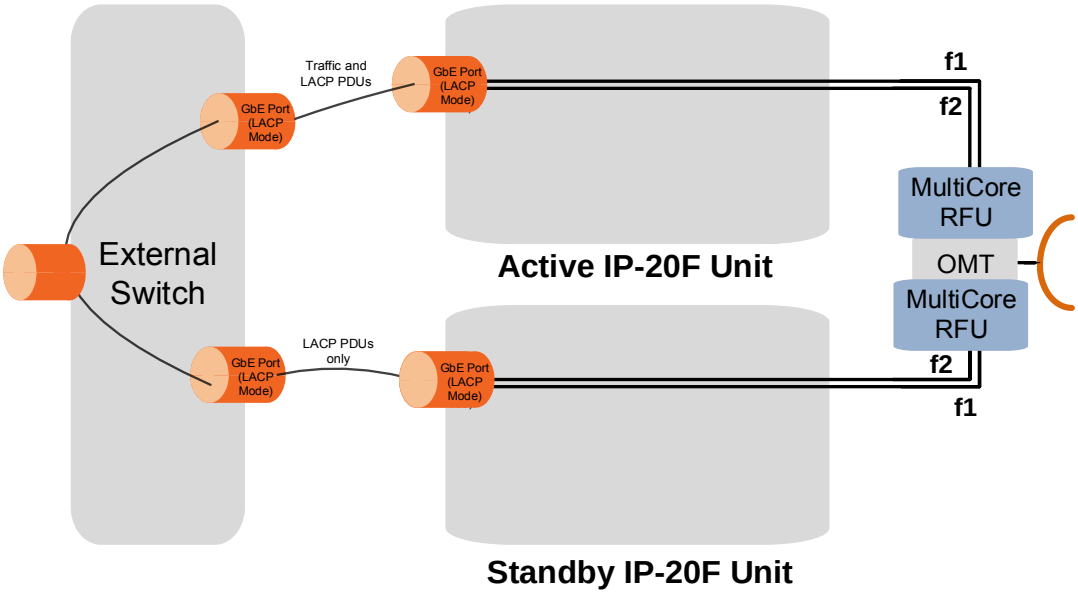


Figure 9: Unit Redundancy – 2 x 2+0 – Ethernet Line Protection Mode

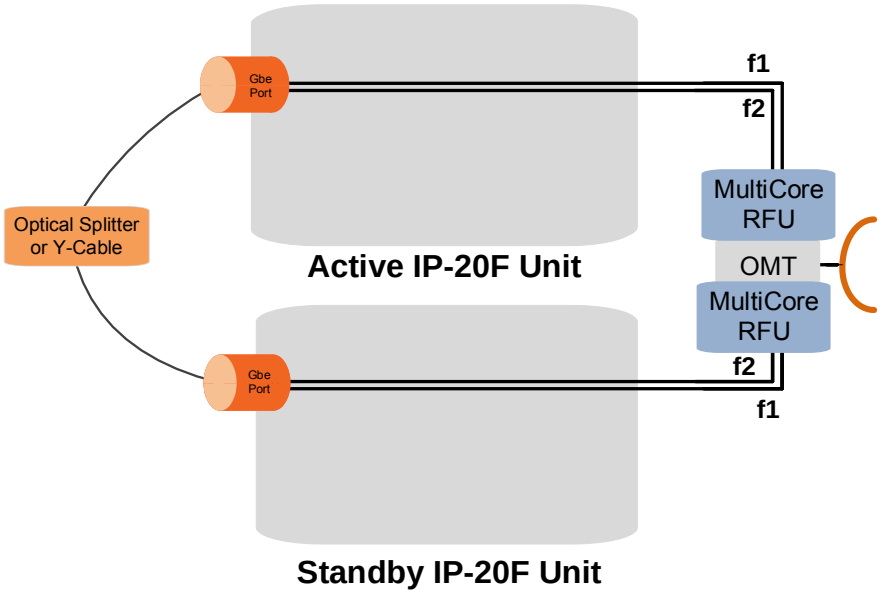


Figure 10: Unit Redundancy – 2 x 2+0 – Splitter Mode

3.14.3 DS1 Interface Protection with IP-20F Unit Redundancy

DS1 traffic is supported with IP-20F unit redundancy. A Y-cable is used to connect the active and standby DS1 ports. The following table shows the Part Number and Marketing Model of the Y-cable required for DS1 protection.

Table 6: Y-Cable for DS1 Protection

Part Number	Marketing Model	Description
wa-0398-0	IP10-CBL-16T1-PROT-Y	CABLE,2xSCSI68 LEFT ANGL SCSI68,0.6M,100 OHM,ADAP

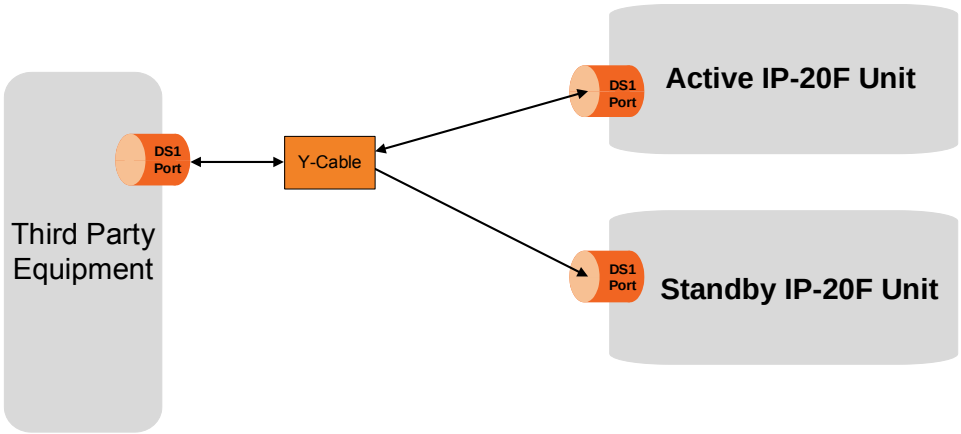


Figure 11: DS1 Interface Protection with IP-20F Unit Redundancy

3.14.4 T3 Synchronization with Unit Redundancy

T3 synchronization input is supported with IP-20F unit redundancy. A Y cable is used to connect to the active and standby Sync interfaces.

3.14.5 Management for Unit Redundancy

IP-20F units in a redundancy configuration must have their CPUs interconnected in order to synchronize their protection status. The same IP address is used for both IP-20F units, to ensure that management is not lost in the event of switchover. A special cable is required to enable this connectivity.

Table 7: Splitter Cable for Protection and Management

Part Number	Marketing Model	Description
WA-0720-0	CBL-IP20-EXT-PROT+MGMT	CABLE,RJ45F TO 2XRJ45,1.34M,CAT-5E,WITH MALE TO MALE CONNECTION

The protection and management splitter cable must be connected to the management interfaces of the two IP-20F units using the RJ-45 plug-ends. The third end of the protection splitter cable (RJ-45 socket) is connected to an external management station.

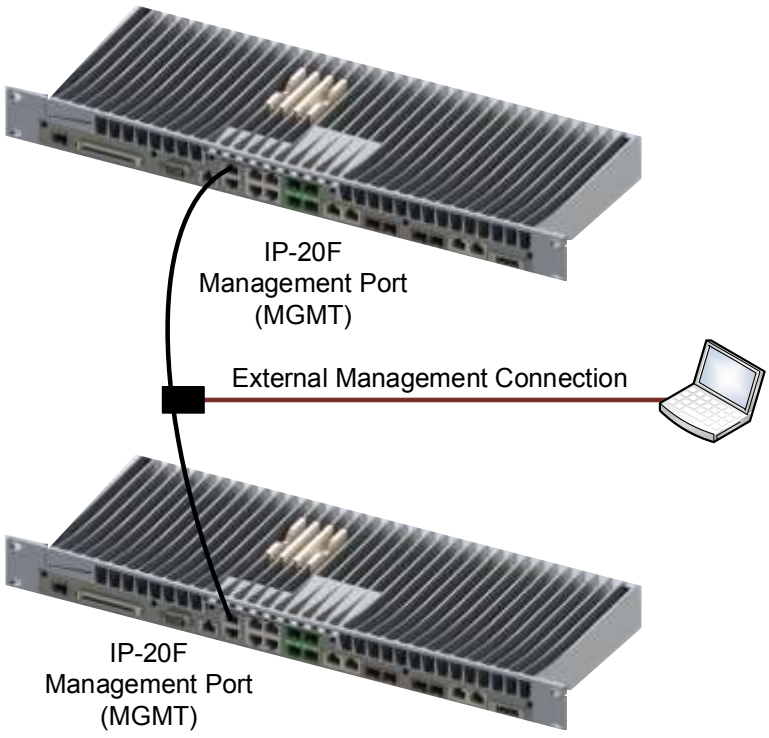


Figure 12: IP-20F with Unit Redundancy – Protection and Management Splitter Connection

The local management connection uses IP-20F management interface 1. The LED on the upper left of the MGMT port is Green when the interface is enabled and the link is operational.

The inter-unit protection connection uses IP-20F management interface 2. The LED on the upper right of the MGMT port is Green when the interface is enabled and the link between the IDUs is operational.

The active and standby units must have the same configuration. The configuration of the active unit can be manually copied to the standby unit. Upon copying, both units are automatically reset. Therefore, it is important to ensure that the units are fully and properly configured when the system is initially brought into service.

3.14.6 Switchover

In the event of switchover, the standby unit becomes the active unit and the active unit becomes the standby unit. Switchover takes less than 50 msec.

The following events trigger switchover according to their priority, with the highest priority triggers listed first:

1 Loss of active unit
2 Force switch
3 Lockout
4 Radio Loss of Frame (LOF) on active unit
5 Change request from the remote unit. This takes place in the event of radio LOF on both units; a change request is sent to the active unit on the other side of the link.
6 Loss of Carrier (LOC) in any of the Ethernet interfaces or Loss of Signal (LOS) in any of the TDM interfaces
7 Manual switch

LOC takes place if the Admin status of the interface is Enabled and the Operational status is Down. If the interface is closed as a result of ASP, the interface is *not* considered to be in LOC state, and switchover is not triggered.

Following switchover triggered by LOC, there is an automatic timeout of one minute before any further switchover can take place due to LOC.

4. RFU Hardware Description and Branching Options

The radio carrier functionality for an IP-20F node is provided by Radio Frequency Units (RFUs). An IP-20F can support up to three RFUs.

IP-20F works with the following RFUs:

Standard Power

- FibeAir RFU-D
- FibeAir RFU-E
- FibeAir RFU-S

High Power

- FibeAir RFU-D-HP

This chapter includes:

- RFU Overview
- RFU Selection Guide
- RFU-D
- RFU-D-HP
- RFU-E
- RFU-S

4.1 RFU Overview

FibeAir Radio Frequency Units (RFUs) were designed with sturdiness, power, simplicity, and compatibility in mind. These advanced systems provide high-power transmission for short and long distances and can be assembled and installed quickly and easily. Any of the RFUs described in this chapter can be used with an IP-20F.

The FibeAir RFU portfolio includes RFUs that operate in the microwave bands (4-42 GHz) and the E-Band (71-86 GHz). In microwave bands, FibeAir RFUs deliver high capacity over 20-80 MHz channels with configurable modulation schemes and a range of modulations from BPSK to 4096 QAM. In E-Band, FibeAir RFU-E delivers high capacity over channels of 62.5, 125, 250, and 500 MHz with configurable modulation schemes and a range of modulations from BPSK to 1024 QAM.

The RFUs support low to high capacities for traditional voice, mission critical, and emerging Ethernet services, with any mix of interfaces, pure Ethernet, pure TDM, or hybrid Ethernet and TDM interfaces (Native^2).

RFUs support advanced features, such as XPIC, to help operators achieve high spectral efficiency and capacity with the lowest possible OPEX. The RFU-D-HP enables operators to double capacity without increasing the equipment's physical footprint.

The following RFUs can be used with IP-20F:

- FibeAir RFU-D (6 – 42 GHz)
- FibeAir RFU-D-HP (4 – 11 GHz)
- FibeAir RFU-E (71-86 and 81-86 GHz)
- FibeAir RFU-S (6 – 42 GHz)

All of these RFUs can be installed in split-mount configurations. In addition, RFU-D-HP can be installed in all-indoor configurations.

For information about the IDU-RFU connection, see *IDU-RFU Cable Connection* on page 328.

4.2 RFU Selection Guide

The following table can be used to help you select the RFU that is appropriate to your location.

Table 8: RFU Selection Guide

Character		RFU-D	RFU-D-HP	RFU-E	RFU-S
Installation Type	**Direct Mount**	√	√[5]	√	√
	Remote Mount	√	√	√	√
	All-Indoor	–	√	–	–
Configuration	**1+0**	√	√	√	√
	2+0	√	√	–	–
	1+1	√[6]	√[6]	–	√[6]
	2+2	√[6]	√[6]	–	–
	N+0 (N>2)	√	√	–	–
	SD support	√ (BBC)[6]	√ (BBC)[6]	–	–
Available Filter Types	**Diplexers**	√	√	√	√
	Channel Filters	–	√	–	–
Lowest Modulation		BPSK	BPSK	BPSK	BPSK
Highest Modulation		4096 QAM	4096 QAM	1024 QAM	4096 QAM
Frequency Range (GHz)		6 – 42	4 – 11	71 – 76, 81 – 86	6 – 42
Carriers per RFU		2	2	1	1

5 Direct Mount is supported for 6 to 11 GHz only.

6 Planned for future release.

4.3 RFU-D

The FibeAir RFU-D brings MultiCore features and capabilities to split-mount configurations. RFU-D incorporates two modems, which are connected to the IDU via a single SFP or RJ-45 interface to the IDU. This enables an IP-20F to support six carriers by interfacing with three MultiCore RFU-D RFUs, each with two carriers. For further information on the advantages of RFU-D's multicore architecture, see *Unique MultiCore Architecture of RFU-D and RFU-D-HP* on page 89.

RFU-D's MultiCore design enables it to support MultiCore capacity-boosting features such as XPIC. Operators using RFU-D RFUs can incorporate these features in IP-20F aggregation site nodes to increase spectral efficiency and capacity, while minimizing the site's footprint.

RFU-D operates in the frequency range of 6-42 GHz. RFU-D supports low to high capacities for traditional voice and Ethernet services, as well as PDH/ or hybrid Ethernet and TDM interfaces.

With RFU-D, traffic capacity throughput and spectral efficiency are optimized with the desired channel bandwidth. For maximum user choice flexibility, channel bandwidths from 20-80 MHz can be selected together with a range of modulations. RFU-D provides a range of modulations from BPSK to 4096 QAM.

Using Ceragon's Easy Set technology, a RFU-D consists of a generic radio unit and a diplexer unit. For 6 to 15 GHz, the diplexer unit is field-replaceable, which means it can be replaced without replacing the radio unit. The generic radio unit covers an entire frequency band. It is the diplexer unit, which is passive, that determines the sub-band coverage for the entire integrated RFU-D unit. This provides operators with major benefits in terms of both deployment time and maintenance.

For maintenance, the operator can reduce the number of spare radio units in its inventory because a single generic radio unit can be used for any sub-band. This means that for a site covering four channel ranges within a single frequency band, a single spare radio unit can be kept on hand, because that unit can be used as a spare for any of the RFU-D units in the site. The diplexer units, because they are passive, are much less likely to require replacement, so the maintenance of spare parts for the diplexer units is much less of a concern for the operator.

The use of separate generic radio units and diplexer units also enables operators to achieve a quicker system deployment time. In the planning stage, when the frequency bands have been determined but the exact sub-band layout is still under consideration, operators can already order all the radio units required for the frequency bands that have been determined, and can begin ordering diplexer units for the approximate sub-bands that are anticipated, while still determining the exact network parameters. This enables faster delivery and deployment of the network.

For 18 to 42 GHz, the diplexer unit is preassembled with the RFU-D and cannot be replaced in the field.

4.3.1 Main Features of RFU-D

- **Frequency range** – Operates in the frequency range 6 – 42 GHz

- **More power in a smaller package -** Up to 29 dBm for extended distance, enhanced availability, use of smaller antennas
- **Configurable Modulation –** BPSK – 4096 QAM
- **Configurable Channel Bandwidth** – 20 MHz – 80 MHz
- **Compact, lightweight form factor -** Reduces installation and warehousing costs
- **Supported configurations**
  - MultiCore 2+0 Single/Dual Polarization
  - 2 x MultiCore 2+0 SP/DP
  - MultiCore 2+2 SP/DP HSB[7]
- **BBC Space Diversity**[7]
- **Efficient and easy installation -** Direct mount installation with different antenna types

For additional information:

- Specifications

4.3.2 RFU-D Functional Block Diagram

The RFU is responsible for RF signal processing, and includes an RF transmitter and an RF receiver with all their related functions.

RFU-D is designed to provide a high-capacity RF module, with a variety of low-loss mediation devices to accommodate different RF configurations.

The following block diagram illustrates the functional modules of an RFU-D in a 2+0 configuration.

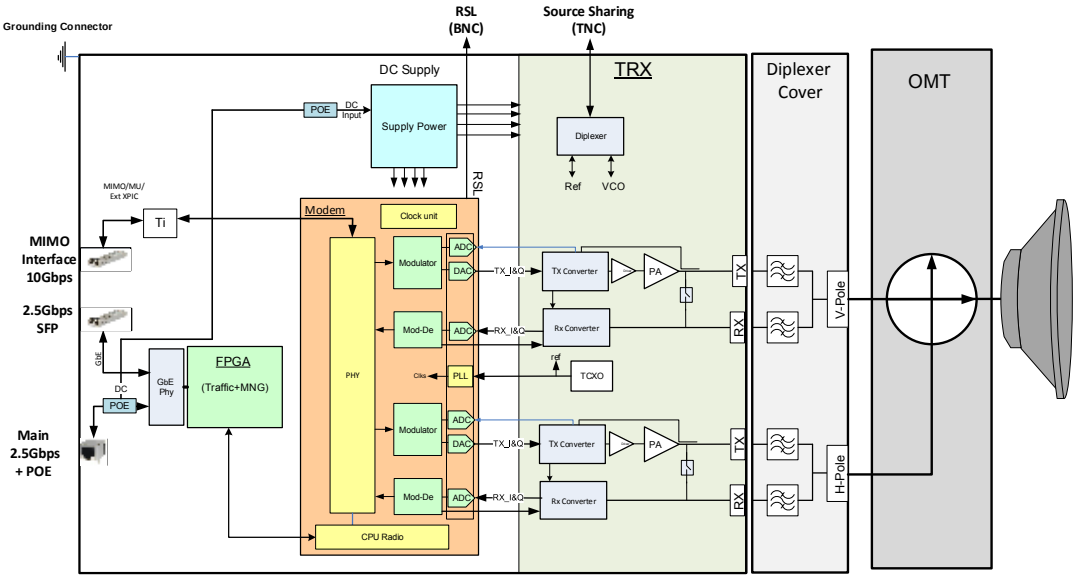


Figure 13: RFU-D Functional Block Diagram – 2+0 Configuration

4.3.3 RFU-D Radio Interfaces

The following figures show the RFU-D TX and RX interfaces.

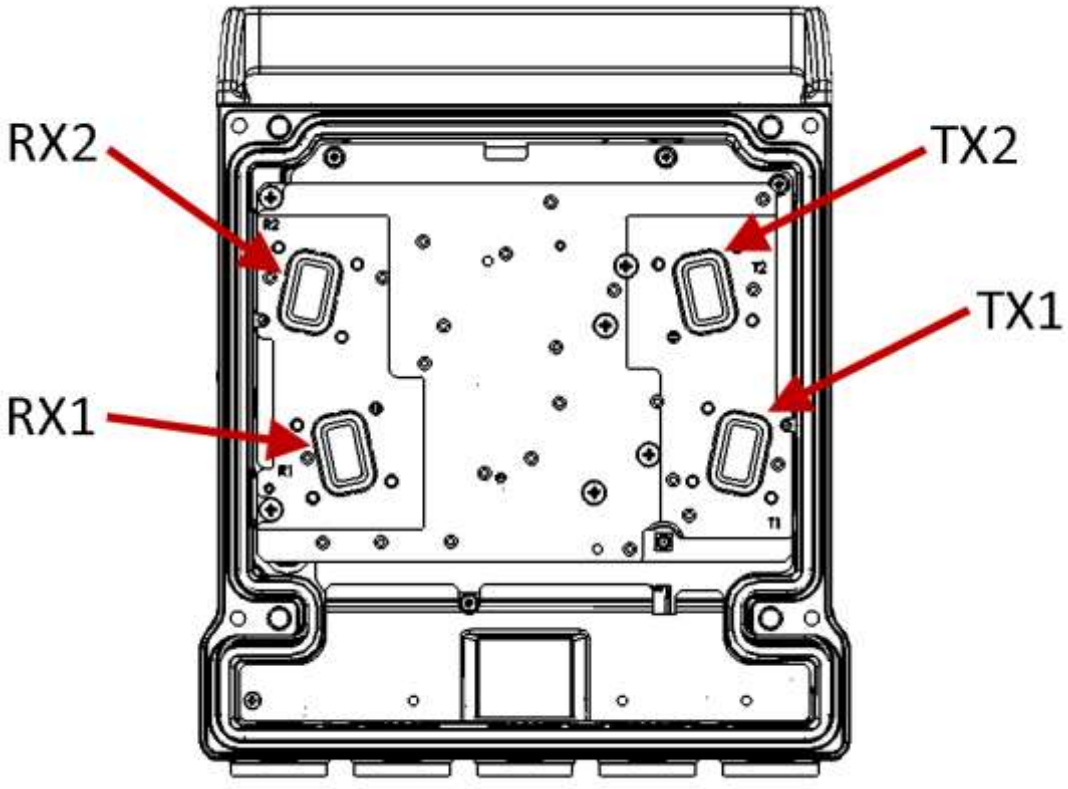


Figure 14: RFU-D Radio Interfaces (6 to 15 GHz)

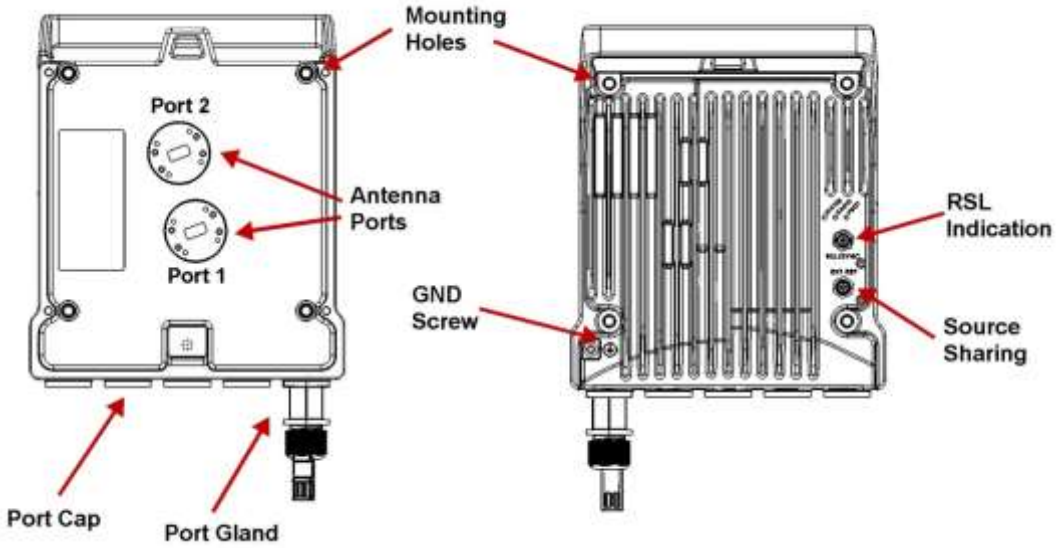


Figure 15: RFU-D Rear View (Left) and Front View (Right)

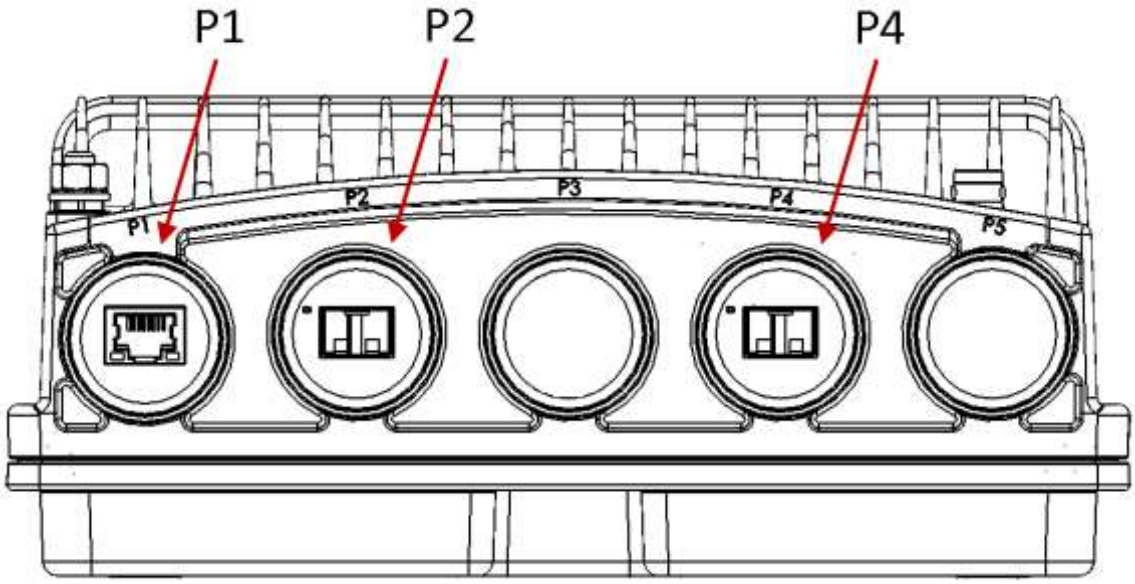


Figure 16: RFU-D Interfaces (All Frequency Bands)

Table 9: RFU-D Interfaces

Interface	Description
P1	PoE / RFU Interface (RJ-45)
P2	RFU Interface (SFP)
P4	Reserved for future use.

4.3.4 RFU-D Marketing Models

For frequencies of 6 to 15 GHz, RFU-D uses the Easy Set technology in which the radio and the diplexer unit are delivered as separate units.

For frequencies of 18 to 42 GHz, the RFU-D unit is delivered as one unit, consisting of both the radio and the diplexers.

This section explains how to read RFU-D marketing models, including marketing models for the diplexer unit for 6-15 GHz links. Constructing a marketing model for the purpose of ordering equipment should always be done using a configurator.

Note:	Not all marketing model fields are always necessary to define a valid marketing model. If a specific field is not applicable, it should be omitted.

4.3.4.1 Marketing Models for Easy Set RFU-D Radio and Diplexer Units, 6 to 15 GHz

For frequencies of 6 to 15 GHz, the RFU-D radio unit and diplexer unit are ordered separately. Using Easy Set technology, the diplexer unit is assembled on the RFU-D radio unit during link installation in the field. The radio unit is generic; only the diplexer unit (DXU) is sub-band specific, which facilities link planning, ordering, and maintenance as described above.

Table 10 provides the marketing model structure for the RFU-D Easy Set radio unit.

Table 11 provides the marketing model structure for the RFU-D Easy Set diplexer unit.

Table 10: RFU-D Marketing Model Structure, 6 to 15 GHz (Radio Unit)

Marketing Model	Description
RFU-D-*ff*	RFU-D, Dual Core, High capacity, Split Mount Radio only, *ff* GHz

Table 11: RFU-D Marketing Model Structure, 6 to 15 GHz (Diplexer Unit)

Marketing Model	Description
DXDff-xxxY-ccWdd-eeWgg-t	RFU-D Diplexers Unit, *ff* GHz, Block *xxxY*, *ccWdd-eeWgg,* High/Low

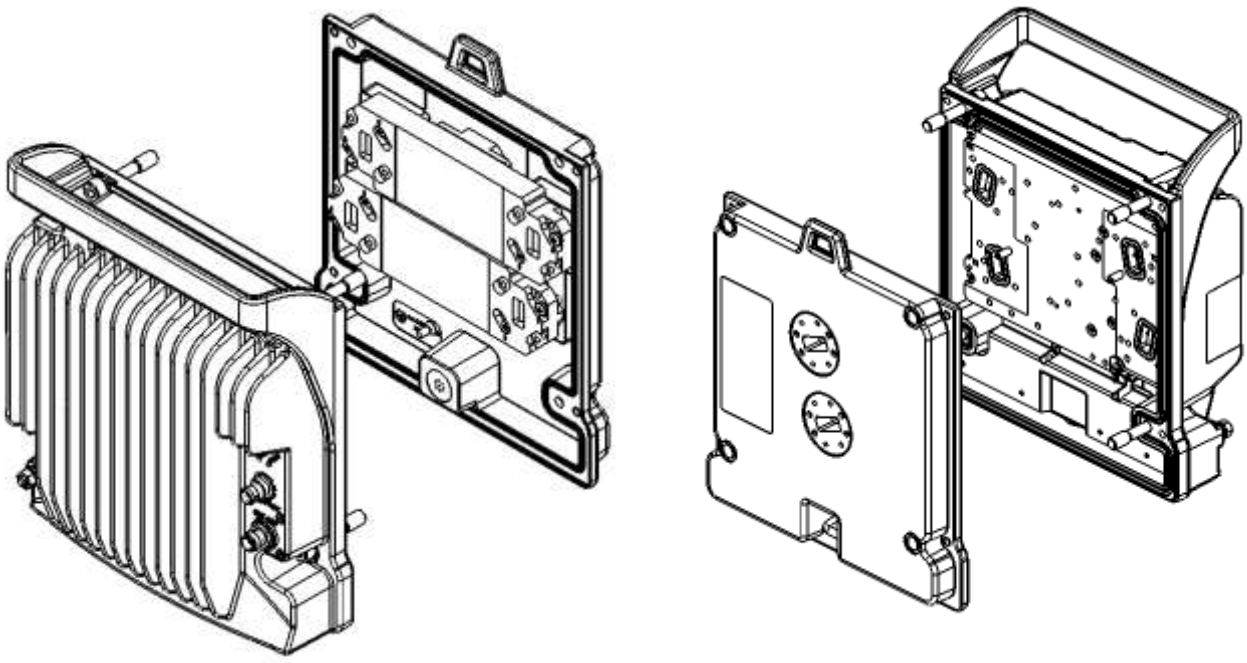


Figure 17: Radio Unit and Diplexer Unit

Table 12: RFU-D Marketing Model Structure– Possible Values (Easy Set - Radio Unit Only)

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	06,07,08,10,11,13,15

Table 13: RFU-D Marketing Model Structure– Possible Values (Easy Set - Diplexer Unit Only)

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	L6,U6,07,08,10,11,13,15
xxxY	TX-RX separation and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
ccWdd, eeWgg	Channel indication or LOW/HIGH or blank	{Start ch}W{End ch} Example: 10W15 (eeWgg is optional when using two different diplexers

Placeholder in Marketing Model	Description	Possible Values
		Example: 1W5, 10W15)
t	TX low / TX high indication	L – TX Low H – TX high

Table 14 provides examples of specific RFU-D diplexer unit marketing models based on the syntax described above.

Table 14: RFU-D Diplexer Unit Marketing Model Examples

Marketing Model Example	Explanation
DXD08-119A-01W03-L	RFU-D Diplexers Unit, 8GHz, TRS=119MHz, two identical Diplexers Uniting channels 1 to 3, TX low
DXDL6-252A-05W06-01W02-H	RFU-D Diplexers Unit, L6GHz, 252MHz TRS, different Diplexers Uniting channels 5 to 6 and 1 to 2, TX high

4.3.4.2 Marketing Model for RFU-D Unit, 18-42 GHz

When ordering an RFU-D, a single unit is ordered according to the following marketing model syntax: *RFU-D-ff-xxxY-ccWdd-eeWgg-t*.

Table 15: RFU-D Marketing Model Structure,18 to 42 GHz

Marketing Model	Description
RFU-D-*ff-xxxY-ccWdd-eeWgg-t*	RFU-D, Dual Core, High Capacity, Split Mount Radio, *ff* GHz, Block *xxxY*, *ccWdd-eeWgg,* High/Low

Table 16: RFU-D Marketing Model Structure– Possible Values

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	18, 23, 24, 26, 28, 32, 36, 38, 42
xxxY	TX-RX separation and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
ccWdd, eeWgg	Channel indication or LOW/HIGH or blank	{Start ch}W{End ch} Example: 10W15 (eeWgg is optional when using two different diplexers Example: 1W5, 10W15)
t	TX low / TX high indication	L – TX Low H – TX high

The following are some examples of specific RFU-D 18 to 42 GHz marketing models based on the syntax specified above.

Table 17: RFU-D Marketing Model Examples (18-42 GHz)

Marketing Model Example	Explanation
RFU-D-08-119A-01W03-L	RFU-D Diplexers Unit, 8GHz, TRS=119MHz, two identical Diplexers Uniting channels 1 to 3, TX low
RFU-D-L6-252A-05W06-01W02-H	RFU-D Diplexers Unit, L6GHz, 252MHz TRS, different Diplexers Uniting channels 5 to 6 and 1 to 2, TX high

4.3.5 RFU-D MultiCore Mediation Devices (MCMD)

The Dual Core Mediation Devices (MCMD) are designed to offer a simple and compact solution for a direct mount installation of the RFU-D on a standard Ceragon antenna interface.

RFU-D is equipped with two antenna ports, which mandates the use of unique mediation devices to facilitate direct mount configurations. The following two examples show dual core mediation devices that enable the connection of a single RFU-D to an antenna. For the full set of mediation devices, refer to the RFU-D Installation Guide.

Table 18: RFU-D Mediation Devices

MCMD type	Functionality
Splitter	Combines the two cores using the same polarization
OMT	Combines the two cores on alternate polarizations (H,V)

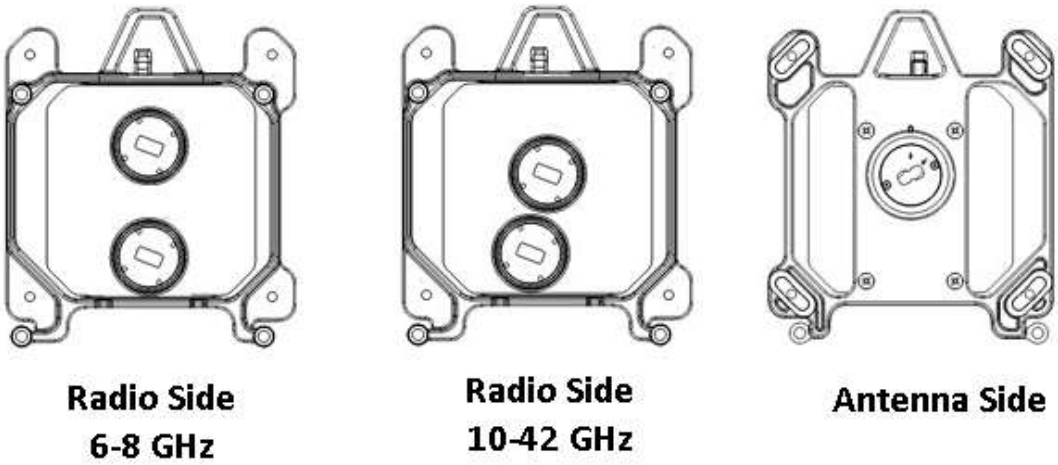


Figure 18: *Splitter*

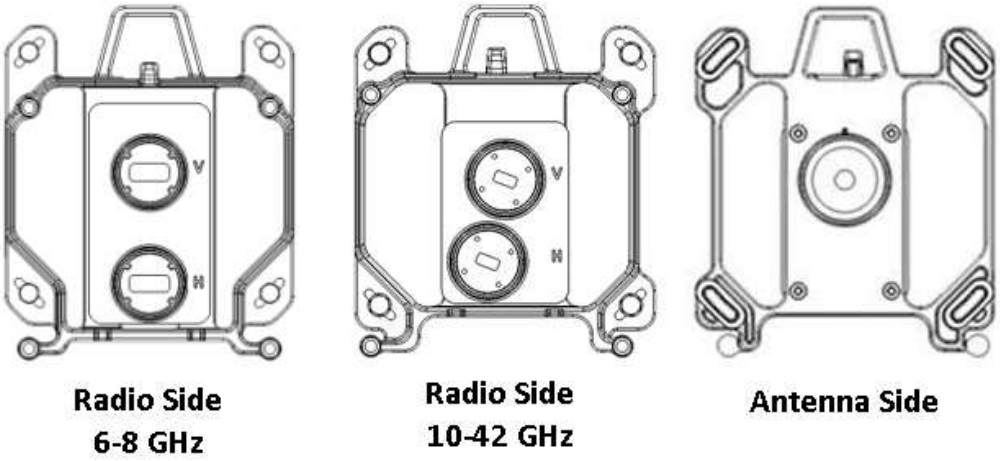


Figure 19: *OMT*

4.4 RFU-D-HP

FibeAir RFU-D-HP is a MultiCore RFU that provides high power for long-haul applications. Like RFU-D, RFU-D-HP incorporates two modems, which are connected to the IDU via a single SFP or RJ-45 interface. For further information on the advantages of RFU-D-HP's Multicore architecture, see *Unique MultiCore Architecture of RFU-D and RFU-D-HP* on page 89.

RFU-D-HP enables operators to benefit from high transmit power of up to 38 dBm, while also benefitting from MultiCore capacity-boosting features such as XPIC. Operators using RFU-D-HP RFUs can incorporate these features in IP-20F aggregation site nodes to increase spectral efficiency and capacity, while minimizing the site's footprint.

RFU-D-HP's usage mode is scalable, enabling operators to limit initial costs by purchasing the basic single core mode, then expanding to MultiCore mode with no additional hardware or installation required when network expansion requires additional capacity. RFU-D-HP can also be used in dual-receiver mode to enable BBC Space Diversity, also with no additional hardware or installation required.

RFU-D-HP offers a flexible and modular branching system that enables the combination of different bands for different carriers. For example, the same link can be used for both L6 and U6 or 7 and 8 GHz channels.

RFU-D-HP can be used with wide diplexer-based branching, enabling direct mount installation. Diplexers can be used for direct mount configurations of up to 4+0.

RFU-D-HP can also be used with channel filter-based branching, enabling configurations of up to 8+0 per polarization in remote mount configurations.

To maximize operational flexibility, both diplexers and channel filters are provided separately for the radio units, enabling the diplexers or filters to be changed in the field with minimal downtime and no risk of impairing the RFU's sealing.

RFU-D-HP operates in the frequency range of 4-11 GHz. RFU-D-HP supports low to high capacities for traditional voice and Ethernet services, as well as PDH/ or hybrid Ethernet and TDM interfaces.

With RFU-D-HP, traffic capacity throughput and spectral efficiency are optimized with the desired channel bandwidth. For maximum user choice flexibility, channel bandwidths from 20-80 MHz can be selected together with a range of modulations. RFU-D-HP provides a range of modulations from BPSK to 4096 QAM.

4.4.1 Main Features of RFU-D-HP

- **Frequency range** – Operates in the frequency range 4 – 11 GHz
- **High transmit power** – Up to 38 dBm, ideal for long-haul/high-power applications
- **Configurable Modulation –** BPSK – 4096 QAM
- **Configurable Channel Bandwidth** – 20 MHz – 80 MHz
- **Compact, form factor -** Reduces installation and warehousing costs
- **Supported configurations**
  - Single Carrier 1+0

- Single Carrier 1+0 with Space Diversity (BBC)
- MultiCore 2+0 Single/Dual Polarization
- 2 x MultiCore 2+0 SP/DP
- MultiCore 2+2 SP/DP HSB[8]

- **BBC Space Diversity**[8]
- **Efficient and easy installation -** Direct mount installation with different antenna types

4.4.2 RFU-D-HP Functional Block Diagram

The RFU is responsible for RF signal processing, and includes an RF transmitter and an RF receiver with all their related functions.

RFU-D-HP is designed to provide a high-power RF module, and the ability to concatenate several carriers with minimal RF branching loss.

The following block diagram illustrates the functional modules of an RFU-D-HP in a 2+0 configuration.

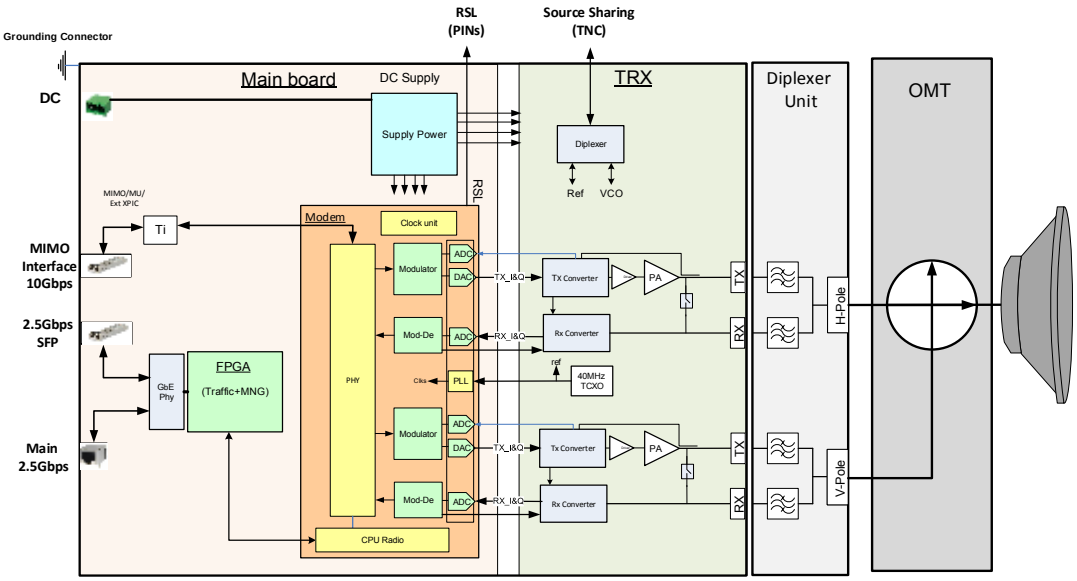


Figure 20: RFU-D-HP Functional Block Diagram – 2+0 Configuration

4.4.3 RFU-D-HP Radio Interfaces

The following figures show the RFU-D-HP TX and RX interfaces.

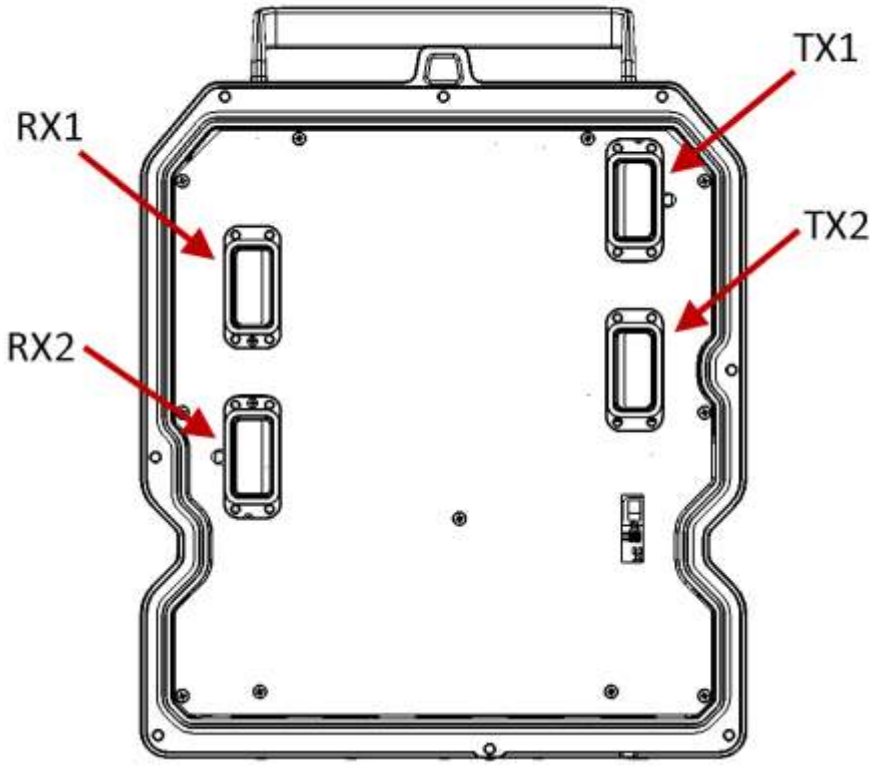


Figure 21: RFU-D-HP Radio Interfaces

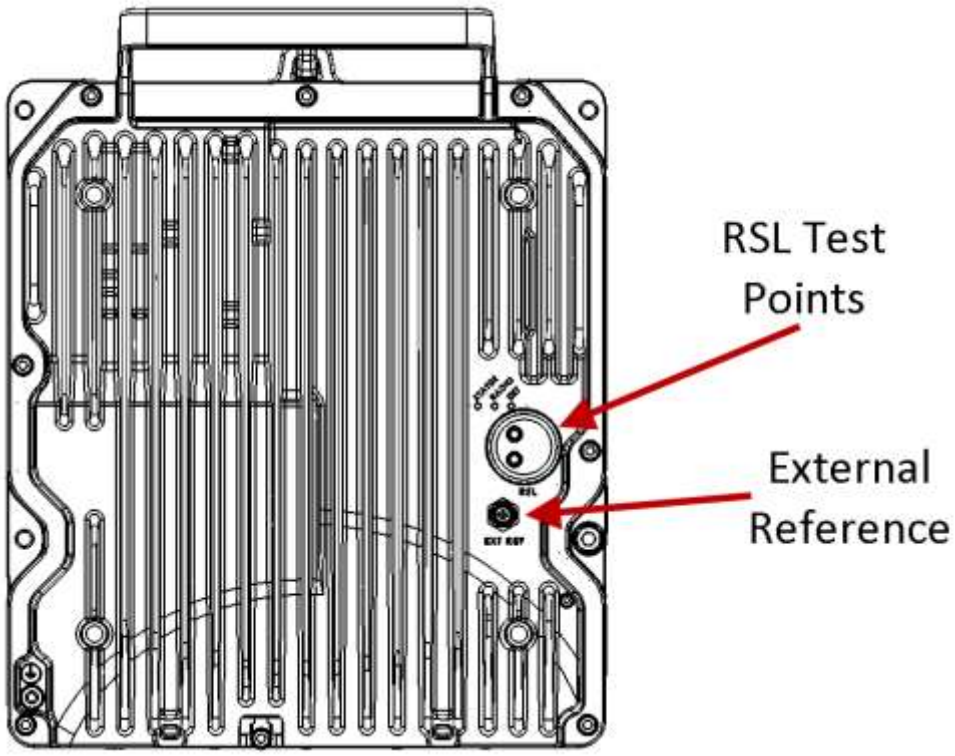


Figure 22: RFU-D-HP Front Side Interfaces

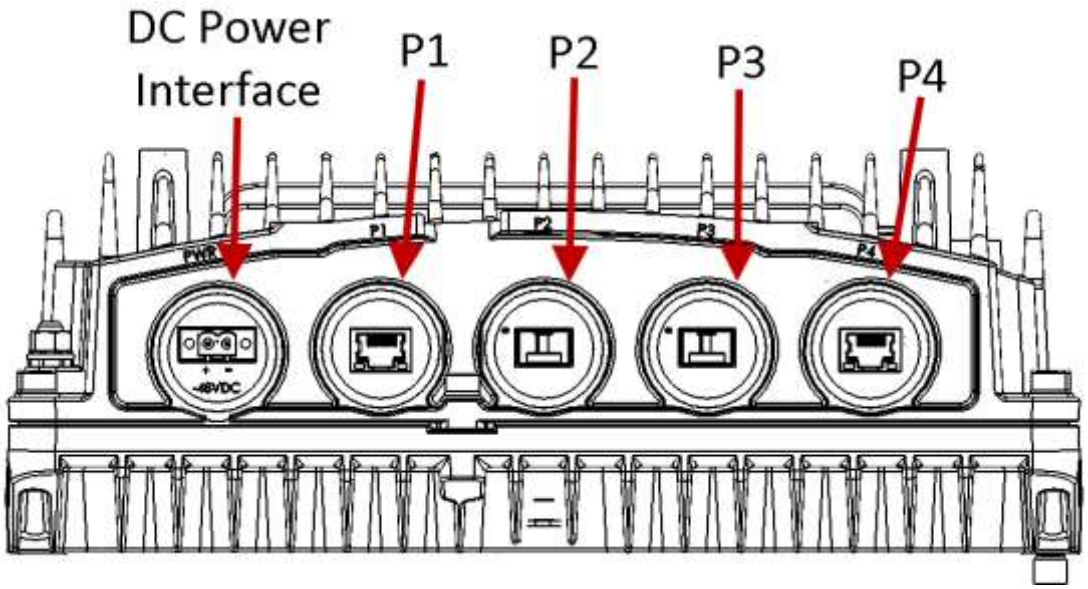


Figure 23: RFU-D-HP Interfaces

Table 19: RFU-D-HP Interfaces

Interface	Description
PWR	Power Connector, 48VDC
P1	RFU Interface (RJ-45)
P2	RFU Interface (SFP)
P3	Reserved for future use.
P4	Reserved for future use.

4.4.4 Space Diversity with Baseband Combining

RFU-D-HP has two receivers, enabling it to perform Space Diversity via Baseband Combining (BBC). The RFU receives and processes both signals, and combines them into a single, optimized signal. The BBC mechanism provides up to 3 dB in system gain.

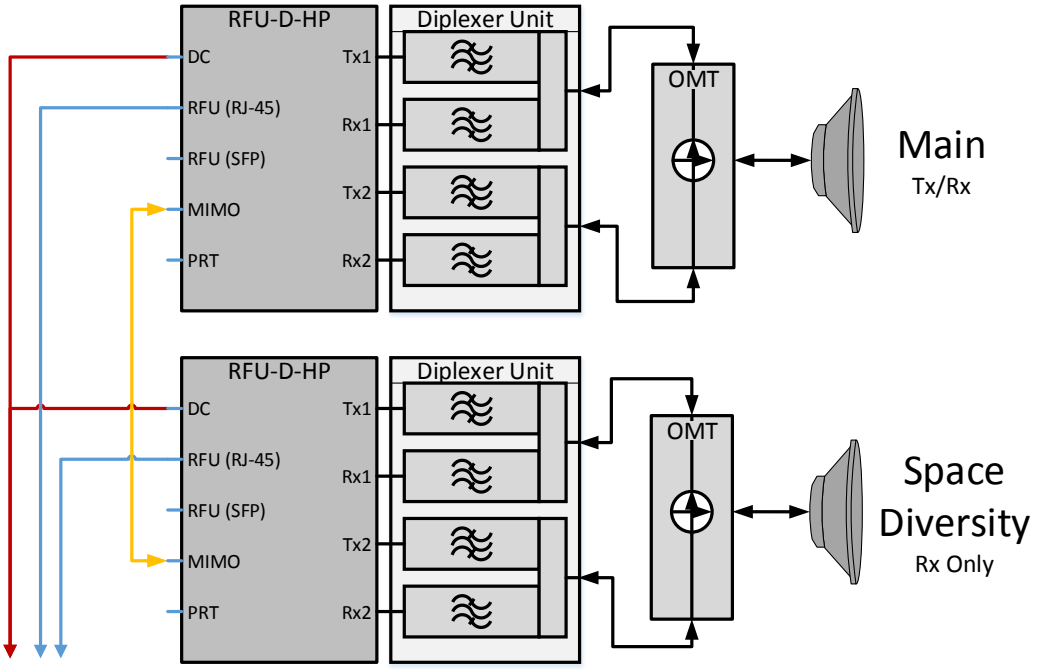


Figure 24: RFU-D-HP – 2+0 SD-BBC Configuration

For additional information:

- Specifications

4.4.5 RFU-D-HP Branching Options

The following branching options are available for RFU-D-HP:

- **Diplexers** – Provides wide diplexer-based branching, enabling direct or remote mount installation. Diplexers can be used for direct mount configurations of up to 4+0.
- **OCU-Based Branching** – Can be used for configurations of up to 16+0 per polarization in remote mount configurations.

To maximize operational flexibility, both diplexers and channel filters are provided separately for the radio units, enabling the diplexers or filters to be changed in the field with minimal downtime and no risk of impairing the RFU's sealing.

4.4.5.1 RFU-D-HP Diplexer Unit (DXU)

The Diplexer Unit (DXU) is used for configurations of up to two radio units. The DXU is assembled directly behind the radio unit to form the complete RFU-D-HP. The radio unit is generic; only the (DXU) is sub-band specific, which facilities link planning, ordering, and maintenance as described above.

Figure 25 shows the radio unit and the diplexer unit from front and back. In each picture, the radio unit is on the right.

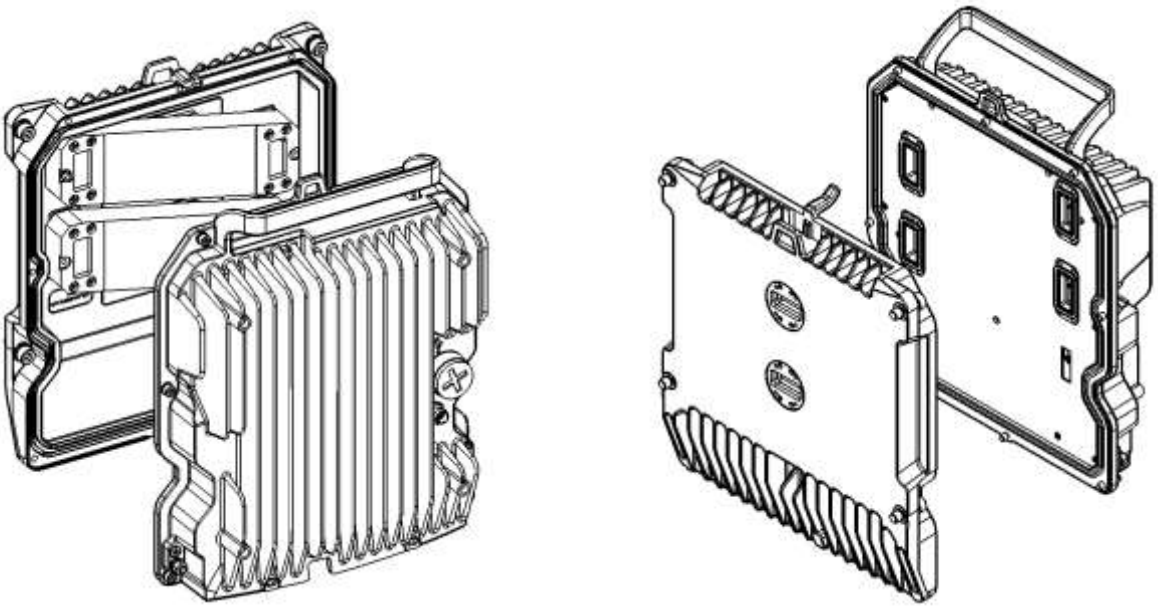


Figure 25: Radio Unit and Diplexer Unit

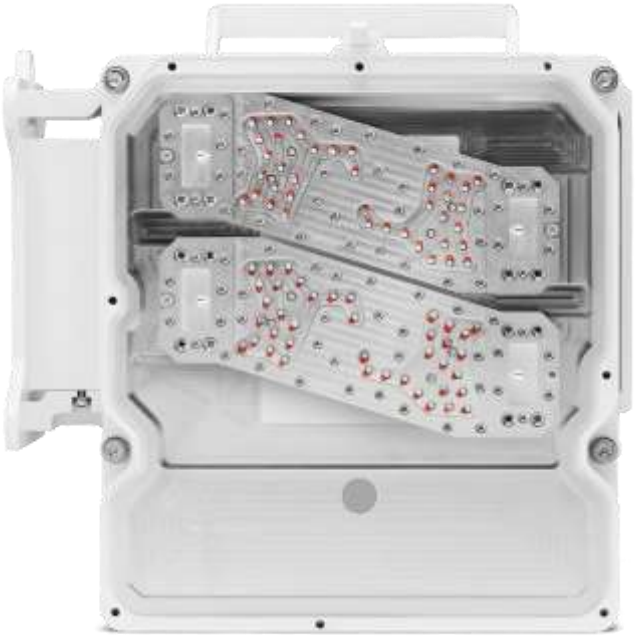


Figure 26: Open Diplexer Unit

For split-mount configurations, diplexer-based filtering can be used with up to two RFU-D-HP units (four carriers). For suitable frequency ranges and antenna sizes, the RFU-D-HP unit, including the diplexer unit, can be installed on the antenna in a direct mount configuration.

A diplexer-based RFU-D-HP unit can also be installed in a remote-mount configuration, using a remote mount kit.

MultiCore Mediation Devices (MCMD)

This section describes the MultiCore Mediation Devices (MCMD) available for installation of RFU-D-HP units using diplexers.

The MCMDs are designed to offer a simple and compact solution for direct mount installations of the MultiCore RFU-D-HP on a standard Ceragon antenna interface.

The RFU-D-HP is equipped with two antenna ports, which mandates the use of unique mediation devices to facilitate direct mount configurations. The following two examples show dual core mediation devices that enable the connection of a single RFU-D-HP unit to an antenna. For the full set of mediation devices, refer to the RFU-D-HP Installation Guide.

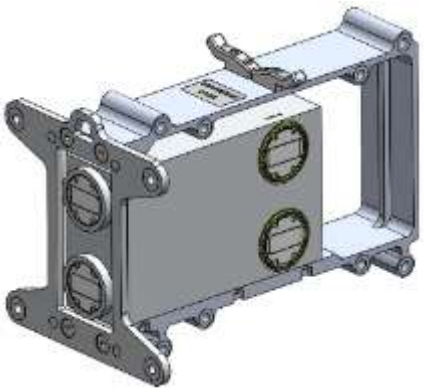


Figure 27: RFU-D-HP Coupler

Table 20: RFU-D-HP Mediation Devices

MCMD Type	Functionality
OMT	Combines the two carriers on alternate polarizations (H,V)
Splitter	Combines the two carriers using the same polarization
Dual Splitter	Combines the four carriers, two carriers on each polarization
Dual Coupler	Couples four carriers, two carriers on each polarization. For 2+2 HSB
Dual Circulator	Low loss combining of four carriers, two carriers on each polarization
Space Diversity	Allows for easy SD connection of the Space Diversity antenna using coaxial cable

4.4.5.2 Channel Filter-Based Split Mount Branching

For multiple carriers, up to four radio units can be cascaded and circulated together to the antenna port. This function is performed by branching networks that consist of OCUs and various components that connect multiple OCUs in the branching chain. The branching network routes the signals from the RFUs to the antenna.

The Tx and the Rx path circulate together to the main OCB port. Each OCU includes Tx and Rx channel filters for two carriers.

When chaining multiple OCBs, each Tx signal is chained to the OCB Rx signal, and both signals are chained to the next OCB using an S-band.

Outdoor Circulator Unit (OCU)

The OCU contains the channel filters, together with circulators, connecting two Tx channels and two Rx channels from the RFU-D-HP radio unit to the antenna port.

Figure 28: RFU-D-HP OCU

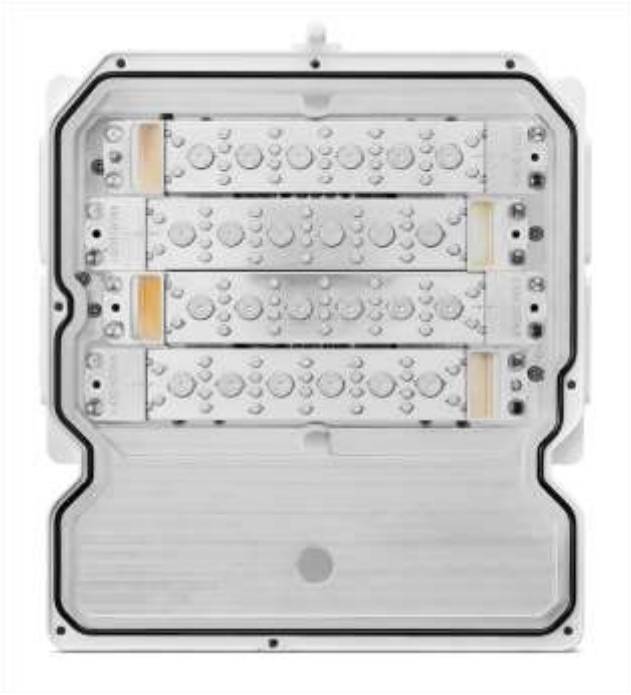


Figure 29: Open OCU Showing the Channel Filters

The OCU includes channel filters for two carriers. The OCU ports towards the RFU-D-HP radio ports become internal ports once the OCU is assembled behind the RFU-D-HP radio unit.

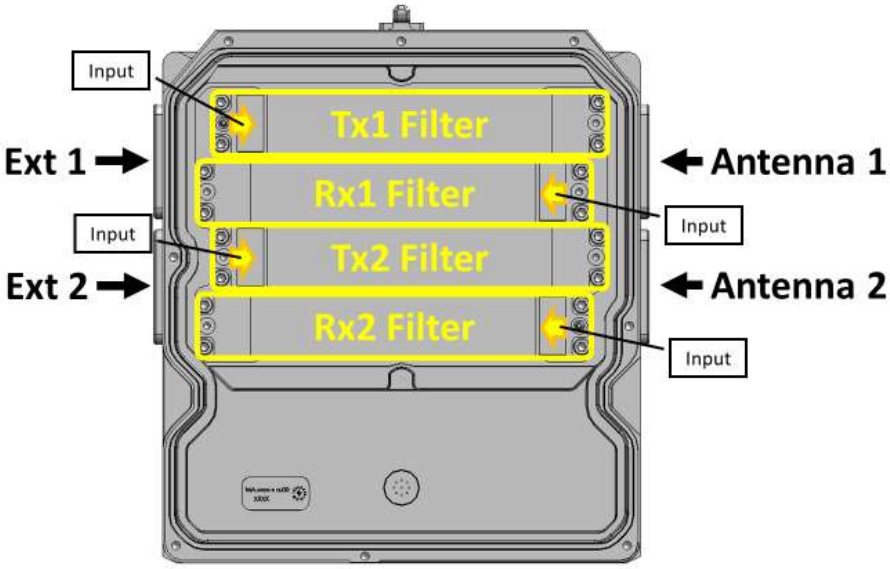


Figure 30: OCU Channel Filters – Functional Description

4.4.5.3 Split Mount Branching Configurations

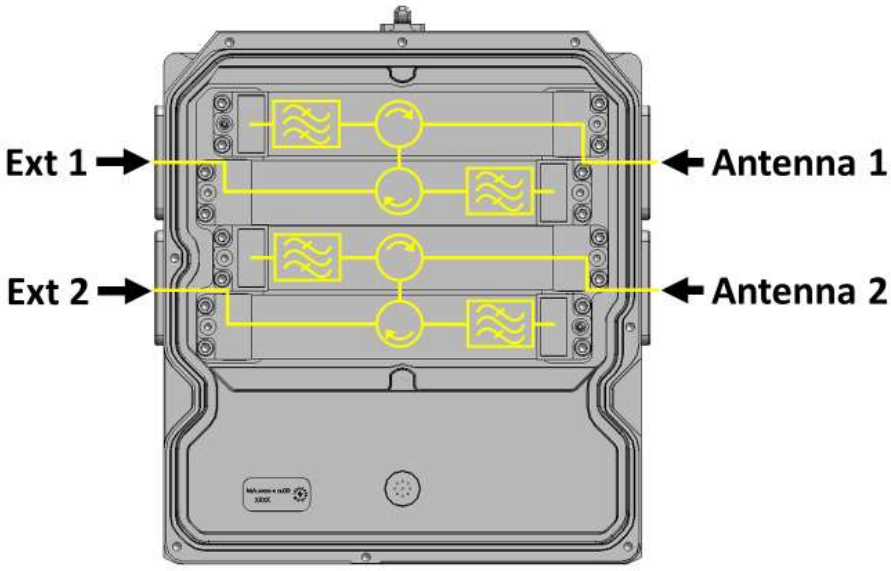


Figure 31: OCU Channel Filters – Internal Electrical Connections

4.4.6 RFU-D-HP Marketing Models

This section explains how to read RFU-D-HP marketing models, including marketing models for the radio unit, and marketing models for the branching unit, either diplexer or OCB-based branching. Constructing a marketing model for the purpose of ordering equipment should always be done using a configurator.

Note:	Not all fields are always necessary to define a valid marketing model. If a specific field is not applicable, it should be omitted.

4.4.6.1 RFU-D-HP Marketing Models – Radio Unit

Table 21 lists and describes the available RFU-D-HP marketing models for the radio unit, which is sub-band generic.

Table 21: RFU-D-HP Marketing Models – Radio Unit

Marketing Model	Description
RFU-D-HP-4L	RFU-D-HP 4GHz lower band Split Mount Radio Unit
RFU-D-HP-4H	RFU-D-HP 4GHz higher band Split Mount Radio Unit
RFU-D-HP-05	RFU-D-HP 5GHz Split Mount Radio Unit
RFU-D-HP-06	RFU-D-HP 6GHz Split Mount Radio Unit
RFU-D-HP-07	RFU-D-HP 7GHz Split Mount Radio Unit
RFU-D-HP-08	RFU-D-HP 8GHz Split Mount Radio Unit
RFU-D-HP-11	RFU-D-HP 11GHz Split Mount Radio Unit

4.4.6.2 RFU-D-HP Marketing Models – Diplexer Unit

This section explains how to read marketing models for the RFU-D-HP DXU. Constructing a marketing model for the purpose of equipment order should always be done using a configurator.

Note: Not all fields are always necessary to define a valid marketing model. If a specific field is not applicable, it should be omitted.

Table 22: DXDHff-xxxY-ccWdd-eeWgg-t

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	04, 05, L6,U6,7,8,10,11
xxxY	TX-RX separation and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
ccWdd, eeWgg	Channel indication or LOW/HIGH or blank	{Start ch}W{End ch} Example: 10W15 (eeWgg is optional when using two different diplexers Example: 1W5, 10W15)
t	TX low / TX high indication	L – TX Low H – TX high

Table 23 provides examples of specific RFU-D-HP DXU marketing models based on the syntax described above.

Table 23: RFU-D-HP Diplexers Unit Marketing Model Example

Marketing Model Example	Explanation
DXDH08-119A-01W03-L	RFU-D-HP Diplexers Unit, 8GHz, TRS=119MHz, two identical Diplexers Uniting channels 1 to 3, TX low
DXDHL6-252A-05W06-01W02-H	RFU-D-HP Diplexers Unit, L6GHz, 252MHz TRS, different Diplexers Uniting channels 5 to 6 and 1 to 2, TX high

4.4.6.3 RFU-D-HP Marketing Models – Mediation Device

Table 24 lists and describes the available RFU-D-HP MCMD marketing models.

Table 24: RFU-D-HP MCMD Marketing Models

Marketing Model	Description
DXDH-MD-OMT-*ff*	RFU-D-HP Diplexers Based Branching OMT Unit, *ff* GHz
DXDH-MD-DUAL-CPLR-*ff*	RFU-D-HP Diplexers Based Branching Dual Coupler Unit, *ff* GHz

DXDH-MD-SPLITTER-*ff*	RFU-D-HP Diplexers Based Branching Splitter Unit, *ff* GHz
DXDH-MD-DUAL-SPLTR-*ff*	RFU-D-HP Diplexers Based Branching Dual Splitter Unit, *ff* GHz
DXDH-MD-DUAL-CIRC-*ff*	RFU-D-HP Diplexers Based Branching Dual Circulator Unit, *ff* GHz
DXDH-MD-SD-*ff*	RFU-D-HP Diplexers Based Branching Space Diversity Unit, *ff* GHz
DXDH-RM-MOUNT-kit	RFU-D-HP RM kit for Direct Mount Mediation Dev.
DXDH-RM-MOUNT-ADPT-ff	RFU-D-HP DC Adaptor Remote Mount Kit, *ff* GHz
DXDH-RM-OMT-ADPT-ff	RFU-D-HP DC OMT Adaptor, *ff* GHz

Where

Place Holder in Marketing Model	Possible Values
ff	04, 05, 06, 7-8, 11

4.4.6.4 RFU-D-HP Marketing Models – OCU

This section explains how to read marketing models for the RFU-D-HP OCU. Constructing a marketing model for the purpose of equipment order should always be done using a configurator.

The OCU uses the following marketing model structure:
FXDHff-xxxYZccT-mmmNZddT-t

Note: Not all fields are always necessary to define a valid marketing model. If a specific field is not applicable, it should be omitted.

Table 25: Marketing Model Structure – OCU

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	L6,U6,07,08,11
xxxY, mmmN	1st Channel Filter TRS and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
Z, N	Indicating the Channel Filter channel bandwidth designator	Channel Filters Channel Bandwidth Designator {A/B/C/D/E} A = 28 MHz B = 40 MHz C = 56MHz

Placeholder in Marketing Model	Description	Possible Values
		D = 80 MHz E = 112 MHz
Cc, dd	Indicating the Channel Number in the Block	
T	Indicating the filter type	Filter Type {N/A} N = Standard Filter A = Adjacent Channel Filter
t	TX low / TX high indication	L – TX Low H – TX high

The following are some examples of specific RFU-D-HP OCU marketing models based on the syntax specified above.

Table 26: RFU-D-HP OCU Marketing Model Example

Marketing Model Example	Explanation
FXDH6H-340FA02A-310AB04N-H	Channel Filters cover for RFU-D-HP, Upper 6 GHz with 1st Filters block TRS block 340F, 28 MHz channels number 02 Adjacent and 2nd Filters block TRS block 310A, 40 MHz channels number 04 Narrow, High

4.4.6.5 Channel Filter-Based Branching Components

The following is a list of RFU-D-HP Channel Filter Branching units. These Branching units are used to build various RFU-D-HP configurations.

Table 27: RFU-D-HP Branching Unit Marketing Models

Marketing Model	Description
FXDH-RM-MOUNT-kit	RFU-D-HP Filters Remote Mount Kit
FXDH-RM-U-Bend-*ff*	RFU-D-HP Filters Cover Branching U Bend
FXDH-RM-LU-Bend-*ff*	RFU-D-HP FLT Cover Branch. Long U Bend
FXDH-RM-Term-*ff*	RFU-D-HP PDR100/CPR90G WG 50ohm termination kit
FXDH-RM-MD-SPLTR-*ff*	RFU-D-HP Filters Cover Branching Splitter MD Unit, *ff* GHz
FXDH-RM-MD-CPLR-*ff*	RFU-D-HP Filters Cover Branching Coupler MD Unit, *ff* GHz

In these marketing models, *ff* represents the frequency. Possible values are: 04, 05, 06, 7-8, and 11.

4.5 RFU-E

FibeAir RFU-E is a compact and versatile RFU that operates in the E-Band frequency range (71-86 and 81-86 GHz). Its light weight and small footprint make it versatile for many different applications. Thanks to its small footprint, low power consumption, and simple installation, RFU-E can be installed in many different types of remote locations.

RFU-E operates over 62.5, 125, 250, and 500 MHz channels to deliver up to 2.5 Gbps of Ethernet throughput in several system configurations.

RFU-E is connected to the IDU via a single radio interface. RFU-E supports low to high capacities for traditional voice and Ethernet services, as well as PDH/ or hybrid Ethernet and TDM interfaces.

With RFU-E provides a range of modulations from BPSK to 1028 QAM.

4.5.1 Main Features of RFU-E

- **Frequency range** – Operates in the frequency range 71-86 and 81-86 GHz
- **Transmit power** – Up to 18 dBm
- **Configurable Modulation –** BPSK to 1028 QAM
- **Configurable Channel Bandwidth** – 62.5 to 500 MHz
- **Compact, lightweight form factor -** Reduces installation and warehousing costs
- **Efficient and easy installation -** Direct mount installation with different antenna types

4.5.2 RFU-E Functional Block Diagram

The RFU is responsible for RF signal processing, and includes an RF transmitter and an RF receiver with all their related functions.

RFU-E is designed to provide a high-capacity RF module, with a variety of low-loss mediation devices to accommodate different RF configurations.

The following block diagram illustrates the functional modules of an RFU-S in a 1+0 configuration.

The RFU is responsible for RF signal processing, and includes an RF transmitter and an RF receiver with all their related functions.

The RFU-E is designed to provide a split-mount solution for the E-Band frequency range.

The following block diagram illustrates the functional modules of an RFU-E in a 1+0 configuration.

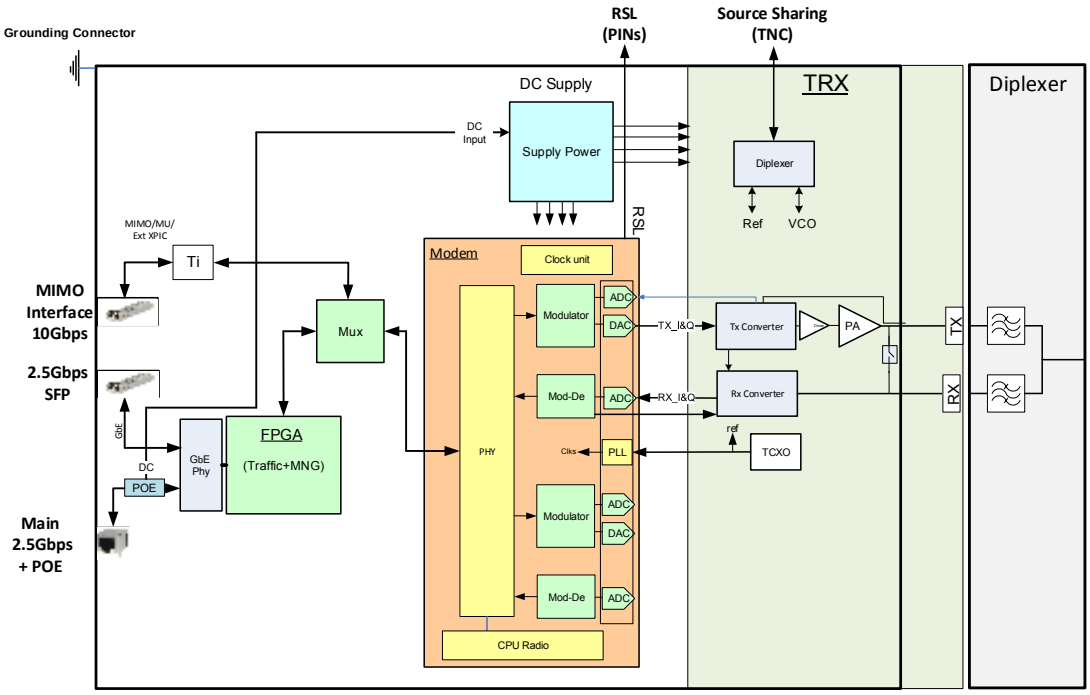


Figure 32: RFU-E Functional Block Diagram – 1+0 Configuration

4.5.3 RFU-E Radio Interfaces

The following figures show the RFU-E TX and RX interfaces.

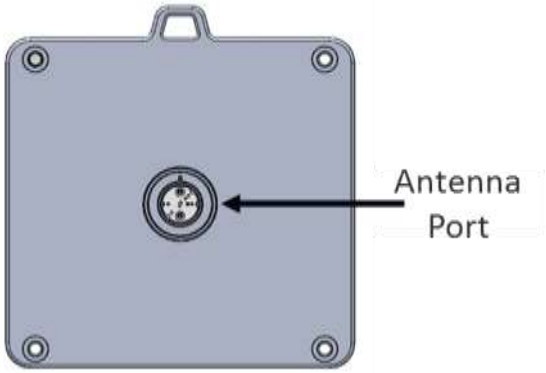


Figure 33: RFU-E Antenna Interfaces

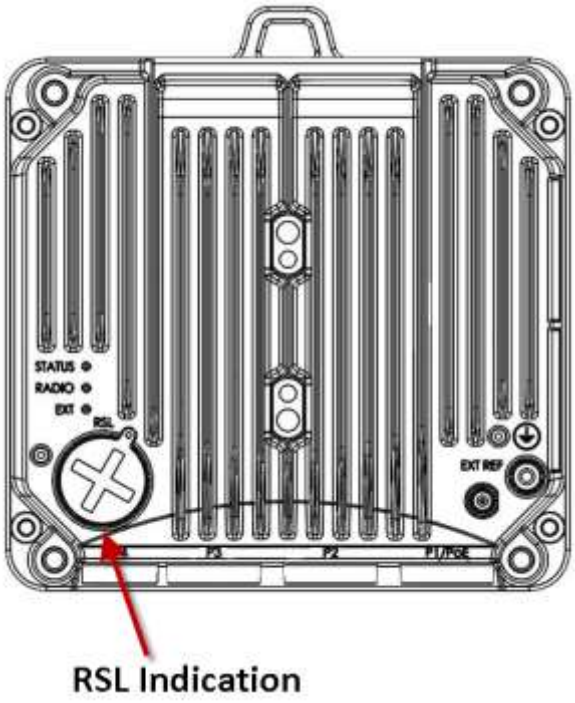


Figure 34: RFU-D Front Side Interfaces

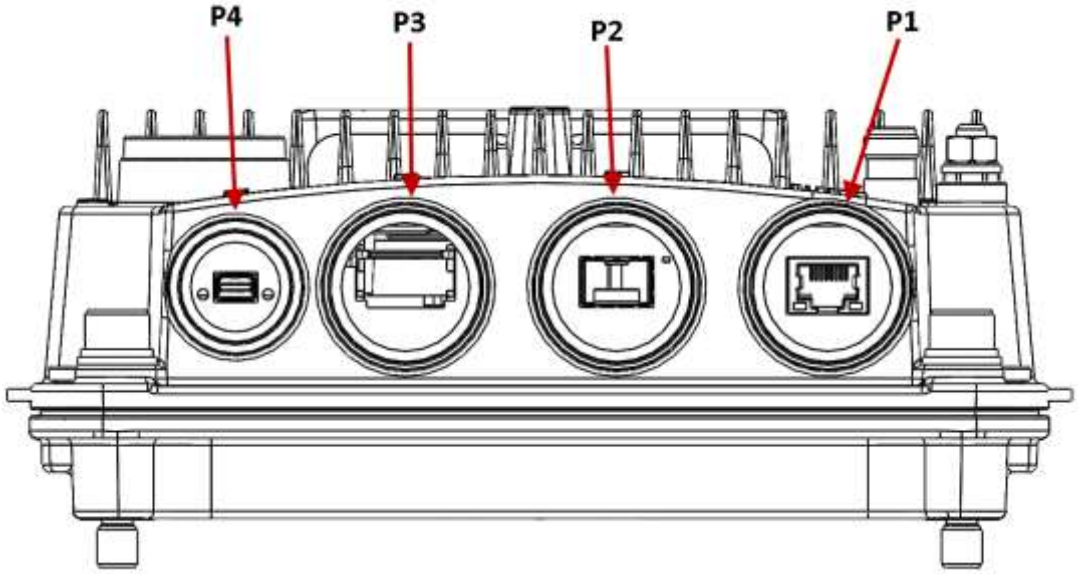


Figure 35: RFU-E Interfaces

Table 28: RFU-E Interfaces

Interface	Description
P1	PoE / RFU Interface (RJ-45)
P2	RFU Interface (SFP)
P3	Reserved for future use
P4	Reserved for future use

4.5.4 RFU-E Marketing Models

The RFU-E is offered in two main configurations:

- Integrated Antenna
- Standalone RFU

The following table lists and describes the available RFU-E marketing models.

Table 29: RFU-E Marketing Models

Marketing Model	Description
RFU-E-{*H/L*}-*Ant*	RFU-E, Split Mount, E-Band, Integrated Antenna. RFU-E-{*H/L*}-Ant
RFU-E-{*H/L*}	RFU-E, Split Mount, E-Band. RFU-E-{*H/L*}

4.6 RFU-S

FibeAir RFU-S is a state-of-the-art RFU that supports a broad range of capacities. RFU-S operates in the frequency range of 6-42 GHz.

RFU-S is connected to the IDU via a single radio interface. RFU-S supports low to high capacities for traditional voice and Ethernet services, as well as PDH/ or hybrid Ethernet and TDM interfaces.

With RFU-S, traffic capacity throughput and spectral efficiency are optimized with the desired channel bandwidth. For maximum user choice flexibility, channel bandwidths from 20-80 MHz can be selected together with a range of modulations. RFU-S provides a range of modulations from BPSK to 4096 QAM.

4.6.1 Main Features of RFU-S

- **Frequency range** – Operates in the frequency range 6 – 42 GHz
- **More power in a smaller package -** Up to 28 dBm, ideal for long-haul applications
- **Configurable Modulation –** BPSK – 4096 QAM
- **Configurable Channel Bandwidth** – 20 MHz – 80 MHz
- **Compact, lightweight form factor -** Reduces installation and warehousing costs
- **Efficient and easy installation -** Direct mount installation with different antenna types

For additional information:

- Specifications

4.6.2 RFU-S Functional Block Diagram

The RFU is responsible for RF signal processing, and includes an RF transmitter and an RF receiver with all their related functions.

RFU-S is designed to provide a high-capacity RF module, with a variety of low-loss mediation devices to accommodate different RF configurations.

The following block diagram illustrates the functional modules of an RFU-S in a 1+0 configuration.

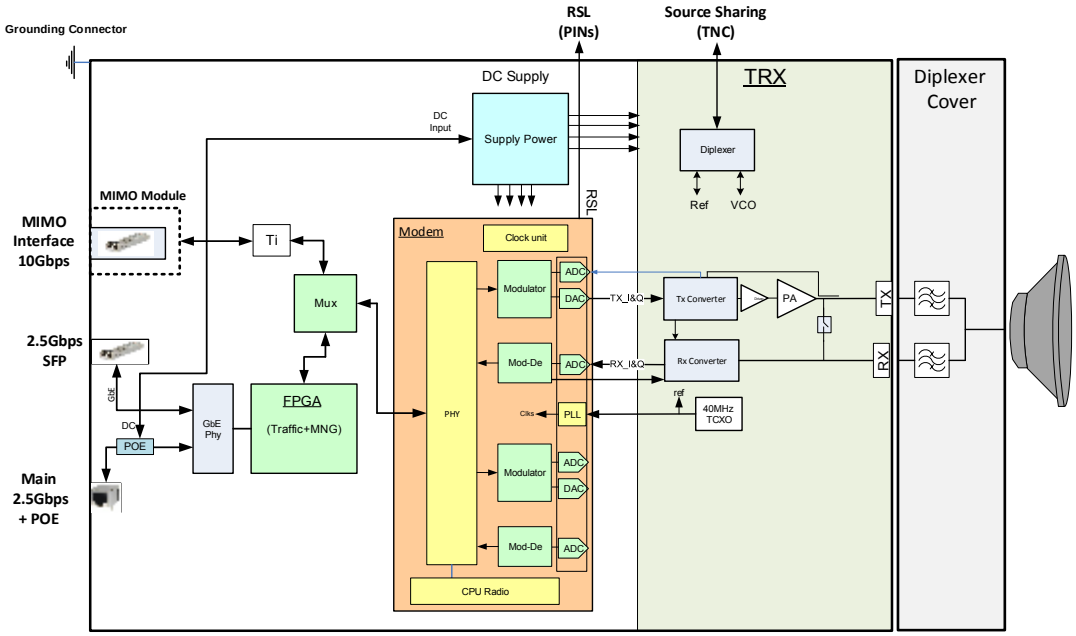


Figure 36: RFU-S Functional Block Diagram – 1+0 Configuration

4.6.3 RFU-S Interfaces

The following figures show the RFU-S interfaces.

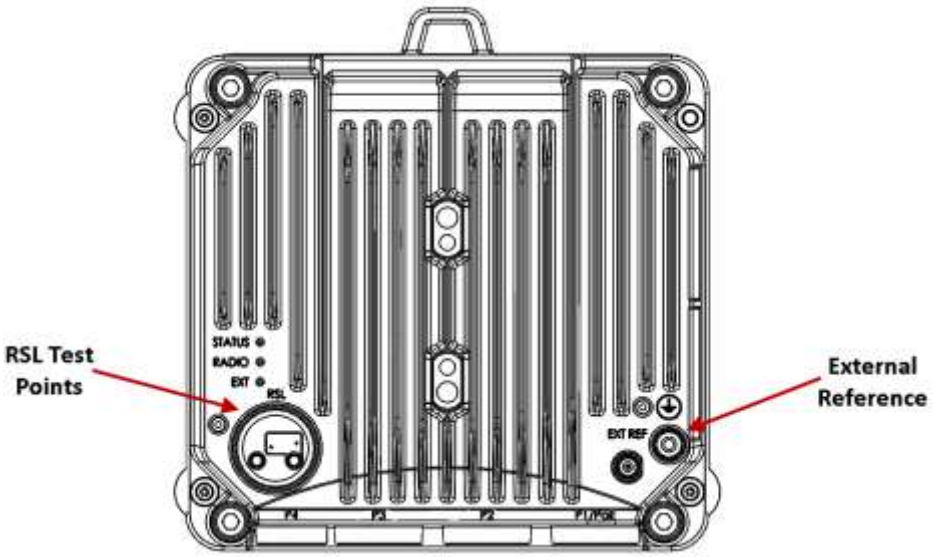


Figure 37: RFU-S Front Side Interfaces

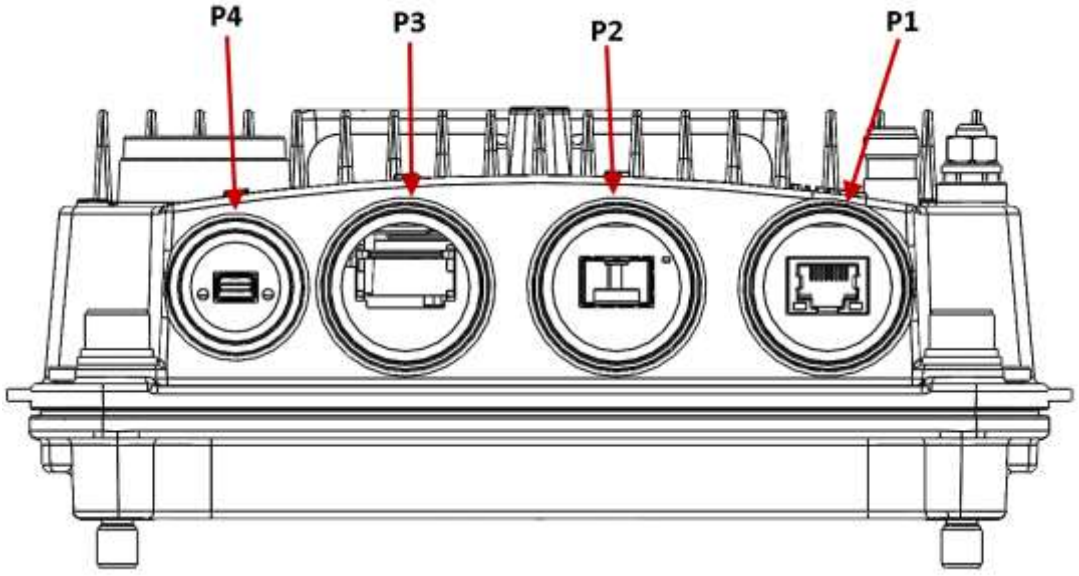


Figure 38: RFU-S Data and Power Interfaces

Table 30: RFU-S Interfaces

Interface	Description
P1	PoE / RFU Interface (RJ-45)
P2	RFU Interface (SFP)
P3	Reserved for future use
P4	Reserved for future use

4.6.4 RFU-S Marketing Models

For frequencies of 6 to 15 GHz, RFU-S uses the Easy Set technology in which two individual units are ordered: a generic radio unit and a diplexer unit.

For frequencies of 18 to 42 GHz, a single RFU-S unit is ordered, consisting of both the radio and the diplexers.

This section explains how to read RFU-S marketing models, including marketing models for the diplexer unit for 6-15 GHz links. Constructing a marketing model for the purpose of ordering equipment should always be done using a configurator.

Note: Not all fields are always necessary to define a valid marketing model. If a specific field is not applicable, it should be omitted.

4.6.4.1 Marketing Models for Easy Set RFU-S Radio and Diplexer Units, 6 to 15 GHz

For frequencies of 6 to 15 GHz, the RFU-S radio unit and diplexer unit are ordered separately. Using Easy Set technology, the diplexer unit is assembled on the RFU-S radio unit during link installation in the field. The radio unit is generic; only the diplexer unit (DXU) is sub-band specific, which facilities link planning, ordering, and maintenance as described above.

Table 31 provides the marketing model syntax for the RFU-S Easy Set radio unit.

Table 32 provides the marketing model syntax for the RFU-S Easy Set diplexer unit.

Table 31: RFU-S Marketing Model Syntax, 6 to 15 GHz (Radio Unit)

Marketing Model	Description
RFU-S-*ff*	RFU-S, Single Core, High Capacity, Split Mount Radio only, *ff* GHz

Table 32: RFU-S Marketing Model Syntax, 6 to 15 GHz (Diplexer Unit)

Marketing Model	Description
DXSff-xxxY-ccWdd-t	RFU-S Diplexers Unit, *ff* GHz, Block *xxxY*, *ccWdd,* High/Low

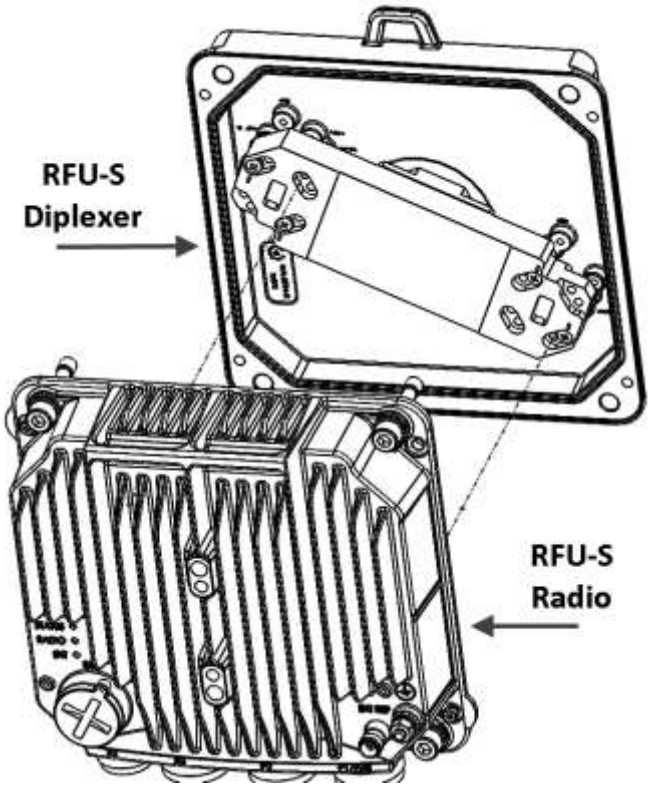


Figure 39: RFU-S Radio Unit and Diplexers Unit (Separate)

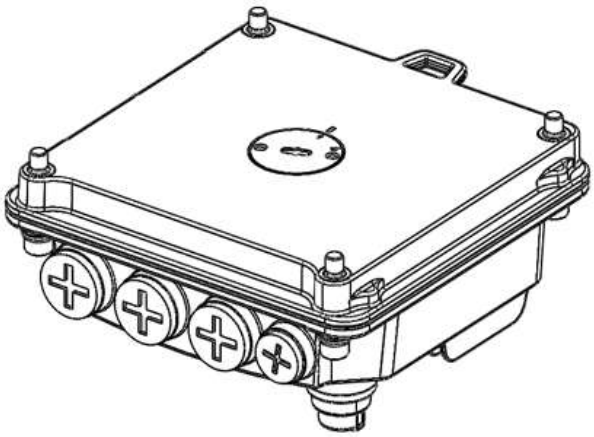


Figure 40: RFU-S Radio Unit and Diplexers Unit (Attached)

Table 33: RFU-S Marketing Model Structure– Possible Values (Easy Set - Radio Unit Only)

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	06,07,08,10,11,13,15

Table 34: : RFU-S Marketing Model Structure– Possible Values (Easy Set - Diplexer Unit Only)

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	L6,U6,07,08,10,11,13,15
xxxY	TX-RX separation and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
ccWdd	Channel indication or LOW/HIGH or blank	{Start ch}W{End ch} Example: 10W15
t	TX low / TX high indication	L – TX Low H – TX high

Table 35 provides examples of specific RFU-S diplexer unit marketing models based on the syntax described above.

Table 35: RFU-S Diplexer Unit Marketing Model Example

Marketing Model Example	Explanation
DXSU6-160A-13W16-L	Diplexer Cover Assembly for RFU-S, Upper 6 GHz. TRS block 160A, Ch 13 to 16, Tx low

4.6.4.2 Marketing Model for RFU-S Unit, 18-42 GHz

When ordering an RFU-S, a single unit is ordered according to the following marketing model syntax: *RFU-S-xxxY-ccWdd-t*.

Table 36: RFU-S Marketing Model Structure,18 to 42 GHz

Marketing Model	Description
RFU-S-*xxxY-ccWdd-t*	RFU-S, Single Core, High Capacity, Split Mount Radio, *ff* GHz, Block *xxxY*, *ccWdd* High/Low

Table 37: RFU-S Marketing Model Structure– Possible Values

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	18, 23, 24, 26, 28, 32, 36, 38, 42
xxxY	TX-RX separation and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
ccWdd	Channel indication or LOW/HIGH or blank	{Start ch}W{End ch} Example: 10W15
t	TX low / TX high indication	L – TX Low H – TX high

The following are some examples of specific RFU-S 18 to 42 GHz marketing models based on the syntax specified above.

Table 38: RFU-S Marketing Model Examples (18-42 GHz)

Marketing Model Example	Explanation
RFU-S-08-119A-01W03-L	RFU-S Diplexers Unit, 8GHz, TRS=119MHz, covering channels 1 to 3, TX low
RFU-S-L6-252A-05W06-H	RFU-S-HP Diplexers Unit, L6GHz, 252MHz TRS, covering channels 5 to 6, TX high

4.6.5 RFU-S Mediation Devices

RFU-S requires a Coupler/Splitter for 1+1 configurations and an OMT for 2+2 configurations.

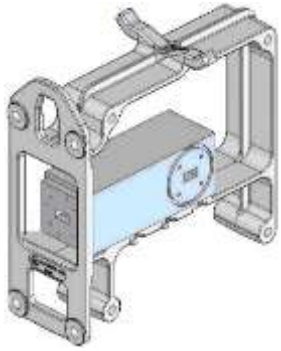


Figure 41: RFU-S Coupler/Splitter

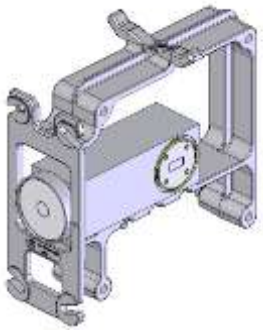


Figure 42: RFU-S OMT

5. Activation Keys

This chapter describes IP-20F's activation key model. IP-20F offers a pay as-you-grow concept in which future capacity growth and additional functionality can be enabled with activation keys. For purposes of the activation keys, each IP-20F chassis is considered a distinct device, regardless of which cards are included in the chassis. Each device contains a single unified activation key cipher.

Activation keys are divided into two categories:

- **Per Carrier** – The activation key is per carrier.
- **Per Device** – The activation key is per device, regardless of the number of carriers supported by the device.

An HSB configuration requires the same set of activation keys for the active and the protected radio carriers.

This chapter includes:

- Working with Activation Keys
- Demo Mode
- Activation Key Reclaim
- Activation Key-Enabled Features

5.1 Working with Activation Keys

Ceragon provides a web-based system for managing activation keys. This system enables authorized users to generate activation keys, which are generated per IDU serial number.

In order to upgrade an activation key, the activation key must be entered into the IP-20F. The system checks and implements the new activation key, enabling access to new capacities and/or features.

In the event that the activation-key-enabled capacity and feature set is exceeded, an Activation Key Violation alarm occurs and the Web EMS displays a yellow background and an activation key violation warning. After a 48-hour grace period, all other alarms are hidden until the capacity and features in use are brought within the activation key's capacity and feature set.

5.2 Demo Mode

The system can be used in demo mode, which enables all features for 60 days. Demo mode expires 60 days from the time it was activated, at which time the most recent valid activation key cipher goes into effect. The 60-day period is only counted when the system is powered up. Ten days before demo mode expires, an alarm is raised indicating to the user that demo mode is about to expire.

5.3 Activation Key Reclaim

If a customer needs to deactivate an IP-20 device, whether to return it for repairs or for any other reason, the customer can reclaim the device's activation key and obtain a credit that can be applied to activation keys for other devices.

Where the customer has purchased upgrade activation keys, credit is given for the full feature or capacity, not for each individual upgrade. For example, if the customer purchased five capacity activation keys for 300M and later purchased three upgrade activation keys to 350M, credit is given as if the customer had purchased three activation keys for 350M and two activation keys for 300M.

5.4 Activation Key-Enabled Features

The default (base) activation key provides each carrier with a capacity of 10 Mbps. In addition, the default activation key provides:

- A single management service, with MSTP available for this service.
- Unlimited Smart Pipe (L1) services.
- A single 1 x GbE port for traffic.
- A single RFU port
- Unlimited Native TDM services (but no TDM pseudowire services)
- Full QoS with basic queue buffer management (fixed queues with 1 Mbit buffer size limit, tail-drop only).
- LAG
- No synchronization

Note:	As described in more detail below, a CET Node activation key allows all CET service/EVC types including Smart Pipe, Point-to-Point, and Multipoint, and MSTP for all services, as well as an additional GbE traffic port for a total of 2 x GbE traffic ports.

As your network expands and additional functionality is desired, activation keys can be purchased for the features described in the following table.

Table 39: Activation Key Types

Marketing Model	Type	Description	For Additional Information
Refer to *Capacity Activation Key Levels* on page 83.	Per Carrier	Enables you to increase your system's radio capacity in gradual steps by upgrading your capacity activation key level. Without a capacity activation key, each carrier has a capacity of 10 Mbps. Activation-key-enabled capacity is available from 50 Mbps to 650 Mbps. Each radio carrier can be activation-key-enabled for a different capacity.	*Capacity Summary*
IP-20-SL-RFU-2nd-Core-Act.	Per RFU	Enables use of second carrier on a MultiCore RFU-D.	*Unique MultiCore Architecture of RFU-D and RFU-D-HP*
IP-20-SL-2nd-Core-Act-HP	Per RFU	Enables use of second carrier on a MultiCore RFU-D-HP.	*Unique MultiCore Architecture of RFU-D and RFU-D-HP*
IP-20-SL-IDU-Radio-Port-Act.	Per Port	Enables use of an additional RFU port.	*Radio Interfaces*
IP-20-SL-LLF	Per Device	Enables you to use Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group.	*Automatic State Propagation and Link Loss Forwarding*
IP-20-SL-ACM	Per Carrier	Enables the use of Adaptive Coding and Modulation (ACM) scripts.	*Adaptive Coding Modulation (ACM)*
IP-20-SL-MC-ABC	Per Carrier	Enables Multi-Carrier ABC.	*Multi-Carrier Adaptive Bandwidth Control (MC-ABC)*
IP-20-SL-Header-DeDuplication	Per Carrier	Enables the use of Header De-Duplication, which can be configured to operate at L2 through L4.	*Header De-Duplication*
IP-20-SL-XPIC	Per Carrier	Enables the use of Cross Polarization Interference Canceller (XPIC). Each carrier in the XPIC pair must be activation-key-enabled.	*Cross Polarization Interference Canceller (XPIC)*

Marketing Model	Type	Description	For Additional Information
IP-20-SL-GE-Port	Per Port	Enables the use of an Ethernet traffic port in 1 or 2.5 GbE mode. An activation key is required for each additional Ethernet traffic port that is used on the device, beyond the one GbE traffic port that is enabled via the default activation key. An activation key can be installed multiple times with dynamic allocation inside the unit to enable multiple GbE ports. **Note:** Two Ethernet ports are enabled in FE mode (10/100baseT) by default without requiring any activation key.	*Ethernet Traffic Interfaces*
Refer to *CET Node Activation Key Levels* on page 85.	Per Device	Enables Carrier Ethernet Transport (CET) and a number of Ethernet services (EVCs), depending on the type of CET Node activation key: • Edge CET Node – Up to 8 EVCs. • Aggregation Level 1 CET Node – Up to 64 EVCs. A CET Node activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Network resiliency (MSTP/RSTP) for all services. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS.	• *Ethernet Service Model* • *Quality of Service (QoS)*
IP-20-SL-Network-Resiliency	Per Device	Enables the following protocols for improving network resiliency: • G.8032 • TDM Services 1:1/1+1 path protection	*Network Resiliency*
IP-20-SL-H-QoS	Per Device	Enables H-QoS.[9] This activation key is required to add service-bundles with dedicated queues to interfaces. Without this activation key, only the default eight queues per port are supported.	*Quality of Service (QoS)*

[9] H-QoS support is planned for future release.

Marketing Model	Type	Description	For Additional Information
IP-20-SL-Enh-Packet-Buffer	Per Device	Enables configurable (non-default) queue buffer size limit for Green and Yellow frames. Also enables WRED. The default queue buffer size limit is 1Mbits for Green frames and 0.5 Mbits for Yellow frames.	*Quality of Service (QoS)*
IP-20-SL-Sync-Unit	Per Device	Enables the G.8262 synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use Synchronous Ethernet (SyncE).	*Synchronization*
IP-20-SL-IEEE-1588-TC	Per Device	Enables IEEE-1588 Transparent Clock support.[10]	IEEE-1588v2 PTP Optimized Transport
IP-20-SL-IEEE-1588-BC	Per Device	Enables IEEE-1588 Boundary Clock support.[11]	IEEE-1588v2 PTP Optimized Transport
IP-20-SL-Frame-Cut-Through	Per Device	Enables Frame Cut-Through.	Frame Cut-Through
IP-20-SL-TDM-PW	Per Device	Enables TDM pseudowire services on units with TDM interfaces. Without this activation key, only native TDM services are supported.	TDM Pseudowire Services
IP-20-SL-Secure-Management	Per Device	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, and RADIUS).	Secure Communication Channels
IP-20-SL-Eth-OAM-FM	Per Device	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only).	Connectivity Fault Management (FM)
IP-20-SL-Eth-OAM-PM	Per Device	Enables performance monitoring pursuant to Y.1731 (CET mode only).[12]	
IP-20-SL-LACP	Per Device	Enables Link Aggregation Control Protocol (LACP).	Link Aggregation Groups (LAG) and LACP

Table 40: Capacity Activation Key Levels

Marketing Model	Description
IP-20-SL-Capacity-50M	IP-20 SL - Capacity 50M, per carrier
IP-20-SL-Capacity-100M	IP-20 SL - Capacity 100M, per carrier

[10] IEEE-1588 Transparent Clock is planned for future release.

[11] IEEE-1588 Boundary Clock is planned for future release.

[12] PM support is planned for future release.

Marketing Model	Description
IP-20-SL-Capacity-150M	IP-20 SL - Capacity 150M, per carrier
IP-20-SL-Capacity-200M	IP-20 SL - Capacity 200M, per carrier
IP-20-SL-Capacity-225M	IP-20 SL - Capacity 225M, per carrier
IP-20-SL-Capacity-250M	IP-20 SL - Capacity 250M, per carrier
IP-20-SL-Capacity-300M	IP-20 SL - Capacity 300M, per carrier
IP-20-SL-Capacity-350M	IP-20 SL - Capacity 350M, per carrier
IP-20-SL-Capacity-400M	IP-20 SL - Capacity 400M, per carrier
IP-20-SL-Capacity-450M	IP-20 SL - Capacity 450M, per carrier
IP-20-SL-Capacity-500M	IP-20 SL - Capacity 500M, per carrier
IP-20-SL-Capacity-650M	IP-20 SL - Capacity 650M, per carrier
IP-20-SL-Capacity-1G	IP-20 SL - Capacity 1G
IP-20-SL-Capacity-1.6G	IP-20 SL - Capacity 1.6G
IP-20-SL-Capacity-2G	IP-20 SL - Capacity 2G
IP-20-SL-Capacity-2.5G	IP-20 SL - Capacity 2.5G
IP-20-SL-Upg-50M-100M	IP-20 SL - Upg 50M - 100M, per carrier
IP-20-SL-Upg-100M-150M	IP-20 SL - Upg 100M - 150M, per carrier
IP-20-SL-Upg-150M-200M	IP-20 SL - Upg 150M - 200M, per carrier
IP-20-SL-Upg-200M-225M	IP-20 SL - Upg 200M - 225M, per carrier
IP-20-SL-Upg-225M-250M	IP-20 SL - Upg 225M - 250M, per carrier
IP-20-SL-Upg-250M-300M	IP-20 SL - Upg 250M - 300M, per carrier
IP-20-SL-Upg-300M-350M	IP-20 SL - Upg 300M - 350M, per carrier
IP-20-SL-Upg-350M-400M	IP-20 SL - Upg 350M - 400M, per carrier
IP-20-SL-Upg-400M-450M	IP-20 SL - Upg 400M - 450M, per carrier
IP-20-SL-Upg-450M-500M	IP-20 SL - Upg 450M - 500M, per carrier
IP-20-SL-Upg-500M-650M	IP-20 SL - Upg 500M - 650M, per carrier
IP-20-SL-Upg-650M-1G	IP-20 SL - Upg 650M - 1G
IP-20-SL-Upg-1G-1.6G	IP-20 SL - Upg 1G - 1.6G
IP-20-SL-Upg-1.6G-2G	IP-20 SL - Upg 1.6G - 2G
IP-20-SL-Upg-2G-2.5G	IP-20 SL - Upg 2G - 2.5G

Table 41: CET Node Activation Key Levels

Marketing Model	# of Bundled GbE Ports for User Traffic	Management Service	# of Pipe (L1) Ethernet Services	# of CET (L2) Ethernet Services[13]	# of Native TDM Services
Default (No Activation Key)	1	Yes	Unlimited	-	512
IP-20-SL-Edge-CET-Node	2	Yes	Unlimited	8	512
IP-20-SL-Agg-Lvl-1-CET-Node	2	Yes	Unlimited	64	512
IP-20-SL-Agg-Lvl-2-CET-Node	2	Yes	Unlimited	1024	512

If a CET activation key is not generated on the IP-20 device upon initial configuration, the device uses by default a base smart pipe activation key (SL-0311-0). If the operator later wants to upgrade from the base smart pipe activation key to a CET activation key, the customer must use a CET upgrade activation key. The following table lists the CET upgrade activation keys:

Table 42: Edge CET Note Upgrade Activation Keys

Marketing Model	Upgrade From	Upgrade To
IP-20-SL-Upg-Pipe/Edge-CET	NG Smart Pipe Activation Key (SL-0311-0)	IP-20-SL-Edge-CET-Node (SL-0312-0)
IP-20-SL-Upg-Edge/Agg-Lvl-1	IP-20-SL-Edge-CET-Node (SL-0312-0)	IP-20-SL-Agg-Lvl-1-CET-Node (SL-0313-0)
IP-20-SL-Upg-Agg-Lvl-1/Lvl-2	IP-20-SL-Agg-Lvl-1-CET-Node (SL-0313-0)	IP-20-SL-Agg-Lvl-2-CET-Node (SL-0314-0)

[13] Including Point-to-Point, Multipoint, and TDM Pseudowire services. An IP-20-SL-TDM-PW activation key is also required to enable TDM Pseudowire services.

6. Feature Description

This chapter describes the main IP-20F features. The feature descriptions are divided into the categories listed below.

This chapter includes:

- Innovative Techniques to Boost Capacity and Reduce Latency
- Radio Features
- Ethernet Features
- Synchronization
- TDM Services

6.1 Innovative Techniques to Boost Capacity and Reduce Latency

IP-20F utilizes Ceragon's innovative technology to provide a high-capacity low-latency solution. IP-20F's Header De-Duplication option is one of the innovative techniques that enables IP-20F to boost capacity and provide operators with efficient spectrum utilization, with no disruption of traffic and no addition of latency.

IP-20F also utilizes established Ceragon technology to provide low latency representing a 50% latency reduction for Ethernet services compared to the industry benchmark for wireless backhaul.

Another of Ceragon's innovative features is Frame Cut-Through, which provides unique delay and delay-variation control for delay-sensitive services. Frame Cut-Through enables high-priority frames to bypass lower priority frames even when the lower-priority frames have already begun to be transmitted. Once the high-priority frames are transmitted, transmission of the lower-priority frames is resumed with no capacity loss and no re-transmission required.

This section includes:

- Capacity Summary
- Unique MultiCore Architecture of RFU-D and RFU-D-HP
- Header De-Duplication
- Latency
- Frame Cut-Through

6.1.1 Capacity Summary

Each carrier in an IP-20F IDU provides the following capacity:

- **Supported Microwave Channels** – 20/25/30/40/50/60/80 MHz channels.
- **Supported E-Band Channels** – 62.5/125/250/500 MHz channels.
- **Microwave Frequency Bands** – 4, 5, L6, U6, 7, 8, 10, 11, 13, 15, 18, 23, 26, 28, 32, 38 GHz
- **E-Band Frequency Bands** – 71-86 GHz
- **High scalability** – From 10 Mbps to 2.5 Gbps, using the same hardware.
- **Modulations**
  - Microwave RFUs – BPSK to 4096 QAM
  - RFU-E – BPSK to 1024 QAM

For additional information:

- Radio Capacity Specifications

6.1.2 Unique MultiCore Architecture of RFU-D and RFU-D-HP

FibeAir RFU-D and RFU-D-HP are MultiCore microwave radios. MultiCore radio architecture marks the beginning of a new era in wireless communications, boosting microwave to new levels of capacity previously reserved to fiber optic cable.

RFU-D and RFU-D-HP's unique MultiCore radio architecture is based on an advanced parallel radio processing engine built around Ceragon's proprietary baseband modem and RFIC chipsets. This architecture is optimized for parallel processing of multiple radio signal flows, and enables RFU-D and RFU-D-HP to multiply capacity and increase system gain in comparison with current technology.

Utilizing common processing resources at the kernel of the radio terminal, the MultiCore system reduces power consumption and maintains a small form-factor. This makes RFU-D/RFU-D-HP an advantageous choice for deployment in numerous heterogeneous network scenarios, such as small cells and fronthaul.

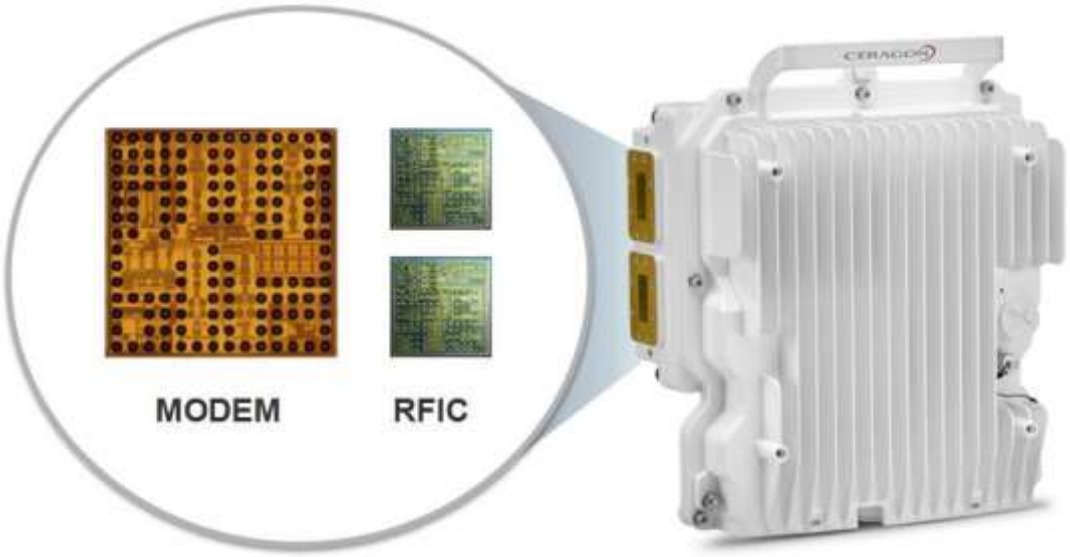


Figure 43: RFU-D/RFU-D-HP MultiCore Modem and RFIC Chipsets

RFU-D/RFU-D-HP's parallel radio processing engine is what differentiates RFU-D/RFU-D-HP from other multiple-core solutions, which are really nothing more than multiple radio systems compacted into a single box. RFU-D/RFU-D-HP's MultiCore architecture enables RFU-D/RFU-D-HP to provide significant improvements in capacity and link distance, as well as low power consumption, smaller antennas, more efficient frequency utilization, less expensive frequency use, and a small form factor.

6.1.2.1 Radio Script Configuration for Multiple Cores

When operating with two cores in a single RFU-D/RFU-D-HP RFU, users can configure different scripts independently for each carrier. Configuring a script in one core has no impact on the other carrier's traffic. When the carrier is reset following configuration of a script in that carrier, only that carrier is reset following the script's configuration. No general reset is performed.

During script configuration, the core being configured is set to mute. The mute is released once the script configuration is completed.

6.1.2.2 Flexible Operating Modes with MultiCore Architecture

RFU-D/RFU-D-HP's MultiCore architecture is inherently versatile and suitable for many different network deployment scenarios. An IP-20F node using RFU-D/RFU-D-HP can operate as a high-capacity, single-carrier solution. At any time in the network's growth cycle, the second carrier can be activated remotely for optimized performance.

To illustrate the many advantages of RFU-D/RFU-D-HP's MultiCore architecture, consider a generic, 1+0 single-carrier radio with high performance in terms of capacity, link distance, and antenna size.

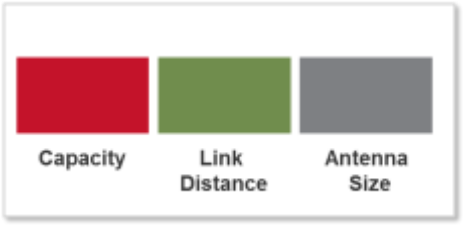


Figure 44: Performance Characteristics of Generic, 1+0 Single-Carrier Radio

RFU-D/RFU-D-HP can operate in single-carrier mode, with similar parameters to a standard radio, but with additional capacity due to its ability to operate at 4096 QAM modulation.

Activating the second carrier does not simply double the capacity of the RFU-D/RFU-D-HP, but rather, provides a package of options for improved performance that can be utilized in a number of ways, according to the requirements of the specific deployment scenario.

Doubling the Capacity

Turning on the RFU-D/RFU-D-HP 's second core automatically doubles the RFU's capacity. This doubling of capacity is achieved without affecting system gain or availability, since it results from the use of an additional core with the same modulation, Tx power, and Rx sensitivity. The RFU-D/RFU-D-HP also maintains the same small form-factor. Effectively, activating the second core provides a pure doubling of capacity without any tradeoffs.

Figure 45: Doubling RFU-D/RFU-D-HP's Capacity by Activating Second Core

Doubling the Link Distance

The increased performance that RFU-D/RFU-D-HP's MultiCore architecture provides can be leveraged to increase link distance. An IP-20F node with an RFU-D/RFU-D-HP can split the bitstream between the two cores of the RFU using Multi-Carrier Adaptive Bandwidth Control (ABC). This makes it possible to utilize a lower modulation scheme that significantly increases system gain for Tx power and Rx sensitivity. This enables the node to support longer signal spans, enabling operators to as much as double their link spans.

For example, consider an RFU-D/RFU-D-HP in a 1+0 configuration with only one core activated, transmitting 280 Mbps over a 30 MHz channel with 4096 QAM modulation. Activating the second core makes it possible to reduce the modulation to 64 QAM and maintain the same capacity of 280 Mbps, consisting of 2 x 140 Mbps over the 30 MHz channel. Reducing the modulation from 4096 QAM to 64 QAM delivers a 5 dB improvement in Tx power and an 18 dB improvement in Rx sensitivity, for a total increase of23 dB in system gain. This improved system gain enables the operator to double the link distance.

Reducing Antenna Size by Half

The increased system gain that RFU-D/RFU-D-HP's antenna size by as much as half. In general, each doubling of antenna size on one side of the link translates into 6dB in additional link budget. The 23 dB increase in system gain that RFU-D/RFU-D-HP's MultiCore architecture can provide can be exploited to halve the antenna size. This uses 12dB of the 23 dB system gain, leaving 11 dB to further reduce antenna size on either side of the link. This enables the operator to realize CAPEX savings from the MultiCore deployment.

Frequency Decongestion and Lower License Fees

Another way in which the increased system gain that RFU-D/RFU-D-HP's MultiCore architecture makes possible can be leveraged is by taking advantage of the increased system gain to shift from congested and expensive frequency bands to uncongested and less costly higher frequency bands. The loss in link budget incurred by moving to higher frequencies is absorbed by the increased system gain provided by RFU-D/RFU-D-HP's MultiCore architecture. Relatively long-span links, which previously required operation in lower, more congested, and more expensive frequencies such as 6, 7, and 8 GHz, can be shifted to higher, less congested, and less expensive frequency bands such as 11 GHz with the help of RFU-D/RFU-D-HP's MultiCore architecture.

For additional information:

- Cross Polarization Interference Canceller (XPIC)

6.1.2.3 TCO Savings as a Result of MultiCore Architecture

The various ways described above in which RFU-D/RFU-D-HP's MultiCore architecture can be leveraged to provide additional capacity, longer link distances, and smaller antenna side, all carry significant cost savings for operators.

Consider the common and practical scenario of a 1+0 link that must be upgraded to MultiCore 2+0 in order to accommodate growing demand for capacity. For a single-carrier node, the upgrade is a complicated process that requires:

- Purchasing a new radio unit.
- Sending an installation team to the site.
- Dismantling the existing radio unit.
- Replacing the single-mount radio-antenna interface with a coupler (for single polarization) or OMT (for dual polarization) to accommodate the two units.
- Re-installing the original radio unit along with the new radio unit.
- Connecting both radios to a switch in order to provide Layer 2 link aggregation (LAG), necessary to achieve a MultiCore 2+0 link.

These steps incur a high initial cost for re-installing and re-configuring the link, as well as high site leasing fees due to the additional equipment required, the larger footprint, and additional ongoing power consumption. The upgrade process involves hours of link down-time, incurring loss of revenue and impaired customer Quality of Experience (QoE) throughput the upgrade process. During its lifetime, the upgraded 2+0 single-carrier system will consume 100% more power than the 1+0 system and will be virtually twice as likely to require on-site maintenance.

With IP-20F using RFU-D/RFU-D-HP, network operators can initially install the MultiCore RFU-D/RFU-D-HP RFU in single-carrier mode, with enough network capacity to meet current needs and the ability to expand capacity on the fly in the future. When an upgrade to MultiCore 2+0 becomes necessary, the operator merely needs to perform the following steps:

- Purchase an activation key for the second core.
- Remotely upload the activation key and activate the second core.

No site visits are required, and virtually no downtime is incurred, enabling customers to enjoy continuous, uninterrupted service. No additional switch is necessary, because IP-20F can use Multi-Carrier ABC internally between the two cores to utilize the multi-channel capacity, in a much more efficient manner than with Layer 2 LAG. Network operators benefit from much lower power consumption than 2+0 systems made up of separate, single-carrier radio units, and site leasing fees do not increase since no additional hardware is required.

The following table summarizes the cost benefits of RFU-D/RFU-D-HP's MultiCore technology in terms of TCO.

Table 43: TCO Comparison Between Single-carrier and MultiCore Systems

	Single-Carrier System	**MultiCore System**
Initial Installation	1+0 link with 1+0 antenna mediation device (remote or direct mount).	2+0 installation (remote or direct mount). Only one core has an activation key and is activated.
Upgrade to 2+0	• Obtain new radio equipment • Send technical team to both ends of the link (at least two site visits). • Dismantle existing radio and mediation device. • Install new mediation device (OMT or splitter). • Re-install old radio with new radio. • Obtain and install Ethernet switch for 2+0 L2 LAG.	• Obtain activation key for second core. • Activate second core remotely. • Remotely define the link as 2+0 with L1 Multi-Carrier ABC (more efficient than LAG).
Downtime	Hours of downtime for complete reconfiguration of the link. Negative impact on end-user QoE.	Negligible downtime.
Power consumption	100% more than 1+0 link (even more with external switch).	Only 55% more power consumption than 1+0 configuration (single core).
Site leasing fees	Approximately double, since equipment is doubled.	No impact, MultiCore system within same small form factor unit
Warehouse management	Complicated, with different equipment for different deployment scenarios (standard/high power, low/high capacity).	Simple with single-spare, versatile radio for many deployment scenarios.

6.1.3 Header De-Duplication

IP-20F offers the option of Header De-Duplication, enabling operators to significantly improve Ethernet throughput over the radio link without affecting user traffic. Header De-Duplication can be configured to operate on various layers of the protocol stack, saving bandwidth by reducing unnecessary header overhead. Header De-duplication is also sometimes known as header compression.

Note:	Without Header De-Duplication, IP-20F still removes the IFG and Preamble fields. This mechanism operates automatically, even if Header De-Duplication is not selected by the user.

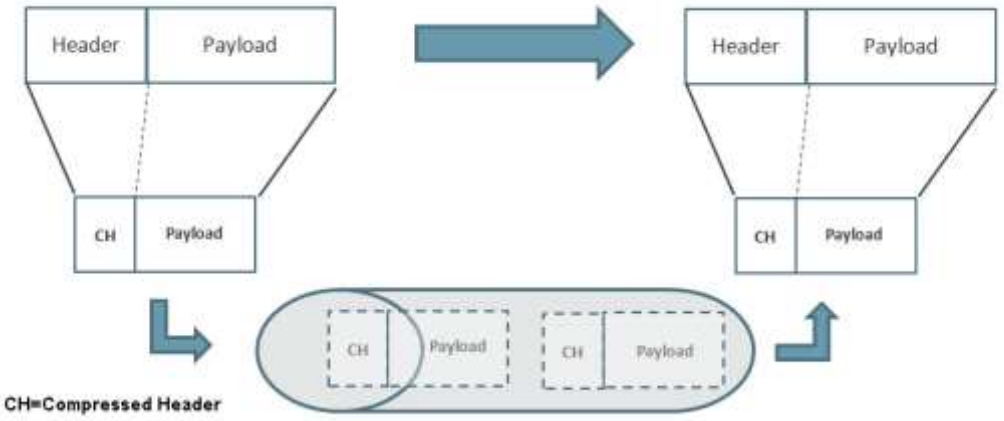


Figure 46: Header De-Duplication

Header De-Duplication identifies traffic flows and replaces the header fields with a "flow ID". This is done using a sophisticated algorithm that learns unique flows by looking for repeating frame headers in the traffic stream over the radio link and compressing them. The principle underlying this feature is that frame headers in today's networks use a long protocol stack that contains a significant amount of redundant information.

Header De-Duplication can be customized for optimal benefit according to network usage. The user can determine the layer or layers on which Header De-Duplication operates, with the following options available:

- Layer2 – Header De-Duplication operates on the Ethernet level.
- MPLS – Header De-Duplication operates on the Ethernet and MPLS levels.
- Layer3 – Header De-Duplication operates on the Ethernet and IP levels.
- Layer4 – Header De-Duplication operates on all supported layers up to Layer 4.
- Tunnel – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel layer for packets carrying GTP or GRE frames.
- Tunnel-Layer3 – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel and T-3 layers for packets carrying GTP or GRE frames.
- Tunnel-Layer4 – Header De-Duplication operates on Layer 2, Layer 3, and on the Tunnel, T-3, and T-4 layers for packets carrying GTP or GRE frames.

Operators must balance the depth of De-Duplication against the number of flows in order to ensure maximum efficiency. Up to 256 concurrent flows are supported.

The following graphic illustrates how Header De-Duplication can save up to 148 bytes per frame.

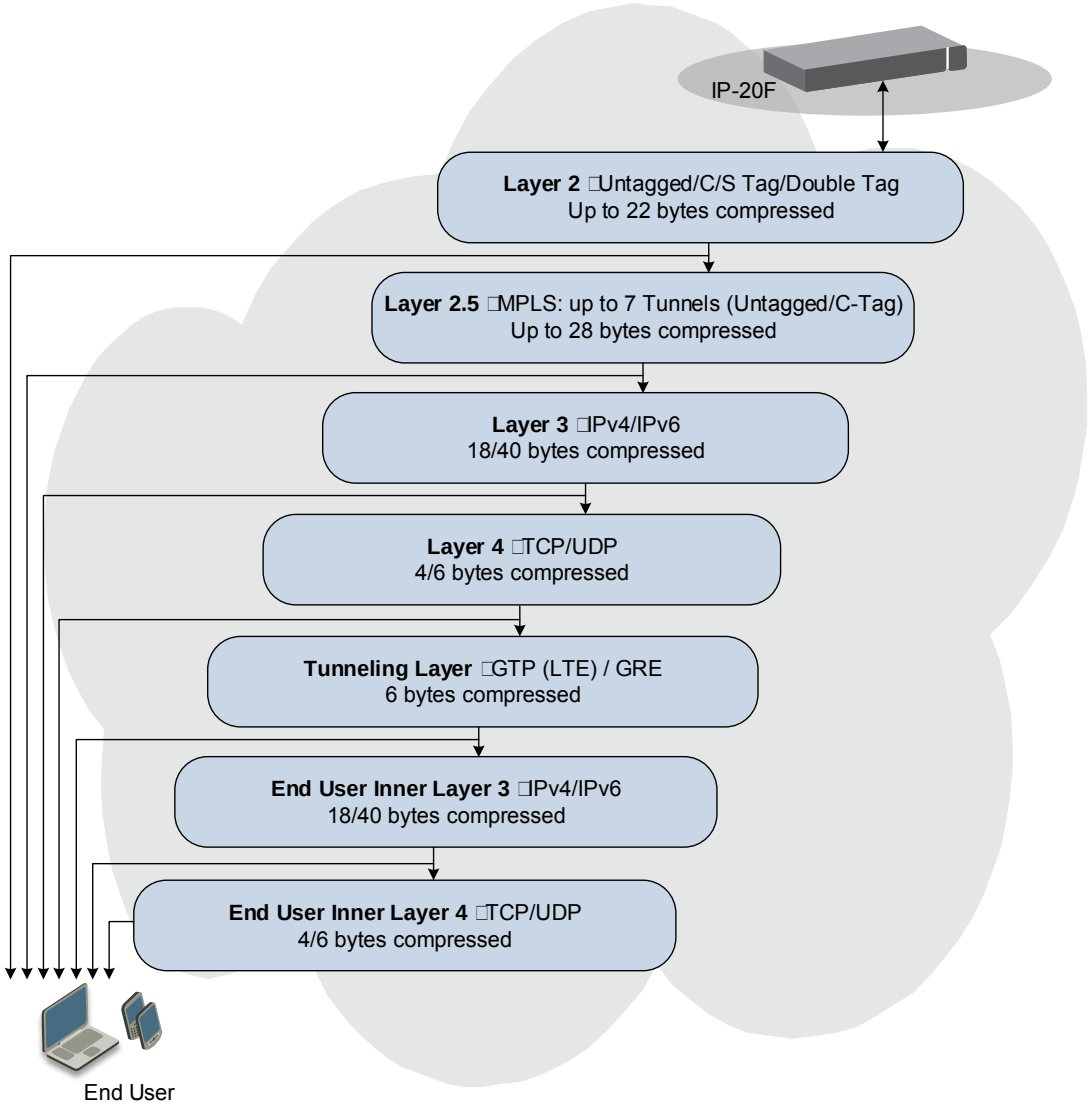


Figure 47: Header De-Duplication Potential Throughput Savings per Layer

Depending on the packet size and network topology, Header De-Duplication can increase capacity by up to:

- 50% (256 byte packets)
- 25% (512 byte packets)
- 8% (1518 byte packets)

6.1.3.1 Header De-Duplication Counters

In order to help operators optimize Header De-Duplication, IP-20F provides counters when Header De-Duplication is enabled. These counters include real-time information, such as the number of currently active flows and the number of flows by specific flow type. This information can be used by operators to monitor network usage and capacity, and optimize the Header De-Duplication settings. By monitoring the effectiveness of the Header De-Duplication settings, the operator can adjust these settings to ensure that the network achieves the highest possible effective throughput.

6.1.4 Latency

IP-20F provides best-in-class latency (RFC-2544) for all channels, making it the obvious choice for LTE (Long-Term Evolution) networks.

IP-20F's ability to meet the stringent latency requirements for LTE systems provides the key to expanded broadband wireless services:

- Longer radio chains
- Larger radio rings
- Shorter recovery times
- More capacity
- Easing of Broadband Wireless Access (BWA) limitations

6.1.5 Frame Cut-Through

Related topics:

- Egress Scheduling

Frame Cut-Through is a unique and innovative feature that ensures low latency for delay-sensitive services, such as CES, VoIP, and control protocols. With Frame Cut-Through, high-priority frames are pushed ahead of lower priority frames, even if transmission of the lower priority frames has already begun. Once the high priority frame has been transmitted, transmission of the lower priority frame is resumed with no capacity loss and no re-transmission required. This provides operators with:

- Immunity to head-of-line blocking effects – key for transporting high-priority, delay-sensitive traffic.
- Reduced delay-variation and maximum-delay over the link:
  - Reduced end-to-end delay for TDM services.
  - Improved QoE for VoIP and other streaming applications.
  - Expedited delivery of critical control frames.

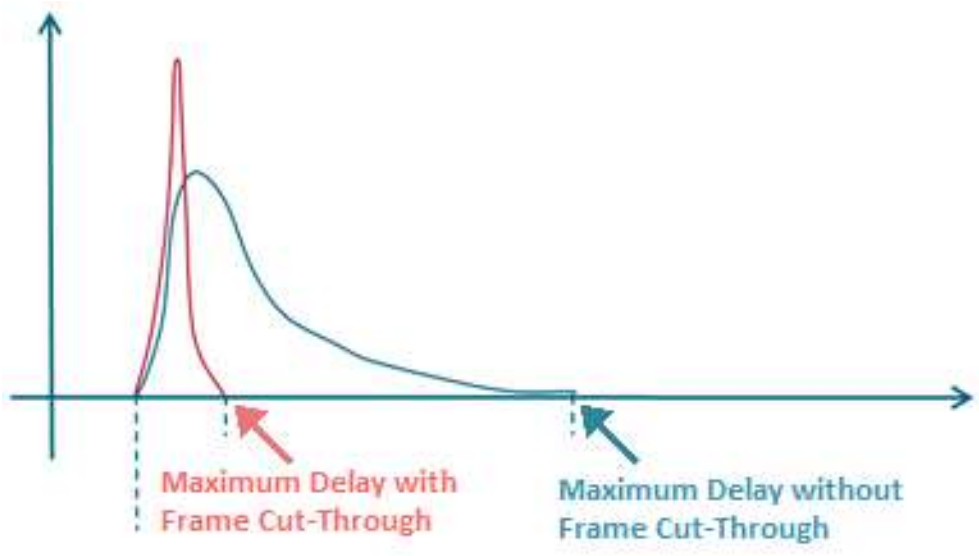


Figure 48: Propagation Delay with and without Frame Cut-Through

6.1.5.1 Frame Cut-Through Basic Operation

Using Frame Cut-Through, frames assigned to high priority queues can pre-empt frames already in transmission over the radio from other queues. Transmission of the preempted frames is resumed after the cut-through with no capacity loss or re-transmission required. This feature provides services that are sensitive to delay and delay variation, such as VoIP and Pseudowires, with true transparency to lower priority services, by enabling the transmission of a high-priority, low-delay traffic stream.

Figure 49: Frame Cut-Through

When enabled, Frame Cut-Through applies to all the high priority frames, i.e., all frames that are classified to a CoS queue with 4th (highest) priority.

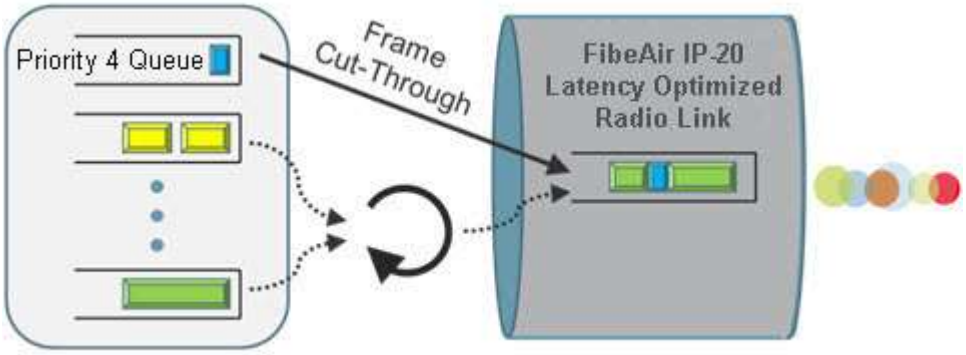


Figure 50: Frame Cut-Through Operation

6.2 Radio Features

This chapter describes the main IP-20F radio features.

Multi-Carrier ABC enables separate radio carriers to be shared by a single Ethernet port. This provides an Ethernet link over the radio with multiple capacity, while still behaving as a single Ethernet interface.

Ceragon was the first to introduce hitless and errorless Adaptive Coding Modulation (ACM) to provide dynamic adjustment of the radio's modulation. ACM shifts modulations instantaneously in response to changes in fading conditions. IP-20F utilizes Ceragon's advanced ACM technology, and extends it to the range of BPSK to 4096 QAM.

IP-20F also supports Cross Polarization Interference Canceller (XPIC). XPIC enables operators to double their capacity by utilizing dual-polarization radio over a single-frequency channel, thereby transmitting two separate carrier waves over the same frequency, but with alternating polarities.

The MultiCore RFU-D and RFU-D-HP support multiple-carrier features such as Multi-Carrier ABC and XPIC with a single MultiCore RFU, utilizing both carriers in the RFU.

This section includes:

- Multi-Carrier Adaptive Bandwidth Control (MC-ABC)
- HSB Radio Protection
- Adaptive Coding Modulation (ACM)
- Cross Polarization Interference Canceller (XPIC)
- ATPC
- Radio Signal Quality PMs
- Radio Utilization PMs

6.2.1 Multi-Carrier Adaptive Bandwidth Control (MC-ABC)

Multi-Carrier Adaptive Bandwidth Control (MC-ABC) is an innovative technology that creates logical bundles of multiple radio links optimized for wireless backhaul applications. Multi-Carrier ABC enables separate radio carriers to be combined into a virtual transport pipe for a high capacity Ethernet link and individual TDM links. Both the Ethernet link and the TDM links will be available over radios with individual variable capacity, and handled by a prioritizing scheme.

In Hybrid Multi-Carrier ABC mode, traffic is split over the available carriers optimally at the radio frame level irrespectively of the traffic type.

For Ethernet traffic, Hybrid MC-ABC eliminates the need for Ethernet link aggregation (LAG). Load balancing is performed regardless of the number of MAC addresses or number of traffic flows.

During fading events which cause ACM modulation changes, each carrier fluctuates independently with hitless switchovers between modulations, increasing capacity over a given bandwidth and maximizing spectrum utilization. In such conditions, the TDM links can be preserved by a sophisticated prioritizing scheme configured by the user. The result is 100% utilization of radio resources in which traffic load is balanced based on instantaneous radio capacity per carrier.

The following diagram illustrates the Multi-Carrier ABC traffic flow.

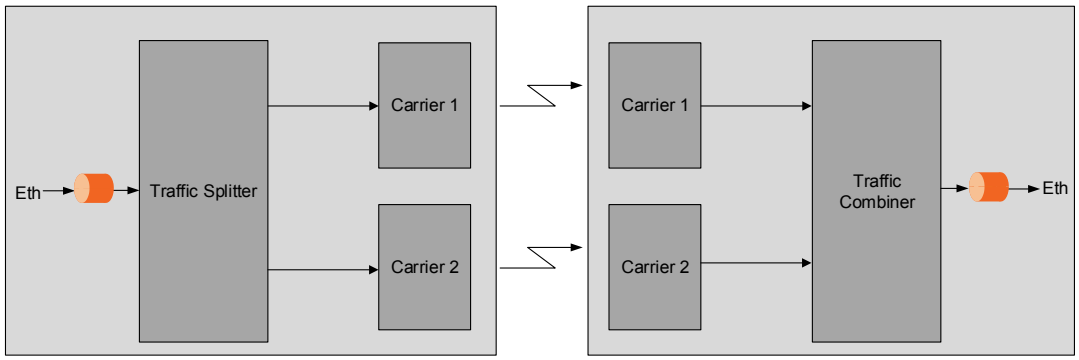


Figure 51: Multi-Carrier ABC Traffic Flow

IP-20F supports Multi-Carrier ABC with RFU-D and RFU-D-HP.

6.2.1.1 Multi-Carrier Configurations

In CeraOS 10.7, IP-20F supports up to two 2+0 Multi-Carrier ABC configurations, each utilizing the two carriers of a MultiCore RFU-D or RFU-D-HP. Multi-Carrier ABC configurations can be used with RFU1 and RFU2.

In addition, support is planned for the following configurations:

- 1+1 HSB
- 2+2 HSB

6.2.1.2 Multi-Carrier ABC Operation

The MC-ABC engine divides the data flows into blocks of data. Each radio carrier is assigned blocks at a rate which is based on the ACM profile of the carrier. Once the ACM profile of a carrier changes, the rate at which the data blocks are delivered to this carrier changes. The higher the ACM profile of a certain carrier, the higher the block rate assigned to this carrier.

On the receiving side of the link, all blocks are synchronized, meaning that blocks are delayed based on the last arriving block. The latency of the aggregated data flow is determined by the slowest arriving block.

A low ACM profile means more latency compared to a higher ACM profile. When all channels run the same radio script, the latency variation for the aggregated data stream is determined by the latency variation of one radio channel. This latency variation is slightly more complicated to predict when the radio carriers runs at different radio scripts, since each radio script has a unique delay distribution. Multi-Carrier ABC can tolerate a large delay variance between the slowest and the fastest arriving blocks.

6.2.1.3 Graceful Degradation of Service

Multi-Carrier ABC provides graceful degradation and protection of service in the event of RFU failure or carrier fading. In the case of carrier fading, the system reduces the number of data blocks assigned to this carrier, until the carrier losses the connection with the other end of the link. In this case, no data blocks will be assigned to this carrier. In case of sudden hardware failure, only data in data blocks that have already been transferred to the radio will be lost. Once the carrier is lost, the system will stop assigning data blocks to this carrier.

The system determines which radio carriers contribute to the aggregated MC-ABC link, based on the received channel qualities. Other criteria, such as ACM profile and latency, are also considered. Adding or removing a carrier is hitless.

When all carriers are up and running, MC-ABC provides the maximum available aggregated capacity. Even when one or more carriers are operating at limited capacity or are totally down, the data path remains error free. In the event of degradation in a particular carrier, the carrier is removed from the aggregated link before bit errors occur, so the aggregated data flow is hitless.

6.2.1.4 Multi-Carrier ABC Minimum Bandwidth Override Option

A Multi-Carrier ABC group can be configured to be placed in Down state if the group's aggregated capacity falls beneath a user-defined threshold. This option is used in conjunction with the LAG override option (see *Link Aggregation Groups (LAG) and LACP* on page 160) in cases where the operator wants traffic from an upstream switch connected to another IP-20 unit to be re-routed whenever the link is providing less than a certain capacity.

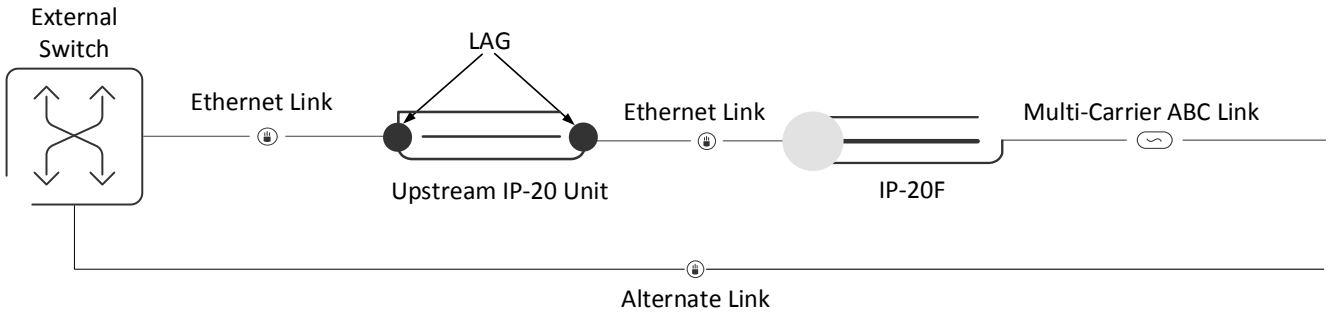


Figure 52: Multi-Carrier ABC Minimum Bandwidth Override

By default, the Multi-Carrier ABC minimum bandwidth override option is disabled. When enabled, the Multi-Carrier ABC group is automatically placed in a Down state in the event that the group's aggregated capacity falls beneath the user-configured threshold. The group is returned to an Up state when the capacity goes above the threshold.

6.2.1.5 Multi-Carrier ABC and ACM

Multi-Carrier ABC automatically adapts to capacity changes that result from changes in the current ACM profile. When an ACM profile change takes place on a specific carrier, MC-ABC responds by changing the block size of that channel. The process of changing the block size is performed dynamically and is hitless. Since the ACM profile changes are also hitless, the overall Multi-Carrier ABC traffic is hitless.

6.2.1.6 Frequency Diversity

In Hybrid Multi-Carrier ABC mode, traffic is split over the available carriers optimally at the radio frame level irrespective of the traffic type. When using 2+0 MC-ABC, the link provides Frequency Diversity protection while having several advantages over standard 1+1 Frequency Diversity configurations:

- Higher traffic resiliency in a fading environment.

  With a 1+1 FD link, throughput is limited by the link with the lowest modulation. With 2+0 MC-ABC, the traffic is aggregated over the two carriers.
- Higher available capacity (combined capacity of the two carriers)
- Additional link resiliency when using Space Diversity (IFC) for each of the carriers

6.2.2 HSB Radio Protection

Note: HSB radio protection is planned for future release.

IP-20F offers radio redundancy via 1+1 and 2+2 HSB protection. 1+1 and 2+2 HSB protection provides full protection in the event of interface, signal, or RFU failure.

2+2 HSB with Multi-Carrier ABC is also supported with optional XPIC.

The interfaces in a protected pair operate in active and standby mode. If there is a failure in the active radio interface or RFU, the standby interface and RFU pair switches to active mode.

Each carrier in a protected pair reports its status to the CPU. The CPU is responsible for determining when a switchover takes place.

In a 1+1 or 2+2 HSB configuration, the RFUs must be the same type and must have the same configuration.

IP-20F includes a mismatch mechanism that detects if there is a mismatch between the radio configurations of the local and mate interfaces and RFUs. This mechanism is activated by the system periodically and independently of other protection mechanisms, at fixed intervals. It is activated asynchronously for both the active and the standby carriers. Once the mismatch mechanism detects a configuration mismatch, it raises a Mate Configuration Mismatch alarm. When the configuration of the active and standby carriers is changed to be identical, the mechanism clears the Mate Configuration Mismatch alarm.

In order to align the configuration between the active and standby carriers, the user must first complete the required configuration of the active radio interface, and then perform a copy to mate command. This command copies the entire configuration of the active interface to the standby interface to achieve full configuration alignment between the active and standby carriers.

When a pair of carriers is defined as a 1+1 HSB pair, any configuration performed on the active carrier will be automatically copied to the standby carrier, in order to maintain the carrier configuration alignment. This makes it unnecessary to perform a copy-to-mate command when a configuration change is made.

6.2.2.1 Revertive HSB Protection

In an HSB protection scheme, the active and standby radios are usually connected to the antenna with an asymmetric coupler. This causes a 6dB loss on one of the radios on each side of the link, which may result (depending on the active/standby status of each radio) in up to12dB total path loss for the link. This additional path loss will either reduce link fade margin or increase the power consumption of the Power Amplifier (PA) in order to compensate for the additional path loss.

Revertive HSB protection ensures that the radios with no loss are active as long as no failures are present, resulting in the best possible link budget (0 dB loss).

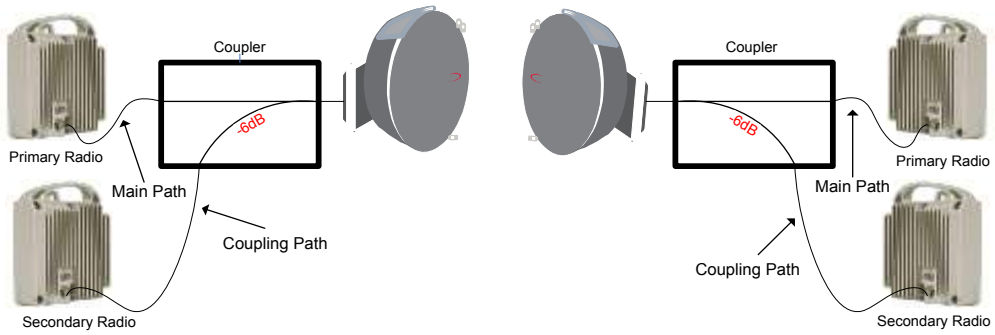


Figure 53: Path Loss on Secondary Path of 1+1 HSB Protection Link

IP-20F supports revertive HSB protection for both 1+1 and 2+2 HSB configurations. In revertive HSB protection mode, user defines the primary radio on each side of the link. The primary radio should be the radio on the coupler's main path and the secondary radio should be the radio on the coupling path.

The system monitors the availability of the primary path at all times. Whenever the primary path is operational and available, without any alarms, but the secondary path is active, a ten-minute timer is activated. If the primary path remains operational and available for ten minutes, the system initiates a revertive protection switch. Every revertive protection switch is recorded as an event in the event log.

Note: Each protection switch causes traffic disruption.

6.2.2.2 Switchover Triggers

The following events trigger switchover for 1+1 HSB protection according to their priority, with the highest priority triggers listed first.

1 Hardware module missing
2 Lockout
3 Force switch
4 Traffic failures
5 Manual switch

6.2.3 Adaptive Coding Modulation (ACM)

This feature requires:

- ACM script

Related topics:

- Cross Polarization Interference Canceller (XPIC)
- Quality of Service (QoS)

FibeAir IP-20F employs full-range dynamic ACM. IP-20F's ACM mechanism copes with 90 dB per second fading in order to ensure high transmission quality. IP-20F's ACM mechanism is designed to work with IP-20F's QoS mechanism to ensure that high priority voice and data frames are never dropped, thus maintaining even the most stringent service level agreements (SLAs).

The hitless and errorless functionality of IP-20F's ACM has another major advantage in that it ensures that TCP/IP sessions do not time-out. Without ACM, even interruptions as short as 50 milliseconds can lead to timeout of TCP/IP sessions, which are followed by a drastic throughout decrease while these sessions recover.

6.2.3.1 Up to 13 Working Points

IP-20F implements ACM with 13 available working points.

Table 44: ACM Working Points (Profiles)

Working Point (Profile)	Modulation
Profile 0	BPSK
Profile 1	QPSK
Profile 2	8 PSK
Profile 3	16 QAM
Profile 4	32 QAM
Profile 5	64 QAM
Profile 6	128 QAM
Profile 7	256 QAM
Profile 8	512 QAM
Profile 9	1024 QAM (Strong FEC)
Profile 10	1024 QAM (Light FEC)
Profile 11	2048 QAM
Profile 12	4096 QAM

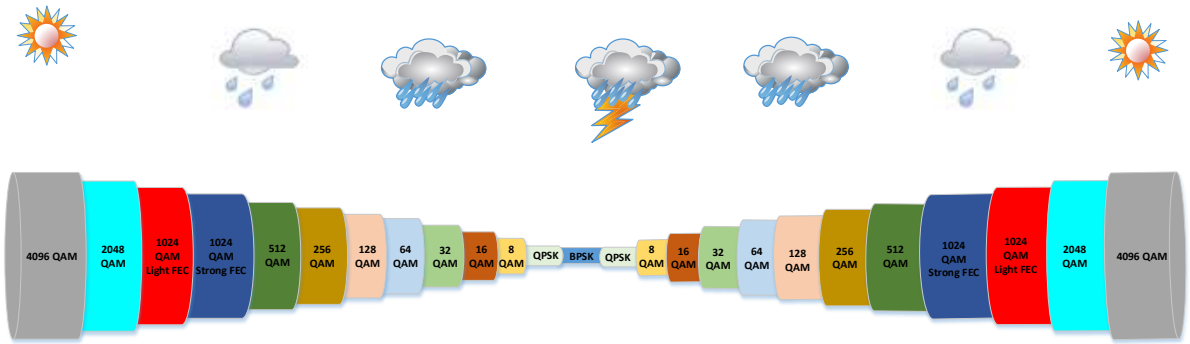


Figure 54: Adaptive Coding and Modulation with 13 Working Points

6.2.3.2 Hitless and Errorless Step-by Step Adjustments

ACM works as follows. Assuming a system configured for 128 QAM with ~170 Mbps capacity over a 30 MHz channel, when the receive signal Bit Error Ratio (BER) level reaches a predetermined threshold, the system preemptively switches to 64 QAM and the throughput is stepped down to ~140 Mbps. This is an errorless, virtually instantaneous switch. The system continues to operate at 64 QAM until the fading condition either intensifies or disappears. If the fade intensifies, another switch takes the system down to 32 QAM. If, on the other hand, the weather condition improves, the modulation is switched back to the next higher step (e.g., 128 QAM) and so on, step by step. The switching continues automatically and as quickly as needed, and can reach all the way down to QPSK during extreme conditions.

6.2.3.3 ACM Radio Scripts

An ACM radio script is constructed of a set of profiles. Each profile is defined by a modulation order (QAM) and coding rate, and defines the profile's capacity (bps). When an ACM script is activated, the system automatically chooses which profile to use according to the channel fading conditions.

The ACM TX profile can be different from the ACM RX profile.

The ACM TX profile is determined by remote RX MSE performance. The RX end is the one that initiates an ACM profile upgrade or downgrade. When MSE improves above a predefined threshold, RX generates a request to the remote TX to upgrade its profile. If MSE degrades below a predefined threshold, RX generates a request to the remote TX to downgrade its profile.

ACM profiles are decreased or increased in an errorless operation, without affecting traffic.

For ACM to be active, the ACM script must be run in Adaptive mode. In this mode, the ACM engine is running, which means that the radio adapts its profile according to the channel fading conditions. Adaptive mode requires an ACM activation key.

Users also have the option of running an ACM script in Fixed mode. In this mode, ACM is not active. Instead, the user can select the specific profile from all available profiles in the script. The selected profile is the only profile that will be valid, and the ACM engine will be forced to be OFF. This mode can be chosen without an ACM activation key.

In the case of XPIC/ACM scripts, all the required conditions for XPIC apply.

The user can define a minimum and maximum profile. For example, if the user selects a maximum profile of 5, the system will not climb above the profile 5, even if channel fading conditions allow it.

6.2.3.4 ACM Benefits

The advantages of IP-20F's dynamic ACM include:

- Maximized spectrum usage
- Increased capacity over a given bandwidth
- 13 modulation/coding work points (~3 db system gain for each point change)
- Hitless and errorless modulation/coding changes, based on signal quality
- Adaptive Radio Tx Power per modulation for maximal system gain per working point
- An integrated QoS mechanism that enables intelligent congestion management to ensure that high priority traffic is not affected during link fading

6.2.3.5 ACM and Built-In QoS

IP-20F's ACM mechanism is designed to work with IP-20F's QoS mechanism to ensure that high priority voice and data frames are never dropped, thus maintaining even the most stringent SLAs. Since QoS provides priority support for different classes of service, according to a wide range of criteria, you can configure IP-20F to discard only low priority frames as conditions deteriorate.

If you want to rely on an external switch's QoS, ACM can work with them via the flow control mechanism supported in the radio.

6.2.3.6 ACM and 1+1 HSB

When ACM is activated together with 1+1 HSB protection, it is essential to feed the active RFU via the main channel of the coupler (lossless channel), and to feed the standby RFU via the secondary channel of the coupler (-6db attenuated channel). This maximizes system gain and optimizes ACM behavior for the following reasons:

- In the TX direction, the power will experience minimal attenuation.
- In the RX direction, the received signal will be minimally attenuated. Thus, the receiver will be able to lock on a higher ACM profile (according to what is dictated by the RF channel conditions).

The following ACM behavior should be expected in a 1+1 or 2+2 configuration:

- In the TX direction, the Active TX will follow the remote Active RX ACM requests (according to the remote Active Rx MSE performance).
- The Standby TX might have the same profile as the Active TX, or might stay at the lowest profile (profile-0). That depends on whether the Standby TX was able to follow the remote RX Active unit's ACM requests (only the active remote RX sends ACM request messages).
- In the RX direction, both the active and the standby carriers follow the remote Active TX profile (which is the only active transmitter).

6.2.3.7 ACM with Adaptive Transmit Power

This feature requires:

- ACM script

ACM with Adaptive Transmit Power enables operators to benefit from the higher transmit power of the radios when fading conditions occur while at the same time benefiting from lower power consumption when the high transmit power is not required.

When planning ACM-based radio links, the radio planner attempts to apply the lowest transmit power that will perform satisfactorily at the highest level of modulation. During fade conditions requiring a modulation drop, most radio systems cannot increase transmit power to compensate for the signal degradation, resulting in a deeper reduction in capacity. IP-20F is capable of adjusting the transmit power on the fly, and optimizing the available capacity at every modulation point.

The following figure contrasts the transmit output power achieved by using ACM with Adaptive Power to the transmit output power at a fixed power level, over an 18-23 GHz link. This figure shows how without Adaptive Transmit Power, operators that want to use ACM to benefit from high levels of modulation (e.g., 2048 QAM) must settle for low system gain, in this case, 16 dB, for all the other modulations as well. In contrast, with IP-20F's Adaptive Transmit Power feature, operators can automatically adjust power levels, achieving the extra system gain that is required to maintain optimal throughput levels under all conditions.

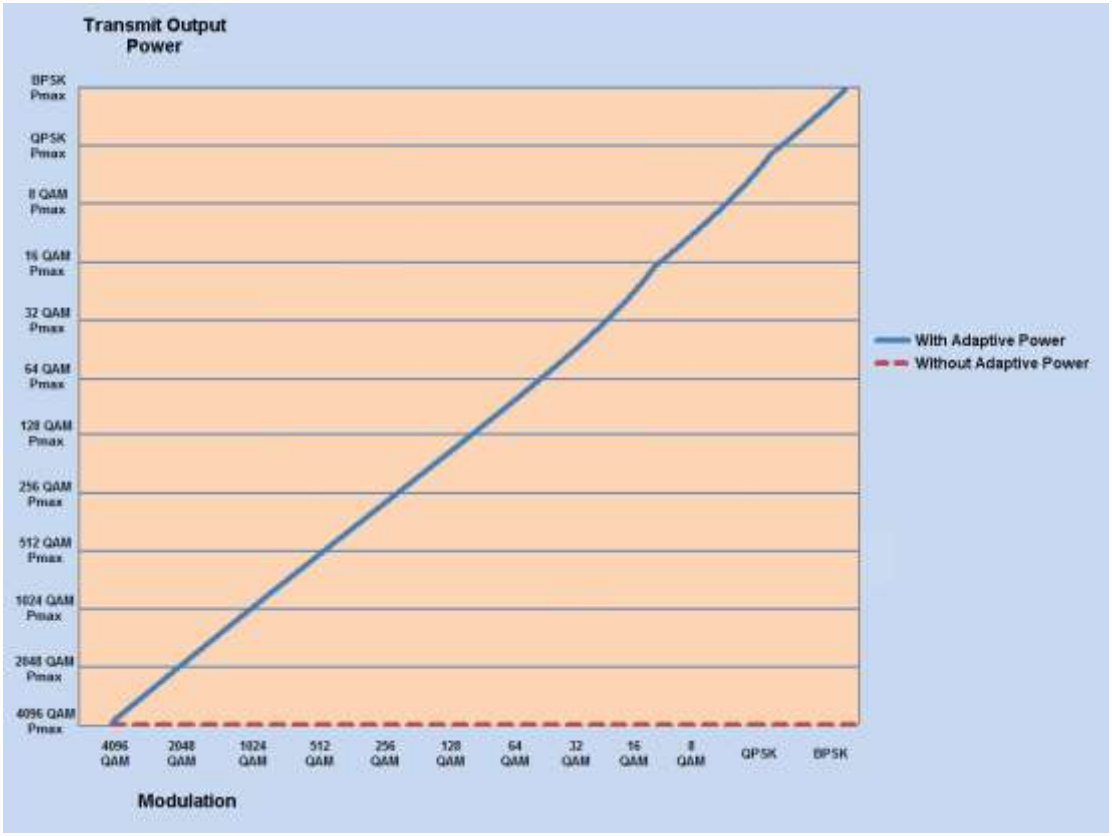


Figure 55: ACM with Adaptive Power Contrasted to Other ACM Implementations

6.2.4 Cross Polarization Interference Canceller (XPIC)

This feature requires:

- 2+0/2+2 configuration
- XPIC script

XPIC is one of the best ways to break the barriers of spectral efficiency. Using dual-polarization radio over a single-frequency channel, a dual polarization radio transmits two separate carrier waves over the same frequency, but using alternating polarities. Despite the obvious advantages of dual-polarization, one must also keep in mind that typical antennas cannot completely isolate the two polarizations. In addition, propagation effects such as rain can cause polarization rotation, making cross-polarization interference unavoidable.

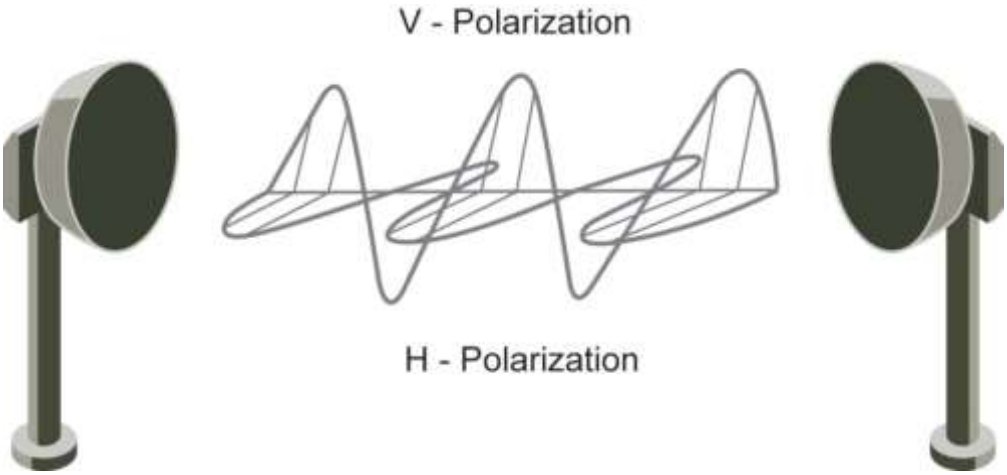


Figure 56: Dual Polarization

The relative level of interference is referred to as cross-polarization discrimination (XPD). While lower spectral efficiency systems (with low SNR requirements such as QPSK) can easily tolerate such interference, higher modulation schemes cannot and require XPIC. IP-20F's XPIC algorithm enables detection of both streams even under the worst levels of XPD such as 10 dB. IP-20F accomplishes this by adaptively subtracting from each carrier the interfering cross carrier, at the right phase and level. For high-modulation schemes such as 2048 QAM, operating at a frequency of 28 GHz, an improvement factor of more than 20 dB is required so that cross-interference does not adversely affect performance.

XPIC is supported with MultiCore RFUs only (RFU-D and RFU-D-HP), using the two carriers in a single RFU as the XPIC pair.

6.2.4.1 XPIC Benefits

The advantages of FibeAir IP-20F's XPIC option include BER of 10e-6 at a co-channel sensitivity of 5 dB.

6.2.4.2 XPIC Implementation

The XPIC mechanism utilizes the received signals from the V and H modems to extract the V and H signals and cancel the cross polarization interference due to physical signal leakage between V and H polarizations.

The following figure is a basic graphic representation of the signals involved in this process.

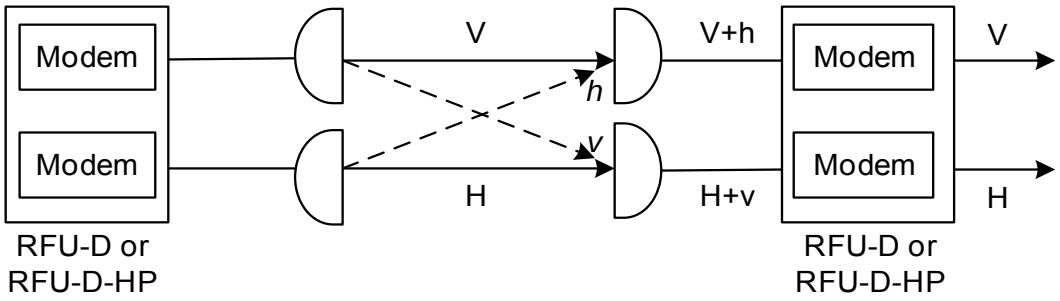


Figure 57: XPIC Implementation

The H+v signal is the combination of the desired signal H (horizontal) and the interfering signal V (in lower case, to denote that it is the interfering signal). The same happens with the vertical (V) signal reception= V+h. The XPIC mechanism uses the received signals from both feeds and, manipulates them to produce the desired data.

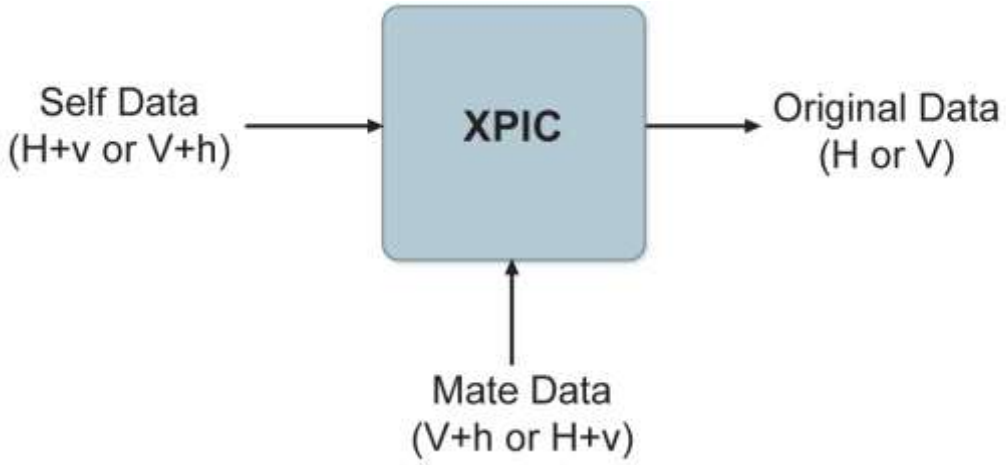


Figure 58: XPIC – Impact of Misalignments and Channel Degradation

IP-20F's XPIC reaches a BER of 10e-6 at a co-channel sensitivity of 5 dB. The improvement factor in an XPIC system is defined as the SNR@threshold of 10e-6, with or without the XPIC mechanism.

6.2.4.3 XPIC Recovery Mechanism

The XPIC mechanism is based on signal cancellation and assumes that both transmitted signals are received (with a degree of polarity separation). If for some reason, such as hardware failure, one of the carriers stops receiving a signal, the working carrier may be negatively affected by the received signals, which cannot be canceled in this condition.

The purpose of the XPIC recovery mechanism is to preserve the working link while attempting to recover the faulty polarization.

The mechanism works as follows:

- The recovery mechanism is automatically activated when the unit detects that one carrier is down (RFU power failure, carrier drawer extraction, carrier reset, etc.). When activated, the system switches to “Single Carrier” state.
- The recovery mechanism causes the remote transmitter of the faulty carrier to mute, thus eliminating the disturbing signal and preserving the working link.
- As soon as the failed carrier goes back into service, the XPIC recovery mechanism adds it back and XPIC operation resumes with both carriers.

The XPIC recovery mechanism is enabled by default, and cannot be disabled by the user.

6.2.4.4 Conditions for XPIC

XPIC is enabled by selecting an XPIC script for each carrier. In order for XPIC to be operational, all the following conditions must be met:

- The frequency of both radios must be equal.
- 1+1 HSB protection must not be enabled.
- The same script must be loaded for both carriers.
- The script must support XPIC

If any of these conditions is not met, an alarm will alert the user. In addition, events will inform the user which conditions are not met.

6.2.5 ATPC

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link.

ATPC enables the transmitter to operate at less than maximum power for most of the time. When fading conditions occur, TX power is increased as needed until the maximum is reached.

The ATPC mechanism has several potential advantages, including less power consumption and longer amplifier component life, thereby reducing overall system cost.

ATPC is frequently used as a means to mitigate frequency interference issues with the environment, thus allowing new radio links to be easily coordinated in frequency congested areas.

6.2.5.1 ATPC Override Timer

This feature complies with NSMA Recommendation WG 18.91.032. With ATPC enabled, if the radio automatically increases its TX power up to the configured maximum it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

To minimize interference, IP-20F provides an ATPC override mechanism. When ATPC override is enabled, a timer begins when ATPC raises the TX power to its maximum. When the timer expires, the ATPC maximum TX power is overridden by the user-configured ATPC override TX power level until the user manually cancels the ATPC override. The unit then returns to normal ATPC operation.

The following parameters can be configured:

- **ATPC Override Admin** – Determines whether the ATPC override mechanism is enabled.
- **Override TX Level** – The TX power, in dBm, used when the unit is in an ATPC override state.
- **Override Timeout** – The amount of time, in seconds, the timer counts from the moment the radio reaches its maximum configured TX power until ATPC override goes into effect.

When the radio enters ATPC override state, the radio transmits no higher than the pre-determined ATPC override TX level, and an ATPC override alarm is raised. The radio remains in ATPC override state until the ATPC override state is manually cancelled by the user (or the unit is reset).

In a configuration with unit redundancy or radio protection, the ATPC override state is propagated to the standby unit or radio in the event of switchover.

Note:	When canceling an ATPC override state, the user should ensure that the underlying problem has been corrected. Otherwise, ATPC may be overridden again.

6.2.6 Radio Signal Quality PMs

IP-20F supports the following radio signal quality PMs. For each of these PM types, users can display the minimum and maximum values, per radio, for every 15-minute interval. Users can also define thresholds and display the number of seconds during which the radio was not within the defined threshold.

- RSL (users can define two RSL thresholds)
- TSL
- MSE
- XPI

Users can display BER PMs, including the current BER per radio, and define thresholds for Excessive BER and Signal Degrade BER. Alarms are issued if these thresholds are exceeded. See *Configurable BER Threshold Alarms and Traps* on page 247. Users can also configure an alarm that is raised if the RSL falls beneath a user-defined threshold. See *RSL Threshold Alarm* on page 247.

6.2.7 Radio Utilization PMs

IP-20F supports the following counters, as well as additional PMs based on these counters:

- Radio Traffic Utilization – Measures the percentage of radio capacity utilization, and used to generate the following PMs for every 15-minute interval:
  - Peak Utilization (%)
  - Average Utilization (%)
  - Over-Threshold Utilization (seconds). The utilization threshold can be defined by the user (0-100%).
- Radio Traffic Throughput – Measures the total effective Layer 2 traffic sent through the radio (Mbps), and used to generate the following PMs for every 15-minute interval:
  - Peak Throughput
  - Average Throughput
  - Over-Threshold Utilization (seconds). The threshold is defined as 0.
- Radio Traffic Capacity – Measures the total L1 bandwidth (payload plus overheads) sent through the radio (Mbps), and used to generate the following PMs for every 15-minute interval:
  - Peak Capacity
  - Average Capacity
  - Over-Threshold Utilization (seconds). The threshold is defined as 0.
- Frame Error Rate – Measures the frame error rate (%), and used to generate Frame Error Rate PMs for every 15-minute interval.

6.3 Ethernet Features

IP-20F features a service-oriented Ethernet switching fabric. The number of Ethernet interfaces is scalable, with a minimum of five GbE combo interfaces (optical or electrical) and two FE interfaces for management.

IP-20F's service-oriented Ethernet paradigm enables operators to configure VLAN definition, CoS, security, and network resiliency on a service, service-point, and interface level.

IP-20F provides personalized and granular QoS that enables operators to customize traffic management parameters per customer, application, service type, or in any other way that reflects the operator's business and network requirements.

This section includes:

- Ethernet Services Overview
- IP-20F's Ethernet Capabilities
- Supported Standards
- Ethernet Service Model
- Ethernet Interfaces
- Quality of Service (QoS)
- Global Switch Configuration
- Automatic State Propagation and Link Loss Forwarding
- Network Resiliency
- OAM

6.3.1 Ethernet Services Overview

The IP-20F services model is premised on supporting the standard MEF services (MEF 6, 10), and builds upon this support by the use of very high granularity and flexibility. Operationally, the IP-20F Ethernet services model is designed to offer a rich feature set combined with simple and user-friendly configuration, enabling users to plan, activate, and maintain any packet-based network scenario.

This section first describes the basic Ethernet services model as it is defined by the MEF, then goes on to provide a basic overview of IP-20F's Ethernet services implementation.

The following figure illustrates the basic MEF Ethernet services model.

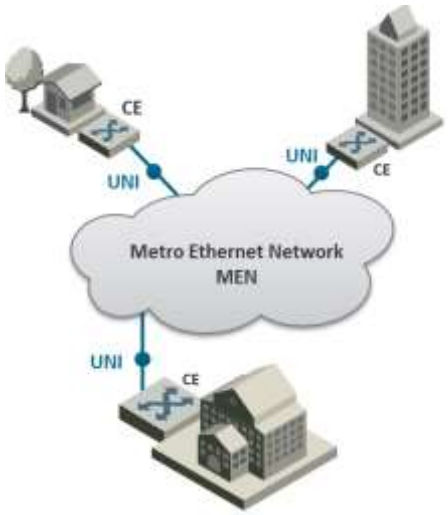


Figure 59: Basic Ethernet Service Model

In this illustration, the Ethernet service is conveyed by the Metro Ethernet Network (MEN) provider. Customer Equipment (CE) is connected to the network at the User Network Interface (UNI) using a standard Ethernet interface (10/100 Mbps, 1 Gbps). The CE may be a router, bridge/switch, or host (end system). A NI is defined as the demarcation point between the customer (subscriber) and provider network, with a standard IEEE 802.3 Ethernet PHY and MAC.

The services are defined from the point of view of the network's subscribers (users). Ethernet services can be supported over a variety of transport technologies and protocols in the MEN, such as SDH, Ethernet, ATM, MPLS, and GFP. However, from the user's perspective, the network connection at the user side of the UNI is only Ethernet.

6.3.1.1 EVC

Subscriber services extend from UNI to UNI. Connectivity between UNIs is defined as an Ethernet Virtual Connection (EVC), as shown in the following figure.

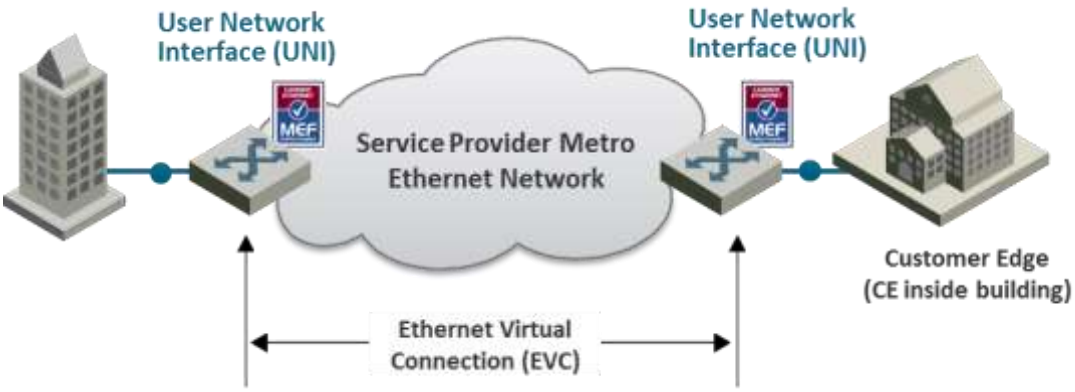


Figure 60: Ethernet Virtual Connection (EVC)

An EVC is defined by the MEF as an association of two or more UNIs that limits the exchange of service frames to UNIs in the Ethernet Virtual Connection. The EVC perform two main functions:

- Connects two or more customer sites (UNIs), enabling the transfer of Ethernet frames between them.
- Prevents data transfer involving customer sites that are not part of the same EVC. This feature enables the EVC to maintain a secure and private data channel.

A single UNI can support multiple EVCs via the Service Multiplexing attribute. An ingress service frame that is mapped to the EVC can be delivered to one or more of the UNIs in the EVC, other than the ingress UNI. It is vital to avoid delivery back to the ingress UNI, and to avoid delivery to a UNI that does not belong to the EVC. An EVC is always bi-directional in the sense that ingress service frames can originate at any UNI in an EVC.

Service frames must be delivered with the same Ethernet MAC address and frame structure that they had upon ingress to the service. In other words, the frame must be unchanged from source to destination, in contrast to routing in which headers are discarded. Based on these characteristics, an EVC can be used to form a Layer 2 private line or Virtual Private Network (VPN).

One or more VLANs can be mapped (bundled) to a single EVC.

The MEF has defined three types of EVCs:

1 Point **to Point EVC** – Each EVC contains exactly two UNIs. The following figure shows two point-to-point EVCs connecting one site to two other sites.

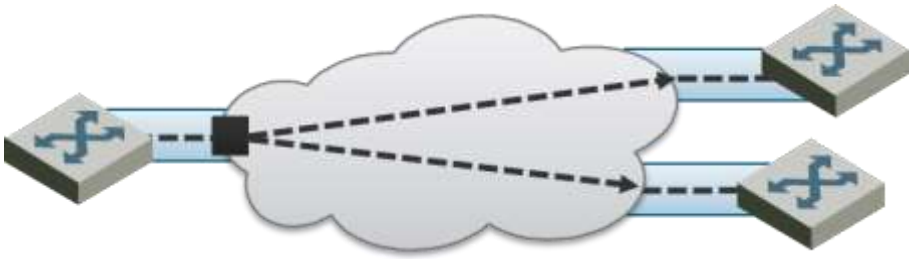


Figure 61: Point to Point EVC

2 **Multipoint (Multipoint-to-Multipoint) EVC** – Each EVC contains two or more UNIs. In the figure below, three sites belong to a single Multipoint EVC and can forward Ethernet frames to each other.

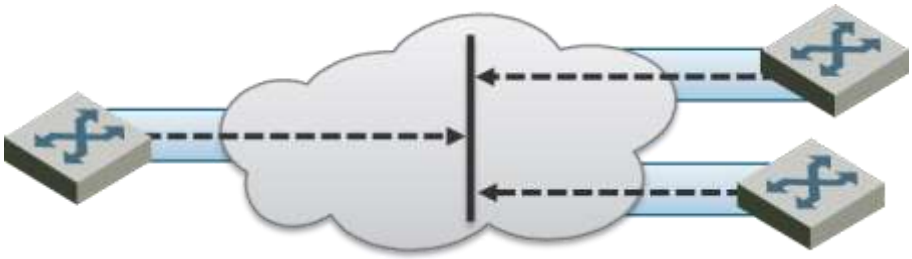


Figure 62: Multipoint to Multipoint EVC

3 **Rooted Multipoint EVC** (Point-to-Multipoint) – Each EVC contains one or more UNIs, with one or more UNIs defined as Roots, and the others defined as Leaves. The Roots can forward frames to the Leaves. Leaves can only forward frames to the Roots, but not to other Leaves.

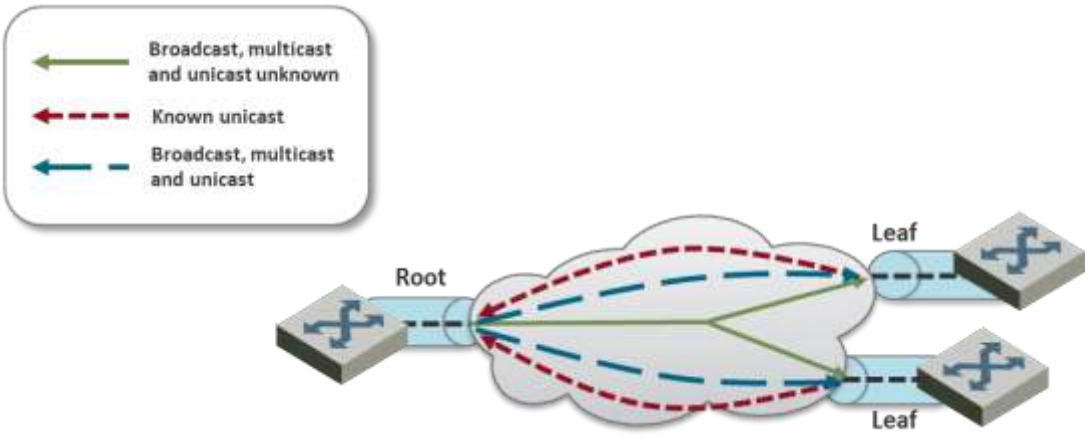


Figure 63: Rooted Multipoint EVC

In the IP-20F, an EVC is defined by either a VLAN or by Layer 1 connectivity (Pipe Mode).

6.3.1.2 Bandwidth Profile

The bandwidth profile (BW profile) is a set of traffic parameters that define the maximum limits of the customer's traffic.

At ingress, the bandwidth profile limits the traffic transmitted into the network:

- Each service frame is checked against the profile for compliance with the profile.
- Bandwidth profiles can be defined separately for each UNI (MEF 10.2).
- Service frames that comply with the bandwidth profile are forwarded.
- Service frames that do not comply with the bandwidth profile are dropped at the ingress interface.

The MEF has defined the following three bandwidth profile service attributes:

- Ingress BW profile per ingress UNI
- Ingress BW profile per EVC
- Ingress BW profile per CoS identifier

The BW profile service attribute consists of four traffic parameters:

- CIR (Committed Information Rate)
- CBS (Committed Burst Size)
- EIR (Excess Information Rate)
- EBS (Excess Burst Size)

Bandwidth profiles can be applied per UNI, per EVC at the UNI, or per CoS identifier for a specified EVC at the UNI.

The Color of the service frame is used to determine its bandwidth profile. If the service frame complies with the CIR and EIR defined in the bandwidth profile, it is marked Green. In this case, the average and maximum service frame rates are less than or equal to the CIR and CBS, respectively.

If the service frame does not comply with the CIR defined in the bandwidth profile, but does comply with the EIR and EBS, it is marked Yellow. In this case, the average service frame rate is greater than the CIR but less than the EIR, and the maximum service frame size is less than the EBS.

If the service frame fails to comply with both the CIR and the EIR defined in the bandwidth profile, it is marked Red and discarded.

In the IP-20F, bandwidth profiles are constructed using a full standardized TrTCM policer mechanism.

6.3.1.3 Ethernet Services Definitions

The MEF provides a model for defining Ethernet services. The purpose of the MEF model is to help subscribers better understand the variations among different types of Ethernet services. IP-20F supports a variety of service types defined by the MEF. All of these service types share some common attributes, but there are also differences as explained below.

Ethernet service types are generic constructs used to create a broad range of services. Each Ethernet service type has a set of Ethernet service attributes that define the characteristics of the service. These Ethernet service attributes in turn are associated with a set of parameters that provide various options for the various service attributes.

Figure 64: MEF Ethernet Services Definition Framework

The MEF defines three generic Ethernet service type constructs, including their associated service attributes and parameters:

- Ethernet Line (E-Line)
- Ethernet LAN (E-LAN)
- Ethernet Tree (E-Tree)

Multiple Ethernet services are defined for each of the three generic Ethernet service types. These services are differentiated by the method for service identification used at the UNIs. Services using All-to-One Bundling UNIs (port-based) are referred to as “Private” services, while services using Service Multiplexed (VLAN-based) UNIs are referred to as “Virtual Private” services. This relationship is shown in the following table.

Table 45: MEF-Defined Ethernet Service Types

Service Type	Port Based (All to One Bundling)	VLAN-BASED (EVC identified by VLAN ID)
E-Line (Point-to-Point EVC)	Ethernet Private Line (EPL)	Ethernet Virtual Private Line (EVPL)
E-LAN (Multipoint-to-Multipoint EVC)	Ethernet Private LAN (EP-LAN)	Ethernet Virtual Private LAN (EVP-LAN)
E-Tree (Rooted Multipoint EVC)	Ethernet Private Tree (EP-Tree)	Ethernet Virtual Private Tree (EVP-Tree)

All-to-One Bundling refers to a UNI attribute in which all Customer Edge VLAN IDs (CE-VLAN IDs) entering the service via the UNI are associated with a single EVC.

Bundling refers to a UNI attribute in which more than one CE-VLAN ID can be associated with an EVC.

To fully specify an Ethernet service, additional service attributes must be defined in addition to the UNI and EVC service attributes. These service attributes can be grouped under the following categories:

- Ethernet physical interfaces
- Traffic parameters
- Performance parameters
- Class of service
- Service frame delivery
- VLAN tag support
- Service multiplexing
- Bundling
- Security filters

E-Line Service

The Ethernet line service (E-Line service) provides a point-to-point Ethernet Virtual Connection (EVC) between two UNIs. The E-Line service type can be used to create a broad range of Ethernet point-to-point services and to maintain the necessary connectivity. In its simplest form, an E-Line service type can provide symmetrical bandwidth for data sent in either direction with no performance assurances, e.g., best effort service between two FE UNIs. In more sophisticated forms, an E-Line service type can provide connectivity between two UNIs with different line rates and can be defined with performance assurances such as CIR with an associated CBS, EIR with an associated EBS, delay, delay variation, loss, and availability for a given Class of Service (CoS) instance. Service multiplexing can occur at one or both UNIs in the EVC. For example, more than one point-to-point EVC can be offered on the same physical port at one or both of the UNIs.

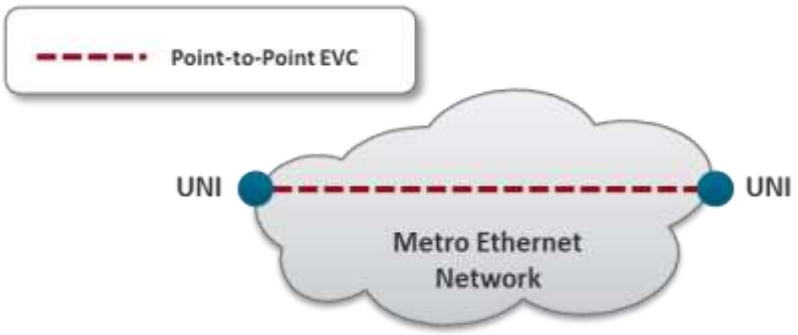


Figure 65: E-Line Service Type Using Point-to-Point EVC

Ethernet Private Line Service

An Ethernet Private Line (EPL) service is specified using an E-Line Service type. An EPL service uses a point-to-point EVC between two UNIs and provides a high degree of transparency for service frames between the UNIs that it interconnects such that the service frame's header and payload are identical at both the source and destination UNI when the service frame is delivered (L1 service). A dedicated UNI (physical interface) is used for the service and service multiplexing is not allowed. All service frames are mapped to a single EVC at the UNI. In cases where the EVC speed is less than the UNI speed, the CE is expected to shape traffic to the ingress bandwidth profile of the service to prevent the traffic from being discarded by the service. The EPL is a port-based service, with a single EVC across dedicated UNIs providing site-to-site connectivity. EPL is the most popular Ethernet service type due to its simplicity, and is used in diverse applications such as replacing a TDM private line.

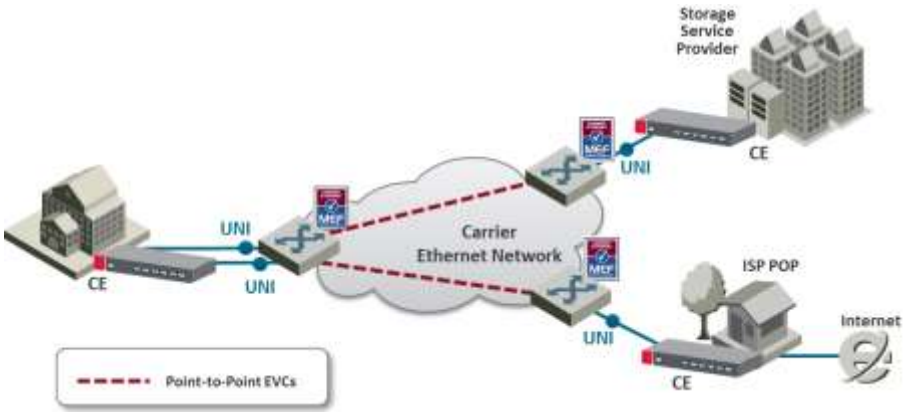


Figure 66: EPL Application Example

Ethernet Virtual Private Line Service

An Ethernet Virtual Private Line (EVPL) is created using an E-Line service type. An EVPL can be used to create services similar to EPL services. However, several characteristics differ between EPL and EVPL services.

First, an EVPL provides for service multiplexing at the UNI, which means it enables multiple EVCs to be delivered to customer premises over a single physical connection (UNI). In contrast, an EPL only enables a single service to be delivered over a single physical connection.

Second, the degree of transparency for service frames is lower in an EVPL than in an EPL.

Since service multiplexing is permitted in EVPL services, some service frames may be sent to one EVC while others may be sent to other EVCs. EVPL services can be used to replace Frame Relay and ATM L2 VPN services, in order to deliver higher bandwidth, end-to-end services.

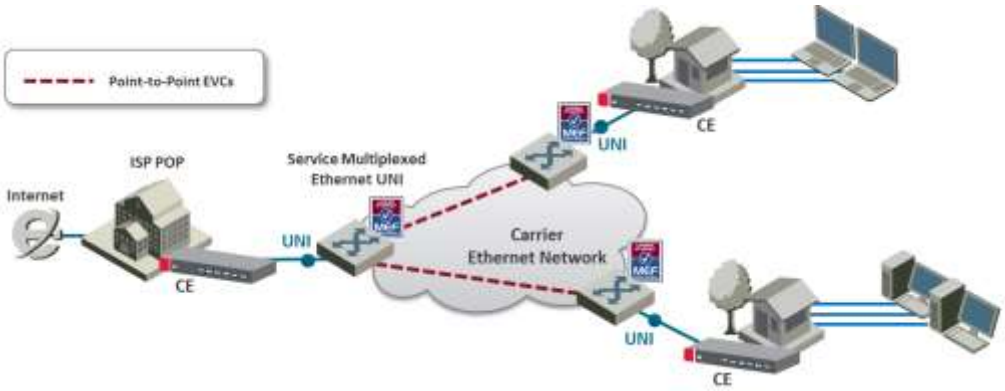


Figure 67: EVPL Application Example

E-LAN Service

The E-LAN service type is based on Multipoint to Multipoint EVCs, and provides multipoint connectivity by connecting two or more UNIs. Each site (UNI) is connected to a multipoint EVC, and customer frames sent from one UNI can be received at one or more UNIs. If additional sites are added, they can be connected to the same multipoint EVC, simplifying the service activation process. Logically, from the point of view of a customer using an E-LAN service, the MEN can be viewed as a LAN.

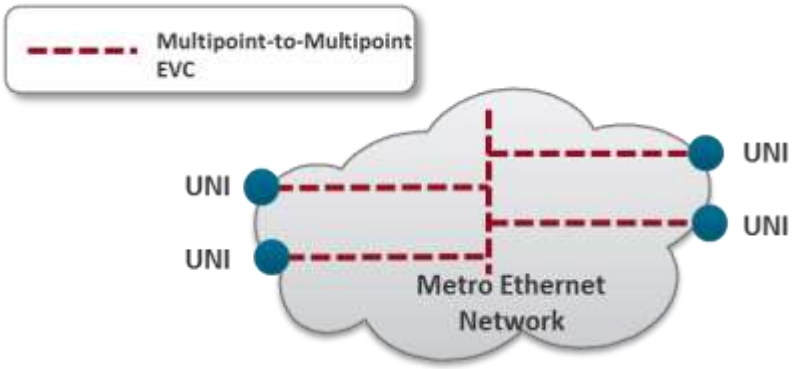


Figure 68: E-LAN Service Type Using Multipoint-to-Multipoint EVC

The E-LAN service type can be used to create a broad range of services. In its basic form, an E-LAN service can provide a best effort service with no performance assurances between the UNIs. In more sophisticated forms, an E-LAN service type can be defined with performance assurances such as CIR with an associated CBS, EIR with an associated EBS, delay, delay variation, loss, and availability for a given CoS instance.

For an E-LAN service type, service multiplexing may occur at none, one, or more than one of the UNIs in the EVC. For example, an E-LAN service type (Multipoint-to-Multipoint EVC) and an E-Line service type (Point-to-Point EVC) can be service multiplexed at the same UNI. In such a case, the E-LAN service type can be used to interconnect other customer sites while the E-Line service type is used to connect to the Internet, with both services offered via service multiplexing at the same UNI.

E-LAN services can simplify the interconnection among a large number of sites, in comparison to hub/mesh topologies implemented using point-to-point networking technologies such as Frame Relay and ATM.

For example, consider a point-to-point network configuration implemented using E-Line services. If a new site (UNI) is added, it is necessary to add a new, separate EVC to all of the other sites in order to enable the new UNI to communicate with the other UNIs, as shown in the following figure.

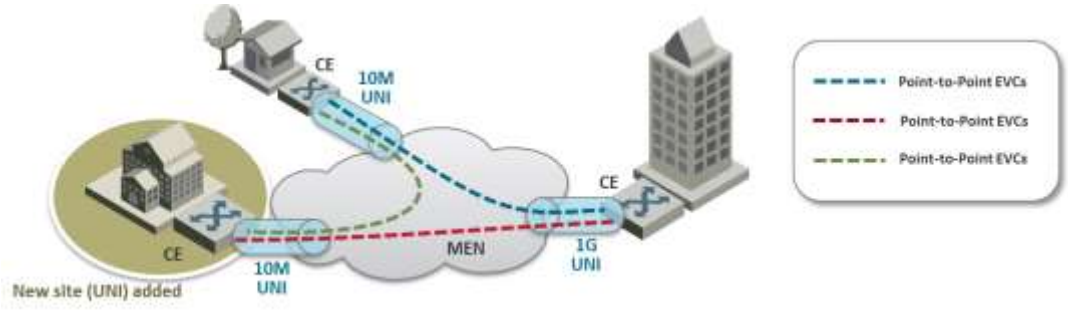


Figure 69: Adding a Site Using an E-Line service

In contrast, when using an E-LAN service, it is only necessary to add the new UNI to the multipoint EVC. No additional EVCs are required, since the E-LAN service uses a multipoint to multipoint EVC that enables the new UNI to communicate with each of the others UNIs. Only one EVC is required to achieve multi-site connectivity, as shown in the following figure.

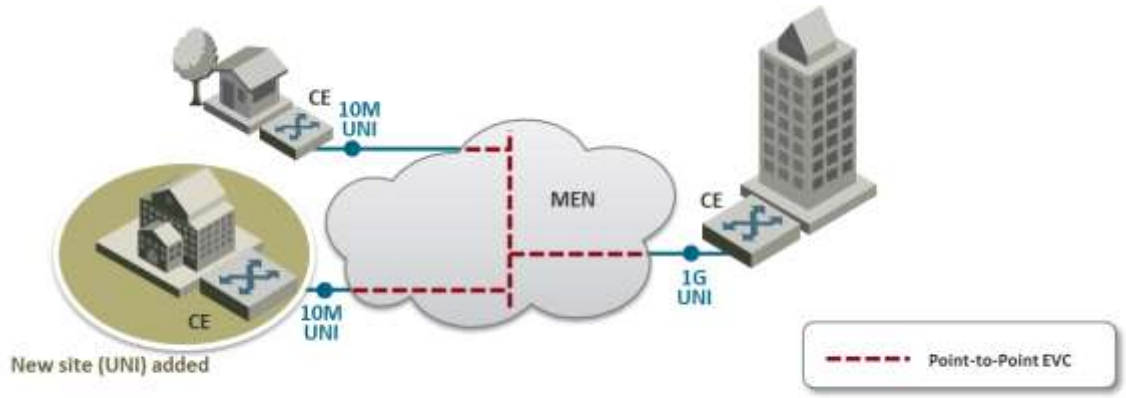


Figure 70: Adding a Site Using an E-LAN service

The E-LAN service type can be used to create a broad range of services, such as private LAN and virtual private LAN services.

Ethernet Private LAN Service

It is often desirable to interconnect multiple sites using a Local Area Network (LAN) protocol model and have equivalent performance and access to resources such as servers and storage. Customers commonly require a highly transparent service that connects multiple UNIs. The Ethernet Private LAN (EP-LAN) service is defined with this in mind, using the E-LAN service type. The EP-LAN is a Layer 2 service in which each UNI is dedicated to the EP-LAN service. A typical use case for EP-LAN services is Transparent LAN.

The following figure shows an example of an EP-LAN service in which the service is defined to provide Customer Edge VLAN (CE-VLAN) tag preservation and tunneling for key Layer 2 control protocols. Customers can use this service to configure VLANs across the sites without the need to coordinate with the service provider. Each interface is configured for All-to-One Bundling, which enables the EP-LAN service to support CE-VLAN ID preservation. In addition, EP-LAN supports CE-VLAN CoS preservation.

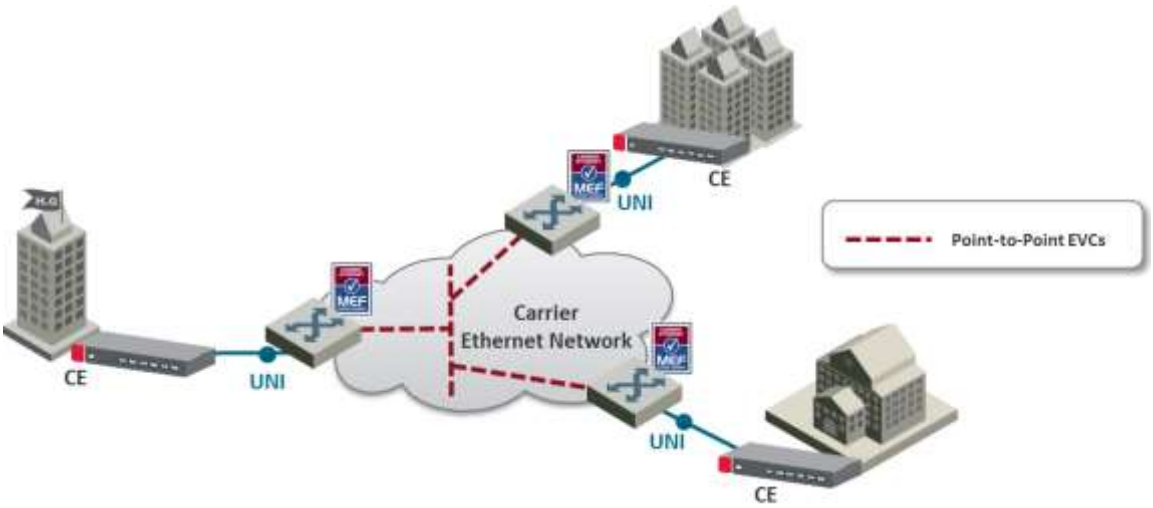


Figure 71: MEF Ethernet Private LAN Example

Ethernet Virtual Private LAN Service

Customers often use an E-LAN service type to connect their UNIs in an MEN, while at the same time accessing other services from one or more of those UNIs. For example, a customer might want to access a public or private IP service from a UNI at the customer site that is also used to provide E-LAN service among the customer's several metro locations. The Ethernet Virtual Private LAN (EVP-LAN) service is defined to address this need. EVP-LAN is actually a combination of EVPL and E-LAN.

Bundling can be used on the UNIs in the Multipoint-to-Multipoint EVC, but is not mandatory. As such, CE-VLAN tag preservation and tunneling of certain Layer 2 control protocols may or may not be provided. Service multiplexing is allowed on each UNI. A typical use case would be to provide Internet access a corporate VPN via one UNI.

The following figure provides an example of an EVP-LAN service.

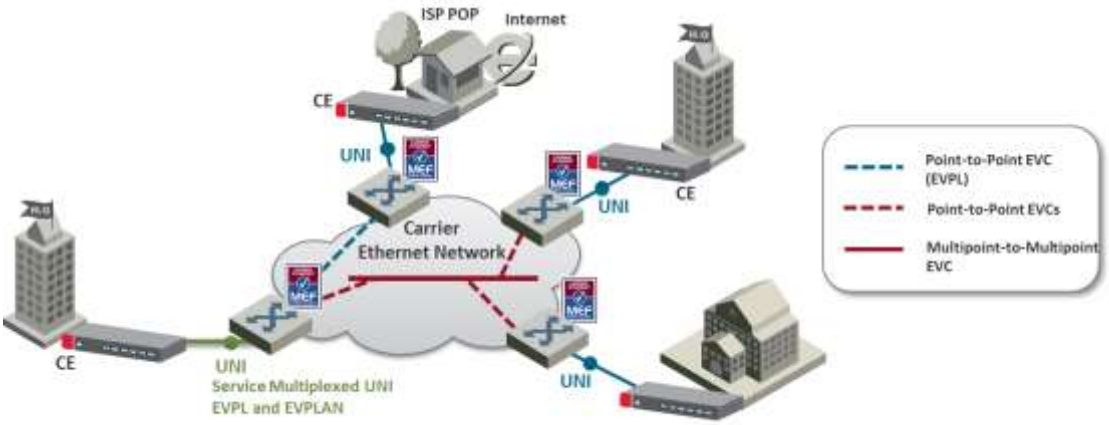


Figure 72: MEF Ethernet Virtual Private LAN Example

E-Tree Service

The E-Tree service type is an Ethernet service type that is based on Rooted-Multipoint EVCs. In its basic form, an E-Tree service can provide a single Root for multiple Leaf UNIs. Each Leaf UNI can exchange data with only the Root UNI. A service frame sent from one Leaf UNI cannot be delivered to another Leaf UNI. This service can be particularly useful for Internet access, and video-over-IP applications such as multicast/broadcast packet video. One or more CoS values can be associated with an E-Tree service.

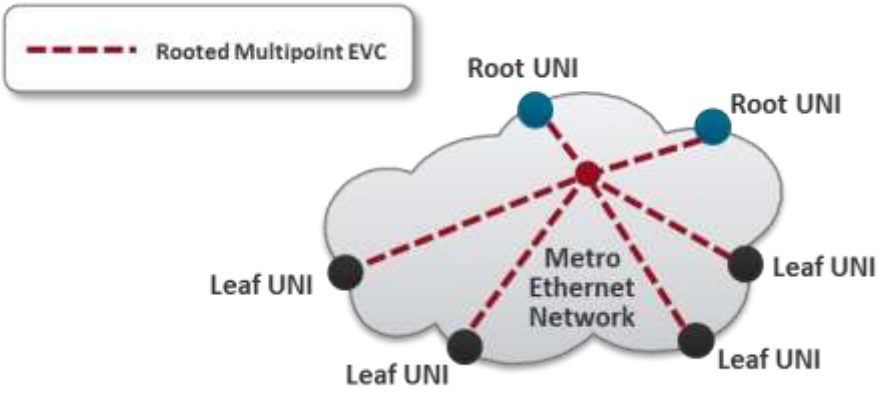


Figure 73: E-Tree Service Type Using Rooted-Multipoint EVC

Two or more Root UNIs can be supported in advanced forms of the E-Tree service type. In this scenario, each Leaf UNI can exchange data only with the Root UNIs. The Root UNIs can communicate with each other. Redundant access to the Root can also be provided, effectively allowing for enhanced service reliability and flexibility.

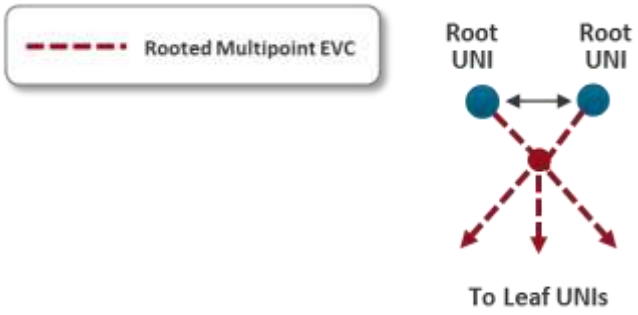


Figure 74: E-Tree Service Type Using Multiple Roots

Service multiplexing is optional and may occur on any combination of UNIs in the EVC. For example, an E-Tree service type using a Rooted-Multipoint EVC, and an E-Line service type using a Point-to-Point EVC, can be service multiplexed on the same UNI. In this example, the E-Tree service type can be used to support a specific application at the Subscriber UNI, e.g., ISP access to redundant PoPs (multiple Roots at ISP PoPs), while the E-Line Service type is used to connect to another enterprise site with a Point-to-Point EVC.

Ethernet Private Tree Service

The Ethernet Private Tree service (EP-Tree) is designed to supply the flexibility for configuring multiple sites so that the services are distributed from a centralized site, or from a few centralized sites. In this setup, the centralized site or sites are designed as Roots, while the remaining sites are designated as Leaves. CE-VLAN tags are preserved and key Layer 2 control protocols are tunneled. The advantage of such a configuration is that the customer can configure VLANs across its sites without the need to coordinate with the service provider. Each interface is configured for All-to-One Bundling, which means that EP-Tree services support CE-VLAN ID preservation. EP-Tree also supports CE-VLAN CoS preservation. EP-Tree requires dedication of the UNIs to the single EP-Tree service.

The following figure provides an example of an EP-Tree service.

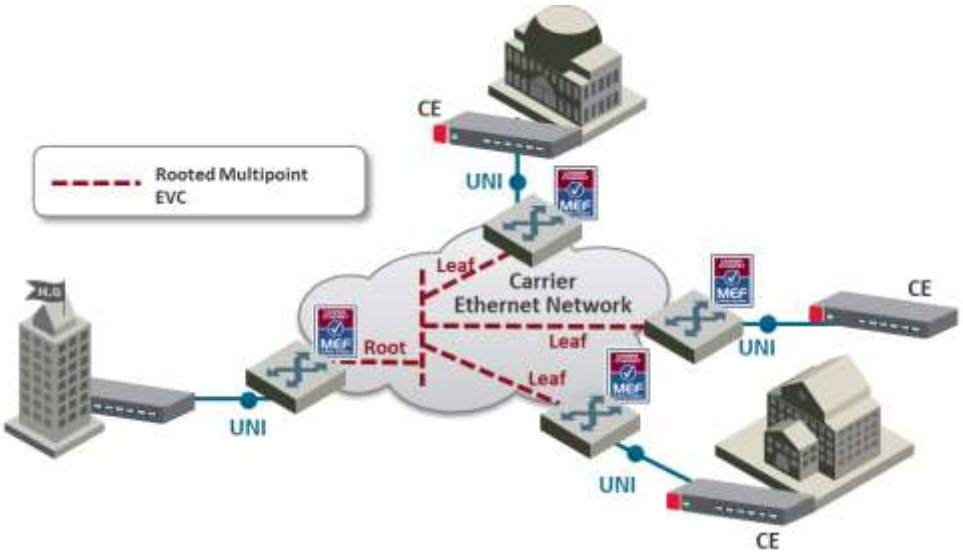


Figure 75: MEF Ethernet Private Tree Example

Ethernet Virtual Private Tree Service

In order to access several applications and services from well-defined access points (Root), the UNIs are attached to the service in a Rooted Multipoint connection. Customer UNIs can also support other services, such as EVPL and EVP-LAN services. An EVP-Tree service is used in such cases. Bundling can be used on the UNIs in the Rooted Multipoint EVC, but it is not mandatory. As such, CE-VLAN tag preservation and tunneling of certain Layer 2 Control Protocols may or may not be provided. EVP-Tree enables each UNI to support multiple services. A good example would be a customer that has an EVP-LAN service providing data connectivity among three UNIs, while using an EVP-Tree service to provide video broadcast from a video hub location. The following figure provides an example of a Virtual Private Tree service.

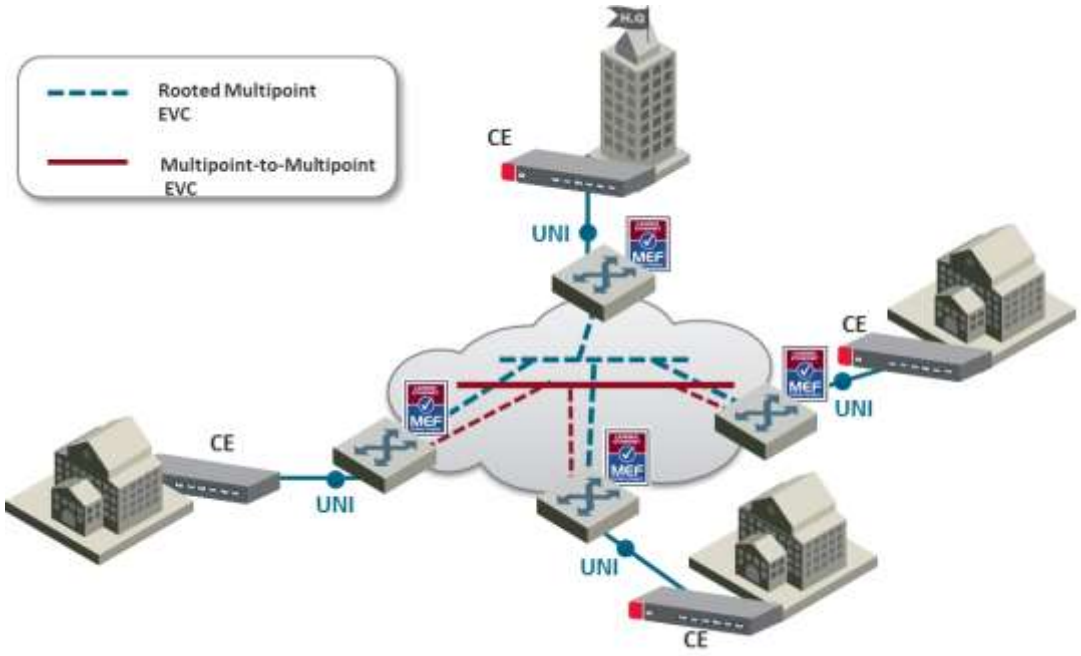


Figure 76: Ethernet Virtual Private Tree Example

IP-20F enables network connectivity for **Mobile Backhaul** cellular infrastructure, fixed networks, private networks and enterprises.

Mobile Backhaul refers to the network between the Base Station sites and the Network Controller/Gateway sites for all generations of mobile technologies. Mobile equipment and networks with ETH service layer functions can support MEF Carrier Ethernet services using the service attributes defined by the MEF.

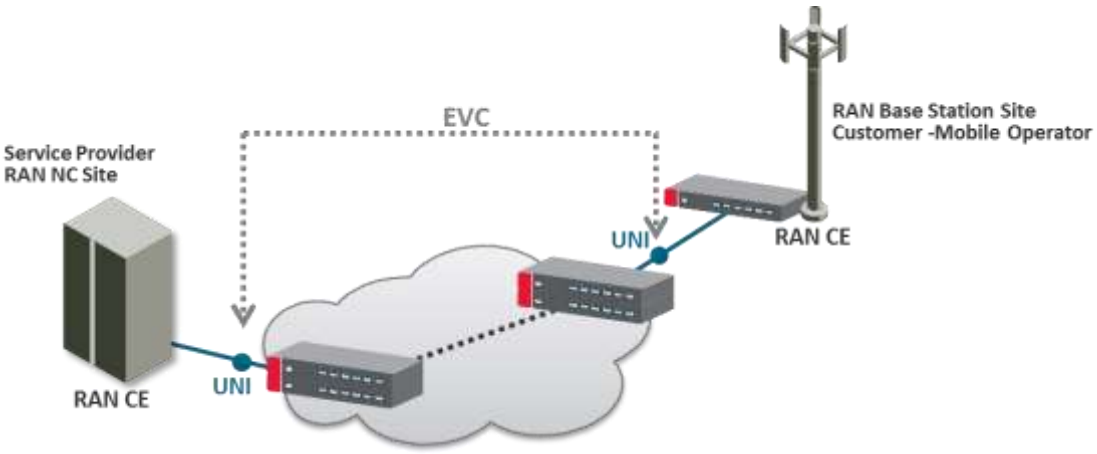


Figure 77: Mobile Backhaul Reference Model

The IP-20F services concept is purpose built to support the standard MEF services for mobile backhaul (MEF 22, mobile backhaul implementation agreement), as an addition to the baseline definition of MEF Services (MEF 6) using service attributes (as well as in MEF 10). E-Line, E-LAN and E-Tree services are well defined as the standard services.

6.3.1.4 IP-20F Universal Packet Backhaul Services Core

IP-20F addresses the customer demand for multiple services of any of the aforementioned types (EPL, EVPL, EP –LAN, EVP-LAN, EP-Tree, and EVP-Tree) through its rich service model capabilities and flexible integrated switch application. Additional Layer 1 point-based services are supported as well, as explained in more detail below.

Services support in the mobile backhaul environment is provided using the IP-20F services core, which is structured around the building blocks shown in the figure below. IP-20F provides rich and secure packet backhaul services over any transport type with unified, simple, and error-free operation.

Figure 78: Packet Service Core Building Blocks

Any Service

- Ethernet services (EVCs)
  - E-Line (Point-to-Point)
  - E-LAN (Multipoint)
  - E-Tree (Point-to-Multipoint)[14]
- Port based (Smart Pipe) services

Any Transport

- Native Ethernet Transport (802.1q or Q-in-Q)
- Any topology and any mix of radio and fiber interfaces
- Seamless interworking with any optical network (NG-SDH, packet optical transport, IP/MPLS service/VPN routers)

[14] E-Tree services are planned for future release.

Virtual Switching/Forwarding Engine

- Clear distinction between user facing service interfaces (UNI) and intra-network interfaces
- Fully flexible C-VLAN and S-VLAN encapsulation (classification and preservation)
- Improved security/isolation without limiting C-VLAN reuse by different customers
- Per-service MAC learning with 128K MAC addresses support

Fully Programmable and Future-Proof

- Network-processor-based services core
- Ready today to support emerging and future standards and networking protocols

Rich Policies and Tools with Unified and Simplified Management

- Personalized QoS (H-QoS)[15]
- Superb service OAM (CFM, PM)
- Carrier-grade service resiliency (G.8032, MSTP)

[15] H-QoS support is planned for future release.

6.3.2 IP-20F's Ethernet Capabilities

IP-20F is built upon a service-based paradigm that provides rich and secure frame backhaul services over any type of transport, with unified, simple, and error-free operation. IP-20F's services core includes a rich set of tools that includes:

- Service-based Quality of Service (QoS).
- Service OAM, including CFM, granular PMs, and service activation.
- Carrier-grade service resiliency using G.8032 and MSTP.

The following are IP-20F's main Carrier Ethernet transport features. This rich feature set provides a future-proof architecture to support backhaul evolution for emerging services.

- Up to 64 services
- Up to 32 service points per service
- All service types:
  - Point-to-Point (E-Line)
  - Multipoint (E-LAN)
  - Point-to-Multipoint (E-Tree) [16]
  - Smart Pipe
  - Management
- Split horizon between service points[17]
- 128K MAC learning table, with separate learning per service (including limiters)
- Flexible transport and encapsulation via 802.1q, 802.1ad (Q-in-Q)
- High precision, flexible frame synchronization solution combining SyncE and 1588v2[18]
- Hierarchical QoS with up to 2.5K service level queues, deep buffering, hierarchical scheduling via WFQ and Strict priority, and shaping at each level
- 1K hierarchical two-rate three-Color policers
  - Port based – Unicast, Multicast, Broadcast, Ethertype
  - Service-based
  - CoS-based
- Up to four link aggregation groups (LAG)
  - Hashing based on L2, L3, MPLS, and L4
- Enhanced <50msec network level resiliency (G.8032) for ring/mesh support

16 E-Tree service support is planned for future release.

17 Split horizon is planned for future release.

18 1588v2 is planned for future release.

6.3.3 Supported Standards

IP-20F is fully MEF-9 and MEF-14 certified for all Carrier Ethernet services. For a full list of standards and certifications supported by IP-20F, refer to the following section:

- Supported Ethernet Standards

6.3.4 Ethernet Service Model

IP-20F's service-oriented Ethernet paradigm is based on Carrier-Ethernet Transport (CET), and provides a highly flexible and granular switching fabric for Ethernet services.

IP-20F's virtual switching/forwarding engine is based on a clear distinction between user-facing service interfaces and intra-network service interfaces. User-facing interfaces (UNIs) are configured as Service Access Points (SAPs), while intra-network interfaces (E-NNIs or NNIs) are configured as Service Network Points (SNPs).

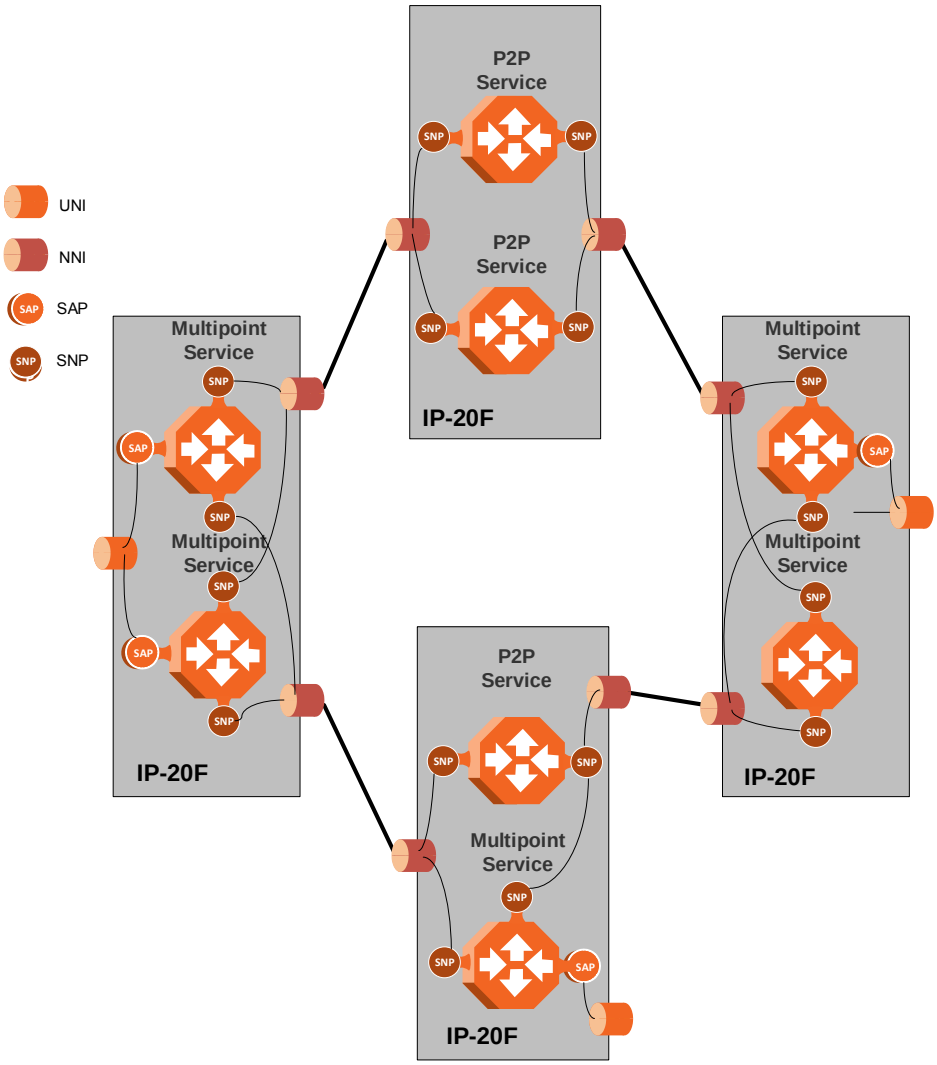


Figure 79: IP-20F Services Model

The IP-20F services core provides for fully flexible C-VLAN and S-VLAN encapsulation, with a full range of classification and preservation options available. Service security and isolation is provided without limiting the C-VLAN reuse capabilities of different customers.

Users can define up to 64 services on a single IP-20F. Each service constitutes a virtual bridge that defines the connectivity and behavior among the network element interfaces for the specific virtual bridge. In addition to user-defined services, IP-20F contains a pre-defined management service (Service ID 1025). If needed, users can activate the management service and use it for in-band management.

To define a service, the user must configure virtual connections among the interfaces that belong to the service. This is done by configuring service points (SPs) on these interfaces.

A service can hold up to 32 service points. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

Note: Management services can hold up to 30 SPs.

The following figure illustrates the IP-20F services model, with traffic entering and leaving the network element. IP-20F's switching fabric is designed to provide a high degree of flexibility in the definition of services and the treatment of data flows as they pass through the switching fabric.

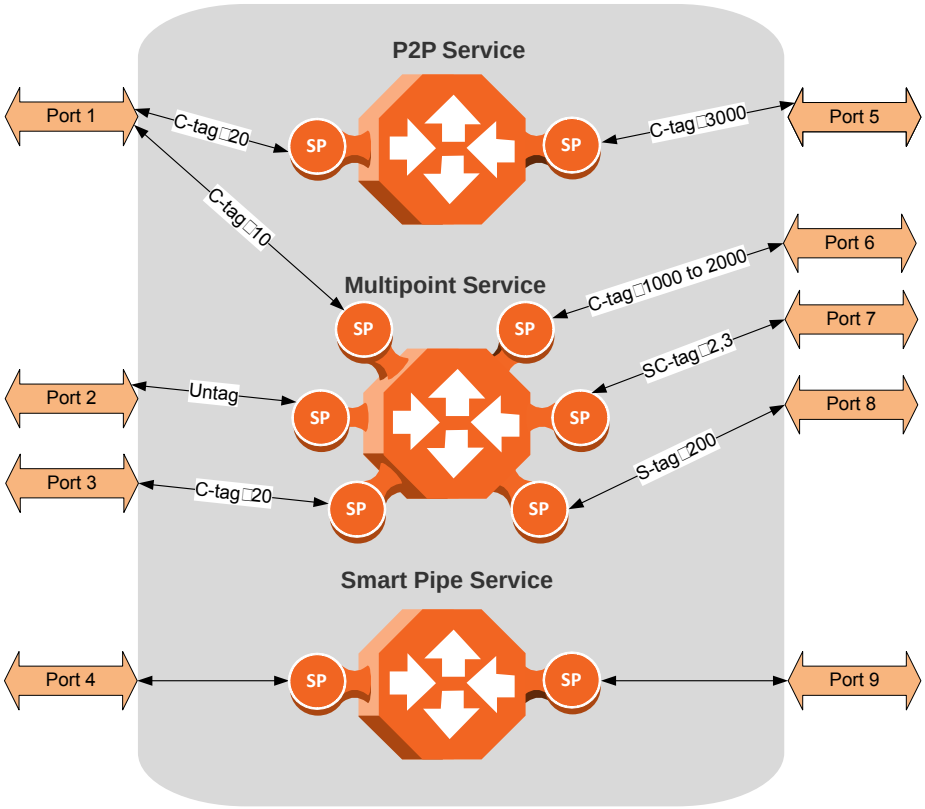


Figure 80: IP-20F Services Core

6.3.4.1 Frame Classification to Service Points and Services

Each arriving frame is classified to a specific service point, based on a key that consists of:

- The Interface ID of the interface through which the frame entered the IP-20F.
- The frame's C-VLAN and/or S-VLAN tags.

If the classification mechanism finds a match between the key of the arriving frame and a specific service point, the frame is associated to the specific service to which the service point belongs. That service point is called the ingress service point for the frame, and the other service points in the service are optional egress service points for the frame. The frame is then forwarded from the ingress service point to an egress service point by means of flooding or dynamic address learning in the specific service. Services include a MAC entry table of up to 131,072 entries, with a global aging timer and a maximum learning limiter that are configurable per-service.

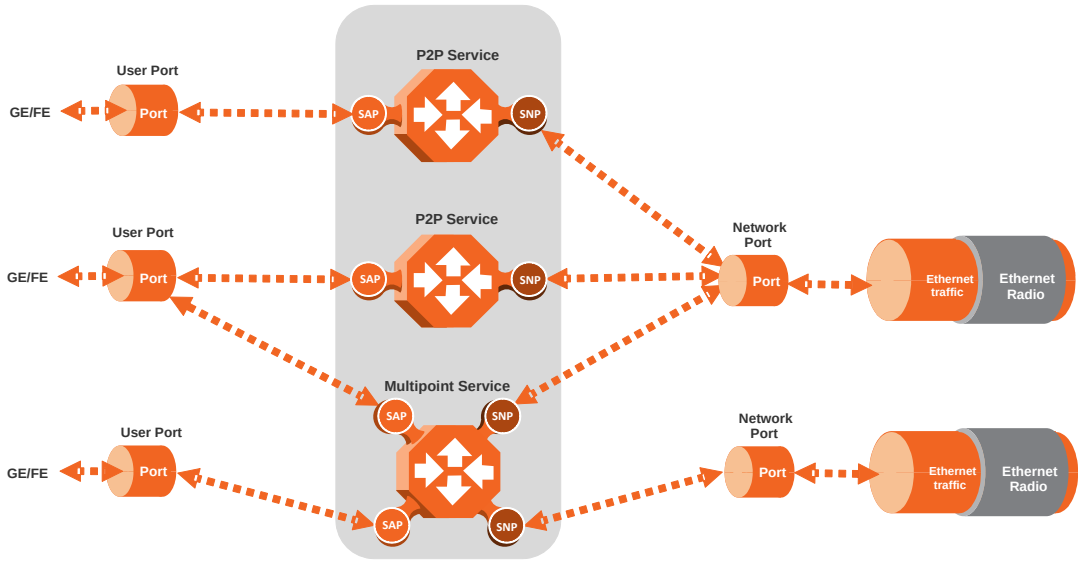


Figure 81: IP-20F Services Flow

6.3.4.2 Service Types

IP-20F supports the following service types:

- Point-to-Point Service (P2P)
- MultiPoint Service (MP)
- Management Service

Point to Point Service (P2P)

Point-to-point services are used to provide connectivity between two interfaces of the network element. When traffic ingresses via one side of the service, it is immediately directed to the other side according to ingress and egress tunneling rules. This type of service contains exactly two service points and does not require MAC address-based learning or forwarding. Since the route is clear, the traffic is tunneled from one side of the service to the other and vice versa.

The following figure illustrates a P2P service.

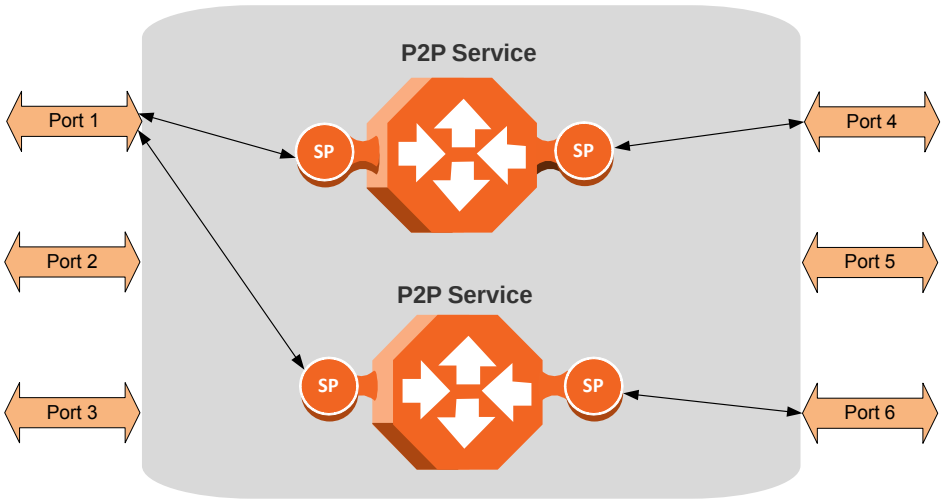


Figure 82: Point-to-Point Service

P2P services provide the building blocks for network services such as E-Line EVC (EPL and EVPL EVCs) and port-based services (Smart Pipe).

Multipoint Service (MP)

Multipoint services are used to provide connectivity between two or more service points. When traffic ingresses via one service point, it is directed to one of the service points in the service, other than the ingress service point, according to ingress and egress tunneling rules, and based on the learning and forwarding mechanism. If the destination MAC address is not known by the learning and forwarding mechanism, the arriving frame is flooded to all the other service points in the service except the ingress service point.

The following figure illustrates a Multipoint service.

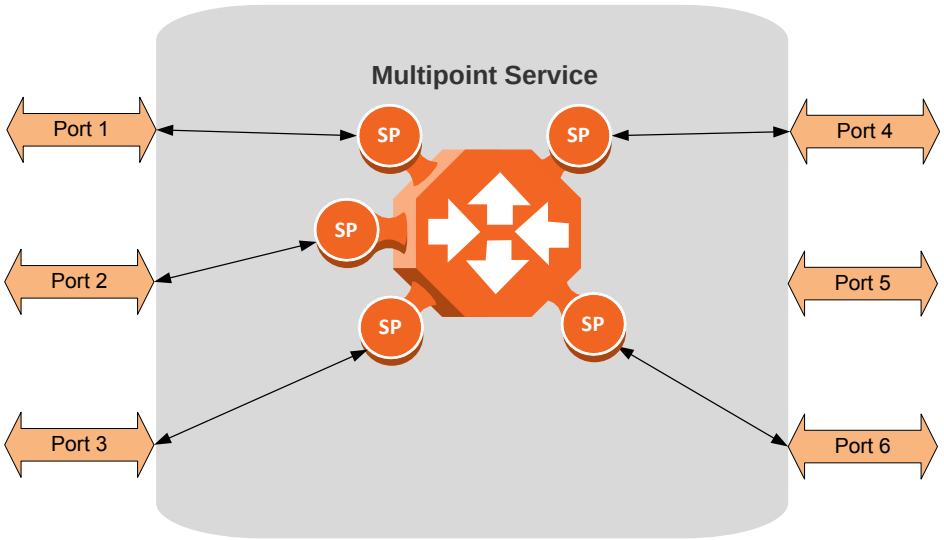


Figure 83: Multipoint Service

Multipoint services provide the building blocks for network services such as E-LAN EVCs (EP-LAN and EVP-LAN EVCs), and for E-Line EVCs (EPL and EVPL EVCs) in which only two service points are active. In such a case, the user can disable MAC address learning in the service points to conserve system resources.

Learning and Forwarding Mechanism

IP-20F can learn up to 131,072 Ethernet source MAC addresses. IP-20F performs learning per service in order to enable the use of 1025 virtual bridges in the network element. If necessary due to security issues or resource limitations, users can limit the size of the MAC forwarding table. The maximum size of the MAC forwarding table is configurable per service in granularity of 16 entries.

When a frame arrives via a specific service point, the learning mechanism checks the MAC forwarding table for the service to which the service point belongs to determine whether that MAC address is known to the service. If the MAC address is not found, the learning mechanism adds it to the table under the specific service.

In parallel with the learning process, the forwarding mechanism searches the service's MAC forwarding table for the frame's destination MAC address. If a match is found, the frame is forwarded to the service point associated with the MAC address. If not, the frame is flooded to all service points in the service.

The following table illustrates the operation of the learning and forwarding mechanism.

Table 46: Ethernet Services Learning and Forwarding

MAC Forwarding Table			
Input Key for learning / forwarding (search) operation		**Result**	**Entry type**
Service ID	**MAC address**	**Service Point**	
95	00:34:67:3a:aa:10	15	dynamic
95	00:0a:25:33:22:12	31	dynamic
128	00:0a:25:11:12:55	31	static
357	00:0a:25:33:22:12	15	dynamic
357	00:c3:20:57:14:89	31	dynamic
357	00:0a:25:11:12:55	31	dynamic

In addition to the dynamic learning mechanism, users can add static MAC addresses for static routing in each service. These user entries are not considered when determining the maximum size of the MAC forwarding table.

Users can manually clear all the dynamic entries from the MAC forwarding table. Users can also delete static entries per service.

The system also provides an automatic flush process. An entry is erased from the table as a result of:

- The global aging time expires for the entry.
- Loss of carrier occurs on the interface with which the entry is associated.
- Resiliency protocols, such as MSTP or G.8032.

Management Service (MNG)

The management service connects the two local management ports, the network element host CPU, and the traffic ports into a single service. The service behavior is same as the Multipoint service behavior.

The management service is pre-defined in the system, with Service ID 1025. The pre-defined management service has a single service point that connects the service to the network element host CPU and the two local management interfaces. To configure in-band management over multiple network elements, the user must connect the management service to the network by adding a service point on an interface that provides the required network connectivity.

Users can modify the attributes of the management service, but cannot delete it. The CPU service point is read-only and cannot be modified. The local management ports are also connected to the service, but their service points are not visible to users. The first management interface is enabled by default. The second management interface must be manually enabled by the user. The management ports can be used to manage the network element or to access a remote network element. They can also be used to manage third-party devices. Users can enable or disable these ports.

The following figure illustrates a management service.

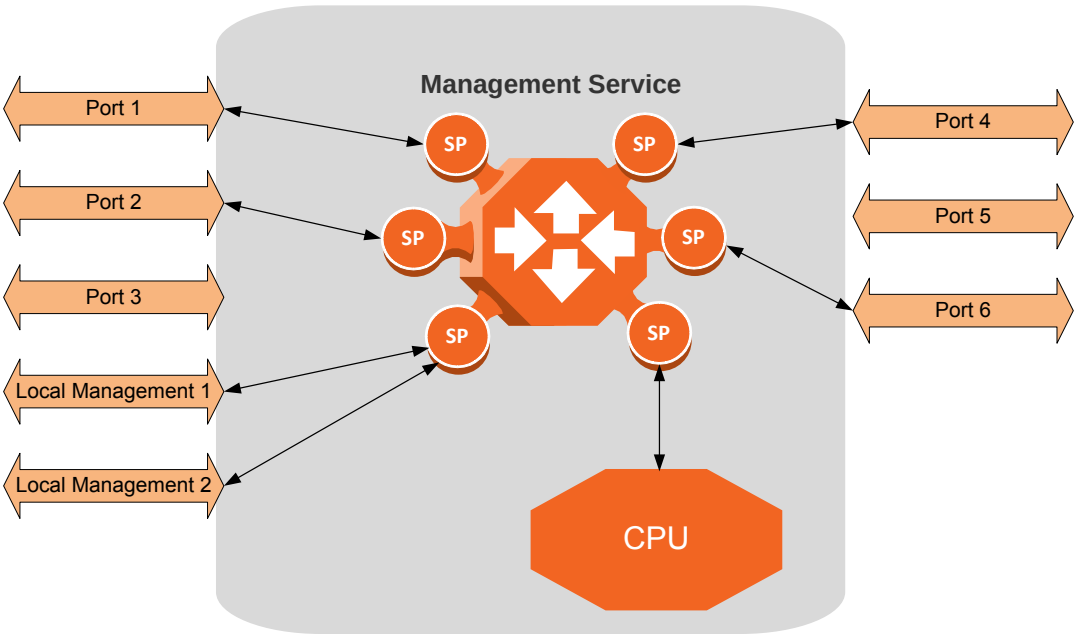


Figure 84: Management Service

Management services can provide building blocks for network services such as E-LAN EVCs (EP-LAN and EVP-LAN), as well as E-Line EVCs (EPL and EVPL EVCs) in which only two service points are active.

Service Attributes

IP-20F services have the following attributes:

- **Service ID** – A running number from 1 to 1025 that identifies the service. The user must select the Service ID upon creating the service. The Service ID cannot be edited after the service has been created. Service ID 1025 is reserved for the pre-defined Management service.
- **Service Type** – Determines the specific functionality that will be provided for Ethernet traffic using the service. For example, a Point-to-Point service provides traffic forwarding between two service points, with no need to learn a service topology based on source and destination MAC addresses. A Multipoint service enables operators to create an E-LAN service that includes several service points.
- **Service Admin Mode** – Defines whether or not the service is functional, i.e., able to receive and transmit traffic. When the Service Admin Mode is set to Operational, the service is fully functional. When the Service Admin Mode is set to Reserved, the service occupies system resources but is unable to transmit and receive data.
- **EVC-ID** – The Ethernet Virtual Connection ID (end-to-end). This parameter does not affect the network element's behavior, but is used by the NMS for topology management.

- **EVC Description** – The Ethernet Virtual Connection description. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
- **Maximum Dynamic MAC Address Learning per Service** – Defines the maximum number of dynamic Ethernet MAC address that the service can learn. This parameter is configured with a granularity of 16, and only applies to dynamic, not static, MAC addresses.
- **Static MAC Address Configuration** – Users can add static entries to the MAC forwarding table. The global aging time does not apply to static entries, and they are not counted with respect to the Maximum Dynamic MAC Address Learning. It is the responsibility of the user not to use all the 131,072 entries in the table if the user also wants to utilize dynamic MAC address learning.
- **CoS Mode** – Defines whether the service inherits ingress classification decisions made at previous stages or overwrites previous decisions and uses the default CoS defined for the service. For more details on IP-20F's hierarchical classification mechanism, refer to *Classification* on page 164.
- **Default CoS** – The default CoS value at the service level. If the CoS Mode is set to overwrite previous classification decisions, this is the CoS value used for frames entering the service.
- **xSTP Instance** (0-46, 4095) – The spanning tree instance ID to which the service belongs. The service can be a traffic engineering service (instance ID 4095) or can be managed by the xSTP engines of the network element.

6.3.4.3 Service Points

Service points are logical entities attached to the interfaces that make up the service. Service points define the movement of frames through the service. Without service points, a service is simply a virtual bridge with no ingress or egress interfaces.

IP-20F supports several types of service points:

- **Management (MNG) Service Point** – Only used for management services. The following figure shows a management service used for in-band management among four network elements in a ring. In this example, each service contains three MNG service points, two for East-West management connectivity in the ring, and one serving as the network gateway.

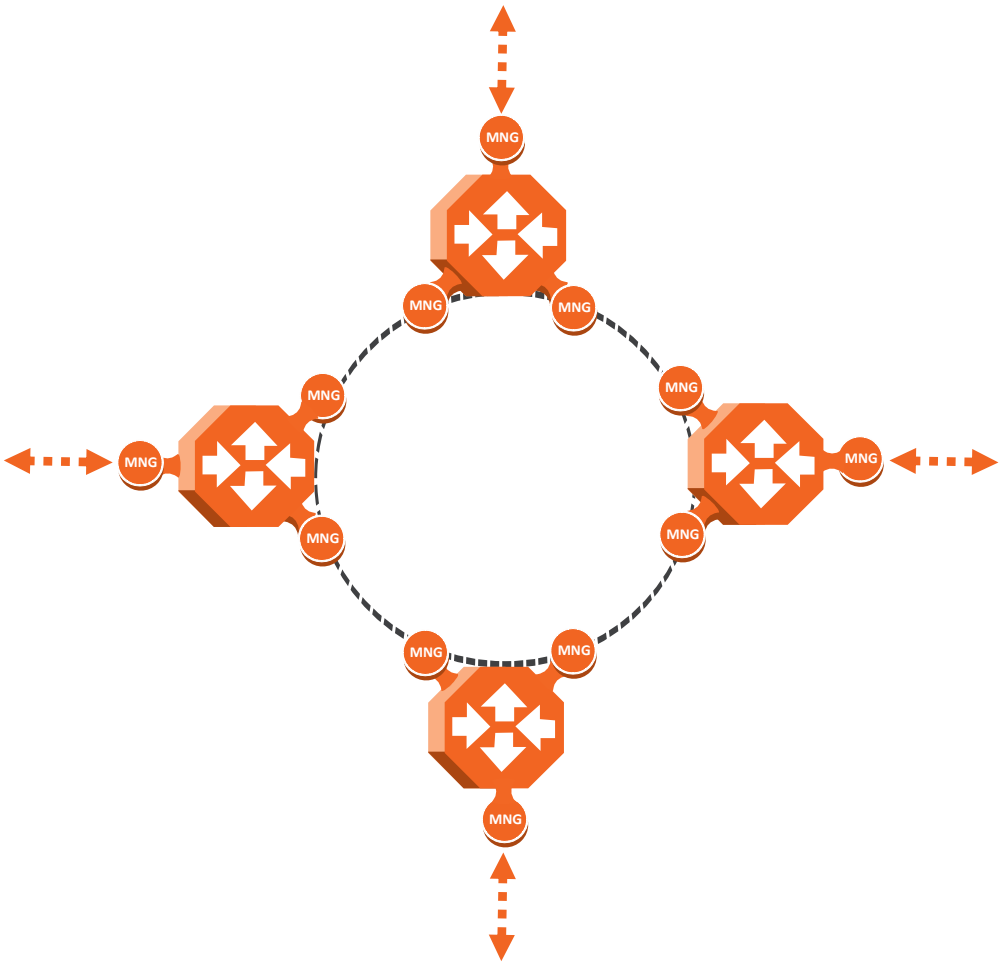


Figure 85: Management Service and its Service Points

- **Service Access Point (SAP) Service Point** – An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.
- **Service Network Point (SNP) Service Point** – An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.

The following figure shows four network elements in ring. An MP Service with three service points provides the connectivity over the network. The SNPs provide the connectivity among the network elements in the user network while the SAPs provide the access points for the network.

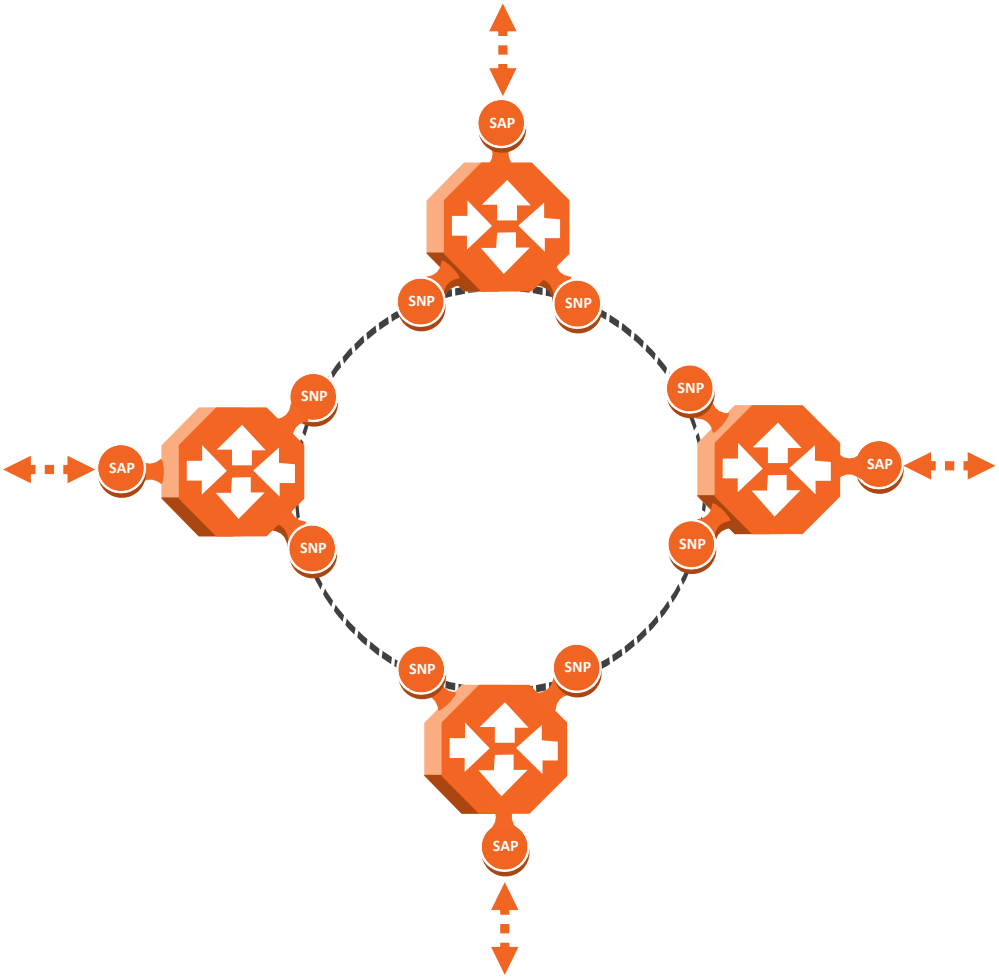


Figure 86: SAPs and SNPs

- **Pipe Service Point** – Used to create traffic connectivity between two points in a port-based manner (Smart Pipe). In other words, all the traffic from one port passes to the other port. Pipe service points are used in Point-to-Point services

The following figure shows a Point-to-Point service with Pipe service points that create a Smart Pipe between Port 1 of the network element on the left and Port 2 of the network element on the right.

Figure 87: Pipe Service Points

The following figure shows the usage of SAP, SNP and PIPE service points in a microwave network. The SNPs are used for interconnection between the network elements while the SAPs provide the access points for the network. A Smart Pipe is also used, to provide connectivity between elements that require port-based connectivity.

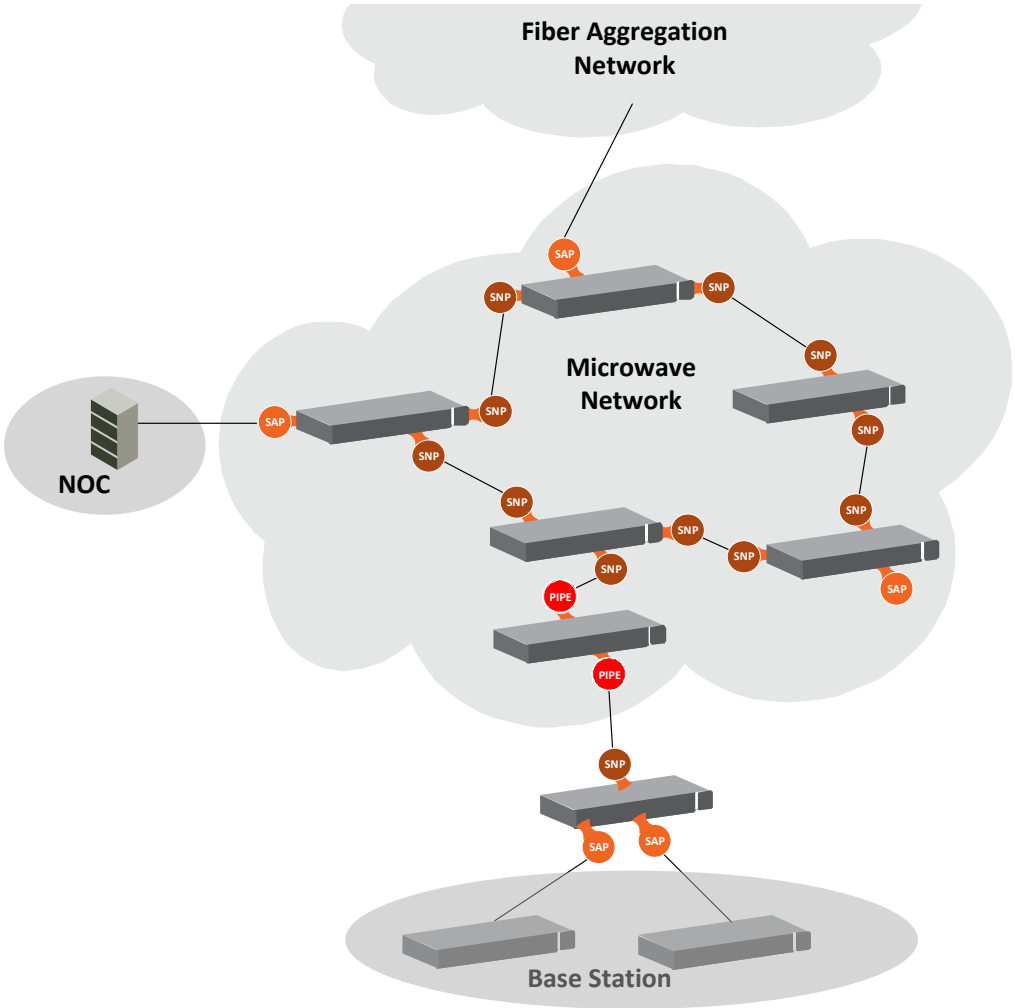


Figure 88: SAP, SNP and Pipe Service Points in a Microwave Network

The following table summarizes the service point types available per service type.

Table 47: Service Point Types per Service Type

		Service point type			
		MNG	**SAP**	**SNP**	**Pipe**
Service Type	Management	Yes	No	No	No
	Point-to-Point	No	Yes	Yes	Yes
	Multipoint	No	Yes	Yes	No

Service Point Classification

As explained above, service points connect the service to the network element interfaces. It is crucial that the network element have a means to classify incoming frames to the proper service point. This classification process is implemented by means of a parsing encapsulation rule for the interface associated with the service point. This rule is called the Attached Interface Type, and is based on a three-part key consisting of:

- The Interface ID of the interface through which the frame entered.
- The frame's C-VLAN and/or S-VLAN tags.

The Attached Interface Type provides a definitive mapping of each arriving frame to a specific service point in a specific service. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict.

SAP Classification

SAPs can be used with the following Attached Interface Types:

- **All to one** – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- **Dot1q** – A single C-VLAN is classified to the service point.
- **QinQ** – A single S-VLAN and C-VLAN combination is classified to the service point.
- **Bundle C-Tag**– A set of multiple C-VLANs are classified to the service point.
- **Bundle S-Tag** – A single S-VLAN and a set of multiple C-VLANs are classified to the service point.

SNP classification

SNPs can be used with the following Attached Interface Types:

- **Dot1q** – A single C VLAN is classified to the service point.
- **S-Tag** – A single S- VLAN is classified to the service point.

MNG classification

Management service points can be used with the following Attached Interface Types:

- **Dot1q** – A single C-VLAN is classified to the service point.
- **S-Tag** – A single S-VLAN is classified to the service point.
- **QinQ** – A single S-VLAN and C-VLAN combination is classified into the service point.

The following table shows which service point types can co-exist on the same interface.

Table 48: Service Point Types that can Co-Exist on the Same Interface

	MNG SP	SAP SP	SNP SP	Pipe SP
MNG SP	Only one MNG SP is allowed per interface.	Yes	Yes	Yes
SAP SP	Yes	Yes	No	No
SNP SP	Yes	No	Yes	No
PIPE SP	Yes	No	No	Only one Pipe SP is allowed per interface.

The following table shows in more detail which service point – Attached Interface Type combinations can co-exist on the same interface.

Table 49: Service Point Type-Attached Interface Type Combinations that can Co-Exist on the Same Interface

	SP Type	SAP					SNP		Pipe		MNG		
SP Type	**Attached Interface Type**	**802.1q**	**Bundle C-Tag**	**Bundle S-Tag**	**All to One**	**QinQ**	**802.1q**	**S-Tag**	**802.1q**	**S-Tag**	**802.1q**	**QinQ**	**S-Tag**
SAP	802.1q	Yes	Yes	No	No	No	No	No	Only for P2P Service	No	Yes	No	No
	Bundle C-Tag	Yes	Yes	No	No	No	No	No	Only for P2P Service	No	Yes	No	No
	Bundle S-Tag	No	No	Yes	No	Yes	No	No	No	No	No	Yes	No
	All to One	No	No	No	Only 1 All to One SP Per Interface	No	No	No	No	No	No	No	No
	QinQ	No	No	Yes	No	Yes	No	No	No	No	No	Yes	No
SNP	802.1q	No	No	No	No	No	Yes	No	Only for P2P Service	No	Yes	No	No
	S-Tag	No	No	No	No	No	No	Yes	No	Only for P2P Service	No	No	Yes
Pipe	802.1q	Only for P2P Service	Only for P2P Service	No	No	No	Only for P2P Service	No	Only one Pipe SP Per Interface	No	Yes	No	No
	S-Tag	No	No	No	No	No	No	Only for P2P Service	No	Only one Pipe SP Per Interface	No	No	Yes
MNG	802.1q	Yes	Yes	No	No	No	Yes	No	Yes	No	No	No	No
	QinQ	No	No	Yes	No	Yes	No	No	No	No	No	No	No
	S-Tag	No	No	No	No	No	No	Yes	No	Yes	No	No	No

Service Point Attributes

As described above, traffic ingresses and egresses the service via service points. The service point attributes are divided into two types:

- **Ingress Attributes** – Define how frames are handled upon ingress, e.g., policing and MAC address learning.
- **Egress Attributes** – Define how frames are handled upon egress, e.g., preservation of the ingress CoS value upon egress, VLAN swapping.

The following figure shows the ingress and egress path relationship on a point-to-point service path. When traffic arrives via port 1, the system handles it using service point 1 ingress attributes then forwards it to service point 2 and handles it using the SP2 egress attributes:

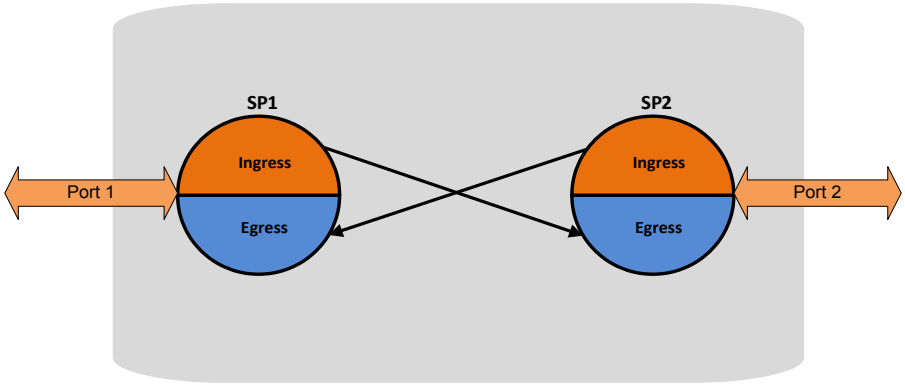


Figure 89: Service Path Relationship on Point-to-Point Service Path

Service points have the following attributes:

General Service Point Attributes

- **Service Point ID** – Users can define up to 32 service points per service, except for management services which are limited to 30 service points in addition to the pre-defined management system service point.
- **Service Point Name** – A descriptive name, which can be up to 20 characters.
- **Service Point Type** – The type of service point, as described above.
- **S-VLAN Encapsulation** – The S-VLAN ID associated with the service point.
- **C-VLAN Encapsulation** – The C-VLAN ID associated with the service point.
- **Attached C VLAN** – For service points with an Attached Interface Type of Bundle C-Tag, this attribute is used to create a list of C-VLANs associated with the service point.
- **Attached S-VLAN** – For service points with an Attached Interface Type of Bundle S-Tag, this attribute is used to create a list of S-VLANs associated with the service point.

Ingress Service Point Attributes

The ingress attributes are attributes that operate upon frames when they ingress via the service point.

- **Attached Interface Type** – The interface type to which the service point is attached, as described above. Permitted values depend on the service point type.
- **Learning Administration** – Enables or disables MAC address learning for traffic that ingresses via the service point. This option enables users to enable or disable MAC address learning for specific service points.
- **Allow Broadcast** – Determines whether to allow frames to ingress the service via the service point when the frame has a broadcast destination MAC address.
- **Allow Flooding** – Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding.
- **CoS Mode** – Determines whether the service point preserves the CoS decision made at the interface level, overwrites the CoS with the default CoS for the service point.
- **Default CoS** – The service point CoS. If the CoS Mode is set to overwrite the CoS decision made at the interface level, this is the CoS value assigned to frames that ingress the service point.
- **Token Bucket Profile** – This attribute can be used to attach a rate meter profile to the service point. Permitted values are 1– 250.
- **CoS Token Bucket Profile** – This attribute can be used to attach a rate meter profile to the service point at the CoS level. Users can define a rate meter for each of the eight CoS values of the service point. Permitted values are 1-250 for CoS 0–7.
- **CoS Token Bucket Admin** – Enables or disables the rate meter at the service point CoS level.

Egress Service Point Attributes

The egress attributes are attributes that operate upon frames egressing via the service point.

- **C-VLAN ID Egress Preservation** – If enabled, C-VLAN frames egressing the service point retain the same C-VLAN ID they had when they entered the service.
- **C-VLAN CoS Egress Preservation** – If enabled, the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service.
- **S-VLAN CoS Egress Preservation** – If enabled, the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service.

- **Marking** – Marking refers to the ability to overwrite the outgoing priority bits and Color of the outer VLAN of the egress frame, either the C-VLAN or the S-VLAN. If marking is enabled, the service point overwrites the outgoing priority bits and Color of the outer VLAN of the egress frame. Marking mode is only relevant if either the outer frame is S-VLAN and S-VLAN CoS preservation is disabled, or the outer frame is C-VLAN and C-VLAN CoS preservation is disabled. When marking is enabled and active, marking is performed according to global mapping tables that map the 802.1p-UP bits and the DEI or CFI bit to a defined CoS and Color value.
- **Service Bundle ID** – This attribute can be used to assign one of the available service bundles from the H-QoS hierarchy queues to the service point. This enables users to personalize the QoS egress path. For details, refer to *Standard QoS and Hierarchical* QoS (H-QoS)on page 178.

6.3.5 Ethernet Interfaces

The IP-20F switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric.

The concept of a physical interface refers to the physical characteristics of the interface, such as speed, duplex, auto-negotiation, master/slave, and standard RMON statistics.

A logical interface can consist of a single physical interface or a group of physical interfaces that share the same function. Examples of the latter are Multi-Carrier ABC groups, protection groups, and link aggregation (LAG) groups. Switching and QoS functionality are implemented on the logical interface level.

It is important to understand that the IP-20F switching fabric regards all traffic interfaces as regular physical interfaces, distinguished only by the media type the interface uses, e.g., RJ-45, SFP, or Radio.

From the user's point of view, the creation of the logical interface is simultaneous with the creation of the physical interface. For example, when the user enables a radio interface, both the physical and the logical radio interface come into being at the same time.

Once the interface is created, the user configures both the physical and the logical interface. In other words, the user configures the same interface on two levels, the physical level and the logical level.

The following figure shows physical and logical interfaces in a one-to-one relationship in which each physical interface is connected to a single logical interface, without grouping.

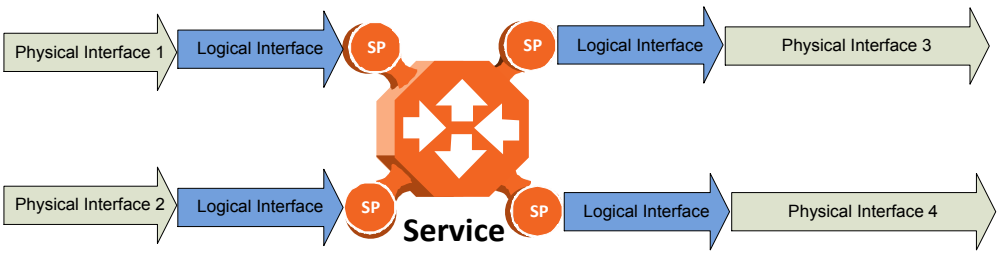


Figure 90: Physical and Logical Interfaces

Note:	For simplicity only, this figure represents a uni-directional rather than a bi-directional traffic flow.

The next figure illustrates the grouping of two or more physical interfaces into a logical interface, a link aggregation group (LAG) in this example. The two physical interfaces on the ingress side send traffic into a single logical interface. The user configures each physical interface separately, and configures the logical interface as a single logical entity. For example, the user might configure each physical interface to 100 Mbps, full duplex, with auto-negotiation off. On the group level, the user might limit the group to a rate of 200 Mbps by configuring the rate meter on the logical interface level.

When physical interfaces are grouped into a logical interface, IP-20F also shows standard RMON statistics for the logical interface, i.e., for the group. This information enables users to determine the cumulative statistics for the group, rather than having to examine the statistics for each interface individually.

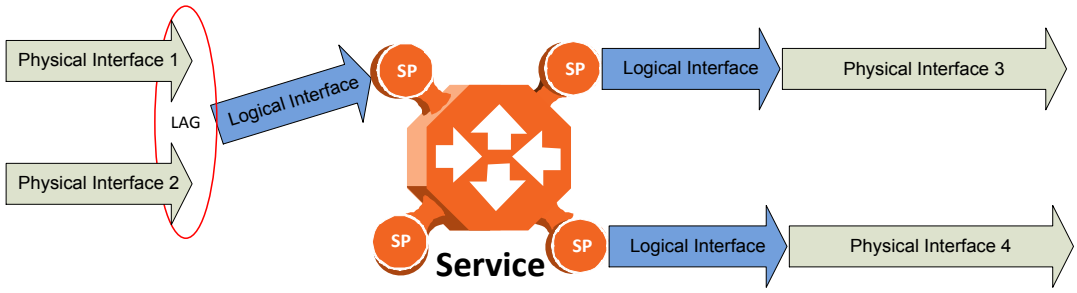


Figure 91: Grouped Interfaces as a Single Logical Interface on Ingress Side

Note:	For simplicity only, this figure represents a uni-directional rather than a bi-directional traffic flow.

The following figure shows the logical interface at the egress side. In this case, the user can configure the egress traffic characteristics, such as scheduling, for the group as a whole as part of the logical interface attributes.

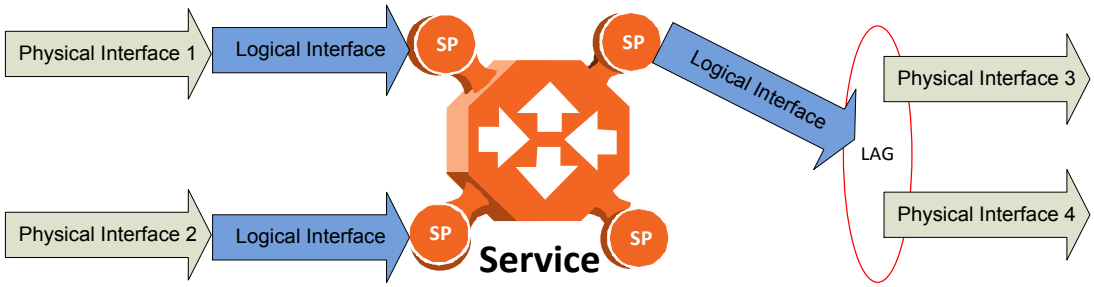


Figure 92: Grouped Interfaces as a Single Logical Interface on Egress Side

Note:	For simplicity only, this figure represents a uni-directional rather than a bi-directional traffic flow.

6.3.5.1 Physical Interfaces

The physical interfaces refer to the real traffic ports (layer 1) that are connected to the network. The Media Type attribute defines the Layer 1 physical traffic interface type, which can be:

- Radio interface.
- RJ-45 or SFP for an Ethernet interface.
- TDM for an DS1 or OC-3 interface.

Physical Interface Attributes

The following physical interface parameters can be configured by users:

- **Admin** – Enables or disables the physical interface. This attribute is set via the Interface Manager section of the Web EMS.
- **Auto Negotiation** – Enables or disables auto-negotiation on the physical interface. Auto Negotiation is always off for radio, SFP, and TDM (pseudowire) interfaces.
- **Speed and Duplex** – The physical interface speed and duplex mode. Permitted values are:
  - **Ethernet RJ-45 interfaces**: 10Mbps HD, 10Mbps FD, 100Mbps HD, 100Mbps FD, and 1000Mbps FD.
  - **Ethernet SFP interfaces**: Only 1000FD is supported
  - **Radio and TDM (pseudowire) interfaces**: The parameter is read-only and set by the system to 1000FD.
- **Flow Control** – The physical port flow control capability. Permitted values are: Symmetrical Pause and/or Asymmetrical Pause. This parameter is only relevant in Full Duplex mode.[19]
- **Media Type** – The physical interface Layer 1 media type. This attribute is only relevant for Ethernet traffic ports (RJ-45 or SFP). Permitted values are Auto Detect, RJ-45, and SFP. When Auto Detect is selected, the system detects whether the optical or electrical port is being used. Auto Detect can only be used when the interface speed is set to 1000 Mbps.
- **IFG** – The physical port Inter-frame gap. Although users can modify the IFG field length, it is strongly recommended not to modify the default value of 12 bytes without a thorough understanding of how the modification will impact traffic. Permitted values are 6 to 15 bytes.
- **Preamble** – The physical port preamble value. Although users can modify the preamble field length, it is strongly recommended not to modify the default values of 8 bytes without a thorough understanding of how the modification will impact traffic. Permitted values are 6 to 15 bytes.
- **Interface description** – A text description of the interface, up to 40 characters.

The following read-only physical interface status parameters can be viewed by users:

- **Operational State** – The operational state of the physical interface (Up or Down).
- **Actual Speed and Duplex** – The actual speed and duplex value for the Ethernet link as agreed by the two sides of the link after the auto negotiation process.
- **Actual Flow Control State** – The actual flow control state values for the Ethernet link as agreed by the two sides after the auto negotiation process.

[19] This functionality is planned for future release.

- **Actual Physical Mode** (only relevant for RJ-45 interfaces) – The actual physical mode (master or slave) for the Ethernet link, as agreed by the two sides after the auto negotiation process.

Ethernet Statistics

The FibeAir IP-20F platform stores and displays statistics in accordance with RMON and RMON2 standards.

Users can display various peak TX and RX rates (in seconds) and average TX and RX rates (in seconds), both in bytes and in packets, for each measured time interval. Users can also display the number of seconds in the interval during which TX and RX rates exceeded the configured threshold.

The following transmit statistic counters are available:

- Transmitted bytes (not including preamble) in good or bad frames. Low 32 bits.
- Transmitted bytes (not including preamble) in good or bad frames. High 32 bits.
- Transmitted frames (good or bad)
- Multicast frames (good only)
- Broadcast frames (good only)
- Control frames transmitted
- Pause control frame transmitted
- FCS error frames
- Frame length error
- Oversized frames – frames with length > 1518 bytes (1522 bytes for VLAN-tagged frames) without errors
- Undersized frames (good only)
- Fragments frames (undersized bad)
- Jabber frames – frames with length > 1518 bytes (1522 for VLAN-tagged frames) with errors
- Frames with length 64 bytes, good or bad
- Frames with length 65-127 bytes, good or bad
- Frames with length 128-255 bytes, good or bad
- Frames with length 256-511 bytes, good or bad
- Frames with length 512-1023 bytes, good or bad.
- Frames with length 1024-1518 bytes, good or bad
- Frames with length 1519-1522 bytes, good or bad

The following receive statistic counters are available:

- Received bytes (not including preamble) in good or bad frames. Low 32 bits.
- Received bytes (not including preamble) in good or bad frames. High 32 bits.
- Received frames (good or bad)
- Multicast frames (good only)
- Broadcast frames (good only)

- Control frames received
- Pause control frame received
- FCS error frames
- Frame length error
- Code error
- Counts oversized frames – frames with length > 1518 bytes (1522 bytes for VLAN-tagged frames) without errors *and* frames with length > MAX_LEN without errors
- Undersized frames (good only)
- Fragments frames (undersized bad)
- Counts jabber frames – frames with length > 1518 bytes (1522 for VLAN-tagged frames) with errors
- Frames with length 64 bytes, good or bad
- Frames with length 65-127 bytes, good or bad
- Frames with length 128-255 bytes, good or bad
- Frames with length 256-511 bytes, good or bad
- Frames with length 512-1023 bytes, good or bad
- Frames with length 1024-1518 bytes, good or bad
- VLAN-tagged frames with length 1519-1522 bytes, good or bad
- Frames with length > MAX_LEN without errors
- Frames with length > MAX_LEN with errors

6.3.5.2 Logical Interfaces

A logical interface consists of one or more physical interfaces that share the same traffic ingress and egress characteristics. From the user's point of view, it is more convenient to define interface behavior for the group as a whole than for each individual physical interface that makes up the group. Therefore, classification, QoS, and resiliency attributes are configured and implemented on the logical interface level, in contrast to attributes such as interface speed and duplex mode, which are configured on the physical interface level.

It is important to understand that the user relates to logical interfaces in the same way in both a one-to-one scenario in which a single physical interface corresponds to a single logical interface, and a grouping scenario such as a Multi-Carrier ABC group, a link aggregation (LAG) group, or a radio protection group, in which several physical interfaces correspond to a single logical interface.

The following figure illustrates the relationship of a 1+1 HSB radio protection group to the switching fabric. From the point of view of the user configuring the logical interface attributes, the fact that there are two radios is not relevant. The user configures and manages the logical interface just as if it represented a single 1+0 radio.

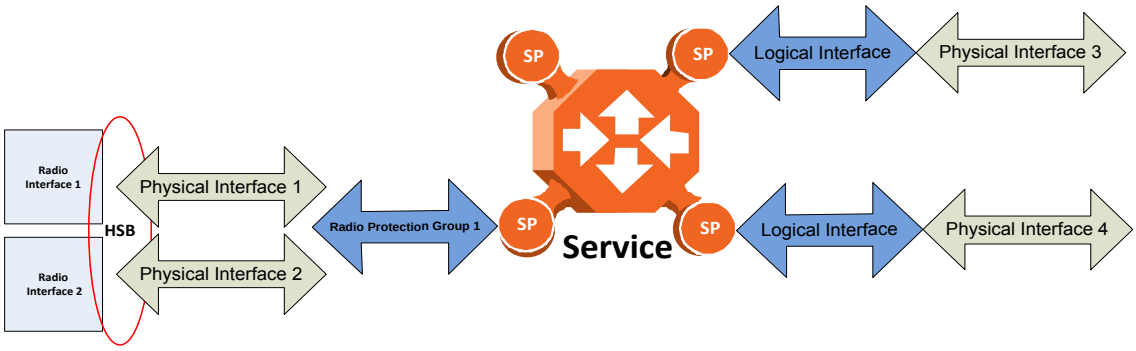


Figure 93: Relationship of Logical Interfaces to the Switching Fabric

Logical Interface Attributes

The following logical interface attributes can be configured by users:

General Attributes

- **Traffic Flow Administration** – Enables traffic via the logical interface. This attribute is useful when the user groups several physical interfaces into a single logical interface. The user can enable or disable traffic to the group using this parameter.

Ingress Path Classification at Logical Interface Level

These attributes represent part of the hierarchical classification mechanism, in which the logical interface is the lowest point in the hierarchy.

- **VLAN ID** – Users can specify a specific CoS and Color for a specific VLAN ID. In the case of double-tagged frames, the match must be with the frame's outer VLAN. Permitted values are CoS 0 to 7 and Color Green or Yellow per VLAN ID. This is the highest classification priority on the logical interface level, and overwrites any other classification criteria at the logical interface level.
- **802.1p Trust Mode** – When this attribute is set to Trust mode and the arriving packet is 802.1Q or 802.1AD, the interface performs QoS and Color classification according to user-configurable tables for 802.1q UP bit (C-VLAN frames) or 802.1AD UP bit (S-VLAN frames) to CoS and Color classification.
- **MPLS Trust Mode** – When this attribute is set to Trust mode and the arriving packet has MPLS EXP priority bits, the interface performs QoS and Color classification according to a user-configurable MPLS EXP bit to CoS and Color classification table. Both 802.1p and DSCP classification have priority over MPLS Trust Mode, so that if a match is found on either the 802.1p or DSCP levels, MPLS bits are not considered.
- **IP DSCP Trust Mode** –When this attribute is set to Trust mode and the arriving packet has IP priority bits, the interface performs QoS and Color classification according to a user-configurable DSCP bit to CoS and Color classification table. 802.1p classification has priority over DSCP Trust Mode, so that if a match is found on the 802.1p level, DSCP bits are not considered.

- **Default CoS** – The default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level. The Color is assumed to be Green.

For more information about classification at the logical interface level, refer to *Logical Interface-Level Classification* on page 165.

Ingress Path Rate Meters at Logical Interface Level

- **Unicast Traffic Rate Meter Admin** – Enables or disables the unicast rate meter (policer) on the logical interface.
- **Unicast Traffic Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Multicast Traffic Rate Meter Admin** – Enables or disables the multicast rate meter (policer) on the logical interface.
- **Multicast Traffic Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Broadcast Traffic Rate Meter Admin** – Enables or disables the broadcast rate meter (policer) on the logical interface.
- **Broadcast Traffic Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 1 Rate Meter Admin** – Enables or disables the Ethertype 1 rate meter (policer) on the logical interface.
- **Ethertype 1 Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 1 Value** – The Ethertype value to which the user wants to apply this rate meter (policer). The field length is 4 nibbles (for example, 0x0806 - ARP).
- **Ethertype 2 Rate Meter Admin** – Enables or disables the Ethertype 2 rate meter (policer) on the logical interface.
- **Ethertype 2 Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 2 Value** – The Ethertype value to which the user wants to apply the rate meter (policer). The field length is 4 nibbles (for example, 0x0806 - ARP).
- **Ethertype 3 Rate Meter Admin** – Enables or disables the Ethertype 3 rate meter (policer) on the logical interface.
- **Ethertype 3 Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 3 Value** – The Ethertype value to which the user wants to apply the rate meter (policer). The field length is 4 nibbles (for example, 0x0806 - ARP).
- **Inline Compensation** – The logical interface's ingress compensation value. The rate meter (policer) attached to the logical interface uses this value to compensate for Layer 1 non-effective traffic bytes.

Egress Path Shapers at Logical Interface Level

- **Logical Port Shaper Profile** – Users can assign a single leaky bucket shaper to each interface. The shaper on the interface level stops traffic from the interface if a specific user-defined peak information rate (PIR) has been exceeded.[20]
- **Outline Compensation** – The logical interface's egress compensation value. Any shaper attached to this interface, in any layer, uses this value to compensate for Layer 1 non-effective traffic bytes. Permitted values are even numbers between 0 and 26 bytes. The default value is 0 bytes.

Egress Path Scheduler at Logical Interface Level

- **Logical Interface Priority Profile** – This attribute is used to attach an egress scheduling priority profile to the logical interface.
- **Logical Port WFQ Profile** – This attribute is used to attach an egress scheduling WFQ profile to the logical interface. The WFQ profile provides a means of allocating traffic among queues with the same priority.

The following read-only logical interface status parameters can be viewed by users:

- **Traffic Flow Operational Status** – Indicates whether or not the logical interface is currently functional.

Logical Interface Statistics

RMON Statistics at Logical Interface Level

As discussed in *Ethernet Statistics* on page 155, if the logical interface represents a group, such as a LAG or a 1+1 HSB pair, the IP-20F platform stores and displays RMON and RMON2 statistics for the logical interface.

Rate Meter (Policer) Statistics at Logical Interface Level

For the rate meter (policer) at the logical interface level, users can view the following statistics counters:

- Green Frames
- Green Bytes
- Yellow Frames
- Yellow Bytes
- Red Frames
- Red Bytes

Note: Rate meter (policer) counters are 64 bits wide.

[20] This attribute is reserved for future use. The current release supports traffic shaping per queue and per service bundle, which provides the equivalent of shaping per logical interface.

Link Aggregation Groups (LAG) and LACP

Link aggregation (LAG) enables users to group several physical interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing function. IP-20F uses a distribution function of up to Layer 4 in order to generate the most efficient distribution among the LAG physical ports, taking into account:

- MAC DA and MAC SA
- IP DA and IP SA
- C-VLAN
- S-VLAN
- Layer 3 Protocol Field
- UDP/TCP Source Port and Destination Port
- MPLS Label

For LAG groups that consist of exactly two interfaces, users can change the distribution function by selecting from ten pre-defined LAG distribution schemes. The feature includes a display of the TX throughput for each interface in the LAG, to help users identify the best LAG distribution scheme for their specific link.

LAG can be used to provide redundancy for Ethernet interfaces, both on the same card (line protection) and on separate cards (line protection and equipment protection). LAGs can also be used to provide redundancy for radio links.

LAG can also be used to aggregate several interfaces in order to create a wider (aggregate) Ethernet link. For example, LAG can be used to create a 4 Gbps channel.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if the customer wants traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.

Up to four LAG groups can be created.

Link Aggregation Control Protocol (LACP) expands the capabilities of static LAG, and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

IP-20's LACP implementation does not include write parameters or churn detection.

Note:	LACP can only be used with Ethernet interfaces. LACP cannot be used with Enhanced LAG Distribution or with the LAG Group Shutdown in Case of Degradation Event feature.

LAG groups can include interfaces with the following constraints:

- Only physical interfaces (including radio interfaces), not logical interfaces, can belong to a LAG group.
- Interfaces can only be added to the LAG group if no services or service points are attached to the interface.
- Any classification rules defined for the interface are overridden by the classification rules defined for the LAG group.
- When removing an interface from a LAG group, the removed interface is assigned the default interface values.

IP-20F enables users to select the LAG members without limitations, such as interface speed and interface type. Proper configuration of a LAG group is the responsibility of the user.

6.3.6 Quality of Service (QoS)

Related topics:

- Ethernet Service Model
- In-Band Management

Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

IP-20F's personalized QoS enables operators to handle a wide and diverse range of scenarios. IP-20F's smart QoS mechanism operates from the frame's ingress into the switching fabric until the moment the frame egresses via the destination port.

QoS capability is very important due to the diverse topologies that exist in today's network scenarios. These can include, for example, streams from two different ports that egress via single port, or a port-to-port connection that holds hundreds of services. In each topology, a customized approach to handling QoS will provide the best results.

The figure below shows the basic flow of IP-20F's QoS mechanism. Traffic ingresses (left to right) via the Ethernet or radio interfaces, on the "ingress path." Based on the services model, the system determines how to route the traffic. Traffic is then directed to the most appropriate output queue via the "egress path."

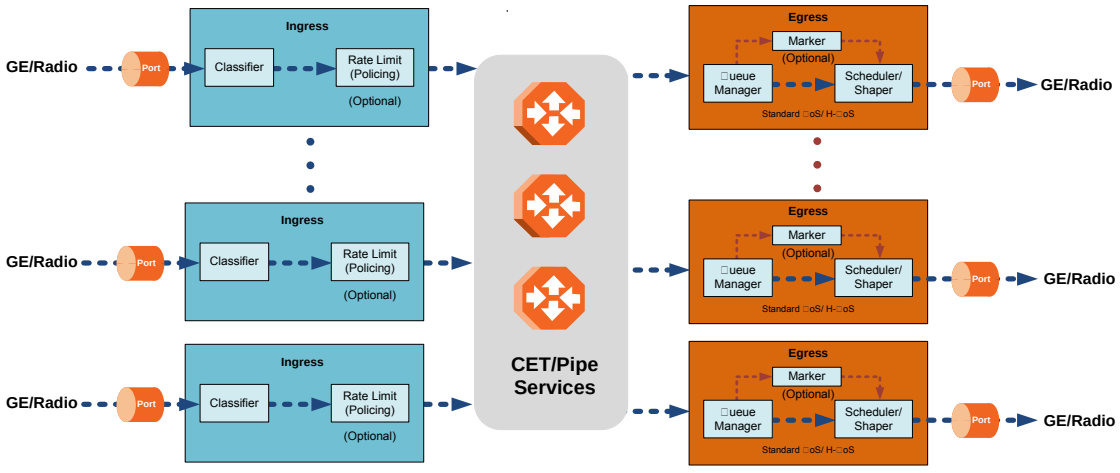


Figure 94: QoS Block Diagram

The ingress path consists of the following QoS building blocks:

- **Ingress Classifier** – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service. The classifier determines the exact traffic stream and associates it with the appropriate service. It also calculates an ingress frame CoS and Color. CoS and Color classification can be performed on three levels, according to the user's configuration.

- **Ingress Rate Metering** – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service point CoS. The rate metering mechanism enables the system to measure the incoming frame rate on different levels using a TrTCM standard MEF rate meter, and to determine whether to modify the color calculated during the classification stage.

The egress path consists of the following QoS building blocks:

- **Queue Manager** – This is the mechanism responsible for managing the transmission queues, utilizing smart WRED per queue and per packet color (Green or Yellow).
- **Scheduling and Shaping** – A hierarchical mechanism that is responsible for scheduling the transmission of frames from the transmission queues, based on priority among queues, Weighted Fair Queuing (WFQ) in bytes per each transmission queue, and eligibility to transmit based on required shaping on several different levels (per queue, per service bundle, and per port).
- **Marker** – This mechanism provides the ability to modify priority bits in frames based on the calculated CoS and Color.

The following two modes of operation are available on the egress path:

- **Standard QoS** – This mode provides eight transmission queues per port.
- **Hierarchical QoS (H-QoS)** – In this mode, users can associate services from the service model to configurable groups of eight transmission queues (service bundles), from a total 2.5K queues. In H-QoS mode, IP-20F performs QoS in a hierarchical manner in which the egress path is managed on three levels: ports, service bundles, and specific queues. This enables users to fully distinguish between streams, therefore providing a true SLA to customers.

The following figure illustrates the difference between how standard QoS and H-QoS handle traffic:

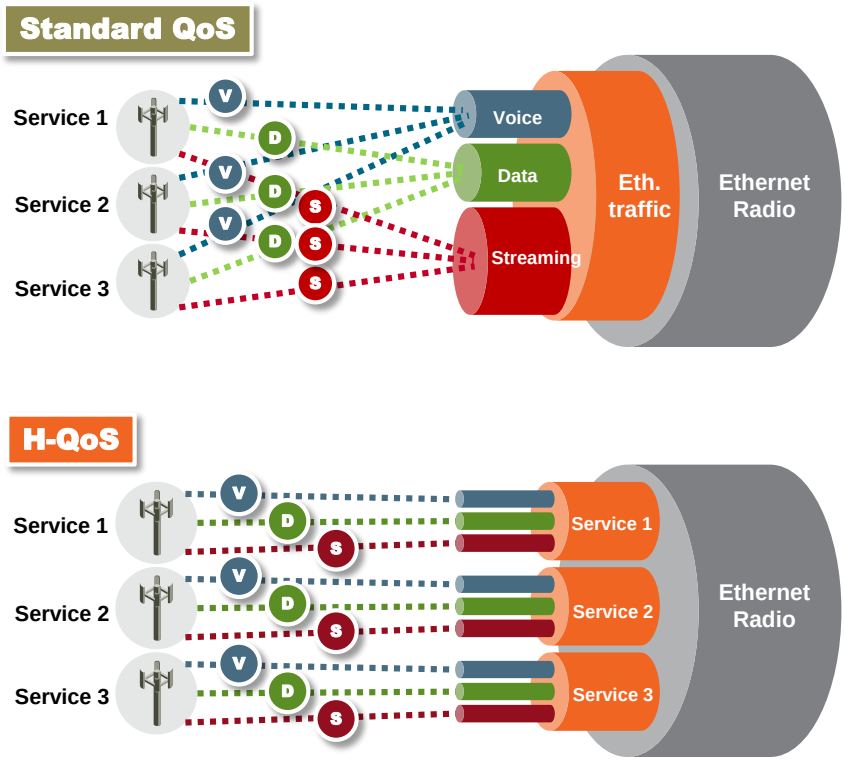


Figure 95: Standard QoS and H-QoS Comparison

6.3.6.1 QoS on the Ingress Path

Classification

IP-20F supports a hierarchical classification mechanism. The classification mechanism examines incoming frames and determines their CoS and Color. The benefit of hierarchical classification is that it provides the ability to “zoom in” or “zoom out”, enabling classification at higher or lower levels of the hierarchy. The nature of each traffic stream defines which level of the hierarchical classifier to apply, or whether to use several levels of the classification hierarchy in parallel.

The hierarchical classifier consists of the following levels:

- Logical interface-level classification
- Service point-level classification
- Service level classification

The following figure illustrates the hierarchical classification model. In this figure, traffic enters the system via the port depicted on the left and enters the service via the SAP depicted on the upper left of the service. The classification can take place at the logical interface level, the service point level, and/or the service level.

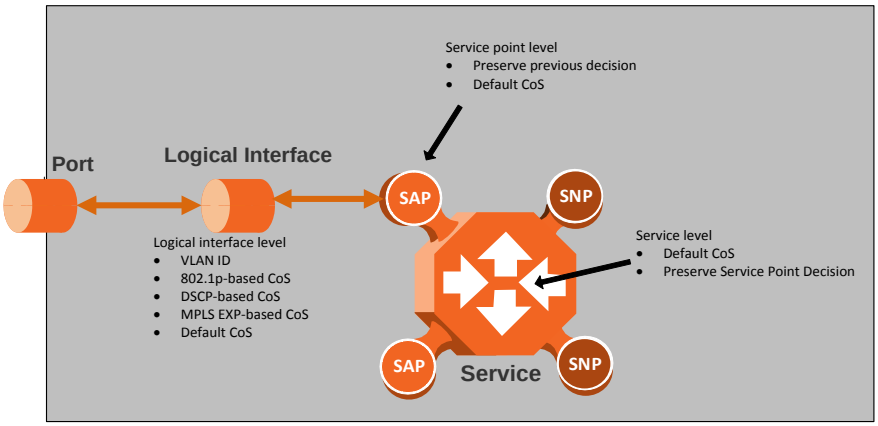


Figure 96: Hierarchical Classification

Logical Interface-Level Classification

Logical interface-level classification enables users to configure classification on a single interface or on a number of interfaces grouped tougher, such as a LAG group.

The classifier at the logical interface level supports the following classification methods, listed from highest to lowest priority. A higher level classification method supersedes a lower level classification method:

- VLAN ID
- 802.1p bits.
- MPLS EXP field.
- DSCP bits.
- Default CoS

IP-20F performs the classification on each frame ingressing the system via the logical interface. Classification is performed step by step from the highest priority to the lowest priority classification method. Once a match is found, the classifier determines the CoS and Color decision for the frame for the logical interface-level.

For example, if the frame is an untagged IP Ethernet frame, a match will not be found until the third priority level (DSCP priority bits). The CoS and Color values defined for the frame's DSCP priority bits will be applied to the frame.

Users can disable some of these classification methods by configuring them as un-trusted. For example, if 802.1p classification is configured as un-trusted for a specific interface, the classification mechanism does not perform classification by VLAN UP bits. This is useful, for example, if the required classification is based on DSCP priority bits.

If no match is found at the logical interface level, the default CoS is applied to incoming frames at this level. In this case, the Color of the frame is assumed to be Green.

The following figure illustrates the hierarchy of priorities among classification methods, from highest (on the left) to lowest (on the right) priority.

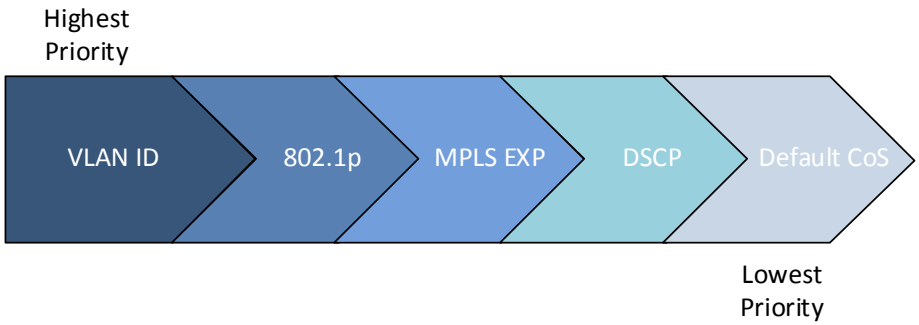


Figure 97: Classification Method Priorities

Interface-level classification is configured as part of the logical interface configuration. For details, refer to *Ingress Path Classification at Logical Interface Level* on page 157.

The following tables show the default values for logical interface-level classification. The key values for these tables are the priority bits of the respective frame encapsulation layers (VLAN, IP, and MPLS), while the key results are the CoS and Colors calculated for incoming frames. These results are user-configurable, but it is recommended that only advanced users should modify the default values.

Table 50: C-VLAN 802.1 UP and CFI Default Mapping to CoS and Color

802.1 UP	CFI	CoS (configurable)	Color (configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green

802.1 UP	CFI	CoS (configurable)	Color (configurable)
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

Table 51: S-VLAN 802.1 UP and DEI Default Mapping to CoS and Color

802.1 UP	DEI	CoS (Configurable)	Color (Configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

Table 52: MPLS EXP Default Mapping to CoS and Color

MPLS EXP bits	CoS (configurable)	Color (configurable)
0	0	Yellow
1	1	Green
2	2	Yellow
3	3	Green
4	4	Yellow
5	5	Green
6	6	Green
7	7	Green

Table 53: DSCP Default Mapping to CoS and Color

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
0 (default)	000000	BE (CS0)	0	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow
14	001110	AF13	1	Yellow
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow
30	011110	AF33	3	Yellow
34	100010	AF41	4	Green
36	100100	AF42	4	Yellow
38	100110	AF43	4	Yellow
46	101110	EF	7	Green
8	001000	CS1	1	Green
16	010000	CS2	2	Green
24	011000	CS3	3	Green
32	100000	CS4	4	Green
40	101000	CS5	5	Green
48	110000	CS6	6	Green
51	110011	DSCP_51	6	Green
52	110100	DSCP_52	6	Green
54	110110	DSCP_54	6	Green
56	111000	CS7	7	Green

Default value is CoS equal best effort and Color equal Green.

Service Point-Level Classification

Classification at the service point level enables users to give special treatment, in higher resolution, to specific traffic flows using a single interface to which the service point is attached. The following classification modes are supported at the service point level. Users can configure these modes by means of the service point CoS mode.

- Preserve previous CoS decision (logical interface level)

- Default service point CoS

If the service point CoS mode is configured to preserve previous CoS decision, the CoS and Color are taken from the classification decision at the logical interface level. If the service point CoS mode is configured to default service point CoS mode, the CoS is taken from the service point's default CoS, and the Color is Green.

Service-Level Classification

Classification at the service level enables users to provide special treatment to an entire service. For example, the user might decide that all frames in a management service should be assigned a specific CoS regardless of the ingress port. The following classification modes are supported at the service level:

- Preserve previous CoS decision (service point level)
- Default CoS

If the service CoS mode is configured to preserve previous CoS decision, frames passing through the service are given the CoS and Color that was assigned at the service point level. If the service CoS mode is configured to default CoS mode, the CoS is taken from the service's default CoS, and the Color is Green.

Rate Meter (Policing)

IP-20F's TrTCM rate meter mechanism complies with MEF 10.2, and is based on a dual leaky bucket mechanism. The TrTCM rate meter can change a frame's CoS settings based on CIR/EIR+CBS/EBS, which makes the rate meter mechanism a key tool for implementing bandwidth profiles and enabling operators to meet strict SLA requirements.

The IP-20F hierarchical rate metering mechanism is part of the QoS performed on the ingress path, and consists of the following levels:

- Logical interface-level rate meter
- Service point-level rate meter[21]
- Service point CoS-level rate meter[22]

MEF 10.2 is the de-facto standard for SLA definitions, and IP-20F's QoS implementation provides the granularity necessary to implement service-oriented solutions.

Hierarchical rate metering enables users to define rate meter policing for incoming traffic at any resolution point, from the interface level to the service point level, and even at the level of a specific CoS within a specific service point. This option enables users to customize a set of eight policers for a variety of traffic flows within a single service point in a service.

---

21 Service point-level rate metering is planned for future release.

22 Service point and CoS-level rate metering is planned for future release.

Another important function of rate metering is to protect resources in the network element from malicious users sending traffic at an unexpectedly high rate. To prevent this, the rate meter can cut off traffic from a user that passes the expected ingress rate.

TrTCM rate meters use a leaky bucket mechanism to determine whether frames are marked Green, Yellow, or Red. Frames within the Committed Information Rate (CIR) or Committed Burst Size (CBS) are marked Green. Frames within the Excess Information Rate (EIR) or Excess Burst Size (EBS) are marked Yellow. Frames that do not fall within the CIR/CBS+EIR/EBS are marked Red and dropped, without being sent any further.

IP-20F provides up to 1120 user-defined TrTCM rate meters. The rate meters implement a bandwidth profile, based on CIR/EIR, CBS/EBS, Color Mode (CM), and Coupling flag (CF). Up to 250 different profiles can be configured.

Ingress rate meters operate at three levels:

- Logical Interface:
  - Per frame type (unicast, multicast, and broadcast)
  - Per frame ethertype
- Per Service Point
- Per Service Point CoS

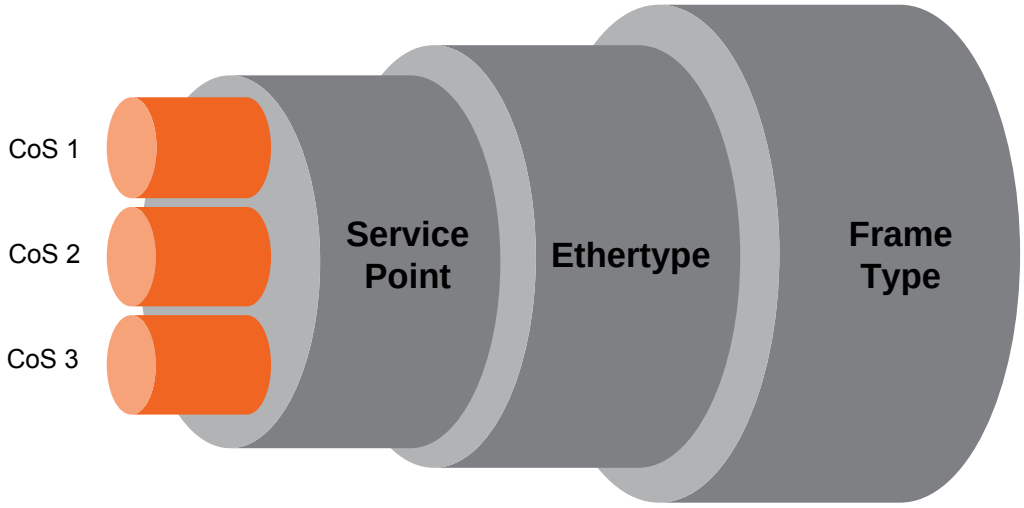


Figure 98: Ingress Policing Model

At each level (logical interface, service point, and service point + CoS), users can attach and activate a rate meter profile. Users must create the profile first, then attach it to the interface, service point, or service point + CoS.

Global Rate Meter Profiles

Users can define up to 250 rate meter user profiles. The following parameters can be defined for each profile:

- **Committed Information Rate (CIR)** – Frames within the defined CIR are marked Green and passed through the QoS module. Frames that exceed the CIR rate are marked Yellow. The CIR defines the average rate in bits/s of Service Frames up to which the network delivers service frames and meets the performance objectives. Permitted values are 0 to 1 Gbps, with a minimum granularity of 32Kbps.
- **Committed Burst Size (CBS)** – Frames within the defined CBS are marked Green and passed through the QoS module. This limits the maximum number of bytes available for a burst of service frames in order to ensure that traffic conforms to the CIR. Permitted values are 0 to 8192 Kbytes, with a minimum granularity of 2 Kbytes.
- **Excess Information Rate (EIR)** – Frames within the defined EIR are marked Yellow and processed according to network availability. Frames beyond the combined CIR and EIR are marked Red and dropped by the policer. Permitted values are 0 to 1 Gbps, with a minimum granularity of 32 Kbps.
- **Excess Burst Size (EBS)** – Frames within the defined EBS are marked Yellow and processed according to network availability. Frames beyond the combined CBS and EBS are marked Red and dropped by the policer. Permitted values are 0 to 8192 Kbytes, with a minimum granularity of 2 Kbytes.
- **Color Mode** – Color mode can be enabled (Color aware) or disabled (Color blind). In Color aware mode, all frames that ingress with a CFI/DEI field set to 1 (Yellow) are treated as EIR frames, even if credits remain in the CIR bucket. In Color blind mode, all ingress frames are treated first as Green frames regardless of CFI/DEI value, then as Yellow frames (when there is no credit in the Green bucket). A Color-blind policer discards any previous Color decisions.
- **Coupling Flag** – If the coupling flag between the Green and Yellow buckets is enabled, then if the Green bucket reaches the maximum CBS value the remaining credits are sent to the Yellow bucket up to the maximum value of the Yellow bucket.

The following parameter is neither a profile parameter, nor specifically a rate meter parameter, but rather, is a logical interface parameter. For more information about logical interfaces, refer to *Logical Interfaces* on page 156.

- **Line Compensation** – A rate meter can measure CIR and EIR at Layer 1 or Layer 2 rates. Layer 1 capacity is equal to Layer 2 capacity plus 20 additional bytes for each frame due to the preamble and Inter Frame Gap (IFG). In most cases, the preamble and IFG equals 20 bytes, but other values are also possible. Line compensation defines the number of bytes to be added to each frame for purposes of CIR and EIR calculation. When Line Compensation is 20, the rate meter operates as Layer 1. When Line Compensation is 0, the rate meter operates as Layer 2. This parameter is very important to users that want to distinguish between Layer 1 and Layer 2 traffic. For example, 1 Gbps of traffic at Layer 1 is equal to ~760 Mbps if the frame size is 64 bytes, but ~986 Mbps if the frame size is 1500 bytes. This demonstrates that counting at Layer 2 is not always fair in comparison to counting at Layer 1, that is, the physical level.

Rate Metering (Policing) at the Logical Interface Level

Rate metering at the logical interface level supports the following:

- Unicast rate meter
- Multicast rate meter
- Broadcast rate mete
- User defined Ethertype 1 rate meter
- User defined Ethertype 2 rate meter
- User defined Ethertype 3 rate meter

For each rate meter, the following statistics are available:

- Green Frames (64 bits)
- Green Bytes (64 bits)
- Yellow Frames (64 bits)
- Yellow Bytes (64 bits)
- Red Frames (64 bits)
- Red Bytes (64 bits)

Rate Metering (Policing) at the Service Point Level

Users can define a single rate meter on each service point, up to a total number of 1024 rate meters per network element at the service point and CoS per service point levels.

The following statistics are available for each service point rate meter:

- Green Frames (64 bits)
- Green Bytes (64 bits)
- Yellow Frames (64 bits)
- Yellow Bytes (64 bits)
- Red Frames (64 bits)
- Red Bytes (64 bits)

Rate Metering (Policing) at the Service Point + CoS Level

Users can define a single rate meter for each CoS on a specific service point, up to a total number of 1024 rate meters per network element at the service point and CoS per service point levels.

The following statistics are available for each service point + CoS rate meter:

- Green Frames (64 bits)
- Green Bytes (64 bits)
- Yellow Frames (64 bits)
- Yellow Bytes (64 bits)
- Red Frames (64 bits)
- Red Bytes (64 bits)

6.3.6.2 QoS on the Egress Path

Queue Manager

The queue manager (QM) is responsible for managing the output transmission queues. IP-20F supports up to 8192 service-level transmission queues, with configurable buffer size. Users can specify the buffer size of each queue independently. The total amount of memory dedicated to the queue buffers is 4 Gigabits.

The following considerations should be taken into account in determining the proper buffer size:

- **Latency considerations** – If low latency is required (users would rather drop frames in the queue than increase latency) small buffer sizes are preferable.
- **Throughput immunity to fast bursts** – When traffic is characterized by fast bursts, it is recommended to increase the buffer sizes to prevent packet loss. Of course, this comes at the cost of a possible increase in latency.

Users can configure burst size as a tradeoff between latency and immunity to bursts, according the application requirements.

The 8192 queues are ordered in groups of eight queues. These eight queues correspond to CoS values, from 0 to 7; in other words, eight priority queues.

The following figure depicts the queue manager. Physically, the queue manager is located between the ingress path and the egress path.

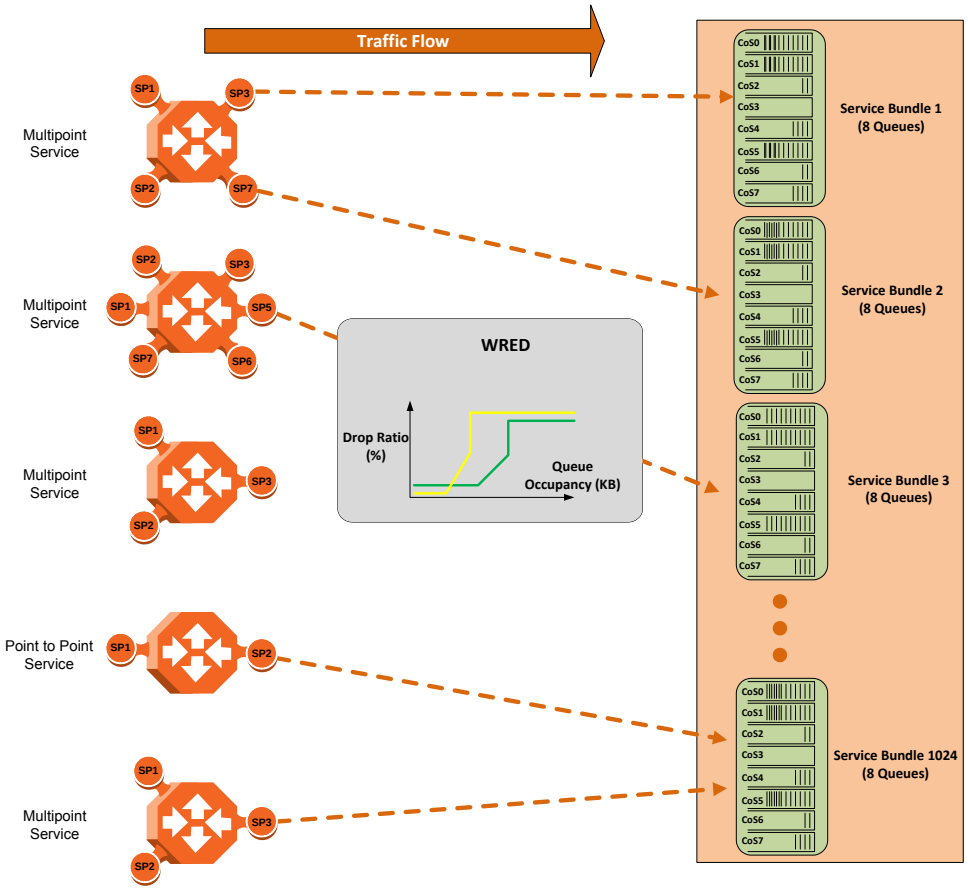


Figure 99: IP-20F Queue Manager

In the figure above, traffic is passing from left to right. The traffic passing from the ingress path is routed to the correct egress destination interfaces via the egress service points. As part of the assignment of the service points to the interfaces, users define the group of eight queues through which traffic is to be transmitted out of the service point. This is part of the service point egress configuration.

After the traffic is tunneled from the ingress service points to the egress service points, it is aggregated into one of the eight queues associated with the specific service point. The exact queue is determined by the CoS calculated by the ingress path. For example, if the calculated CoS is 6, the traffic is sent to queue 6, and so on.

Before assigning traffic to the appropriate queue, the system makes a determination whether to forward or drop the traffic using a WRED algorithm with a predefined green and yellow curve for the desired queue. This operation is integrated with the queue occupancy level.

The queues share a single memory of 2 Gbits. IP-20F enables users to define a specific size for each queue which is different from the default size. Moreover, users can create an over-subscription scenario among the queues for when the buffer size of the aggregate queues is lower than the total memory allocated to all the queues. In doing this, the user must understand both the benefits and the potential hazards, namely, that if a lack of buffer space occurs, the queue manager will drop incoming frames without applying the usual priority rules among frames.

The queue size is defined by the WRED profile that is associated with the queue. For more details, refer to *WRED* on page 175.

WRED

The Weighted Random Early Detection (WRED) mechanism can increase capacity utilization of TCP traffic by eliminating the phenomenon of global synchronization. Global synchronization occurs when TCP flows sharing bottleneck conditions receive loss indications at around the same time. This can result in periods during which link bandwidth utilization drops significantly as a consequence of simultaneous falling to a “slow start” of all the TCP flows. The following figure demonstrates the behavior of two TCP flows over time without WRED.

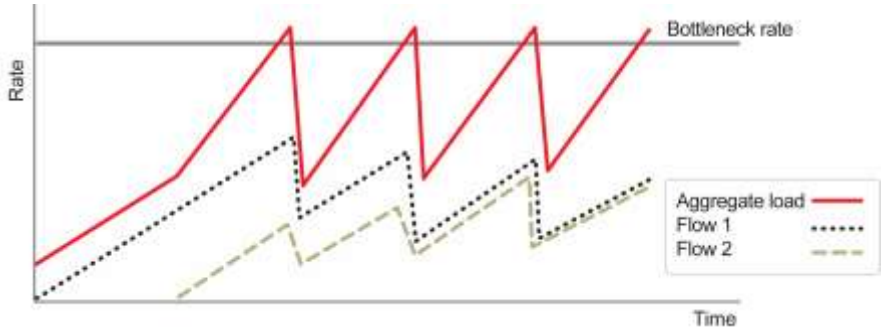


Figure 100: Synchronized Packet Loss

WRED eliminates the occurrence of traffic congestion peaks by restraining the transmission rate of the TCP flows. Each queue occupancy level is monitored by the WRED mechanism and randomly selected frames are dropped before the queue becomes overcrowded. Each TCP flow recognizes a frame loss and restrains its transmission rate (basically by reducing the window size). Since the frames are dropped randomly, statistically each time another flow has to restrain its transmission rate as a result of frame loss (before the real congestion occurs). In this way, the overall aggregated load on the radio link remains stable while the transmission rate of each individual flow continues to fluctuate similarly. The following figure demonstrates the transmission rate of two TCP flows and the aggregated load over time when WRED is enabled.

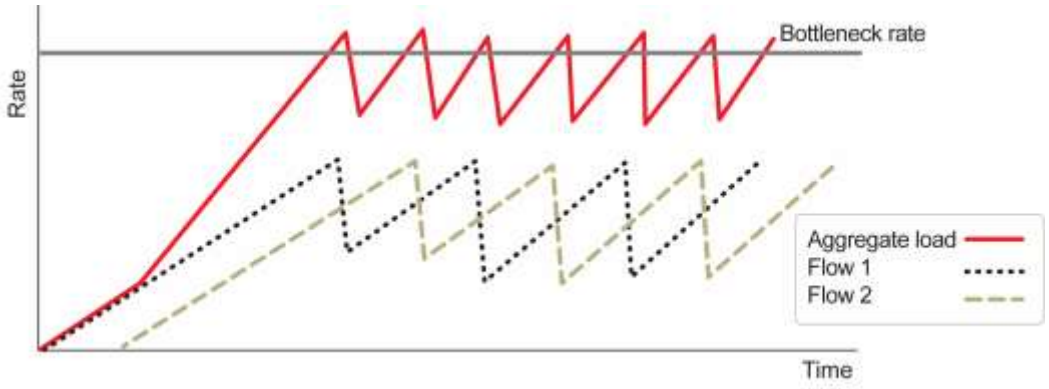


Figure 101: Random Packet Loss with Increased Capacity Utilization Using WRED

When queue occupancy goes up, this means that the ingress path rate (the TCP stream that is ingressing the switch) is higher than the egress path rate. This difference in rates should be fixed in order to reduce packet drops and to reach the maximal media utilization, since IP-20F will not egress packets to the media at a rate which is higher than the media is able to transmit.

To deal with this, IP-20F enables users to define up to 30 WRED profiles. Each profile contains a Green traffic curve and a Yellow traffic curve. These curves describe the probability of randomly dropping frames as a function of queue occupancy. In addition, using different curves for Yellow packets and Green packets enables users to enforce the rule that Yellow packets be dropped before Green packets when there is congestion.

IP-20F also includes two pre-defined read-only WRED profile.

- Profile number 31 defines a tail-drop curve and is configured with the following values:
  - 100% Yellow traffic drop after 64kbytes occupancy.
  - 100% Green traffic drop after 128kbytes occupancy.
  - Yellow maximum drop is 100%
  - Green maximum drop is 100%
- Profile number 32 defines a profile in which all will be dropped. It is for internal use and should not be applied to traffic.

A WRED profile can be assigned to each queue. The WRED profile assigned to the queue determines whether or not to drop incoming packets according to the occupancy of the queue. Basically, as queue occupancy grows, the probability of dropping each incoming frame increases as well. As a consequence, statistically more TCP flows will be restrained before traffic congestion occurs.

The following figure provides an example of a WRED profile.

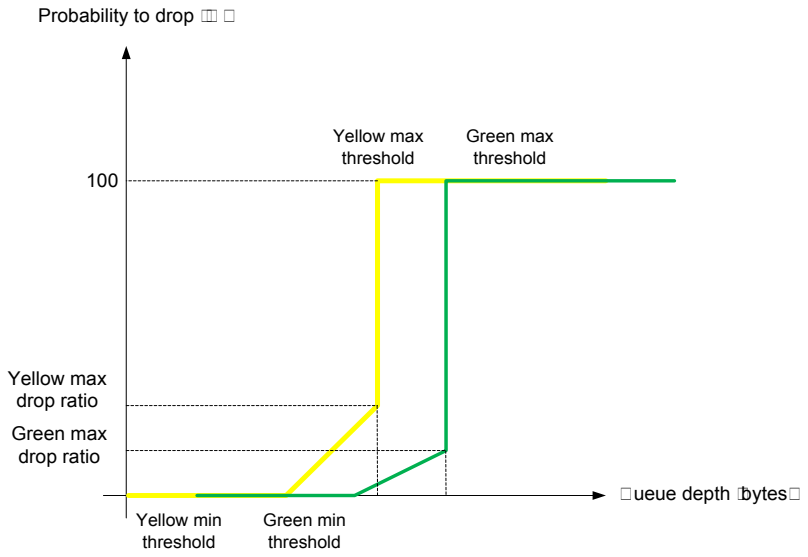


Figure 102: WRED Profile Curve

Note:	The tail-drop profile, Profile 31, is the default profile for each queue. A tail drop curve is useful for reducing the effective queue size, such as when low latency must be guaranteed.

Global WRED Profile Configuration

IP-20F supports 30 user-configurable WRED profiles and one pre-defined (default) profile. The following are the WRED profile attributes:

- **Green Minimum Threshold** – Permitted values are 0 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Green Maximum Threshold** – Permitted values are 0 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Green-Maximum Drop** – Permitted values are 1% to 100%, with 1% drop granularity.
- **Yellow Minimum Threshold** – Permitted values are 0 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Yellow Maximum Threshold** – Permitted values are 0 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Yellow Maximum Drop** – Permitted values are 1% to 100%, with 1% drop granularity.

Notes:	K is equal to 1024. Users can enter any value within the permitted range. Based on the value entered by the user, the software automatically rounds off the setting according to the granularity. If the user enters a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

For each curve, frames are passed on and not dropped up to the minimum Green and Yellow thresholds. From this point, WRED performs a pseudo-random drop with a ratio based on the curve up to the maximum Green and Yellow thresholds. Beyond this point, 100% of frames with the applicable Color are dropped.

The system automatically assigns the default “tail drop” WRED profile (Profile ID 31) to every queue. Users can change the WRED profile per queue based on the application served by the queue.

Standard QoS and Hierarchical QoS (H-QoS)

In a standard QoS mechanism, egress data is mapped to a single egress interface. This single interface supports up to eight priority queues, which correspond to the CoS of the data. Since all traffic for the interface egresses via these queues, there is no way to distinguish between different services and traffic streams within the same priority.

The figure below shows three services, each with three distinct types of traffic streams:

- Voice – high priority
- Data – medium priority
- Streaming – lower priority

While the benefits of QoS on the egress path can be applied to the aggregate streams, without H-QoS they will not be able to distinguish between the various services included in these aggregate streams. Moreover, different behavior among the different traffic streams that constitute the aggregate stream can cause unpredictable behavior between the streams. For example, in a situation in which one traffic stream can transmit 50 Mbps in a shaped manner while another can transmit 50 Mbits in a burst, frames may be dropped in an unexpected way due to a lack of space in the queue resulting from a long burst.

Hierarchical QoS (H-QoS) solves this problem by enabling users to create a real egress tunnel for each stream, or for a group of streams that are bundled together. This enables the system to fully perform H-QoS with a top-down resolution, and to fully control the required SLA for each stream.

H-QoS Hierarchy

The egress path hierarchy is based on the following levels:

- Queue level
- Service bundle level
- Logical interface level

The queue level represents the physical priority queues. This level holds 8192 queues. Each eight queues are bundled and represent eight CoS priority levels. One or more service points can be attached to a specific bundle, and the traffic from the service point to one of the eight queues is based on the CoS that was calculated on the ingress path.

Note:	With standard QoS, all services are assigned to a single default service bundle.

The service bundle level represents the groups of eight priority queues. Every eight queues are managed as a single service bundle. There are a total number of 1024 service bundles.

The interface level represents the physical port through which traffic from the specified service point egresses.

The following summarizes the egress path hierarchy:

- Up to 16 physical interfaces
- One service bundle per interface in standard QoS / 1024 service bundles in H-QoS.
- Eight queues per service bundle

H-QoS on the Interface Level

Users can assign a single leaky bucket shaper to each interface. The shaper on the interface level stops traffic from the interface if a specific user-defined peak information rate (PIR) has been exceeded.

In addition, users can configure scheduling rules for the priority queues, as follows:

- Scheduling (serve) priorities among the eight priority queues.
- Weighted Fair Queuing (WFQ) among queues with the same priority.

Note:	The system assigns the rules for all service bundles under the interface.

RMON counters are valid on the interface level.

H-QoS on the Service Bundle Level

Users can assign a dual leaky bucket shaper to each service bundle. On the service bundle level, the shaper changes the scheduling priority if traffic via the service bundle is above the user-defined CIR and below the PIR. If traffic is above the PIR, the scheduler stops transmission for the service bundle.

Service bundle traffic counters are valid on this level.

Note:	With standard QoS, users assign the egress traffic to a single service bundle (Service Bundle ID 1).

H-QoS on the Queue Level

The egress service point points to a specific service bundle. Depending on the user application, the user can connect either a single service point or multiple service points to a service bundle. Usually, if multiple service points are connected to a service bundle, the service points will share the same traffic type and characteristics. Mapping to the eight priority queues is based on the CoS calculated on the ingress path, before any marking operation, which only changes the egress CoS and Color.

Users can assign a single leaky bucket to each queue. The shaper on the queue level stops traffic from leaving the queue if a specific user-defined PIR has been exceeded.

Traffic counters are valid on this level.

The following figure provides a detailed depiction of the H-QoS levels.

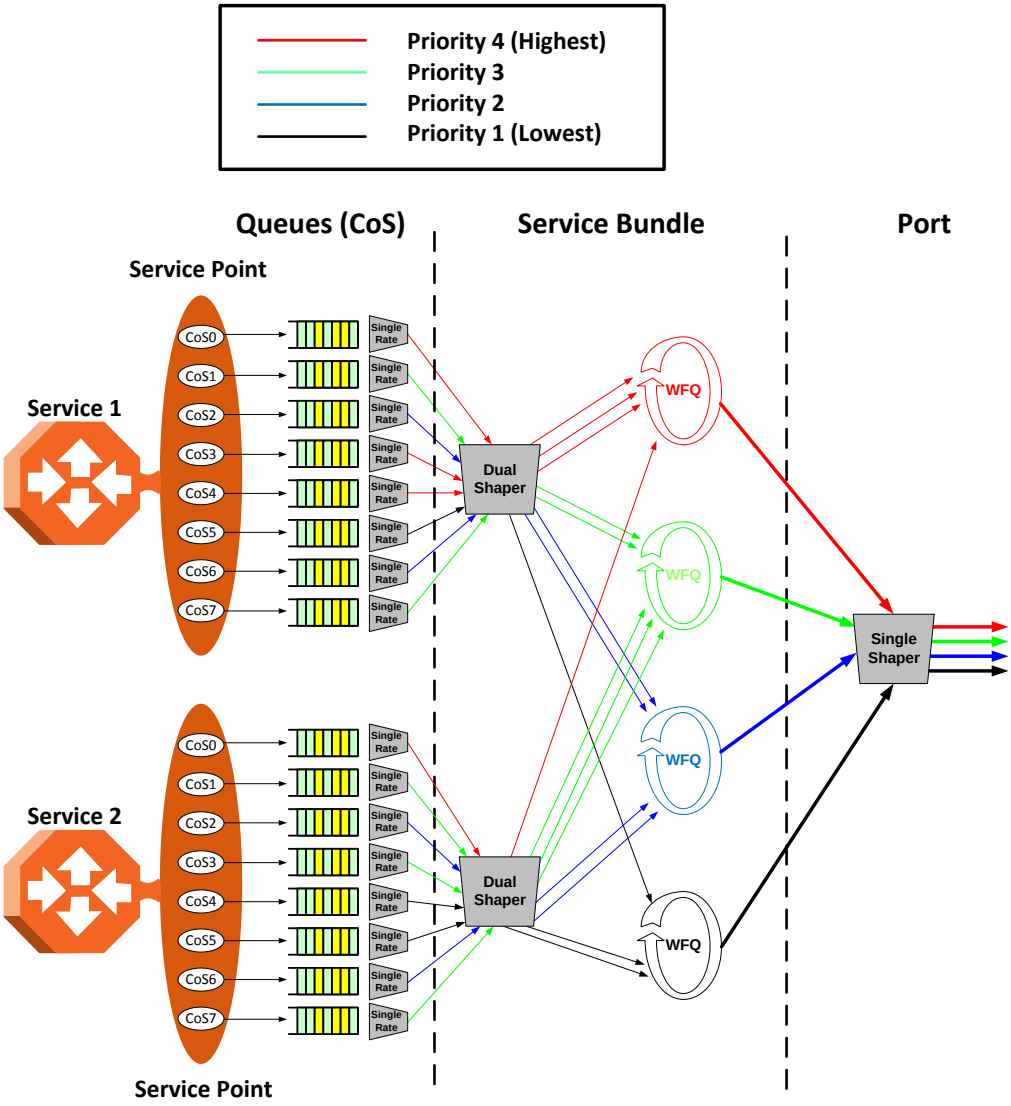


Figure 103: Detailed H-QoS Diagram

H- QoS Mode

As discussed above, users can select whether to work in Standard QoS mode or H-QoS mode.

- If the user configured all the egress service points to transmit traffic via a single service bundle, the operational mode is Standard QoS. In this mode, only Service Bundle 1 is active and there are eight output transmission queues.
- If the user configured the egress service points to transmit traffic via multiple service bundles, the operational mode is H-QoS. H-QoS mode enables users to fully distinguish among the streams and to achieve SLA per service.

Shaping on the Egress Path

Egress shaping determines the traffic profile for each queue. IP-20F performs egress shaping on the following three levels:

- Queue level – Single leaky bucket shaping.
- Service Bundle level – Dual leaky bucket shaping
- Interface level – Single leaky bucket shaping

Queue Shapers

Users can configure up to 31 single leaky bucket shaper profiles. The CIR value can be set to the following values:

- 16,000 – 32,000,000 bps – granularity of 16,000 bps
- 32,000,000 – 131,008,000 bps – granularity of 64,000 bps

Note:	Users can enter any value within the permitted range. Based on the value entered by the user, the software automatically rounds off the setting according to the granularity. If the user enters a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

Users can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

Service Bundle Shapers

Users can configure up to 255 dual leaky bucket shaper profiles. The profiles can be configured as follows:

- Valid CIR values are:
  - 0 – 32,000,000 bps – granularity of 16,000 bps
  - 32,000,000 – 1,000,000,000 bps – granularity of 64,000 bps
- Valid PIR values are:
  - 16,000 – 32,000,000 bps – granularity of 16,000 bps
  - 32,000,000 – 1,000,000,000 bps – granularity of 64,000 bps

Note:	Users can enter any value within the permitted range. Based on the value entered by the user, the software automatically rounds off the setting according to the granularity. If the user enters a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.

Users can attach one of the configured service bundle shaper profiles to each service bundle. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.

Interface Shapers

Users can configure up to 31 single leaky bucket shaper profiles. The CIR can be set to the following values:

- 0 – 8,192,000 bps – granularity of 32,000 bps
- 8,192,000 – 32,768,000 bps – granularity of 128,000 bps
- 32,768,000 – 131,072,000 bps – granularity of 512,000 bps
- 131,072,000 – 999,424,000 bps – granularity of 8,192,000 bps

Note:	Users can enter any value within the permitted range. Based on the value entered by the user, the software automatically rounds off the setting according to the granularity. If the user enters a value below the value (except 0), the software adjusts the setting to the minimum.

Users can attach one of the configured interface shaper profiles to each interface. If no profile is attached to the interface, no egress shaping is performed on that interface.

Line Compensation for Shaping

Users can configure a line compensation value for all the shapers under a specific logical interface. For more information, refer to *Global Rate Meter Profiles* on page 171.

Egress Scheduling

Egress scheduling is responsible for transmission from the priority queues. IP-20F uses a unique algorithm with a hierarchical scheduling model over the three levels of the egress path that enables compliance with SLA requirements.

The scheduler scans all the queues over all the service bundles, per interface, and determines which queue is ready to transmit. If more than one queue is ready to transmit, the scheduler determines which queue transmits first based on:

- **Queue Priority** – A queue with higher priority is served before lower-priority queues.
- **Weighted Fair Queuing (WFQ) –** If two or more queues have the same priority and are ready to transmit, the scheduler transmits frames from the queues based on a WFQ algorithm that determines the ratio of frames per queue based on a predefined weight assigned to each queue.

The following figure shows the scheduling mechanism for a single service bundle (equivalent to Standard QoS). When a user assigns traffic to more than a single service bundle (H-QoS mode), multiple instances of this model (up to 64 per port) are valid.

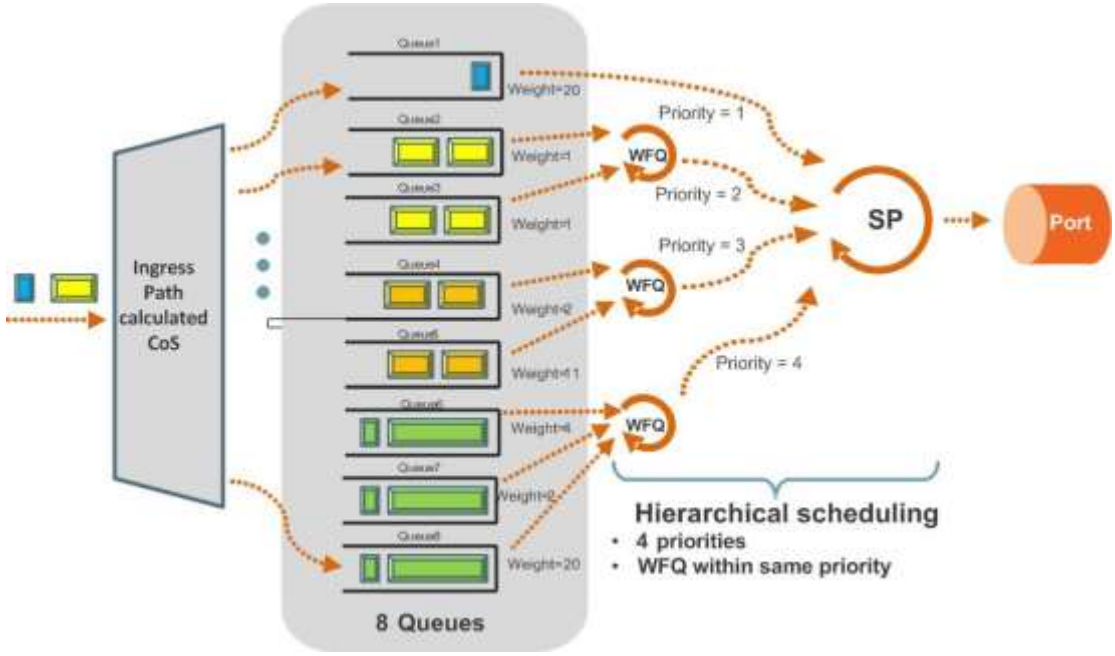


Figure 104: Scheduling Mechanism for a Single Service Bundle

Interface Priority

The profile defines the exact order for serving the eight priority queues in a single service bundle. When the user attaches a profile to an interface, all the service bundles under the interface inherit the profile.

The priority mechanism distinguishes between two states of the service bundle:

- Green State – Committed state
- Yellow state – Best effort state

Green State refers to any time when the *service bundle total rate* is below the user-defined CIR. Yellow State refers to any time when the *service bundle total rate* is above the user-defined CIR but below the PIR.

User can define up to four Green priority profiles, from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically.

The following table provides a sample of an interface priority profile. This profile is also used as the default interface priority profile.

Table 54: QoS Priority Profile Example

Profile ID (1-9)

CoS	Green Priority (user defined)	Yellow Priority (read only)	Description
0	1	1	Best Effort
1	2	1	Data Service 4
2	2	1	Data Service 3
3	2	1	Data Service 2
4	2	1	Data Service 1
5	3	1	Real Time 2 (Video with large buffer)
6	3	1	Real Time 1 (Video with small buffer)
7	4	4	Management (Sync, PDUs, etc.)

When the service bundle state is Green (committed state), the service bundle priorities are as defined in the Green Priority column. When the service bundle state is Yellow (best effort state), the service bundle priorities are system-defined priorities shown in the Yellow Priority column.

Note: CoS 7 is always marked with the highest priority, no matter what the service bundle state is, since it is assumed that only high priority traffic will be tunneled via CoS 7.

The system supports up to nine interface priority profiles. Profiles 1 to 8 are defined by the user, while profile 9 is the pre-defined read-only default interface priority profile.

The following interface priority profile parameters can be configured by users:

- **Profile ID** – Profile ID number. Permitted values are 1 to 8.
- **CoS 0 Priority** – CoS 0 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 0 Description** – CoS 0 user description field, up to 20 characters.
- **CoS 1 Priority** – CoS 1 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 1 Description** – CoS 1 user description field, up to 20 characters.
- **CoS 2 Priority** – CoS 2 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 2 Description** – CoS 2 user description field, up to 20 characters.
- **CoS 3 Priority** – CoS 3 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 3 Description** – CoS 3 user description field, up to 20 characters.
- **CoS 4 Priority** – CoS 4 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 4 Description** – CoS 4 user description field, up to 20 characters.
- **CoS 5 Priority** – CoS 5 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 5 Description** – CoS 5 user description field, up to 20 characters.
- **CoS 6 Priority** – CoS 6 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 6 Description** – CoS 6 user description field, up to 20 characters.

- **CoS 7 Priority** – CoS 7 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 7 Description** – CoS 7 user description field, up to 20 characters.

Users can attach one of the configured interface priority profiles to each interface. By default, the interface is assigned Profile ID 9, the pre-defined system profile.

Weighted Fair Queuing (WFQ)

As described above, the scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses Weighted Fair Queuing (WFQ) to determine the priorities within each priority. WFQ defines the transmission ratio, in bytes, between the queues. All the service bundles under the interface inherit the WFQ profile attached to the interface.

The system supports up to six WFQ interface profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

The following table provides an example of a WFQ profile.

Table 55: WFQ Profile Example

Profile ID (1-7)

CoS	Queue Weight (Green)	Queue Weight (Yellow – not visible to users)
0	20	20
1	20	20
2	20	20
3	20	20
4	20	20
5	20	20
6	20	20
7	20	20

For each CoS, the user can define;

- **Profile ID** – Profile ID number. Permitted values are 2 to 6.
- **Weight** – Transmission quota in bytes. Permitted values are 1 to 20.

Users can attach one of the configured interface WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile.

Egress PMs and Statistics

Queue-Level Statistics

IP-20F supports the following counters per queue at the queue level:

- Transmitted Green Packet (64 bits counter)
- Transmitted Green Bytes (64 bits counter)
- Transmitted Green Bits per Second (32 bits counter)
- Dropped Green Packets (64 bits counter)
- Dropped Green Bytes (64 bits counter)
- Transmitted Yellow Packets (64 bits counter)
- Transmitted Yellow Bytes (64 bits counter)
- Transmitted Yellow Bits per Second (32 bits counter)
- Dropped Yellow Packets (64 bits counter)
- Dropped Yellow Bytes (64 bits counter)

Service Bundle-Level Statistics

IP-20F supports the following counters per service bundle at the service bundle level:

- Transmitted Green Packets (64 bits counter)
- Transmitted Green Bytes (64 bits counter)
- Transmitted Green Bits per Second (32 bits counter)
- Dropped Green Packets (64 bits counter)
- Dropped Green Bytes (64 bits counter)
- Transmitted Yellow Packets (64 bits counter)
- Transmitted Yellow Bytes (64 bits counter)
- Transmitted Yellow Bits per Second (32 bits counter)
- Dropped Yellow Packets (64 bits counter)
- Dropped Yellow Bytes (64 bits counter)

PMs for Queue Traffic

For each logical interface, users can configure thresholds for Green and Yellow traffic per queue. Users can then display the following PMs for 15-minute and 24-hour intervals, per queue and color:

- Maximum bytes passed per second
- Minimum bytes passed per second
- Average bytes passed per second
- Maximum bytes dropped per second
- Minimum bytes dropped per second
- Average bytes dropped per second
- Maximum packets passed per second
- Minimum packets passed per second
- Average packets passed per second
- Maximum packets dropped per second
- Minimum packets dropped per second
- Average packets dropped per second
- Seconds bytes per second were over the configured threshold per interval

Interface-Level Statistics

For information on statistics at the interface level, refer to *Ethernet Statistics* on page 155.

Marker

Marking refers to the ability to overwrite the outgoing priority bits and Color of the outer VLAN of the egress frame. Marking mode is only applied if the outer frame is S-VLAN and S-VLAN CoS preservation is disabled, or if the outer frame is C-VLAN and C-VLAN CoS preservation is disabled. If outer VLAN preservation is enabled for the relevant outer VLAN, the egress CoS and Color are the same as the CoS and Color of the frame when it ingressed into the switching fabric.

Marking is performed according to a global table that maps CoS and Color values to the 802.1p-UP bits and the DEI or CFI bits. If Marking is enabled on a service point, the CoS and Color of frames egressing the service via that service point are overwritten according to this global mapping table.

If marking and CoS preservation for the relevant outer VLAN are both disabled, marking is applied according to the Green frame values in the global marking table.

When marking is performed, the following global tables are used by the marker to decide which CoS and Color to use as the egress CoS and Color bits.

Table 56: 802.1q UP Marking Table (C-VLAN)

CoS	Color	802.1q UP (Configurable)	CFI Color (Configurable)
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

Table 57: 802.1ad UP Marking Table (S-VLAN)

CoS	Color	802.1ad UP (configurable)	DEI Color (configurable)
0	Green	0	0
0	Yellow	0	1
1	Green	1	0
1	Yellow	1	1
2	Green	2	0
2	Yellow	2	1
3	Green	3	0
3	Yellow	3	1
4	Green	4	0
4	Yellow	4	1
5	Green	5	0
5	Yellow	5	1

CoS	Color	802.1ad UP (configurable)	DEI Color (configurable)
6	Green	6	0
6	Yellow	6	1
7	Green	7	0
7	Yellow	7	1

The keys for these tables are the CoS and Color. The results are the 802.1q/802.1ad UP and CFI/DEI bits, which are user-configurable. It is strongly recommended that the default values not be changed except by advanced users.

Standard QoS and Hierarchical QoS (H-QoS) Summary

The following table summarizes and compares the capabilities of standard QoS and H-QoS.

Table 58: Summary and Comparison of Standard QoS and H-QoS

Capability	Standard QoS	Hierarchical QoS
Number of transmission queues per port	8	256
Number of service bundles	1 (always service bundle id equal 1)	32
WRED	Per queue (two curves – for green traffic and for yellow traffic via the queue)	Per queue (two curves – for green traffic and for yellow traffic via the queue)
Shaping at queue level	Single leaky bucket	Single leaky bucket
Shaping at service bundle level	Dual leaky bucket	Dual leaky bucket
Shaping at port level	Single leaky bucket (this level is not relevant since it is recommended to use service bundle level with dual leaky bucket)	Single leaky bucket
Transmission queues priority	Per queue priority (4 priorities).	Per queue priority (4 priorities). All service bundles for a specific port inherit the 8-queues priority settings.
Weighted fair Queue (WFQ)	Queue level (between queues)	Queue level (between queues) Service Bundle level (between service bundles)
Marker	Supported	Supported
Statistics	Queue level (8 queues) Service bundle level (1 service bundle) Port level	Queue level (256 queues) Service bundle level (32 service bundles) Port level

6.3.7 Global Switch Configuration

The following parameters are configured globally for the IP-20F switch:

- **S- VLAN Ethertype** –Defines the ethertype recognized by the system as the S-VLAN ethertype. IP-20F supports the following S-VLAN ethertypes:
  - 0x8100
  - 0x88A8 (default)
  - 0x9100
  - 0x9200
- **C-VLAN Ethertype** – Defines the ethertype recognized by the system as the C-VLAN ethertype. IP-20F supports 0x8100 as the C-VLAN ethertype.
- **MRU** – The maximum segment size defines the maximum receive unit (MRU) capability and the maximum transmit capability (MTU) of the system. Users can configure a global MRU for the system. Permitted values are 64 bytes to 9612 bytes.

6.3.8 Automatic State Propagation and Link Loss Forwarding

Related topics:

- Network Resiliency

Automatic State Propagation (ASP) enables propagation of radio failures back to the Ethernet port. You can also configure ASP to close the Ethernet port based on a radio failure at the remote carrier. ASP improves the recovery performance of resiliency protocols.

Note: It is recommended to configure both ends of the link to the same ASP configuration.

6.3.8.1 Automatic State Propagation Operation

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface. Multiple pairs can be configured using the same Monitored Interface and multiple Controlled Interfaces.

The Monitored Interface is a radio interface, a radio protection group, or a Multi-Carrier ABC group. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Each Controlled Interface is assigned an LLF ID. If **ASP trigger by remote fault** is enabled on the remote side of the link, the ASP state of the Controlled Interface is propagated to the Controlled Interface with the same LLF ID at the remote side of the link. This means if ASP is triggered locally, it is propagated to the remote side of the link, but only to Controlled Interfaces with LLF IDs that match the LLF IDs of the affected Controlled Interfaces on the local side of the link.

The following events in the Monitored Interface trigger ASP:

- Radio LOF
- Radio Excessive BER
- Remote Radio LOF
- Remote Excessive BER
- Remote LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

When a triggering event takes place:

- If the Controlled Interface is an electrical GbE port, the port is closed.
- If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

Users can configure a trigger delay time, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed.

6.3.8.2 Automatic State Propagation and Protection

When the Controlled Interface is part of a 1+1 protection pair, a port shutdown message is only sent to the remote side of the link if both of the protected interfaces are shut down.

When the Monitored interface is part of a 1+1 HSB configuration, ASP is only triggered if both interfaces fail.

Closing an Ethernet port because of ASP does not trigger a protection switch.

6.3.9 Network Resiliency

IP-20F provides carrier-grade service resiliency using the following protocols:

- G.8032 Ethernet Ring Protection Switching (ERPS)
- Multiple Spanning Tree Protocol (MSTP)

These protocols are designed to prevent loops in ring/mesh topologies.

6.3.9.1 G.8032 Ethernet Ring Protection Switching (ERPS)

ERPS, as defined in the G.8032 ITU standard, is currently the most advanced ring protection protocol, providing convergence times of sub-50ms. ERPS prevents loops in an Ethernet ring by guaranteeing that at any time, traffic can flow on all except one link in the ring. This link is called the Ring Protection Link (RPL). Under normal conditions, the RPL is blocked, i.e., not used for traffic. One designated Ethernet Ring Node, the RPL Owner Node, is responsible for blocking traffic at one end of the RPL. When an Ethernet ring failure occurs, the RPL Owner unblocks its end of the RPL, allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the RPL Neighbor Node, may also participate in blocking or unblocking its end of the RPL. A number of ERP instances (ERPIs) can be created on the same ring.

Note:	P2P services are not affected by G.8032, and continue to traverse ports that are blocked by G.8032.

G.8032 ERPS Benefits

ERPS, as the most advanced ring protection protocol, provides the following benefits:

- Provides sub-50ms convergence times.
- Provides service-based granularity for load balancing, based on the ability to configure multiple ERPIs on a single physical ring.
- Provides configurable timers to control switching and convergence parameters per ERPI.

G.8032 ERPS Operation

The ring protection mechanism utilizes an APS protocol to implement the protection switching actions. Forced and manual protection switches can also be initiated by the user, provided the user-initiated switch has a higher priority than any other local or far-end request.

Ring protection switching is based on the detection of defects in the transport entity of each link in the ring. For purposes of the protection switching process, each transport entity within the protected domain has a state of either Signal Fail (SF) or Non-Failed (OK). R-APS control messages are forwarded by each node in the ring to update the other nodes about the status of the links.

Note:	An additional state, Signal Degrade (SD), is planned for future release. The SD state is similar to SF, but with lower priority.

Users can configure up to 16 ERPIs. Each ERPI is associated with an Ethernet service defined in the system. This enables operators to define a specific set of G.8032 characteristics for individual services or groups of services within the same physical ring. This includes a set of timers that enables operators to optimize protection switching behavior per ERPI:

- **Wait to Restore (WTR) Timer** – Defines a minimum time the system waits after signal failure is recovered before reverting to idle state.
- **Guard Time** – Prevents unnecessary state changes and loops.
- **Hold-off Time** – Determines the time period from failure detection to response.

Each ERPI maintains a state machine that defines the node's state for purposes of switching and convergence. The state is determined according to events that occur in the ring, such as signal failure and forced or manual switch requests, and their priority. Possible states are:

- Idle
- Protecting
- Forced Switch (FS)
- Manual Switch (MS)
- Pending

As shown in the following figure, in idle (normal) state, R-APS messages pass through all links in the ring, while the RPL is blocked for traffic. The RPL can be on either edge of the ring. R-APS messages are sent every five seconds.

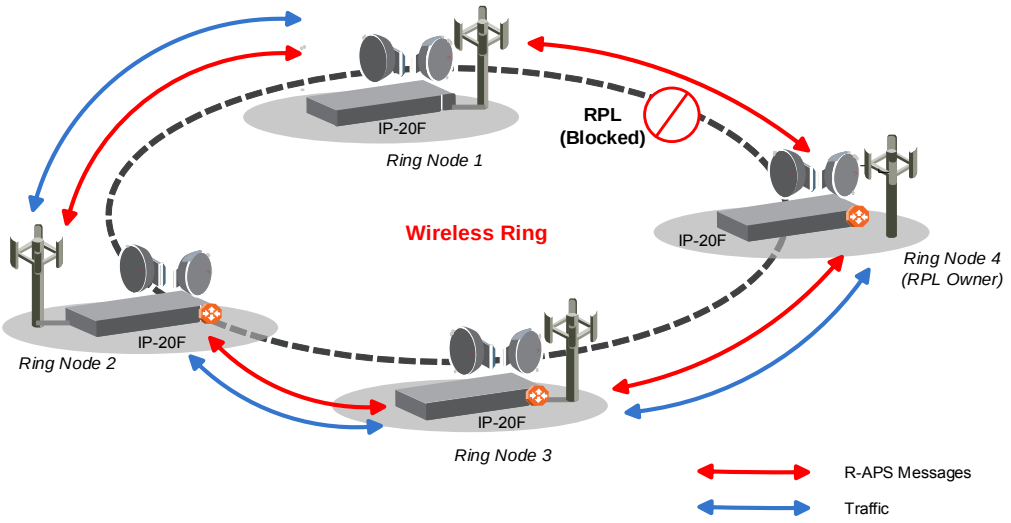


Figure 105: G.8032 Ring in Idle (Normal) State

Once a signal failure is detected, the RPL is unblocked for each ERPI. As shown in the following figure, the ring switches to protecting state. The nodes that detect the failure send periodic SF messages to alert the other nodes in the link of the failure and initiate the protecting state.

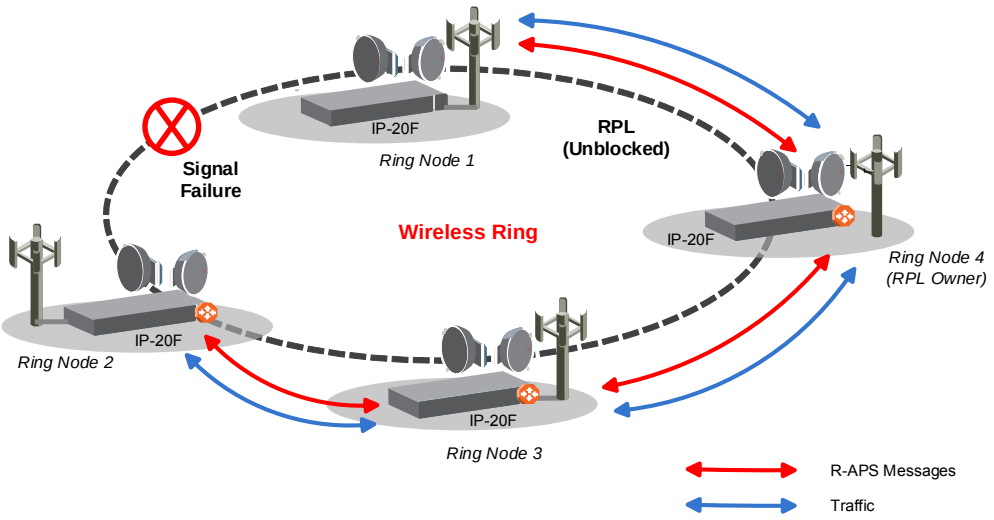


Figure 106: G.8032 Ring in Protecting State

The ability to define multiple ERPIs and assign them to different Ethernet services or groups of services enables operators to perform load balancing by configuring a different RPL for each ERPI. The following figure illustrates a ring in which four ERPIs each carry services with 33% capacity in idle state, since each link is designated the RPL, and is therefore idle, for a different ERPI.

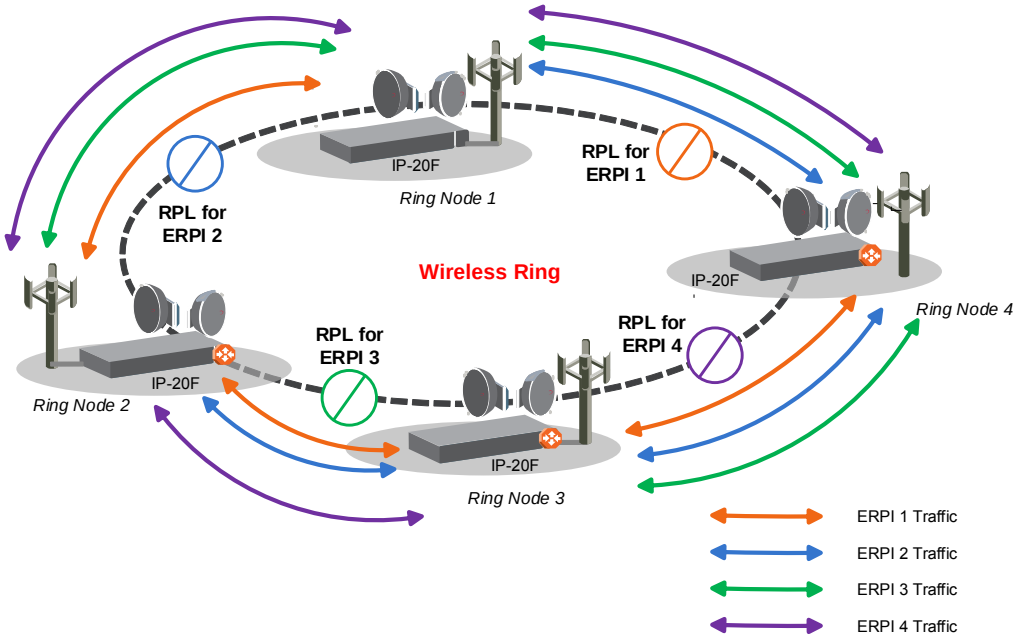


Figure 107: Load Balancing Example in G.8032 Ring

G.8032 Interoperability

G.8032 in IP-20F units is interoperable with IP-20A, IP-20G, and IP-20GX units running G.8032, as well as third-party bridges running standard implementations of G.8032.

6.3.9.2 Multiple Spanning Tree Protocol (MSTP)

MSTP, as defined in IEEE 802.1q, provides full connectivity for frames assigned to any given VLAN throughout a bridged LAN consisting of arbitrarily interconnected bridges.

With MSTP, an independent multiple spanning tree instance (MSTI) is configured for each group of services, and only one path is made available (unblocked) per spanning tree instance. This prevents network loops and provides load balancing capability. It also enables operators to differentiate among Ethernet services by mapping them to different, specific MSTIs. The maximum number of MSTIs is configurable, from 2 to 16.

Note:	P2P services are not affected by MSTP, and continue to traverse ports that are blocked by MSTP.

MSTP is an extension of, and is backwards compatible with, Rapid Spanning Tree Protocol (RSTP).

IP-20F supports MSTP according to the following IEEE standards:

- 802.1q
- 802.1ad amendment (Q-in-Q)
- 802.1ah (TE instance)

MSTP Benefits

MSTP significantly improves network resiliency in the following ways:

- Prevents data loops by configuring the active topology for each MSTI such that there is never more than a single route between any two points in the network.
- Provides for fault tolerance by automatically reconfiguring the spanning tree topology whenever there is a bridge failure or breakdown in a data path.
- Automatically reconfigures the spanning tree to accommodate addition of bridges and bridge ports to the network, without the formation of transient data loops.
- Enables frames assigned to different services or service groups to follow different data routes within administratively established regions of the network.
- Provides for predictable and reproducible active topology based on management of the MSTP parameters.
- Operates transparently to the end stations.

- Consumes very little bandwidth to establish and maintain MSTIs, constituting a small percentage of the total available bandwidth which is independent of both the total traffic supported by the network and the total number of bridges or LANs in the network.
- Does not require bridges to be individually configured before being added to the network.

MSTP Operation

MSTP includes the following elements:

- **MST Region** – A set of physically connected bridges that can be portioned into a set of logical topologies.
- **Internal Spanning Tree (IST)** – Every MST Region runs an IST, which is a special spanning tree instance that disseminates STP topology information for all other MSTIs.
- **CIST Root** – The bridge that has the lowest Bridge ID among all the MST Regions.
- **Common Spanning Tree (CST)** – The single spanning tree calculated by STP, RSTP, and MSTP to connect MST Regions. All bridges and LANs are connected into a single CST.
- **Common Internal Spanning Tree (CIST)** – A collection of the ISTs in each MST Region, and the CST that interconnects the MST regions and individual spanning trees. MSTP connects all bridges and LANs with a single CIST.

MSTP specifies:

- An MST Configuration Identifier that enables each bridge to advertise its configuration for allocating frames with given VIDs to any of a number of MSTIs.
- A priority vector that consists of a bridge identifier and path cost information for the CIST.
- An MSTI priority vector for any given MSTI within each MST Region.

Each bridge selects a CIST priority vector for each port based on the priority vectors and MST Configuration Identifiers received from the other bridges and on an incremental path cost associated with each receiving port. The resulting priority vectors are such that in a stable network:

- One bridge is selected to be the CIST Root.
- A minimum cost path to the CIST Root is selected for each bridge.
- The CIST Regional Root is identified as the one root per MST Region whose minimum cost path to the root is not through another bridge using the same MST Configuration Identifier.

Based on priority vector comparisons and calculations performed by each bridge for each MSTI, one bridge is independently selected for each MSTI to be the MSTI Regional Root, and a minimum cost path is defined from each bridge or LAN in each MST Region to the MSTI Regional Root.

The following events trigger MSTP re-convergence:

- Addition or removal of a bridge or port.

- A change in the operational state of a port or group (LAG or protection).
- A change in the service to instance mapping.
- A change in the maximum number of MSTIs.
- A change in an MSTI bridge priority, port priority, or port cost.

Note:	All except the last of these triggers can cause the entire MSTP to re-converge. The last trigger only affects the modified MSTI.

MSTP Interoperability

MSTP in IP-20F units is interoperable with:

- FibeAir IP-20A, IP-20G, and IP-20GX units running MSTP.
- Third-party bridges running MSTP.

6.3.10 OAM

FibeAir IP-20F provides complete Service Operations Administration and Maintenance (SOAM) functionality at multiple layers, including:

- Fault management status and alarms.
- Maintenance signals, such as AIS, and RDI.
- Maintenance commands, such as loopbacks and Linktrace commands.

IP-20F is fully compliant with G.8013/Y.1731, MEF-17, MEF-20, MEF-30, and MEF-31.

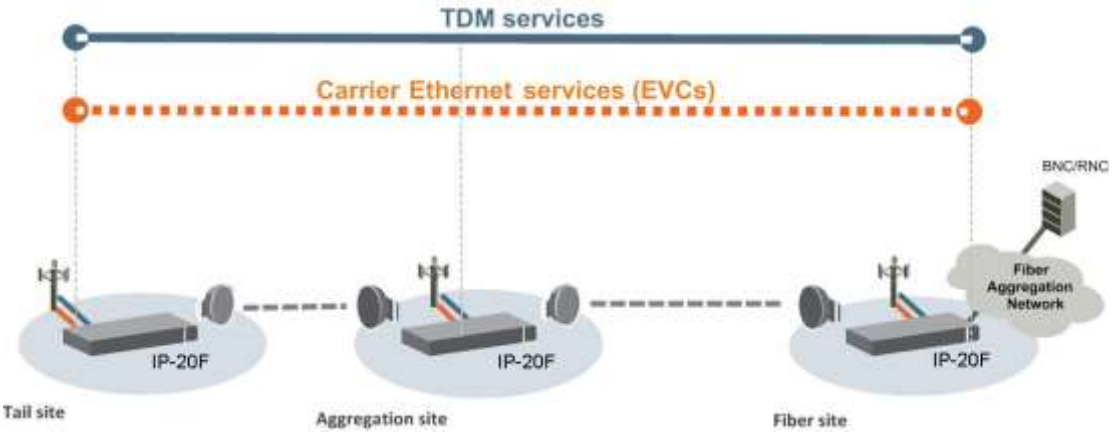


Figure 108: IP-20F End-to-End Service Management

6.3.10.1 Connectivity Fault Management (FM)

The Y.1731 standard and the, MEF-30 specifications define SOAM. SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

Y.1731 Ethernet FM (Connectivity Fault Management) consists of three protocols that operate together to aid in fault management:

- Continuity check
- Link trace
- Loopback

Note: Link trace is planned for future release.

FibeAir IP-20F utilizes these protocols to maintain smooth system operation and non-stop data flow.

The following are the basic building blocks of FM:

- Maintenance domains, their constituent maintenance points, and the managed objects required to create and administer them.

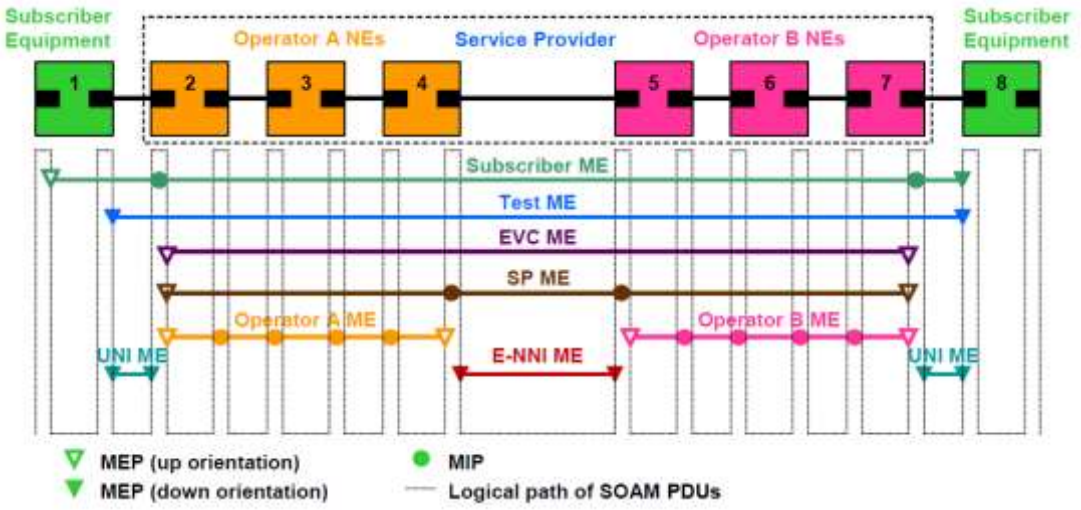


Figure 109: SOAM Maintenance Entities (Example)

- Protocols and procedures used by maintenance points to maintain and diagnose connectivity faults within a maintenance domain.
  - CCM (Continuity Check Message): CCM can detect Connectivity Faults (loss of connectivity or failure in the remote MEP).
  - Loopback: LBM/LBR mechanism is an on-demand mechanism. It is used to verify connectivity from any MEP to any certain Maintenance Point in the MA/MEG. A session of loopback messages can include up to 1024 messages with varying intervals ranging from 1 to 60 seconds. Message size can reach jumbo frame size.
  - Linktrace: The LTM/LTR mechanism is an on-demand mechanism. It can detect the route of the data from any MEP to any other MEP in the MA/MEG. It can be used for the following purposes:
    - Adjacent relation retrieval – The ETH-LT function can be used to retrieve the adjacency relationship between an MEP and a remote MEP or MIP. The result of running ETH-LT function is a sequence of MIPs from the source MEP until the target MIP or MEP.
    - Fault localization – The ETH-LT function can be used for fault localization. When a fault occurs, the sequence of MIPs and/or MEP will probably be different from the expected sequence. The difference between the sequences provides information about the fault location.
    - AIS: AIS (defined in Y.1731) is the Ethernet alarm indication signal function used to suppress alarms following detection of defect conditions at the server (sub) layer.

6.3.10.2 Ethernet Line Interface Loopback

FibeAir IP-20F supports loopback testing for its radio and TDM interfaces, which enables loopback testing of the radio and TDM traffic interfaces as well as the IDU-RFU connection.

In addition, the Ethernet Line Interface Loopback feature provides the ability to run loopbacks over the link. When Ethernet loopback is enabled on an interface, the system loops back all packets ingressing the interface. This enables loopbacks to be performed over the link from other points in the network.

For example, as shown in the figure below, a loopback can be performed from test equipment over the line to an Ethernet interface. A loopback can also be performed from the other side of the radio link.

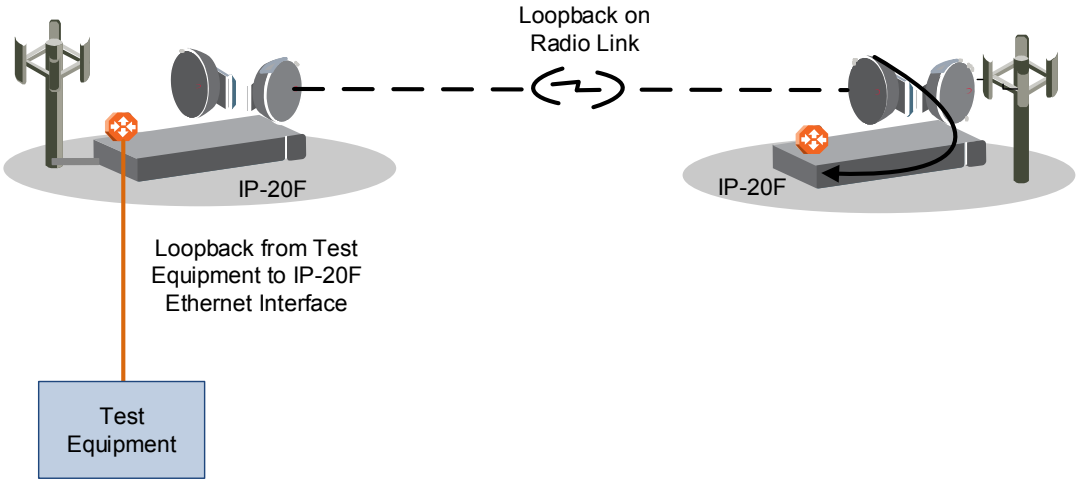


Figure 110: Ethernet Line Interface Loopback – Application Examples

Ethernet loopbacks can be performed on any logical interface. This includes optical and electrical GbE interfaces, radio interfaces, Multi-Carrier ABC groups, LAGS, and 1+1 HSB groups. Ethernet loopbacks cannot be performed on the management interfaces.

The following parameters can be configured for an Ethernet loopback:

- The interface can be configured to swap DA and SA MAC addresses during the loopback. This prevents Ethernet loops from occurring. It is recommended to enable MAC address swapping if MSTP or LLDP is enabled.
- Ethernet loopback has a configurable duration period of up to 15 minutes, but can be disabled manually before the duration period ends. Permanent loopback is not supported.

Ethernet loopbacks can be configured on more than one interface simultaneously.

When an Ethernet loopback is active, network resiliency protocols (G.8032 and MSTP) will detect interface failure due to the failure to receive BPDUs.

In a system using in-band management, Ethernet loopback activation on the remote side of the link causes loss of management to the remote unit. The duration period of the loopback should take this into account.

6.4 Synchronization

This section describes IP-20F's flexible synchronization solution that enables operators to configure a combination of synchronization techniques, based on the operator's network and migration strategy, including:

- Native Sync Distribution, for end-to-end distribution using GbE, FE, DS1, T3 sync interface, and/or OC-3 input and output.
- SyncE PRC Pipe Regenerator mode, providing PRC grade (G.811) performance for pipe ("regenerator") applications.
- IEEE-1588v2 PTP Optimized Transport, providing both frequency and phase synchronization for compliance with rigorous LTE and LTE-A requirements.

This section includes:

- Synchronization Overview
- IP-20F Synchronization Solution
- Native Sync Distribution Mode
- SyncE PRC Pipe Regenerator Mode
- IEEE-1588v2 PTP Optimized Transport

6.4.1 Synchronization Overview

Synchronization is essential to ensuring optimal performance in telecommunications networks. Proper synchronization prevents packet loss, dropped frames, and degradation of quality of experience that can adversely affect end-user services.

Synchronization is particularly critical to mobile networks in order to ensure successful call-signal handoff and proper transmission between base stations, as well as for the transport of real-time services. If individual base stations drift outside specified frequencies, this can cause mobile handoff delays, resulting in high dropped-call rates, impaired data services, and, ultimately, lost subscribers. Mobile base stations require a highly accurate timing signal that must be shared across the entire network. If any base station drifts outside of the specified +/- 50 ppb threshold, mobile handoff performance degrades, resulting in a high disconnect rate and poor data-service quality.

6.4.1.1 Types of Synchronization in Mobile Networks

Synchronization in a mobile network involves frequency and phase (time) synchronization.

Frequency synchronization maintains consistency between the frequencies of clock signals to ensure that all devices operate at the same rate. Information is coded into discrete pulses through pulse code modulation (PCM) and transmitted on the data communication network. If the clock frequencies of two digital switching devices are different, the bits in the buffer of the digital switching system may be lost or duplicated, resulting in a slip in the bit stream.

Phase synchronization, also known as time synchronization, adjusts the internal clock of a local device according to received time information. In contrast to frequency synchronization, time synchronization adjusts the clock at irregular intervals.

Phase synchronization involves two major functions: time service and time keeping. Time service adjusts the clock according to the standard time. By adjusting the clock at irregular intervals, a device synchronizes its phase with the standard reference time. Time keeping refers to frequency synchronization, and ensures that the difference between the time on the local device and the standard reference time is within a reasonable range during the interval of clock adjustment.

6.4.1.2 Additional Synchronization Requirements of LTE Networks

LTE imposes additional challenges with respect to synchronization. Synchronization solutions must meet the rigorous LTE timing and delivery requirements that ensure network quality and availability.

While TDM networks were able to exploit GPS for synchronization purposes, LTE enables deployment of small cells in locations where access to GPS is not reliable. Without the GPS signals that are traditionally used to provide accurate frequency and time-of-day synchronization information, LTE networks must find other means for synchronization.

There are additional difficulties with ensuring proper synchronization in LTE networks. For example, the LTE downlink radio interface relies on an OFDMA transmission technique in the downlink. OFDMA presents tremendous benefits in terms of high spectral efficiency, support of advanced features such as frequency selective scheduling, immunity to multipath interference, and interference coordination. However, these advantages require that the orthogonality between OFDMA subcarriers be strictly preserved. The orthogonality between the subcarriers prevents overlapping of the subcarriers' spectra which would result in interference between subcarriers.

A frequency offset can also lead to dropped calls during handover between base stations. During the handover procedure, user equipment (UE) must determine the timing and frequency parameters of the base station in order to be able to demodulate the downlink signal and also to transmit correctly on the uplink. The frequency-stability tolerance of the UE oscillator is typically maintained at 0.1 ppm to minimize cost. Its stability is maintained by tracking the base station carrier frequency, a critical synchronization requirement.

In addition, in LTE-TDD systems, downlink and uplink transmission occur in the same channel but in different time slots. Both frequency and phase synchronization are required in LTE-TDD to avoid interference between the uplink and the downlink transmissions on neighboring base stations.

6.4.2 IP-20F Synchronization Solution

Ceragon's synchronization solution ensures maximum flexibility by enabling the operator to select any combination of techniques suitable for the operator's network and migration strategy.

- Native Sync Distribution
  - End-to-End Native Synchronization distribution
  - GbE/FE/DS1[23]/T3[24]/OC-3 input[25]
  - GbE/FE/DS1[26]/T4[27]/OC-3 output[28]
  - Supports any radio link configuration and network topology
  - Synchronization Status Messages (SSM) to prevent loops and enable use of most reliable clock source
  - User-defined clock source priority and quality level
  - Automated determination of relative clock source quality levels
- SyncE PRC Pipe Regenerator mode[29]
  - PRC grade (G.811) performance for pipe ("regenerator") applications
- IEEE-1588v2 PTP Optimized Transport[30]
  - Transparent Clock – Resides between master and slave nodes, and measurers and adjusts for delay variation to guarantee ultra-low PDV.
  - Boundary Clock – Regenerates frequency and phase synchronization, providing, increasing the scalability of the synchronization network while rigorously maintaining timing accuracy.

---

23 E1 input is planned for future release.

24 T3 input is planned for future release.

25 OC-3 input is planned for future release.

26 E1 output is planned for future release.

27 T4 output is planned for future release.

28 OC-3 output is planned for future release.

29 SyncE PRC Pipe Regenerator mode is planned for future release.

30 IEEE-1588 PTP Optimized Transport is planned for future release.

6.4.3 Native Sync Distribution Mode

In this mode, synchronization is distributed end-to-end over the radio links in the network. No TDM trails or DS1 interfaces at the tail sites are required.

Synchronization is typically provided by one or more clock sources (SSU/GPS) at fiber hub sites.

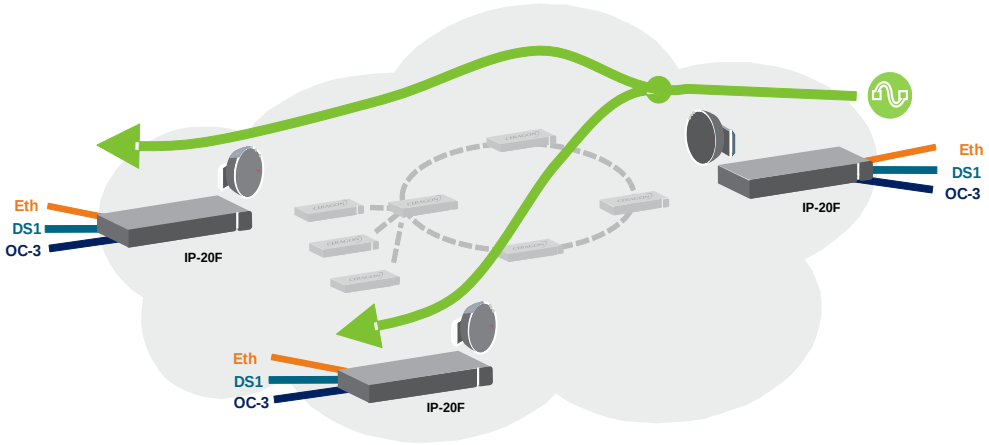


Figure 111: Native Sync Distribution Mode

Native Sync Distribution mode can be used in any link configuration and any network topology.

Ring topologies present special challenges for network synchronization. Any system that contains more than one clock source for synchronization, or in which topology loops may exist, requires an active mechanism to ensure that:

- A single source is used as the clock source throughout the network, preferably the source with the highest accuracy.
- There are no reference loops. In other words, no element in the network will use an input frequency from an interface that ultimately derived that frequency from one of the outputs of that network element.

IP-20F's Native Sync Distribution mechanism enables users to define a priority level for each possible clock source. Synchronization Status Messages (SSM) are sent regularly through each interface involved in frequency distribution, enabling the network to gather and maintain a synchronization status for each interface according to the system's best knowledge about the frequency quality that can be conveyed by that interface.

Based on these parameters, the network assigns each interface a quality level and determines which interface to use as the current clock source. The network does this by evaluating the clock quality of the available source interfaces and selecting, from those interfaces with the highest quality, the interface with the highest user-defined priority.

The synchronization is re-evaluated whenever one of the following occurs:

- Any synchronization source is added, edited, or deleted by a user.
- The clock quality status changes for any source interface.
- The synchronization reference is changed for the node.

6.4.3.1 Available Interfaces for Native Sync Distribution

Frequency signals can be taken by the system from a number of different interfaces (one reference at a time). The reference frequency may also be conveyed to external equipment through different interfaces.

Table 59: Native Sync Interface Options

Interface	Available for Input	Available for Output
Ethernet Interfaces	Yes	Yes
Traffic DS1	No	No
1.5MHz via T3 input from Sync Interface, supporting both 2048 Kbp/s and 2048 KHz	No	n/a
DS1 via T3 input from Sync Interface	No	n/a
1.5MHz via T4 output from Sync interface	n/a	No
DS1 via T4 output from Sync Interface	n/a	No
Radio Carrier	Yes	Yes

It is possible to configure up to 16 synchronization sources in the system. At any given moment, only one of these sources is active; the clock is taken from the active source onto all other appropriately configured interfaces.

6.4.3.2 Configuring Native Sync Distribution

Frequency is distributed by configuring the following parameters in each node:

- System synchronization sources. These are the interfaces from which the frequency is taken and distributed to other interfaces. Up to 16 sources can be configured in each node. A revertive timer can be configured. For each interface, user must configure:
  - Its clock quality level. The quality level may be fixed (according to ITU-T G.781 option I) or automatic. When the quality level is automatic, it is determined by SSM messages.
  - Its priority (1-16). No two interfaces may have the same priority.
- For each interface, the source of its outgoing signal clock. This can be:
  - **Local clock:** Causes the interface to generate its signal from a local oscillator, unrelated to the system reference frequency.
  - **Synchronization reference:** Causes the interface to generate its signal from the system reference clock, which is taken from the synchronization source.
  - **Loop Timing:** Causes the interface to generate the signal from its own input.
- The node's synchronization mode. This can be:
  - **Automatic:** In this mode, the active source is automatically selected based on the interface with highest available quality. Among interfaces with identical quality, the interface with the highest priority is used.

- **Force:** The user can force the system to use a certain interface as the reference clock source.[31]

By configuring synchronization sources and transporting the reference frequency to the related interfaces in a network, a frequency "flow" can be achieved, as shown in the example below, where the reference frequency from a single node is distributed to a number of base stations.

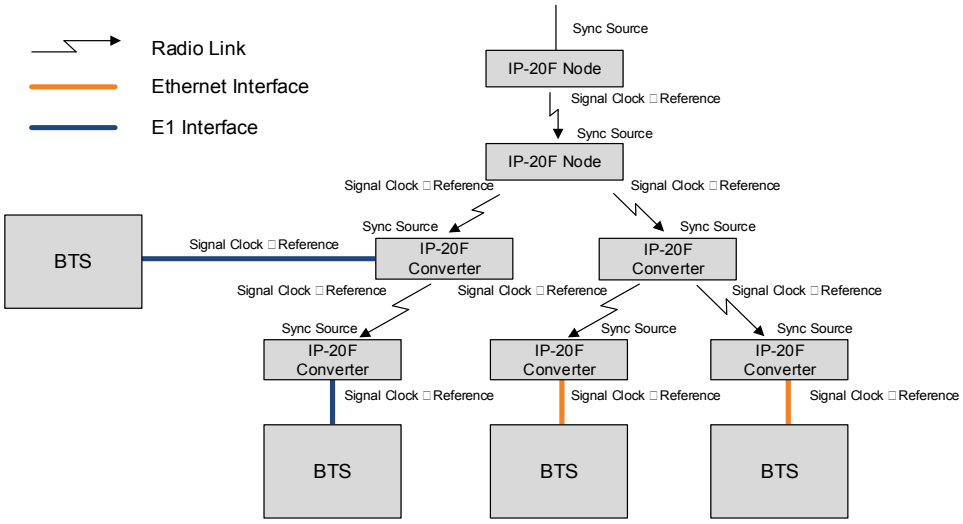


Figure 112: Synchronization Configuration

The following restrictions apply for frequency distribution configuration:

- An interface can either be used as a synchronization source or can take its signal from the system reference, but not both (no loop timing available, except locally in SDH interfaces).
- The clock taken from a line interface (DS1, SDH, VC-11/12, Ethernet) cannot be conveyed to another line interface in the same card.
- The clock taken from a radio channel cannot be conveyed to another radio channel in the same radio.

If the signal driving the synchronization fails, an alarm will alert the user and the system will enter holdover mode until another synchronization source signal is found.

6.4.3.3 SSM Support and Loop Prevention

In order to provide topological resiliency for synchronization transfer, IP-20F implements the passing of SSM messages over the radio interfaces. SSM timing in IP-20F complies with ITU-T G.781.

In addition, the SSM mechanism provides reference source resiliency, since a network may have more than one source clock.

---

31 Force mode is planned for future release.

The following are the principles of operation:

- At all times, each source interface has a “quality status” which is determined as follows:
  - If quality is configured as fixed, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF, etc.).
  - If quality is automatic, then the quality is determined by the received SSMs or becomes “failure” upon interface failure (such as LOS, LOC, LOF, etc.).
- Each unit holds a parameter which indicates the quality of its reference clock. This is the quality of the current synchronization source interface.
- The reference source quality is transmitted through SSM messages to all relevant radio interfaces.
- Each unit determines the current active clock reference source interface:
  - The interface with the highest available quality is selected.
  - From among interfaces with identical quality, the interface with the highest priority is selected.
- In order to prevent loops, an SSM with quality “Do Not Use” is sent towards the active source interface

At any given moment, the system enables users to display:

- The current source interface quality.
- The current received SSM status for every source interface.
- The current node reference source quality.

As a reference, the following are the possible quality values (from highest to lowest):

  - AUTOMATIC (available only in interfaces for which SSM support is implemented)
  - PRS
  - Stratum 2
  - Transmit Node
  - Stratum 3E
  - Stratum 3
  - SMC
  - Unknown
  - DO NOT USE
  - Failure (cannot be configured by user)

6.4.3.4 Native Sync Distribution Examples

The figure below provides a Native Sync Distribution mode usage example in which synchronization is provided to all-frame Node-Bs using SyncE. In this illustration, an IP-20F at a fiber node is synchronized to:

- SyncE input from an Ethernet uplink
- External synchronization input via an DS1 interface

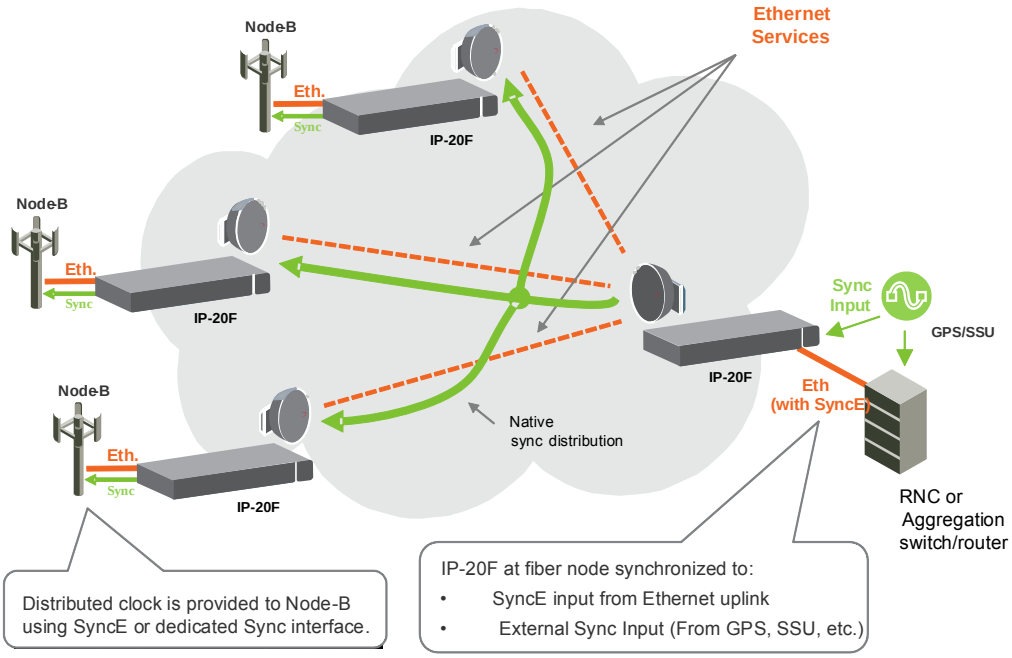


Figure 113: Native Sync Distribution Mode Usage Example

The following figure illustrates Native Sync Distribution in a tree scenario.

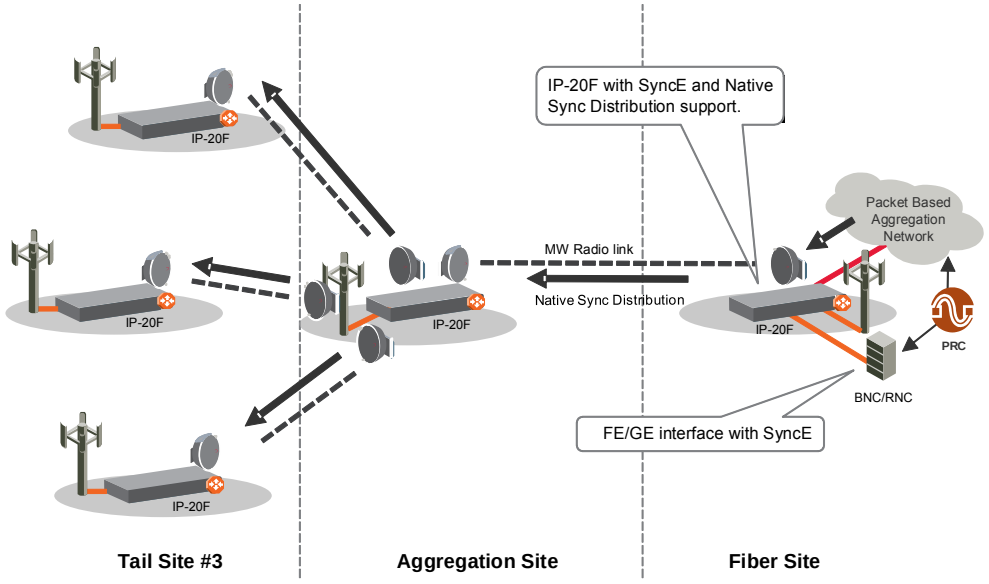


Figure 114: Native Sync Distribution Mode – Tree Scenario

The following figure illustrates Native Sync Distribution in a ring scenario, during normal operation.

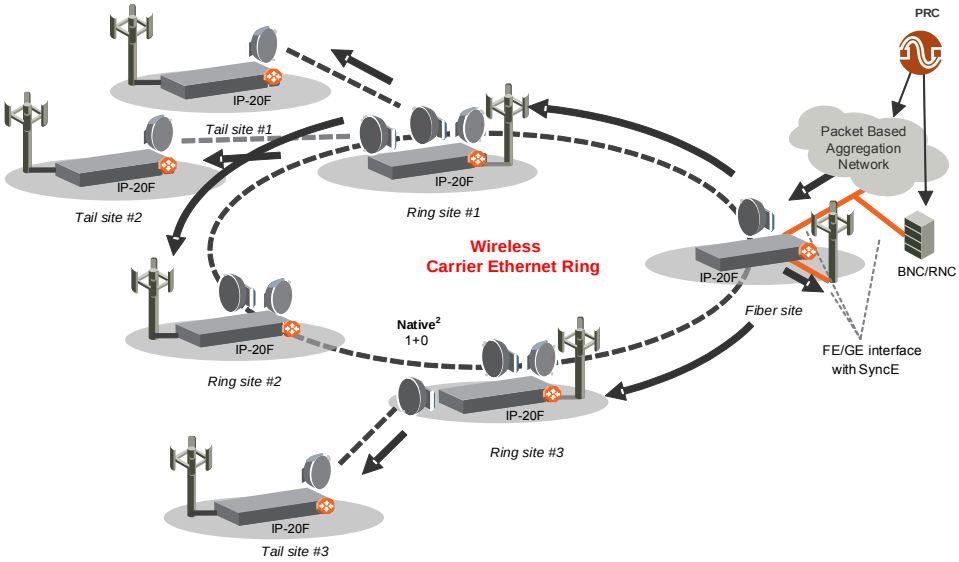


Figure 115: Native Sync Distribution Mode – Ring Scenario (Normal Operation)

The following figure illustrates Native Sync Distribution in a ring scenario, where a link has failed and the Native Sync timing distribution has been restored over an alternate path by using SSM messages.

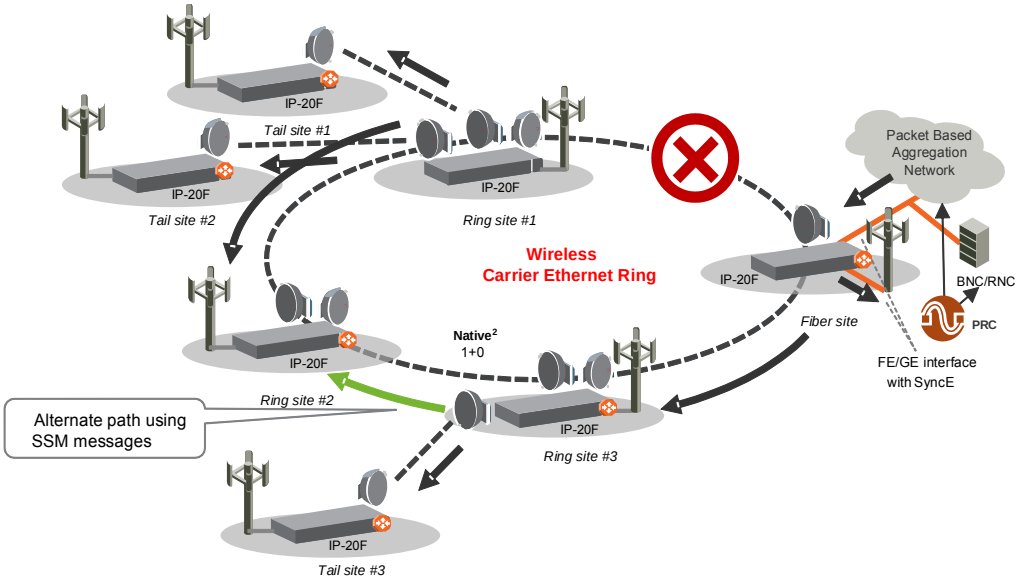


Figure 116: Native Sync Distribution Mode – Ring Scenario (Link Failure)

6.4.4 SyncE PRC Pipe Regenerator Mode

Note: SyncE PRC Pipe Regenerator mode is planned for future release.

Synchronous Ethernet (SyncE) is standardized in ITU-T G.8261 and G.8262, and refers to a method whereby the frequency is delivered on the physical layer. SyncE delivers a frequency reference, but not ToD or phase synchronization. It is used to distribute timing to applications that rely on precise frequency synchronization, such as wireless backhaul.

SyncE is based on SDH/TDM timing, with similar performance, and does not change the basic Ethernet standards. The SyncE technique supports synchronized Ethernet outputs as the timing source to an all-IP BTS/NodeB. This method offers the same synchronization quality provided over DS1 interfaces to legacy BTS/NodeB. SyncE is not affected by Path Delay Variation (PDV) and Packet Jitter, which are inherent in Ethernet networks.

The primary disadvantage of SyncE is that it since it is a physical-layer technology, it cannot be deployed in legacy Ethernet networks without upgrade of all hardware and interfaces in the network, since synchronous timing circuitry is necessary at every node.

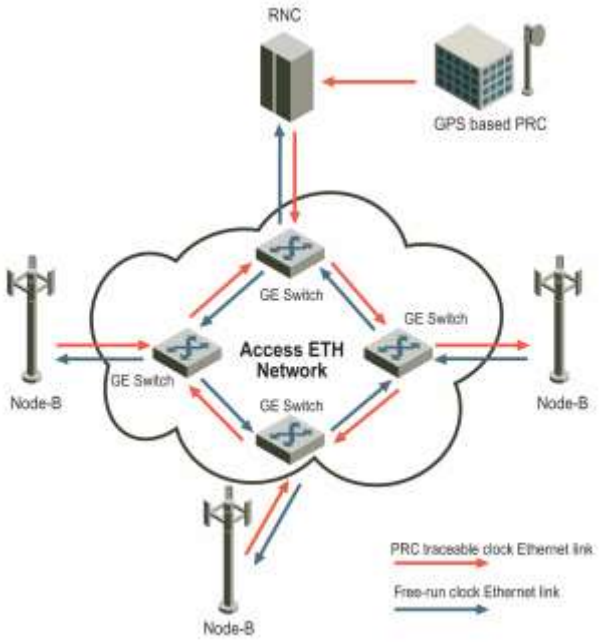


Figure 117: Synchronous Ethernet (SyncE)

IP-20F supports SyncE PRC pipe regenerator. In SyncE PRC pipe regenerator mode, frequency is transported between two GbE interfaces through the radio link.

PRC pipe regenerator mode makes use of the fact that the system is acting as a simple link (so no distribution mechanism is necessary) in order to achieve the following:

- Improved frequency distribution performance, with PRC quality.
- Simplified configuration

In PRC pipe regenerator mode, frequency is taken from the incoming GbE Ethernet or radio interface signal, and used as a reference for the radio frame. On the receiver side, the radio frame frequency is used as the reference signal for the outgoing Ethernet PHY.

Frequency distribution behaves in a different way for optical and electrical GbE interfaces, because of the way these interfaces are implemented:

- For optical interfaces, separate and independent frequencies are transported in each direction.
- For electrical interfaces, each PHY must act either as clock master or as clock slave in its own link. For this reason, frequency can only be distributed in one direction, determined by the user.

6.4.5 IEEE-1588v2 PTP Optimized Transport

Note: IEEE-1588v2 PTP Optimized Transport is planned for future release.

Precision Timing Protocol (PTP) refers to the distribution of frequency, phase, and absolute time information across an asynchronous frame switched network. PTP can use a variety of protocols to achieve timing distribution, including:

- IEEE-1588
- NTP
- RTP

IEEE-1588 PTP provides both frequency and phase (time) synchronization with the precision that is necessary in packet-switched mobile networks. With IEEE-1588 PTP, clocks distributed throughout the network are synchronized to sub-microsecond accuracy, suitable for mobile networks.

IP-20F supports IEEE-1588v2 PTP optimized transport, a message-based protocol that can be implemented across packet-based networks. IEEE-1588v2 provides both frequency and phase synchronization, and is designed to provide higher accuracy and precision, to the scale of nanoseconds, and up to 1.5 µs.

IEEE-1588v2 PTP synchronization is based on a master-slave architecture in which the master and slave exchange PTP packets carrying clock information. The master is connected to a reference clock, and the slave synchronizes itself to the master.

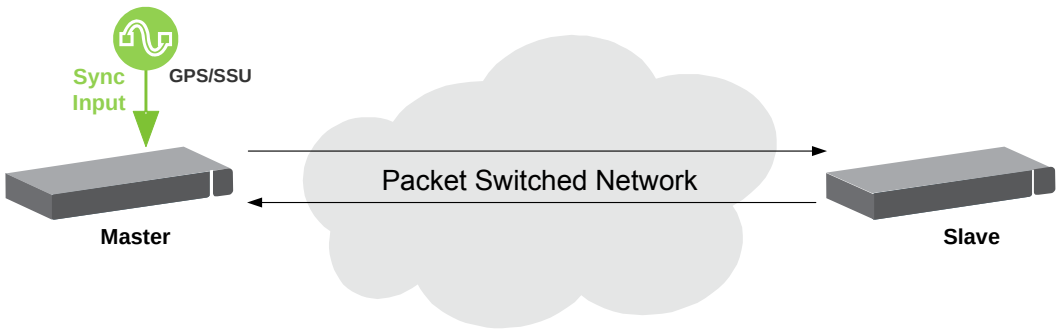


Figure 118: IEEE-1588v2 PTP Optimized Transport – General Architecture

Accurate synchronization requires a determination of the propagation delay for PTP packets. Propagation delay is determined by a series of messages between the master and slave.

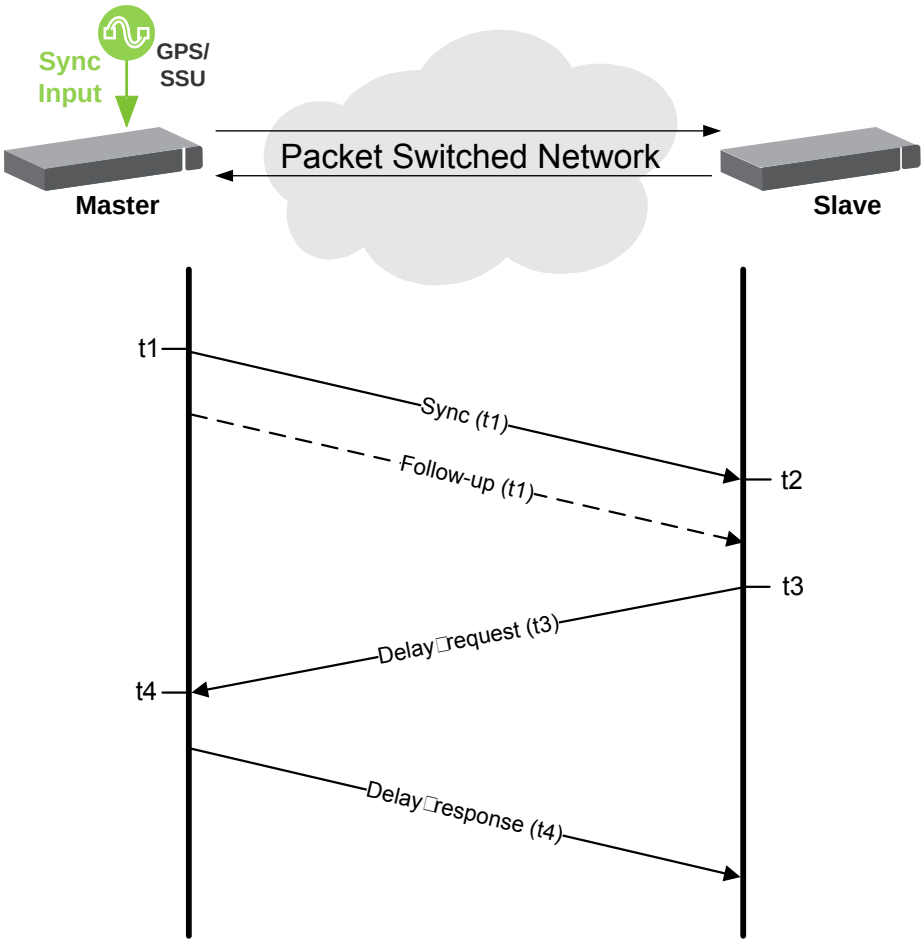


Figure 119: Calculating the Propagation Delay for PTP Packets

In this information exchange:

1 The master sends a Sync message to the slave and notes the time (t1) the message was sent.
2 The slave receives the Sync message and notes the time the message was received (t2).
3 The master conveys the t1 timestamp to the slave, in one of the following ways:
   - Embedding the t1 timestamp in the Sync message (requires L1 processing).
   - Embedding the t1 timestamp in a Follow-up message.
4 The slave sends a Delay_request message to the master and notes the time the message was sent (t3).
5 The master receives the Delay_request message and notes the time the message was received (t4).
6 The master conveys the t4 timestamp to the slave by embedding the t4 timestamp in a Delay_response message.

Based on this message exchange, the protocol calculates both the clock offset between the master and slave and the propagation delay, based on the following formulas:

Offset = [(t2 – t1) – (t4 – t3)]/2

Propagation Delay = [(t2 – t1) + (t4 – t3)]/2

The calculation is based on the assumption that packet delay is constant and that delays are the same in each direction. For information on the factors that may undermine these assumptions and how IP-20F's IEEE-1588v2 implementations mitigate these factors, see *Mitigating PDV* on page 214.

6.4.5.1 IEEE-1588v2 Benefits

IEEE-1588v2 provides packet-based synchronization that can transmit both frequency accuracy and phase information. This is essential for LTE applications, and provides a clear advantage over SyncE, which transmits frequency accuracy but not phase information.

Other IEEE-1588v2 benefits include:

- Fractional nanosecond precession.
- Meets strict LTE-A requirements for rigorous frequency and phase timing.
- Hardware time stamping of PTP packets.
- Standard protocol compatible with third-party equipment.
- Short frame and higher message rates.
- Supports unicast as well as multicast.
- Enables smooth transition from unsupported networks.
- Mitigates PDV issues by using Transparent Clock and Boundary Clock (see *Mitigating PDV* on page 214).
- Minimal consumption of bandwidth and processing power.
- Simple configuration.

6.4.5.2 Mitigating PDV

To get the most out of PTP and minimize PDV, IP-20F supports Transparent Clock and Boundary Clock.

PTP calculates path delay based on the assumption that packet delay is constant and that delays are the same in each direction. Delay variation invalidates this assumption. High PDV in wireless transport for synchronization over packet protocols, such as IEEE-1588, can dramatically affect the quality of the recovered clock. Slow variations are the most harmful, since in most cases it is more difficult for the receiver to average out such variations.

PDV can arise from both packet processing delay variation and radio link delay variation.

Packet processing delay variation can be caused by:

- Queuing Delay – Delay associated with incoming and outgoing packet buffer queuing.

- Head of Line Blocking – Occurs when a high priority frame, such as a frame that contains IEEE-1588 information, is forced to wait until a lower-priority frame that has already started to be transmitted completes its transmission.
- Store and Forward – Used to determine where to send individual packets. Incoming packets are stored in local memory while the MAC address table is searched and the packet's cyclic redundancy field is checked before the packet is sent out on the appropriate port. This process introduces variations in the time latency of packet forwarding due to packet size, flow control, MAC address table searches, and CRC calculations.

Radio link delay variation is caused by the effect of ACM, which enables dynamic modulation changes to accommodate radio path fading, typically due to weather changes. Lowering modulation reduces link capacity, causing traffic to accumulate in the buffers and producing transmission delay.

Note:	When bandwidth is reduced due to lowering of the ACM modulation point, it is essential that high priority traffic carrying IEEE-1588 packets be given the highest priority using IP-20F's enhanced QoS mechanism, so that this traffic will not be subject to delays or discards.

These factors can combine to produce a minimum and maximum delay, as follows:

- Minimum frame delay can occur when the link operates at a high modulation and no other frame has started transmission when the IEEE-1588 frame is ready for transmission.
- Maximum frame delay can occur when the link is operating at QPSK modulation and a large (e.g., 1518 bytes) frame has just started transmission when the IEEE-1588 frame is ready for transmission.

The worst case PDV is defined as the greatest difference between the minimum and maximum frame delays. The worst case can occur not just in the radio equipment itself but in every switch across the network.

To ensure minimal packet delay variation (PDV), IP-20F's synchronization solution includes 1588v2-compliant Transparent Clock and Boundary Clock synchronization protocols. The following two sections describe these protocols and how they counter PDV.

6.4.5.3 Transparent Clock

IP-20F supports end-to-end Transparent Clock, which updates the time-interval correction field for the delay associated with individual packet transfers. End-to-End Transparent Clock is the most appropriate option for the Telecom industry.

A Transparent Clock node resides between a master and a slave node, and updates the timestamps of PTP packets passing from the master to the slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock node is itself neither a master nor a slave node, but rather, serves as a bridge between master and slave nodes.

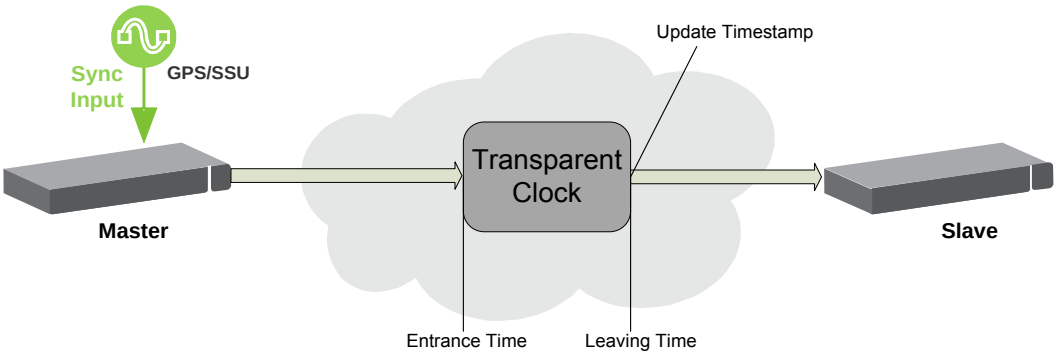


Figure 120: Transparent Clock – General Architecture

IP-20F uses 1588v2-compliant Transparent Clock to counter the effects of delay variation. Transparent Clock measures and adjusts for delay variation, enabling the IP-20F to guarantee ultra-low PDV.

The Transparent Clock algorithm forwards and adjusts the messages to reflect the residency time associated with the Sync, Follow_Up, and Delay_Request messages as they pass through the device. The delays are inserted in the 64-bit time-interval correction field.

As shown in the figure below, IP-20F measures and updates PTP messages based on both the radio link delay, and the packet processing delay that results from the network processor (switch operation).

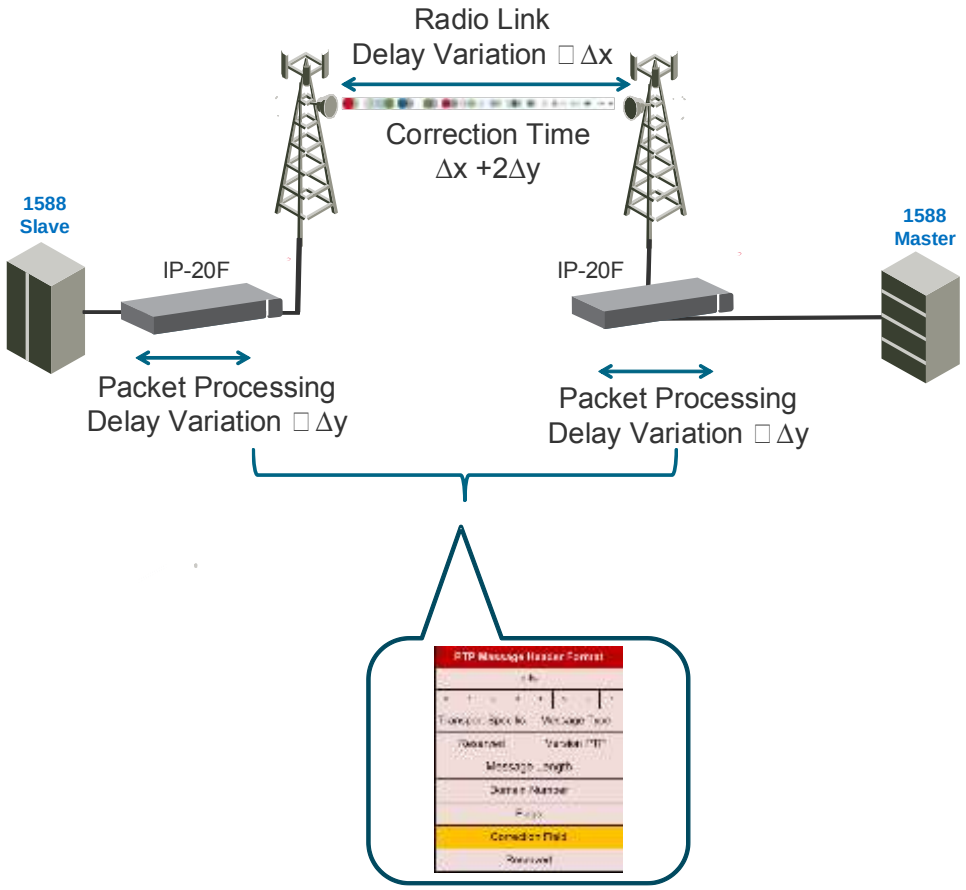


Figure 121: Transparent Clock Delay Compensation

6.4.5.4 Boundary Clock

IEEE-1588v2 Boundary Clock enables the IP-20F to regenerate phase synchronization via standard Ethernet. Boundary Clock provides better performance than other synchronization methods, enabling compliance with ITU-T Telecom Profile G.8275.1. This enables IP-20F, with Boundary Clock, to meet the rigorous synchronization requirements of LTE-Advanced (LTE-A) networks.

In Boundary Clock, a single node can serve in both master and slave roles. The Boundary Clock node terminates the PTP flow, recovers the clock and timestamp, and regenerates the PTP flow. The Boundary Clock node selects the best synchronization source from a higher domain and regenerates PTP towards lower domains. This reduces the processing load from master clocks and increases the scalability of the synchronization network, while rigorously maintaining timing accuracy.

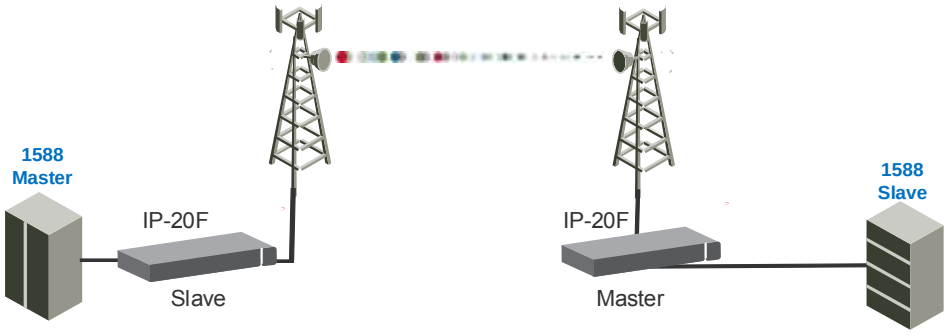


Figure 122: Boundary Clock – General Architecture

Boundary Clock uses the Best Master Clock (BMC) algorithm to determine which of the clocks in the network has the highest quality. This clock is designated the Grand Master clock, and it synchronizes all other clocks (slave clocks) in the network. If the Grand Master clock is removed from the network, or the BMC algorithm determines that another clock has superior quality, the BMC algorithm defines a new Grand Master clock and adjusts all other clocks accordingly. This process is fault tolerant, and no user input is required.

A node running as master clock can use the following inputs and outputs.

Table 60: Boundary Clock Input Options

Synchronization Input	Frequency/Phase
Ethernet packets from PTP 1588 Remote Master via radio or Ethernet interface	Phase
SyncE (including ESMC) via radio or Ethernet interface	Frequency

Table 61: Boundary Clock Output Options

Synchronization Input	Frequency/Phase
Ethernet packets from PTP 1588 master via radio or Ethernet interface	Phase
SyncE (including ESMC) via radio or Ethernet interface	Frequency

Users can configure the following parameters for the sending of PTP messages:

- UDP/IPv4, per IEEE 1588 Annex D, or IEEE 802.3 Ethernet, per IEEE 1588 Annex F.
- Unicast or multicast mode.

6.5 TDM Services

IP-20F provides integrated support for transportation of TDM (DS1) services with integrated DS1 and ch-OC-3 interfaces.

Note:	OC-3 requires the addition of an optional rear-mounted OC-3 module, which is planned for future release.

Two types of TDM services are supported using the same hardware:

- Native TDM trails
- TDM Pseudowire services (enabling interoperability with third party packet/PW equipment)

IP-20F also offers hybrid Ethernet and TDM services. Hybrid services can utilize either Native TDM or pseudowire.

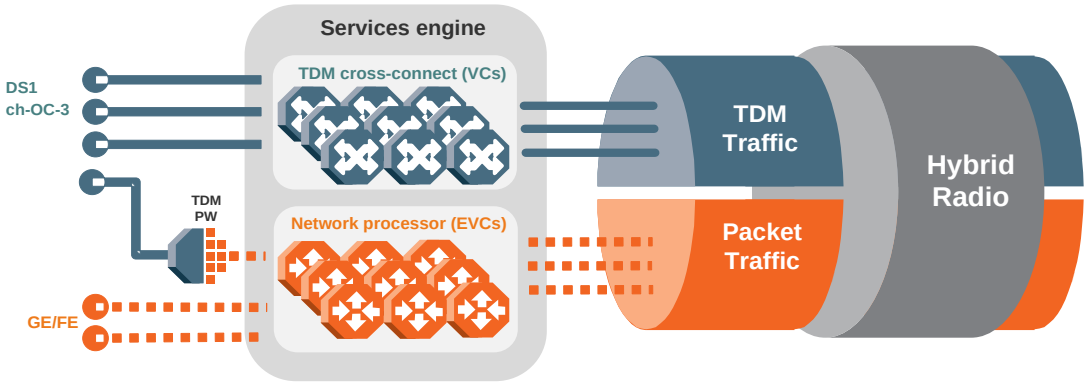


Figure 123: Hybrid Ethernet and TDM Services

Hybrid Ethernet and TDM services can also be transported via cascading interfaces. This enables the creation of links among multiple IP-20F and IP-20A units in a node for multi-carrier and multi-directional applications.

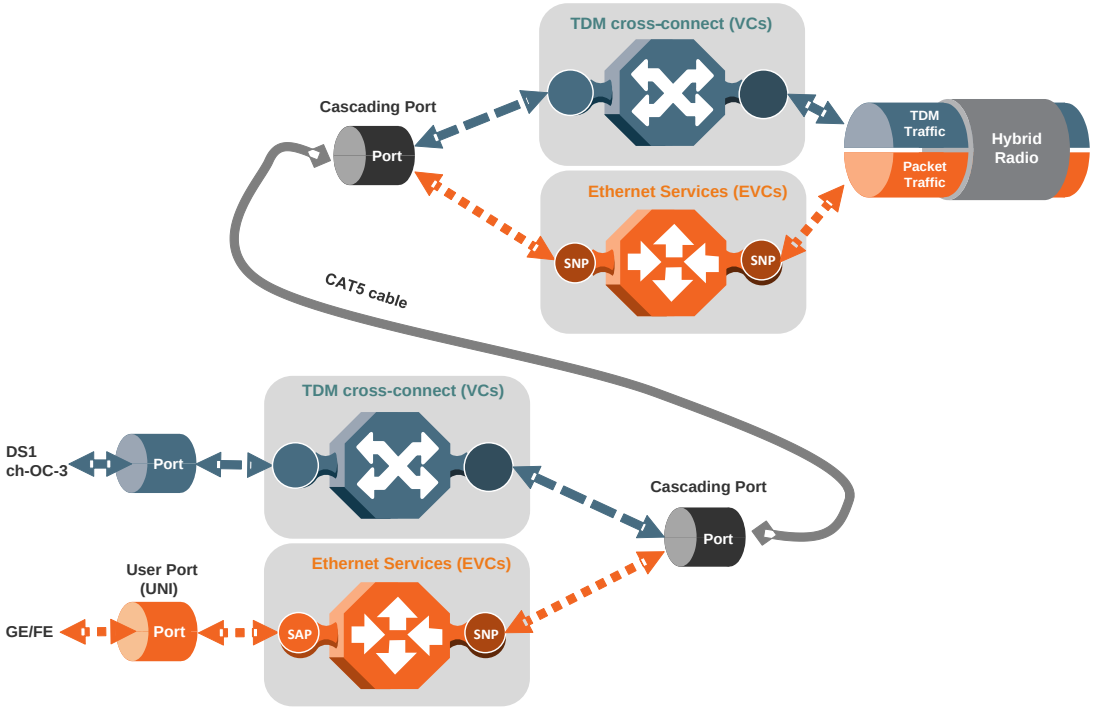


Figure 124: Hybrid Ethernet and TDM Services Carried Over Cascading Interfaces

6.5.1 Native TDM Trails

IP-20F provides native TDM support, utilizing a cross-connect module to support up to 256 TDM trails.

IP-20F also supports hybrid Ethernet and native TDM services, utilizing cascading ports. The following figure shows an example of a hybrid service package that includes a Point-to-Point and a Multipoint Ethernet service, along with a TDM trail utilizing virtual connections (VCs) via IP-20F's cross-connect.

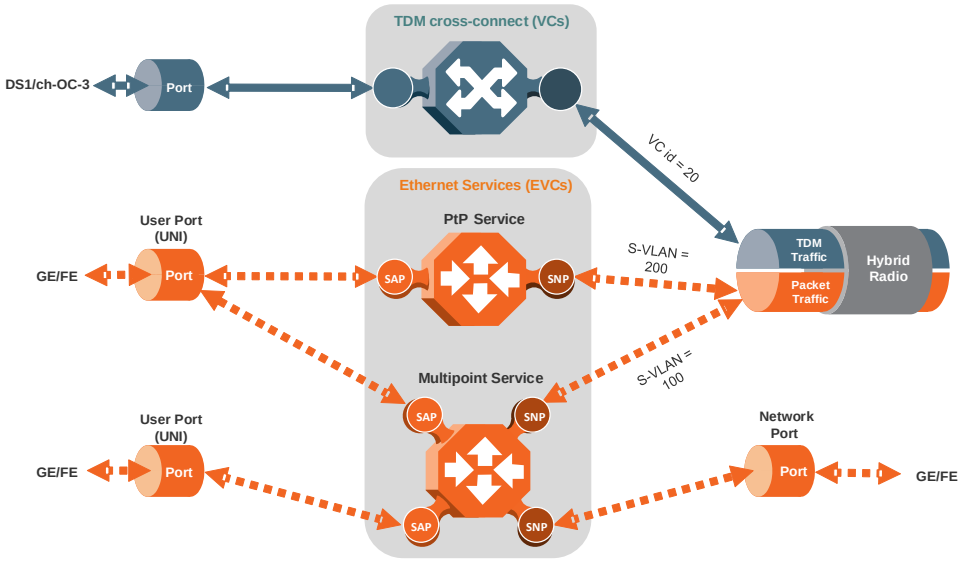


Figure 125: Hybrid Ethernet and Native TDM Services

6.5.1.1 Native TDM Trails Provisioning

The IP-20F Web EMS provides a simple and easy-to-use GUI that enables users to provision end-to-end TDM trails. The Services Provisioning GUI includes the following trail-creation end points:

- TDM interface
- Radio interface
- Cascading interface

6.5.1.2 TDM Trails and Synchronization

Related topics:

- Synchronization

Synchronization for TDM trails can be provided by any of the following synchronization methods:

- **Loop Timing** – Timing is taken from incoming traffic.
- **Recovered Clock** – Clock information is recovered on the egress path. Extra information may be located in an RTP header that can be used to correct frequency offsets. Recovered Clock can provide very accurate synchronization, but requires low PDV.
- **System Reference Clock** – Trails are synchronized to the system reference clock.

6.5.1.3 TDM Path Protection

TDM path protection enables the operator to define two separate network paths for a single TDM service. Two different kinds of path protection are available, each suitable for a different network topology:

- 1:1 TDM path protection is suitable for ring networks that consist entirely of IP-20F and/or IP-20A elements with two end-point interfaces for the TDM trail.
- 1+1 TDM path protection is suitable for dual homing topologies in which the IP-20F and/or IP-20A elements are set up as a chain connected to the third party networks at two different sites. The ring is closed on one side by the IP-20F and/or IP-20A elements, and on the other by third party equipment supporting standard SNCP. In this case, there are three end-point interfaces in the IP-20F and/or IP-20A section of the network.

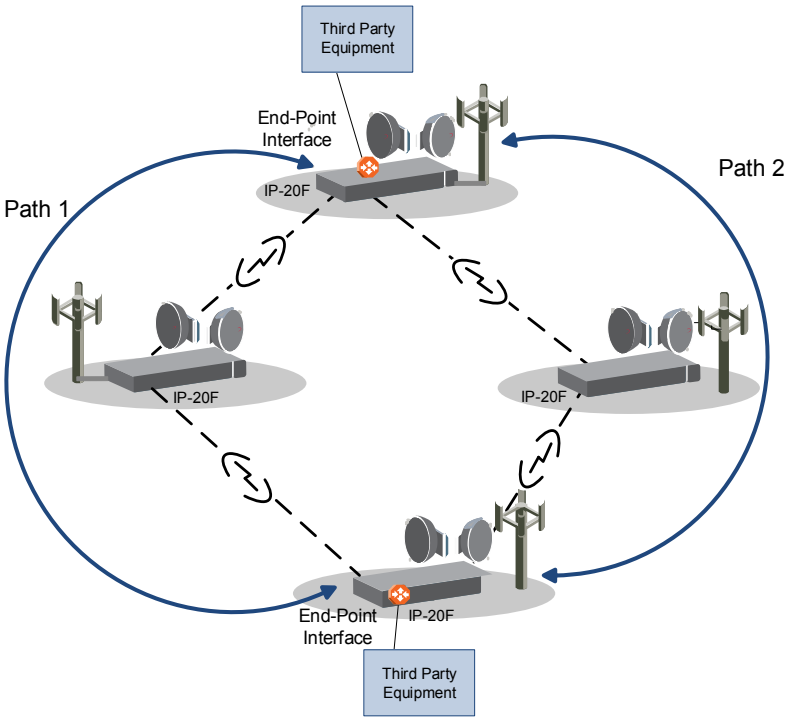


Figure 126: 1:1 TDM Path Protection – Ring Topology

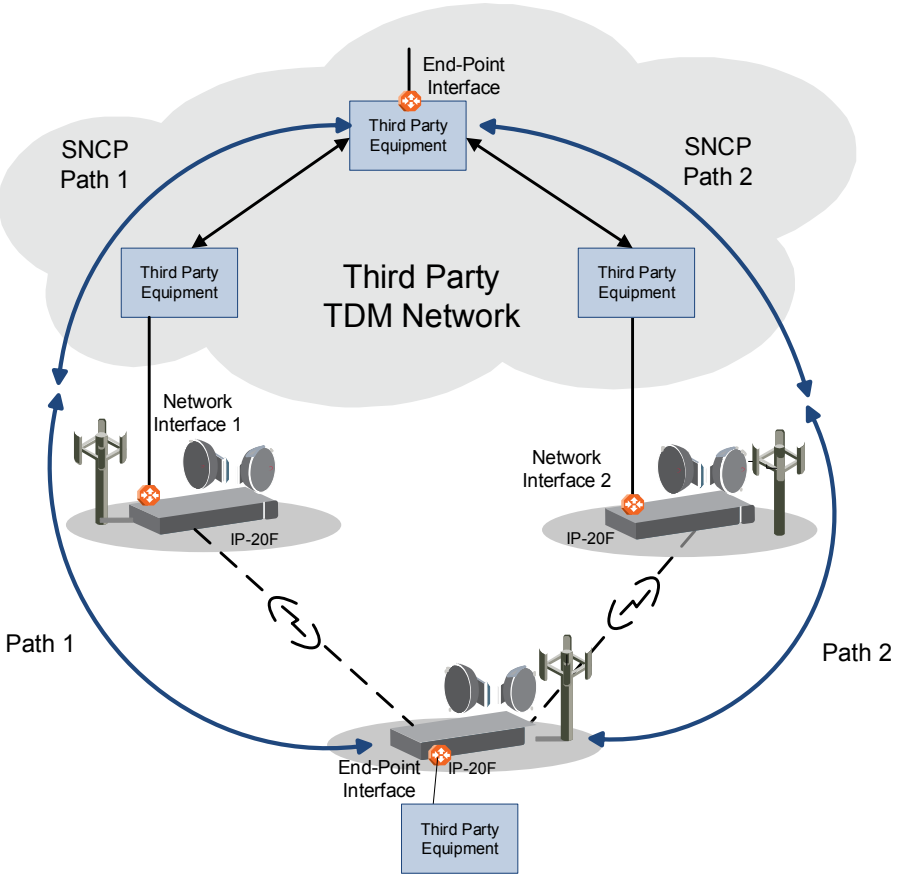


Figure 127: 1+1TDM Path Protection – Dual Homing Topology

1:1 TDM Path Protection

1:1 TDM path protection enables the operator to define two separate network paths for a single TDM trail. Each trail has the same TDM interface end points, but traffic flows to the destination via different paths. Bandwidth is utilized only on the active path, freeing up resources on the standby path.

For native TDM services TDM path protection is done by means of configuring active and backup path at the TDM service end-points.

1:1 TDM path protection can be configured to operate in revertive mode. In revertive mode, the system monitors the availability of the protected path at all times. After switchover to the protecting path, once the protected path is operational and available without any alarms, the system waits the user-configured Wait to Restore (WTR) time and then, if the protected path remains operational and available, initiates a revertive protection switch. A single WTR time is configured for all the TDM trails in the system.

1+1 TDM Path Protection

1+1 TDM path protection is used for dual homing topologies in which the IP-20F and/or IP-20A network elements are set up as a chain connected to third party networks at two different sites, where one end-point is located on an IP-20F and/or IP-20A unit and the other end-point is located on third-party equipment supporting standard SNCP.

As with 1:1 TDM path protection, the operator defines two separate network paths for a single TDM trail. However, unlike 1:1 path protection, traffic flows through both paths simultaneously, thereby supporting standard SNCP in the third party equipment.

6.5.1.4 TDM Performance Monitoring

The following monitoring features are available for TDM trails and interfaces. PMs are computed at the TDM card and reported at 15-minute intervals, with one second granularity.

- PMs for the outgoing TDM trail:
  - Errored seconds
  - Severely errored seconds
  - Unavailable seconds
- PMs for incoming native DS1 signal:
  - Errored seconds
  - Severely errored seconds
  - Unavailable seconds
- PMs for incoming SONET 155MHz signal:
  - Errored seconds
  - Severely errored seconds
  - Severely errored framing seconds
  - Coding Violations

6.5.2 TDM Pseudowire

IP-20F's TDM Pseudowire provides TDM-over-packet capabilities by means of optional TDM line cards that process TDM data, send the data through the system in frame format that can be processed by the IP-20F's Ethernet ports, and convert the data back to TDM format.

IP-20F also supports all-packet Ethernet and TDM pseudowire services. The following figure shows an example of an all-packet service package that includes two Point-to-Point services and one Multipoint Ethernet service, where the first Point-to-Point service carries DS1/OC-3 pseudowire traffic. This service package can be carried on any of the IP-20F's Ethernet ports.

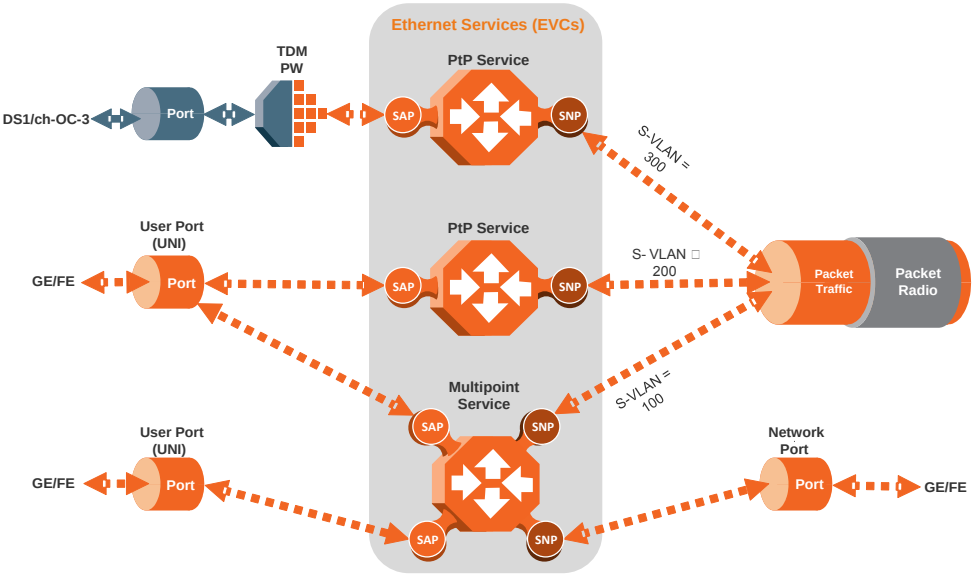


Figure 128: All-Packet Ethernet and TDM Pseudowire Services

6.5.2.1 TDM Pseudowire Supported Standards

TDM Pseudowire supports the following standards:

- SAToP – RFC 4553
- CESoP – RFC 5086[32]

TDM Pseudowire is compliant with the following encapsulations:

- Ethernet VLAN (MEF-8)
- IP/UDP (IETF)[33]
- MPLS (MFA8)[34]

---

32 CESoP mode is planned for future release.

33 IP/UDP (IETF) encapsulation is planned for future release.

34 MPLS (MFA8) encapsulation is planned for future release.

6.5.2.2 TDM Pseudowire Services

A Pseudowire service is a user-defined, bidirectional flow of information between a TDM signal and a packed flow, which is always transported over Layer 2 Ethernet. Such a service interconnects and makes use of the following elements:

- TDM Signal
  - The TDM signal may be an entire DS1 or a subset of DS0s (or DS1 time-slots).[35]
- PSN Tunnel
  - A PSN tunnel is the means by which the frames containing the TDM information are sent and received through a PSN network. The type of tunnel to be used should match the relevant transport network.
  - Three types of PSN tunnels are supported: MEF-8 (Ethernet), UDP/IP, and MPLS (MFA8).[36]
  - For IP tunnels, the pseudowire services make use of the TDM LIC's IP address, which is user-configurable. For MEF-8 tunnels, the addressing is done through the TDM LIC's MAC address, which is fixed, but readable by users. MAC addresses are fixed per slot in each unit, so that replacing a TDM LIC in a certain slot does not change the MAC address.
- PSN Tunnel Group
  - A PSN tunnel group is a grouping of two TDM tunnels, one of which will carry the pseudowire service frames at any given time.
  - A PSN tunnel group is used when path protection is required for a pseudowire service.
  - One of the tunnels is designated as "primary." The primary tunnel carries the pseudowire frames in the absence of any failures. The other tunnel is designated as "secondary." The secondary tunnel is used whenever the primary path fails.
- Pseudowire Profile
  - A profile is a set of parameters that determine various operational settings of a PW service. A single profile can be used for any number of services.
  - The following is a short explanation of the main parameters:
    - Payload size – In terms of DS1 frames per frame.
    - Jitter buffer – In milliseconds.
    - LOPS detection thresholds.
    - RTP timestamp usage details (for adaptive clock recovery).
    - Payload suppression and transmission patterns in case of errors.

---

[35] A subset of DS0 is supported in CESoP, which is planned for a future release.

[36] UDP/IP and MPLS are planned for future release.

In addition, there are a number of parameters at the PW Card level that must be configured properly to ensure proper operation:

- Ethernet traffic port settings
  - Speed
  - Duplex
  - Auto-negotiation
  - Flow control
- TDM LIC IP address and subnet mask
- Clock distribution

6.5.2.3 Pseudowire Services Provisioning

The IP-20A Web EMS provides a simple and easy-to-use GUI that enables users to provision end-to-end pseudowire services. The Services Provisioning GUI includes the following service-creation end points:

- TDM interface
- Radio interface
- Cascading interface

6.5.2.4 TDM Pseudowire and Synchronization

Related topics:

- Synchronization

A key requirement of pseudowire technology is managing the synchronization of TDM signals. IP-20F's TDM Pseudowire supports the following synchronization methods:

- **Absolute Reference Clock (Common Clock)** – All DS1 lines are synchronized to the system reference clock.
- **Adaptive Clock Recovery** – Clock information is included in the frames that contain the TDM data. Extra information may be located in an RTP header that can be used to correct frequency offsets. The clock information is extracted at the point where the frames are received and reconverted to TDM. The extracted clock information is used for the reconversion to TDM. Adaptive Clock Recovery can provide very accurate synchronization, but requires low PDV.
- **Differential Clock Recovery** – A single common clock is given, while each DS1 line has its independent clock referenced to this common clock.[37]
- **Loop Timing** – The pseudowire output signal uses the clock of the incoming DS1 lines Timing will be independent for each DS1 line.

6.5.2.5 TDM Pseudowire Path Protection

For TDM pseudowire traffic redundancy, IP-20F offers 1:1 TDM path protection, which protects the traffic along the path.

Note: Alternatively, protection for the traffic along the path can be achieved using 1+1HSB protection for the radios.[38]

1:1 TDM Path protection requires the use of SOAM (FM) at both end-point interfaces. The TDM module sends two data streams to the CPU. Only the data stream for the active path contains actual traffic. Both data streams contain continuity messages (CCMs). This enables the TDM module to monitor the status of both paths without doubling the amount of data being sent over the network. The TDM module determines when a switchover is necessary based on the monitored network status.

In order to achieve TDM Pseudowire path protection, different provisioning should be made for the Ethernet service corresponding to each of the two data streams. In order to do this, it is recommended to map the corresponding Ethernet services to MSTP instance number 63, which is meant for Traffic Engineering (ports are always forwarding) and to map the two different transport VLANs over two different paths.

[37] Differential Clock Recovery is planned for future release.

[38] 1+1 HSB radio protection is planned for future release.

1:1 TDM pseudowire path protection uses SOAM to monitor the network paths. Because SOAM is configured on the TDM module level, the TDM module can determine the status of the entire network path, up to and including the card's TDM interface.

6.5.2.6 TDM Pseudowire Performance Monitoring

The following monitoring features are available for TDM Pseudowire services and interfaces:

TDM Pseudowire PMs

Standard PM measurements are provided for each configured service:

- Number of frames transmitted
- Number of frames received
- Number of lost frames detected
- Number of frames received out-of-sequence but successfully reordered
- Number of transitions from normal state to LOPS (loss of frame state)
- Number of malformed frames received
- Number of frames dropped because the receive buffer exceeded the maximum allowed depth (jitter overruns)
- Maximum deviation from the middle of the jitter buffer (maximum jitter buffer deviation)
- Minimum jitter buffer usage registered during the prior one second (current minimum jitter buffer count)
- Maximum jitter buffer usage registered during the prior one second (current maximum jitter buffer count)

TDM Pseudowire Signal PMs[39]

PMs are computed at the PW card and reported at 15-minute intervals, with one second granularity.

- PMs for the recovered DS1:
  - Errored seconds
  - Severely errored seconds
  - Unavailable seconds
- PMs for the pseudowire Ethernet connection:
  - Frame Error Ratio (FER) performance
- RFC 5604 PMs:
  - Lost frames
  - Reordered frames
  - Buffer underruns

[39] Support for TDM signal PMs is planned for future release.

- Misordered frames dropped
- Malformed frames

- PMs for incoming native DS1 signal:
  - Errored seconds
  - Severely errored seconds
  - Unavailable seconds
- PMs for incoming SONET 155MHz signal:
  - Errored seconds
  - Severely errored seconds
  - Severely errored framing seconds
  - Coding Violations

6.5.3 OC-3 Interfaces

Note:	OC-3 requires the addition of an optional rear-mounted OC-3 module, which is planned for future release.

IP-20F provides two OC-3 ports that can be used in a 1+1 OC-3 protection configuration. These ports provide a convenient interface for numerous TDM signals (DS1).

In the ingress direction the SONET signals and headers are all terminated at the card, and the DS1 signals contained within the SONET signals are extracted. From this point on, they are treated the same as the TDM signals in the LIC-T16 (16x DS1) card.

In the egress direction, the DS1 signals are mapped onto SONET signals which are generated at the card.

The following standard signal mappings are used for SONET configurations: VT1.5 SPE -> VT1.5 -x4-> VT-Group -x7-> STS-1 SPE -> STS1 -x3-> STS3 -> OC3.

The following SONET functionality is supported by the LIC-T155 (1x ch-OC-3) card:

- J0 and J2 trace identifier support (transmitted, received, expected) for all standard lengths.
- VC-11 VT-AIS standard signaling and detection.
- SSM (S1) support (transmitted and received value)
- SONET – Level LOS, LOF, excessive BER, Signal Degrade alarms.
- SFP alarms: SFP exist, SFP tx failure.
- SFP mute/unmute support.

6.5.4 TDM Interface Protection

Two different schemes are available for OC-3 interface protection:

- 1+1 HSB Card Protection
- OC-3 Linear APS Card Protection

Both schemes provide full protection against hardware failure. OC-3 Linear APS also provides full protection against interface failure due to cable disconnection or failure of the far-end equipment, while 1+1 HSB card protection provides protection against interface failure due to cable disconnection at the IP-20F side of the link.

In both schemes, configuration of the active card is automatically copied to the standby card. The entire configuration can also be copied and stored for maintenance purposes.

1+1 OC-3 Protection

1+1 OC-3 protection offers full redundancy for the OC-3 interface. This form of redundancy is appropriate for connections with third party equipment at which a single OC-3 interface is available.

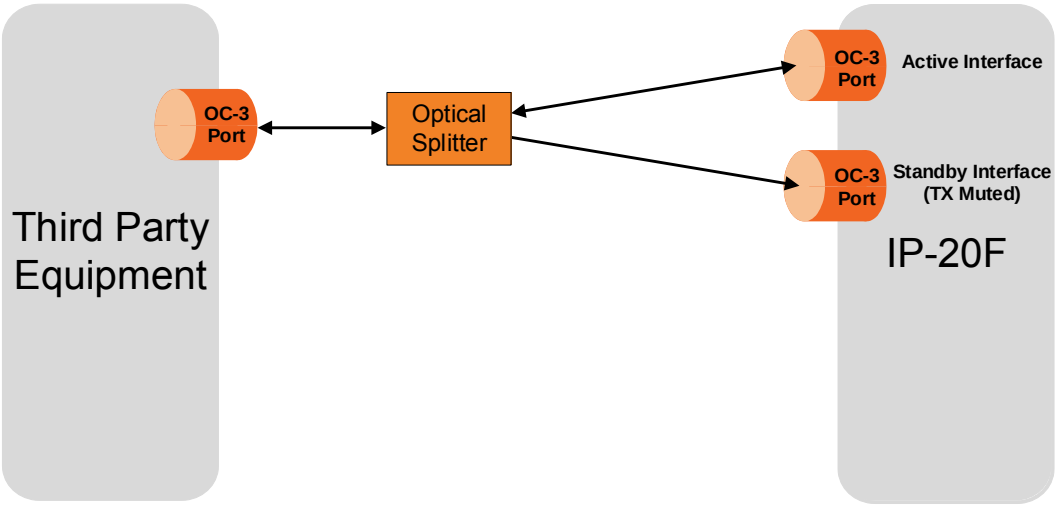


Figure 129: 1+1 OC-3 Protection

In a 1+1 OC-3 protection configuration, the single port on the third party equipment is connected to each of the two OC-3 interfaces on the IP-20F. A 1+1 OC-3 configuration uses an optical splitter cable to connect the two interfaces. This ensures that an identical signal is received by each OC-3 interface on the IP-20F. The IP-20F determines which interface is active, based on traffic loss indications such as LOS, LOF, or other errors.

While both interfaces on the IP-20F receive traffic, only the active interface transmits. The standby interface is automatically muted.

OC-3 Linear APS

OC-3 Linear APS is a standard procedure which provides equipment protection for LIC-T155 cards, as well as for the OC-3 interfaces in third party equipment. OC-3 Linear APS requires two OC-3 ports in the third party equipment, each of which must be connected to the IP-20F.

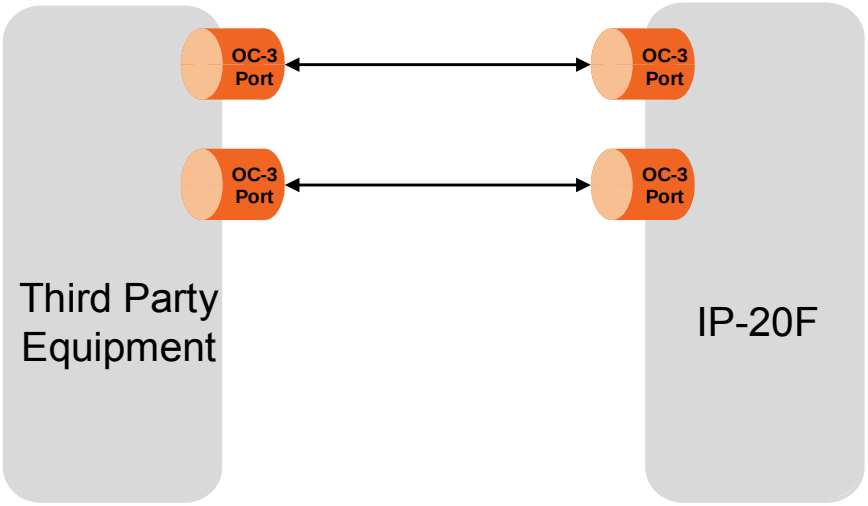


Figure 130: Uni-directional MSP

In OC-3 Linear Automatic Protection Switching (APS), the element at each end of the OC-3 link transmits traffic through both connections. On the receiving side, each IP-20F element unilaterally decides, based on traffic loss indications such as LOS, LOF, or other errors, from which interface to receive the traffic, and declares that interface the active interface. There is no need for a protocol between the two connected elements.

Each OC-3 interface on the IP-20F is connected directly to separate ports in the third party network element. There is no need for a splitter or Y-cable. This ensures protection to the optical ports in the third party equipment and to the optical fiber cable, as well as to the IP-20F.

6.5.5 TDM Reference Solutions

This section provides several examples of how IP-20F's end-to-end TDM service solutions can be used in various migration scenarios.

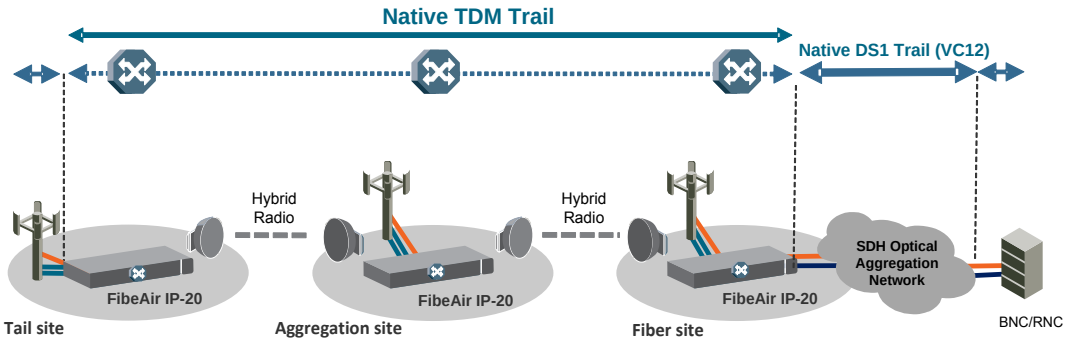


Figure 131: Native TDM Trail Interoperability with Optical SDH Equipment

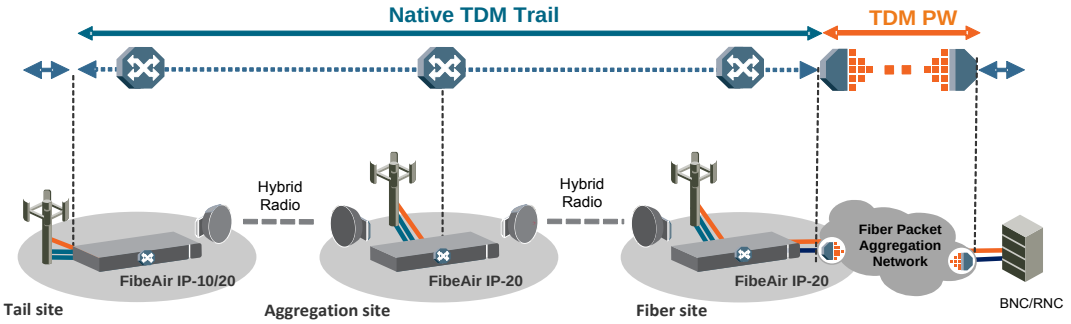


Figure 132: Native TDM Trail Interoperability with TDM Pseudowire-over-Packet Aggregation

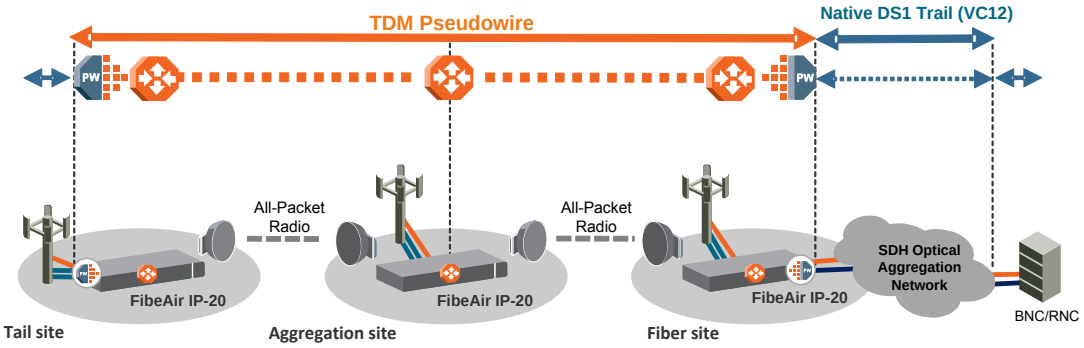


Figure 133: TDM Pseudowire Interoperability with Optical SDH Equipment

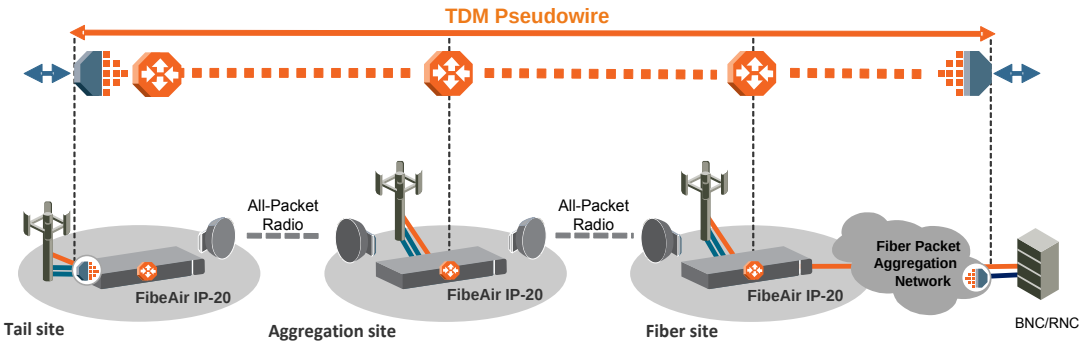


Figure 134: TDM Pseudowire Interoperability with Third-Party Packet Aggregation Equipment

7. FibeAir IP-20F Management

This chapter includes:

- Management Overview
- Automatic Network Topology Discovery with LLDP Protocol
- Management Communication Channels and Protocols
- Web-Based Element Management System (Web EMS)
- Command Line Interface (CLI)
- Configuration Management
- Software Management
- CeraPlan Service for Creating Pre-Defined Configuration Files
- IPv6 Support
- In-Band Management
- Local Management
- IP-20F provides two FE interfaces for local management. The two management interfaces give users the ability not only to manage the IP-20F directly via a laptop or PC, but also to manage other devices via the second management port of the IP-20F.

For additional information:

- Ethernet Management Interfaces
- Alarms
- External Alarms
- NTP Support
- UTC Support
- System Security Features

7.1 Management Overview

The Ceragon management solution is built on several layers of management:

- NEL – Network Element-level CLI
- EMS – HTTP web-based EMS
- NMS and SML –PolyView/NetMaster platform

Every FibeAir IP-10 and IP-20 network element includes an HTTP web-based element manager (CeraWeb) that enables the operator to perform element configuration, performance monitoring, remote diagnostics, alarm reports, and more.

In addition, Ceragon provides an SNMP v1/v2c/v3 northbound interface on the IP-20F.

Ceragon offers the NetMaster network management system (NMS), which provides centralized operation and maintenance capability for the complete range of network elements in an IP-20F system. To facilitate automated network topology discovery via NMS, IP-20F supports the Link Layer Discovery Protocol (LLDP).

In addition, management, configuration, and maintenance tasks can be performed directly via the IP-20F Command Line Interface (CLI). The CLI can be used to perform configuration operations for IP-20F units, as well as to configure several IP-20F units in a single batch command.

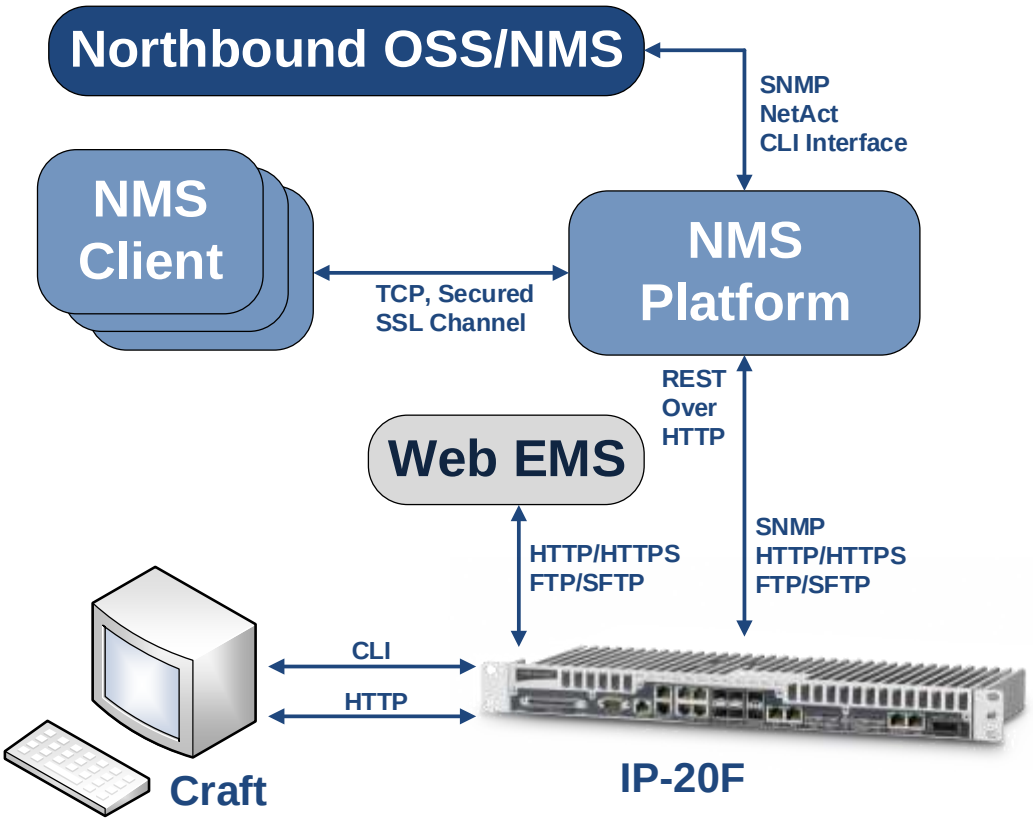


Figure 135: Integrated IP-20F Management Tools

7.2 Automatic Network Topology Discovery with LLDP Protocol

FibeAir IP-20F supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral layer 2 protocol that can be used by a station attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. IP-20F's LLDP implementation is based on the IEEE 802.1AB – 2009 standard.

LLDP provides automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. The port exchanges information with its peer and advertises this information to the NMS managing the unit. This enables the NMS to quickly identify changes to the network topology.

Enabling LLDP on IP-20 units enables the NMS to:

- Automatically detect the IP-20 unit neighboring the managed IP-20 unit, and determine the connectivity state between the two units.
- Automatically detect a third-party switch or router neighboring the managed IP-20 unit, and determine the connectivity state between the IP-20 unit and the switch or router.

7.3 Management Communication Channels and Protocols

Related Topics:

- Secure Communication Channels

Network Elements can be accessed locally via serial or Ethernet management interfaces, or remotely through the standard Ethernet LAN. The application layer is indifferent to the access channel used.

The NMS can be accessed through its GUI interface application, which may run locally or in a separate platform; it also has an SNMP-based northbound interface to communicate with other management systems.

Table 62: Dedicated Management Ports

Port number	Protocol	Frame structure	Details
161	SNMP	UDP	Sends SNMP Requests to the network elements
162 Configurable	SNMP (traps)	UDP	Sends SNMP traps forwarding (optional)
80	HTTP	TCP	Manages devices
443	HTTPS	TCP	Manages devices (optional)
From port 21 (default) to any remote port (>1023). Initial port (21) is configurable.	FTP Control Port	TCP	Downloads software and configuration files, uploads security and configuration logs, and unit info files. (FTP Server responds to client's control port) (optional)
From Any port (>1023) to any remote port (>1023)	FTP Data Port	TCP	Downloads software and configuration files, uploads security and configuration logs, and unit info files. The FTP server sends ACKs (and data) to client's data port.
From port 22 (default) to any remote port (>1023). Initial port (22) is configurable.	SFTP Control Port	TCP	Downloads software and configuration files, and CSR certificates, uploads security and configuration logs, and unit info files. (SFTP Server responds to client's control port) (optional)
From Any port (>1023) to any remote port (>1023)	SFTP Data Port	TCP	Downloads software and configuration files, and CSR certificates, uploads security and configuration logs, and unit info files. The SFTP server sends ACKs (and data) to client's data port.
23	telnet	TCP	Remote CLI access (optional)
22	SSH	TCP	Secure remote CLI access (optional)

All remote system management is carried out through standard IP communications. Each NE behaves as a host with a single IP address.

The communications protocol used depends on the management channel being accessed.

As a baseline, these are the protocols in use:

- Standard HTTP for web-based management
- Standard telnet for CLI-based management

7.4 Web-Based Element Management System (Web EMS)

The IP-20F Element Management System (Web EMS) is an HTTP web-based element manager that enables the operator to perform configuration operations and obtain statistical and performance information related to the system, including:

- **Configuration Management** – Enables you to view and define configuration data for the IP-20F system.
- **Fault Monitoring** – Enables you to view active alarms.
- **Performance Monitoring** – Enables you to view and clear performance monitoring values and counters.
- **Diagnostics and Maintenance** – Enables you to define and perform loopback tests, software updates, and IDU-RFU interface monitoring.
- **Security Configuration** – Enables you to configure IP-20F security features.
- **User Management** – Enables you to define users and user profiles.

A Web-Based EMS connection to the IP-20F can be opened using an HTTP Browser (Explorer or Mozilla Firefox). The Web EMS uses a graphical interface. Most system configurations and statuses are available via the Web EMS. However, some advanced configuration options are only available via CLI.

Note:	For optimal Web EMS performance, it is recommended to ensure that the network speed is at least 100 Kbps for most operations, and at least 5 Mbps for software download operations.

The Web EMS shows the actual chassis configuration and provides easy access to any card and interface in the chassis. The Web EMS opens to a Unit and Radio Summary page that displays the key unit, link, and radio parameters on a single page for quick viewing. This page can be customized to include only specific columns and tables, enabling the user to hide information that he does not need in order to focus on the information that is most relevant to his needs in monitoring and managing the unit.

The Web EMS includes a Quick Platform Setup page designed to simplify initial configuration and minimize the time it takes to configure a working link.

The Web EMS also includes quick link configuration wizards that guide the user, step-by-step, through the creation of:

- 1+0 links with Pipe services
- 1+0 repeater links (radio to radio) with Pipe services
- 2+0 Multi-Carrier ABC groups
- TDM services
- Pseudowire services

7.5 Command Line Interface (CLI)

A CLI connection to the IP-20F can be opened via terminal (serial COM, speed: 115200, Data: 8 bits, Stop: 1 bit, Flow-Control: None), or via telnet. The Terminal format should be VT-100 with a screen definition of 80 columns X 24 rows.

Note:	Telnet access can be blocked by user configuration.

All parameter configurations can be performed via CLI.

7.6 Configuration Management

The system configuration file consists of a set of all the configurable system parameters and their current values.

IP-20F configuration files can be imported and exported. This enables you to copy the system configuration to multiple IP-20F units.

System configuration files consist of a zip file that contains three components:

- A binary configuration file which is used by the system to restore the configuration.
- A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.
- An additional text file which enables users to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.[40]

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to restore points by creating backups of the current system state or by importing them from an external server.

Note:	In the Web EMS, these restore points are referred to as “file numbers.”

For example, a user may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

Any of the restore points can be used to apply a configuration file to the system.

The user can determine whether or not to include security-related settings, such as users and user profiles, in the exported configuration file. By default, security settings are included.

Note:	The option to enable or disable import and export of security parameters is planned for future release.

[40] The option to edit the backup configuration is planned for future release.

7.7 Software Management

The IP-20F software installation and upgrade process includes the following steps:

- **Download** – The files required for the installation or upgrade are downloaded from a remote server.
- **Installation** – The files are installed in the appropriate modules and components of the IP-20F.
- **Reset** – The IP-20F is restarted in order to boot the new software and firmware versions.

IP-20F software and firmware releases are provided in a single bundle that includes software and firmware for all components and card types supported by the system, including RFUs. When the user downloads a software bundle, the system verifies the validity of the bundle. The system also compares the files in the bundle to the files currently installed in the IP-20F and its components, so that only files that differ between the new version bundle and the current version in the system are actually downloaded. A message is displayed to the user for each file that is actually downloaded.

Note:	When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via FTP, SFTP, HTTP, or HTTPS. When downloading software via HTTP or HTTPS, the IP-20F unit acts as an HTTP server, and the software can be downloaded directly to the unit. When downloading software via FTP or SFTP, the IP-20F functions as an FTP or SFTP client, and FTP or SFTP server software must be installed on the PC or laptop being using to perform the upgrade.

After the software download is complete, the user initiates the installation. A timer can be used to perform the installation after a defined time interval. When an installation timer is used, the system performs an automatic reset after the installation.

Although RFU software is included in the standard installation bundle, the current software version is not automatically updated in the radio slots when an installation is performed. To upgrade the software in an RFU, you must perform the upgrade manually, per slot. This enables users to manage IDU and RFU software versions separately.

7.7.1 Backup Software Version

Note:	Backup software version support is planned for future release.

IP-20F maintains a backup copy of the software bundle. In the event that the working software version cannot be found, or the operating system fails to start properly, the system automatically boots from the backup version, and the previously active version becomes the backup version.

Users can also update the backup version manually. The Web EMS includes a field that indicates whether or not the active and backup software versions are identical.

7.8 CeraPlan Service for Creating Pre-Defined Configuration Files

IP-20 units running CeraOS 9.2 or higher can be configured from the Web EMS in a single step by applying a pre-defined configuration file. This drastically reduces the initial installation and setup time in the field.

Using pre-defined configuration files also reduces the risk of configuration errors and enables operators to invest less time and money training installation personnel. Installers can focus on hardware configuration, relying on the pre-defined configuration file to implement the proper software configuration on each device.

The pre-defined configuration file is generated by Ceragon Professional Services and provided as a service.

A pre-defined configuration file can be prepared for multiple IP-20 units, with the relevant configuration details specified and differentiated per-unit. This simplifies administration, since a single file can be used with multiple devices.

Pre-defined configuration files can include all the parameters necessary to configure basic links, including:

- ETSI to ANSI conversion
- Activation Key (or Demo mode) configuration
- Radio Parameters
- Interface Groups (LAG, Multi-Carrier ABC, XPIC)
- Management Service

All configurations that can be implemented via the Web EMS Quick Configuration wizards can also be configured using pre-defined configuration files.

Pre-defined configuration files can be created by Ceragon Professional Services, according to customer specifications. For further information on CeraPlan, consult your Ceragon representative.

7.9 IPv6 Support

FibeAir IP-20F management communications can use both IPv4 and IPv6. The unit IP address for management can be configured in either or both formats.

Additionally, other management communications can utilize either IPv4 or IPv6. This includes:

- Software file downloads
- Configuration file import and export
- Trap forwarding
- Unit information file export (used primarily for maintenance and troubleshooting)

7.10 In-Band Management

FibeAir IP-20F can optionally be managed In-Band, via its radio and Ethernet interfaces. This method of management eliminates the need for a dedicated management interface. For more information, refer to *Management Service (MNG)* on page 140.

7.11 Local Management

IP-20F provides two FE interfaces for local management. The two management interfaces give users the ability not only to manage the IP-20F directly via a laptop or PC, but also to manage other devices via the second management port of the IP-20F.

For additional information:

- Ethernet Management Interfaces

7.12 Alarms

7.12.1 Configurable BER Threshold Alarms and Traps

Users can configure alarm and trap generation in the event of Excessive BER and Signal Degrade BER above user-defined thresholds. Users have the option to configure whether or not excessive BER is propagated as a fault and considered a system event.

7.12.2 RSL Threshold Alarm

Users can configure an alarm that is raised if the RSL falls beneath a user-defined threshold. This feature can be enabled or disabled per radio carrier. By default, it is disabled. The RSL threshold alarm provides a preventative maintenance tool for monitoring the health of the link and ensuring that problems can be identified and corrected quickly.

7.12.3 Editing and Disabling Alarms and Events

Users can change the description text (by appending extra text to the existing description) or the severity of any alarm in the system. Users can also choose to disable specific alarms and events. Any alarm or event can be disabled, so that no indication of the alarm or event is displayed, and no traps are sent for the alarm or event.

This is performed as follows:

- Each alarm and event in the system is identified by a unique name (see separate list of system alarms and events).
- The user can perform the following operations on any alarm:
  - View current description and severity
  - Define the text to be appended to the description and/or severity
  - Return the alarm to its default values
  - Disable or re-enable the alarm (or event)
- The user can also return all alarms and events to their default values.

7.12.4 Timeout for Trap Generation

Users can configure a wait time of 0 to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously.

This means that when the alarm is cleared, the alarm continues to be displayed and no *clear alarm* trap is sent until the timeout period is finished.

The timeout for trap generation can be configured via CLI. By default, the timeout is 10 seconds.

7.13 External Alarms

IP-20F includes a DB9 dry contact external alarms interface. The external alarms interface supports five input alarms. For each alarm input, the user can configure the following:

1 Alarm administration (On or Off)
2 Alarm text
3 Alarm severity

Alarm severity can be configured to:

1 Indeterminate
2 Critical
3 Major
4 Minor
5 Warning

7.14 NTP Support

IP-20F supports Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.

IP-20F supports NTPv3 and NTPv4. NTPv4 provides interoperability with NTPv3 and with SNTP.

7.15 UTC Support

IP-20F uses the Coordinated Universal Time (UTC) standard for time and date configuration. UTC is a more updated and accurate method of date coordination than the earlier date standard, Greenwich Mean Time (GMT).

Every IP-20F unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information (CLI and Web EMS) uses its own UTC offset to present the information in the correct time.

7.16 System Security Features

To guarantee proper performance and availability of a network as well as the data integrity of the traffic, it is imperative to protect it from all potential threats, both internal (misuse by operators and administrators) and external (attacks originating outside the network).

System security is based on making attacks difficult (in the sense that the effort required to carry them out is not worth the possible gain) by putting technical and operational barriers in every layer along the way, from the access outside the network, through the authentication process, up to every data link in the network.

7.16.1 Ceragon's Layered Security Concept

Each layer protects against one or more threats. However, it is the combination of them that provides adequate protection to the network. In most cases, no single layer protection provides a complete solution to threats.

The layered security concept is presented in the following figure. Each layer presents the security features and the threats addressed by it. Unless stated otherwise, requirements refer to both network elements and the NMS.

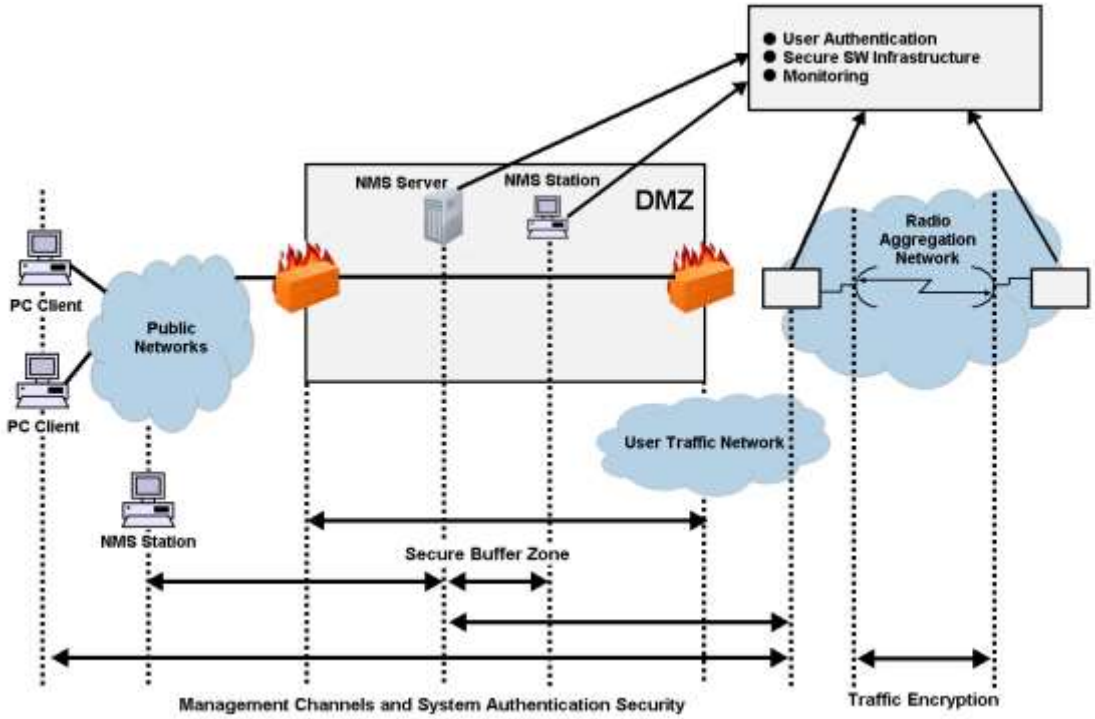


Figure 136: Security Solution Architecture Concept

7.16.2 Defenses in Management Communication Channels

Since network equipment can be managed from any location, it is necessary to protect the communication channels' contents end to end.

These defenses are based on existing and proven cryptographic techniques and libraries, thus providing standard secure means to manage the network, with minimal impact on usability.

They provide defense at any point (including public networks and radio aggregation networks) of communications.

While these features are implemented in Ceragon equipment, it is the responsibility of the operator to have the proper capabilities in any external devices used to manage the network.

In addition, inside Ceragon networking equipment it is possible to control physical channels used for management. This can greatly help deal with all sorts of DoS attacks.

Operators can use secure channels instead or in addition to the existing management channels:

- SNMPv3 for all SNMP-based protocols for both NEs and NMS
- HTTPS for access to the NE's web server
- SSH-2 for all CLI access SFTP for all software and configuration download between NMS and NEs

All protocols run with secure settings using strong encryption techniques. Unencrypted modes are not allowed, and algorithms used must meet modern and client standards.

Users are allowed to disable all insecure channels.

In the network elements, the bandwidth of physical channels transporting management communications is limited to the appropriate magnitude, in particular, channels carrying management frames to the CPU.

Attack types addressed

- Tempering with management flows
- Management traffic analysis
- Unauthorized software installation
- Attacks on protocols (by providing secrecy and integrity to messages)
- Traffic interfaces eavesdropping (by making it harder to change configuration)
- DoS through flooding

7.16.3 Defenses in User and System Authentication Procedures

7.16.3.1 User Configuration and User Profiles

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the IP-20F GUI, these roles are called user profiles. Up to 50 user profiles can be configured. Each profile contains a set of privilege levels per functionality group, and defines the management protocols (access channels) that can be used to access the system by users to whom the user profile is assigned.

The system parameters are divided into the following functional groups:

- Security
- Management
- Radio
- TDM
- Ethernet
- Synchronization

A user profile defines the permitted access level per functionality group. For each functionality group, the access level is defined separately for read and write operations. The following access levels can be assigned:

- **None** – No access to this functional group.
- **Normal** – The user has access to parameters that require basic knowledge about the functional group.
- **Advance** – The user has access to parameters that require advanced knowledge about the functional group, as well as parameters that have a significant impact on the system as a whole, such as restoring the configuration to factory default settings.

7.16.3.2 User Identification

IP-20F supports the following user identification features:

- Configurable inactivity time-out for automatically closing unused management channels
- Optional password strength enforcement. When password strength enforcement is enabled; passwords must comply with the following rules:
  - Password must be at least eight characters long.
  - Password must include at least three of the following categories: lower-case characters, upper-case characters, digits, and special characters.
  - When calculating the number of character categories, upper-case letters used as the first character and digits used as the last character of a password are not counted.
  - The password cannot have been used within the user's previous five passwords.
- Users can be prompted to change passwords after a configurable amount of time (password aging).
- Users can be blocked for a configurable time period after a configurable number of unsuccessful login attempts.
- Users can be configured to expire at a certain date
- Mandatory change of password at first time login can be enabled and disabled upon user configuration. It is enabled by default.

7.16.3.3 Remote Authentication

Note:	Remote authorization is planned for future release.

Certificate-based strong standard encryption techniques are used for remote authentication. Users may choose to use this feature or not for all secure communication channels.

Since different operators may have different certificate-based authentication policies (for example, issuing its own certificates vs. using an external CA or allowing the NMS system to be a CA), NEs and NMS software provide the tools required for operators to enforce their policy and create certificates according to their established processes.

Server authentication capabilities are provided.

7.16.3.4 RADIUS Support

The RADIUS protocol provides centralized user management services. IP-20F supports RADIUS server and provides a RADIUS client for authentication and authorization.

RADIUS can be enabled or disabled. When RADIUS is enabled, a user attempting to log into the system from any access channel (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard RADIUS server which indicates to the IP-20F whether the user is known, and which privilege is to be given to the user. RADIUS uses the same user attributes and privileges defined for the user locally.

Note:	When using RADIUS for user authentication and authorization, the access channels configured per IP-20 user profile are not applicable. Instead, the access channels must be configured as part of the RADIUS server configuration.

RADIUS login works as follows:

- If the RADIUS server is reachable, the system expects authorization to be received from the server:
  - The server sends the appropriate user privilege to the IP-20F, or notifies the IP-20F that the user was rejected.
  - If rejected, the user will be unable to log in. Otherwise, the user will log in with the appropriate privilege and will continue to operate normally.
- If the RADIUS server is unavailable, the IP-20F will attempt to authenticate the user locally, according to the existing list of defined users.

Note:	Local login authentication is provided in order to enable users to manage the system in the event that RADIUS server is unavailable. This requires previous definition of users in the system. If the user is only defined in the RADIUS server, the user will be unable to login locally in case the RADIUS server is unavailable.

In order to support IP-20F - specific privilege levels, the vendor-specific field is used. Ceragon's IANA number for this field is 2281.

The following RADIUS servers are supported:

- FreeRADIUS
- RADIUS on Windows Server (IAS)
  - Windows Server 2008

7.16.4 Secure Communication Channels

IP-20F supports a variety of standard encryption protocols and algorithms, as described in the following sections.

7.16.4.1 SSH (Secured Shell)

SSH protocol can be used as a secured alternative to Telnet. In IP-20F:

- SSHv2 is supported.
- SSH protocol will always be operational. Admin users can choose whether to disable Telnet protocol, which is enabled by default. Server authentication is based on IP-20F's public key.
- RSA and DSA key types are supported.
- MAC (Message Authentication Code): SHA-1-96 (MAC length = 96 bits, key length = 160 bit). Supported MAC: hmac-md5, hmac-sha1, hmac-ripemd160, hmac-sha1-96, hmac-md5-96'
- The server authenticates the user based on user name and password. The number of failed authentication attempts is not limited.
- The server timeout for authentication is 10 minutes. This value cannot be changed.

7.16.4.2 HTTPS (Hypertext Transfer Protocol Secure)

HTTPS combines the Hypertext Transfer protocol with the SSLv3/TLS (1.0, 1.1, 1.2) protocol to provide encrypted communication and secure identification of a network web server. IP-20F enables administrators to configure secure access via HTTPS protocol.

Users can configure the IP-20 to operate in HTTPS strong mode. In HTTPS strong mode, SSLv3, TLSv1.0, and TLSv1.1 are disabled completely and only certain ciphers are supported for TLSv1.2.

For a list of supported HTTPS ciphers, including an indication of which ciphers are supported in HTTPS strong mode, see *Annex B – Supported Ciphers for Secured Communication Protocols* in the Release Notes for the CeraOS version you are using.

7.16.4.3 SFTP (Secure FTP)

SFTP can be used for the following operations:

- Configuration upload and download,
- Uploading unit information
- Uploading a public key
- Downloading certificate files
- Downloading software

7.16.4.4 Creation of Certificate Signing Request (CSR) File

In order to create a digital certificate for the NE, a Certificate Signing Request (CSR) file should be created by the NE. The CSR contains information that will be included in the NE's certificate such as the organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate. Certificate authority (CA) will use the CSR to create the desired certificate for the NE.

While creating the CSR file, the user will be asked to input the following parameters that should be known to the operator who applies the command:

- **Common name** – The identify name of the element in the network (e.g., the IP address). The common name can be a network IP or the FQDN of the element.
- **Organization** – The legal name of the organization.
- **Organizational Unit** - The division of the organization handling the certificate.
- **City/Locality** - The city where the organization is located.
- **State/County/Region** - The state/region where the organization is located.
- **Country** - The two-letter ISO code for the country where the organization is location.
- **Email address** - An email address used to contact the organization.

7.16.4.5 SNMP

IP-20F supports SNMP v1, V2c, and v3. The default community string in NMS and the SNMP agent in the embedded SW are disabled. Users are allowed to set community strings for access to IDUs.

IP-20F supports the following MIBs:

- RFC-1213 (MIB II)
- RMON MIB
- Ceragon (proprietary) MIB.

Access to all IDUs in a node is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

For additional information:

- FibeAir IP-20 Series MIB Reference

7.16.4.6 Server Authentication (SSLv3/TLS (1.0, 1.1, 1.1))

- All protocols making use of SSL (such as HTTPS) use SLLv3/TLS (1.0, 1.1, 1.2) and support X.509 certificates-based server authentication.
- Users with type of “administrator” or above can perform the following server (IDU) authentication operations for certificates handling:
  - Generate server key pairs (private + public)
  - Export public key (as a file to a user-specified address)
  - Install third-party certificates
    - The Admin user is responsible for obtaining a valid certificate.
  - Load a server RSA key pair that was generated externally for use by protocols making use of SSL.
- Non-SSL protocols using asymmetric encryption, such as SSH and SFTP, can make use of public-key based authentication.
  - Users can load trusted public keys for this purpose.

7.16.5 Security Log

The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

Note:	In order to read the security log, the user must upload the log to his or her server.

The security log file has the following attributes:

- The file is of a “cyclic” nature (fixed size, newest events overwrite oldest).
- The log can only be read by users with "admin" or above privilege.
- The contents of the log file are cryptographically protected and digitally signed.
  - In the event of an attempt to modify the file, an alarm will be raised.
- Users may not overwrite, delete, or modify the log file.

The security log records:

- Changes in security configuration
  - Carrying out “security configuration copy to mate”
  - Management channels time-out
  - Password aging time
  - Number of unsuccessful login attempts for user suspension
  - Warning banner change
  - Adding/deleting of users
  - Password changed
  - SNMP enable/disable
  - SNMP version used (v1/v3) change
  - SNMPv3 parameters change
    - Security mode
    - Authentication algorithm

        - User
        - Password
    - SNMPv1 parameters change
        - Read community
        - Write community
        - Trap community for any manager
    - HTTP/HTTPS change
    - FTP/SFTP change
    - Telnet and web interface enable/disable
    - FTP enable/disable
    - Loading certificates
    - RADIUS server
    - Radius enable/disable
    - Remote logging enable/disable (for security and configuration logs)
    - System clock change
    - NTP enable/disable
- Security events
- Successful and unsuccessful login attempts
- N consecutive unsuccessful login attempts (blocking)
- Configuration change failure due to insufficient permissions
- SNMPv3/PV authentication failures
- User logout
- User account expired

For each recorded event the following information is available:

- User ID
- Communication channel (WEB, terminal, telnet/SSH, SNMP, NMS, etc.)
- IP address, if applicable
- Date and time

8. Standards and Certifications

This chapter includes:

- Supported Ethernet Standards
- MEF Certifications for Ethernet Services
- Supported TDM Pseudowire Encapsulations
- Standards Compliance
- Network Management, Diagnostics, Status, and Alarms

8.1 Supported Ethernet Standards

Table 63: Supported Ethernet Standards

Standard	Description
802.3	10base-T
802.3u	100base-T
802.3ab	1000base-T
802.3z	1000base-X
802.3ac	Ethernet VLANs
802.1Q	Virtual LAN (VLAN)
802.1p	Class of service
802.1ad	Provider bridges (QinQ)
802.3ad	Link aggregation
Auto MDI/MDIX for 1000baseT	
RFC 1349	IPv4 TOS
RFC 2474	IPv4 DSCP
RFC 2460	IPv6 Traffic Classes

8.2 MEF Certifications for Ethernet Services

Table 64: Supported MEF Specifications

Specification	Description
MEF-2	Requirements and Framework for Ethernet Service Protection
MEF-6.1	Metro Ethernet Services Definitions Phase 2
MEF-8	Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks
MEF-10.3	Ethernet Services Attributes Phase 3
MEF 22.1	Mobile Backhaul Implementation Agreement Phase 2
MEF-30.1	Service OAM Fault Management Implementation Agreement Phase 2
MEF-35	Service OAM Performance Monitoring Implementation Agreement

Table 65: MEF Certifications

Certification	Description
CE 2.0	Second generation Carrier Ethernet certification
MEF-18	Abstract Test Suite for Circuit Emulation Services
MEF-9	Abstract Test Suite for Ethernet Services at the UNI. Certified for all service types (EPL, EVPL & E-LAN). This is a 1st generation certification. It is fully covered as part of CE2.0)
MEF-14	Abstract Test Suite for Traffic Management Phase 1. Certified for all service types (EPL, EVPL & E-LAN). This is a first generation certification. It is fully covered as part of CE2.0)

8.3 Supported TDM Pseudowire Encapsulations

Certification	Description	Availability
VLAN (MEF-8)	Circuit Emulation Services over native Ethernet frames	Available.
IP/UDP (IETF)	Layer 3 encapsulation over Ethernet	Planned for future release.
MPLS (MFA8)	MPLS encapsulation over Ethernet	Planned for future release.

8.4 Standards Compliance

Specification	Standard
Radio	EN 302 217-2-2
EMC	EN 301 489-4 EN 301 489-1 FCC 47 CFR, part 15, class B
Safety	EN 60950-1 IEC 60950-1 UL 60950-1 CSA-C22.2 No.60950-1 EN 60950-22 UL 60950-22 CSA C22.2.60950-22
Ingress Protection (RFUs)	RFU-D: IP67 RFU-D-HP: IP67 RFU-E: IP67 RFU-S: IP67
Operation	Class 3.1
Storage	Class 1.2
Transportation	Class 2.3

8.5 Network Management, Diagnostics, Status, and Alarms

Network Management System	**NetMaster/PolyView**
NMS Interface protocol	SNMPv1/v2c/v3 XML over HTTP/HTTPS toward the NMS
Element Management	Web based EMS, CLI
Management Channels & Protocols	HTTP/HTTPS Telnet/SSH-2 FTP/SFTP
Authentication, Authorization & Accounting	User access control X-509 Certificate
Management Interface	Dedicated Ethernet interfaces or in-band in traffic ports
In-Band Management	Support dedicated VLAN for management
TMN	The NMS functions are in accordance with ITU-T recommendations for TMN
RSL Indication	Power reading (dBm) available at RFU[41], and NMS
Performance Monitoring	Integral with onboard memory per ITU-T G.826/G.828

[41] Note that the voltage measured at the BNC port is not accurate and should be used only as an aid.

9. Specifications

This chapter includes:

- General Radio Specifications
- Radio Scripts
- Radio Capacity Specifications
- Transmit Power Specifications (dBm)
- Receiver Threshold Specifications
- Frequency Bands
- Ethernet Latency Specifications
- Mediation Device and Branching Network Losses
- Ethernet Specifications
- TDM Specifications
- Mechanical Specifications
- Environmental Specifications
- Supported Antenna Types
- Power Input Specifications
- Power Consumption Specifications
- IDU-RFU Cable Connection

Related Topics:

- Standards and Certifications

Note: All specifications are subject to change without prior notification.

9.1 General Radio Specifications

9.1.1 General Radio Specifications for Microwave RFUs

Note: The 4-5.8 GHz bands are only relevant for RFU-D-HP. Bands above 11 GHz are not relevant for RFU-D-HP.

Table 66: Radio Frequencies – Microwave RFUs

Frequency (GHz)	Operating Frequency Range (GHz)	Tx/Rx Spacing (MHz)
4	3.4-4.2	213, 266, 320
5	4.4-5.0	100, 300, 312
5.8	5.725-5.875	65, 75
6L,6H	5.85-6.45, 6.4-7.125	252.04, 240, 266, 300, 340, 160, 170, 500
7,8	7.1-7.9, 7.7-8.5	154, 119, 161, 168, 182, 196, 208, 245, 250, 266, 300,310, 311.312, 500, 530
10	10.0-10.7	91, 168,350, 550
11	10.7-11.7	490, 520, 530
13	12.75-13.3	266
15	14.4-15.35	315, 420, 475, 644, 490, 728
18	17.7-19.7	1010, 1120, 1008, 1560
23	21.2-23.65	1008, 1200, 1232
24UL	24.0-24.25	Customer-defined
26	24.2-26.5	800, 1008
28	27.35-29.5	350, 450, 490, 1008
32	31.8-33.4	812
36	36.0-37.0	700
38	37-40	1000, 1260, 700
42	40.55-43.45	1500

Table 67: General Radio Specifications – Microwave RFUs

Standards	FCC, ITU-R, CEPT
Frequency Stability	+0.001%
Frequency Source	Synthesizer
RF Channel Selection	Via EMS/NMS
Tx Range (Manual/ATPC)	The dynamic TX range with ATPC is the same as the manual TX range, and depends on the RFU type, the frequency, and the ACM profile. The maximum TX power with ATPC is no higher than the maximum manually configured TX power.

9.1.2 General Radio Specifications for E-Band

Table 68: Radio Frequencies and General Radio Specifications – RFU-E

Specification	Description
Standards	ETSI, ITU-R, CEPT
Operating mode	FDD
Operating Frequency Range	71-76GHz, 81-86GHz
Channel Spacing	62.5 MHz, 125 MHz, 250 MHz, 500 MHz
Frequency Stability	+0.001%

Table 69: Frequency Tuning Range for RFU-E

Low Range [MHz]	High Range [MHz]	TX-RX Separation [MHz]	Low BW [MHz]	High BW [MHz]
71,000 - 76000	81,000 – 86,000	10,000	5000	5000

9.2 Radio Scripts

Note: Although in some cases it may be possible to configure higher profiles, the maximum supported profiles are those listed in the tables below.

9.2.1 MRMC Scripts Supported with RFU-D, RFU-D-HP, and RFU-S

Note: XPIC is only supported with RFU-D and RFU-D-HP.

Table 70: MRMC Scripts for RFU-D, RFU-D-HP, and RFU-S

Script ID	Channel BW	Occupied BW	XPIC (CCDP)	Max Profile (ACM)	Max Profile (Fixed)
4521	20	18.5	Yes	10 (1024 QAM Light FEC))	9 (1024 QAM Strong FEC)
4525	25	23.4	Yes	12 (4096 QAM)	11 (2048 QAM)
4505	30	28	Yes	12	11
4507	40	37.4	Yes	12	11
4517	40	33.5	Yes	12	11
4510	50	47.2	Yes	12	11
4506	60	55.7	Yes	12	11
4501	80	74	Yes	11	10

9.2.2 MRMC Scripts Supported with RFU-E

Table 71: MRMC Scripts for RFU-E

Script ID	Channel BW	Occupied BW	Maximum Profile (ACM)	Maximum Profile (Fixed)
4701	62.5 MHz	57 MHz	9 (1024 QAM)	7 (256 QAM)
4700	125 MHz	115 MHz	8 (512 QAM)	7 (256 QAM)
4702	250 MHz	230 MHz	7 (256 QAM)	6 (128 QAM)
4704	500 MHz	460 MHz	5 (64 QAM)	ACM mode only

9.3 Radio Capacity Specifications

Each table in this section includes ranges of capacity specifications according to frame size, with ranges given for no Header De-Duplication, Layer-2 Header De-Duplication, and LTE-optimized Header De-Duplication. Actual values may differ from these ranges by up to 3 Mbps.

Notes:
- Ethernet capacity depends on average frame size.
- For LTE-Optimized Header De-Duplication, the capacity figures are for LTE packets encapsulated inside GTP tunnels with IPv4/UDP encapsulation and double VLAN tagging (QinQ). Capacity for IPv6 encapsulation is higher.

9.3.1 Radio Capacity Specifications – Microwave RFUs

9.3.1.1 20 MHz – Script ID 4521

Table 72: Radio Capacity for 20 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	10	8	13-16	13-20	14-52
1	QPSK	50	16	28-34	28-41	29-108
2	8 QAM	50	24	42-51	42-62	44-163
3	16 QAM	50	33	57-70	57-84	60-223
4	32 QAM	100	44	75-92	76-111	79-294
5	64 QAM	100	54	92-113	93-137	97-362
6	128 QAM	100	65	112-136	112-165	117-437
7	256 QAM	150	74	126-155	127-187	133-495
8	512 QAM	150	81	138-169	139-205	145-541
9	1024 QAM (Strong FEC)	150	86	147-180	148-218	154-576
10	1024 QAM (Light FEC)	150	91	156-191	157-231	164-611

9.3.1.2 25 MHz – Script ID 4525

Table 73: Radio Capacity for 25 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	10	17-21	17-25	18-67
1	QPSK	50	21	35-43	36-52	37-139
2	8 QAM	50	31	53-65	53-79	56-207
3	16 QAM	100	42	72-88	73-107	76-283
4	32 QAM	100	56	95-117	96-141	100-374
5	64 QAM	100	68	117-143	118-174	123-459
6	128 QAM	150	82	141-173	142-210	149-554
7	256 QAM	150	94	161-197	162-239	169-631
8	512 QAM	200	104	178-217	179-264	187-697
9	1024 QAM (Strong FEC)	200	110	189-231	190-280	199-740
10	1024 QAM (Light FEC)	200	117	201-245	202-297	211-786
11	2048 QAM	225	125	215-263	217-319	226-843
12	4096 QAM	225	136	233-285	235-345	245-913

9.3.1.3 30 MHz – Script ID 4505

Table 74: Radio Capacity for 30 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	12	21-25	21-31	22-81
1	QPSK	50	25	43-52	43-63	45-167
2	8 QAM	50	36	62-76	63-92	65-243
3	16 QAM	100	51	87-107	88-129	92-342
4	32 QAM	100	67	115-140	116-170	121-450
5	64 QAM	150	83	141-173	143-210	149-554
6	128 QAM	150	99	170-208	172-252	179-667
7	256 QAM	200	114	196-239	197-290	206-767
8	512 QAM	200	122	209-255	210-309	219-818
9	1024 QAM (Strong FEC)	225	133	228-278	229-337	239-892
10	1024 QAM (Light FEC)	225	141	241-295	243-357	253-945
11	2048 QAM	250	153	263-321	265-390	276-1031
12	4096 QAM	300	163	280-342	282-415	294-1097

9.3.1.4 40 MHz – Script ID 4507

Table 75: Radio Capacity for 40 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	17	28-35	29-42	30-111
1	QPSK	50	34	58-70	58-85	61-226
2	8 QAM	100	50	86-105	87-128	90-337
3	16 QAM	100	68	117-143	118-174	123-459
4	32 QAM	150	90	154-189	156-229	162-605
5	64 QAM	200	111	190-232	191-281	199-743
6	128 QAM	225	134	229-280	231-340	241-899
7	256 QAM	250	144	247-301	249-366	259-966
8	512 QAM	300	157	270-330	272-401	284-1059
9	1024 QAM (Strong FEC)	300	179	306-375	309-454	322-1201
10	1024 QAM (Light FEC)	300	190	325-398	328-482	342-1275
11	2048 QAM	350	205	352-430	355-522	370-1379
12	4096 QAM	400	215	369-451	372-547	388-1445

9.3.1.5 40 MHz – Script ID 4517

Table 76: Radio Capacity for 40 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	10	25-30	25-37	26-97
1	QPSK	50	21	50-62	51-75	53-198
2	8 QAM	100	32	75-92	76-112	79-296
3	16 QAM	100	43	103-126	104-152	108-403
4	32 QAM	150	57	135-166	136-201	142-531
5	64 QAM	150	70	166-203	168-247	175-652
6	128 QAM	200	85	201-246	203-298	211-789
7	256 QAM	225	92	217-265	218-321	228-849
8	512 QAM	250	106	250-305	252-370	262-978
9	1024 QAM (Strong FEC)	300	115	272-332	274-403	286-1065
10	1024 QAM (Light FEC)	300	122	288-353	291-428	303-1130
11	2048 QAM	300	132	313-382	315-463	328-1225
12	4096 QAM	350	141	333-407	335-493	350-1304

9.3.1.6 50 MHz – Script ID 4510

Table 77: Radio Capacity for 50 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	21	36-44	36-53	38-141
1	QPSK	100	41	70-86	71-104	74-275
2	8 QAM	100	64	109-133	110-162	115-427
3	16 QAM	150	86	148-181	149-219	155-580
4	32 QAM	200	108	186-227	187-276	195-728
5	64 QAM	225	140	240-293	242-356	252-940
6	128 QAM	300	163	280-342	282-415	294-1097
7	256 QAM	300	193	332-405	334-492	349-1300
8	512 QAM	350	210	360-440	363-534	378-1411
9	1024 QAM (Strong FEC)	400	228	392-479	395-581	412-1535
10	1024 QAM (Light FEC)	400	242	416-509	419-617	437-1631
11	2048 QAM	450	261	449-548	452-665	471-1758
12	4096 QAM	450	271	465-569	469-690	489-1823

9.3.1.7 60 MHz – Script ID 4506

Table 78: Radio Capacity for 60 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	25	43-52	43-63	45-168
1	QPSK	100	51	87-106	88-129	91-340
2	8 QAM	150	74	127-155	128-188	133-496
3	16 QAM	200	103	176-215	177-261	185-689
4	32 QAM	225	135	232-283	233-343	243-907
5	64 QAM	300	166	284-348	287-422	299-1114
6	128 QAM	350	200	344-420	346-510	361-1347
7	256 QAM	400	231	397-485	400-588	417-1554
8	512 QAM	450	248	426-521	430-632	448-1671
9	1024 QAM (Strong FEC)	450	270	464-567	467-688	487-1817
10	1024 QAM (Light FEC)	500	287	493-602	497-731	518-1931
11	2048 QAM	500	311	534-653	538-792	561-2000
12	4096 QAM	500	320	549-672	554-815	577-2000

9.3.1.8 80 MHz – Script ID 4501

Table 79: Radio Capacity for 80 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	24	57-69	57-84	59-222
1	QPSK	100	48	114-140	115-170	120-448
2	8 QAM	150	69	162-198	164-241	171-636
3	16 QAM	225	98	231-283	233-343	243-906
4	32 QAM	300	128	304-371	306-450	319-1190
5	64 QAM	400	157	371-454	374-551	390-1456
6	128 QAM	450	186	439-536	442-651	461-1720
7	256 QAM	500	214	505-618	509-749	531-1980
8	512 QAM	500	235	555-679	560-823	583-2000
9	1024 QAM (Strong FEC)	650	255	604-738	609-895	635-2000
10	1024 QAM (Light FEC)	650	271	641-784	646-951	674-2000
11	2048 QAM	650	287	679-829	684-1006	713-2000

9.3.2 Radio Capacity Specifications – RFU-E

9.3.2.1 62.5 MHz

Table 80: Radio Capacity for 62.5 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	50	19	42-51	42-62	44-160
1	QPSK	100	42	93-114	94-138	98-355
2	8 QAM	150	63	139-170	140-205	146-528
3	16 QAM	200	85	188-230	190-278	198-716
4	32 QAM	250	112	247-302	249-365	259-939
5	64 QAM	300	137	301-368	303-445	316-1145
6	128 QAM	350	165	362-442	365-535	380-1377
7	256 QAM	400	187	412-504	416-609	433-1569
8	512 QAM	450	206	453-554	457-670	476-1724
9	1024 QAM	500	230	505-617	508-746	530-1920

9.3.2.2 125 MHz

Table 81: Radio Capacity for 125 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	100	41	90-110	90-132	94-341
1	QPSK	200	85	188-230	189-278	197-715
2	8 QAM	300	127	279-341	281-412	293-1062
3	16 QAM	400	172	379-463	382-560	398-1443
4	32 QAM	500	227	499-610	502-737	524-1898
5	64 QAM	650	278	612-748	617-904	643-2329
6	128 QAM	1000	335	737-900	742-1089	774-2500
7	256 QAM	1000	381	838-1025	845-1239	880-2500
8	512 QAM	1000	420	923-1128	930-1364	969-2500

9.3.2.3 250 MHz

Table 82: Radio Capacity

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	200	82	180-221	182-267	189-687
1	QPSK	400	171	377-461	380-557	396-1435
2	8 QAM	500	254	559-683	563-826	587-2128
3	16 QAM	1000	345	759-928	765-1122	797-2500
4	32 QAM	1000	454	998-1220	1006-1475	1048-2500
5	64 QAM	1600	512	1225-1497	1234-1810	1286-2500
6	128 QAM	1600	512	1474-1802	1486-2179	1548-2500
7	256 QAM	1600	512	1653-2021	1666-2443	1736-2500

9.3.2.4 500 MHz

Table 83: Radio Capacity for 500 MHz

Profile	Modulation	Minimum required capacity activation key	Max # of supported DS1s	Ethernet throughput		
				No Header De-Duplication	L2 Header De-Duplication	LTE-Optimized Header De-Duplication
0	BPSK	350	165	362-442	NA	NA
1	QPSK	1000	343	755-923	NA	NA
2	8 QAM	1600	509	1119-1368	NA	NA
3	16 QAM	1600	512	1520-1858	NA	NA
4	32 QAM	2000	512	1998-2442	NA	NA
5	64 QAM	2500	512	2451-2500	NA	NA

9.4 Transmit Power Specifications (dBm)

9.4.1 Transmit Power with RFU-D

Notes:	The values listed in this section are typical. Actual values may differ in either direction by up to 1 dB. Transmit Power for RFU-D is measured at the Antenna Port of the RFU (Port C').

Table 84: Transmit power specifications for RFU-D (dBm)

Modulation	6 GHz	7 GHz	8 GHz	11 GHz	13 GHz	15 GHz	18 GHz	23 GHz	24GHz UL[42]	26 GHz	28- 32 GHz	38 GHz
BPSK	28	28	28	29	27	24	22	25	0	21	18	19
QPSK	28	28	28	29	27	24	22	25	0	21	18	19
8 PSK	28	28	28	29	27	24	22	25	0	21	18	18
16 QAM	28	27	27	29	26	24	22	25	0	20	17	18
32 QAM	27	27	26	29	25	24	22	24	0	19	16	17
64 QAM	27	26	26	27	24	24	22	22	0	19	16	17
128 QAM	27	26	26	26	23	24	22	21	0	19	16	17
256 QAM	27	26	26	25	22	22	20	18	0	17	14	16
512 QAM	25	25	24	25	22	22	20	18	0	17	14	14
1024 QAM	25	24	24	24	20	20	20	17	0	16	13	12
2048 QAM	23	23	22	23	19	20	18	16	0	15	12	10
4096 QAM	21	21	20	21	17	18	16					

9.4.1.1 Pmin Power with RFU-D

Table 85: Pmin Power for RFU-D

Frequency Band	Pmin	Frequency Band	Pmin
6-15 GHz	2	24 GHz FCC	-20
18-24 GHz	-1	26-42 GHz	-1

[42] For 1ft ant or lower.
Under FCC rules, the transmit power at the antenna port should be limited to 0 dBm.

9.4.2 Transmit Power with RFU-D-HP

Notes:

The values listed in this section are typical. Actual values may differ in either direction by up to 1 dB.

The Tx Power of the RFU-D-HP is measured at the transmitter port (Port A') of the RFU-D-HP.

The Tx Power of the RFU-D-HP is measured at the transmitter port (Port A') of the RFU-D-HP. To determine the Transmit Power at the antenna port of the radio and branching system (Port C'), diplexer losses, branching losses, and mediation devices losses must also be considered. See *Diplexer Unit Typical Losses with RFU-D-HP* on page 279, *RFU-D and RFU-D-HP Mediation Device Losses* on page 311, and *RFU-D-HP Branching Losses* on page 313.

Table 86: Transmit power specifications for RFU-D-HP (dBm)

Modulation	4-5 GHz	6 GHz	7 GHz	8 GHz	11 GHz
BPSK	35	38	38	37	36
QPSK	35	37	37	37	36
8 PSK	35	37	37	37	36
16 QAM	35	37	37	37	35
32 QAM	35	37	37	37	35
64 QAM	35	36	36	35	34
128 QAM	32	36	35	35	33
256 QAM	32	35	34	33	32
512 QAM	31	34	33	33	32
1024 QAM	30	33	32	32	31
2048 QAM	30	33	31	31	31
4096 QAM	30	31	29	29	29

The Pmin for RFU-D-HP is 15 dBm.

9.4.2.1 Diplexer Unit Typical Losses with RFU-D-HP

Table 87: Diplexer Unit Typical Losses with RFU-D-HP

Frequency	4-5 GHz	6-8 GHz	10 GHz	11 GHz
Losses	2 dB	1.3 dB	1.0 dB	0.7 dB

9.4.3 Transmit Power with RFU-S

Notes:	The values listed in this section are typical. Actual values may differ in either direction by up to 1 dB. Transmit Power for RFU-S is measured at the Antenna Port of the RFU (Port C').

Table 88: Transmit Power Specifications for RFU-S (dBm)

Modulation	6 GHz	7 GHz	8 GHz	11 GHz	13 GHz	15 GHz	18 GHz	23 GHz	24GHz UL[43]	26 GHz	28- 38 GHz
BPSK	28	28	28	28	27	24	22	25	0	21	18
QPSK	28	28	28	28	27	24	22	25	0	21	18
8 PSK	28	28	28	28	27	24	22	25	0	21	18
16 QAM	28	27	27	28	26	24	22	25	0	20	17
32 QAM	27	26	26	28	25	24	22	24	0	19	16
64 QAM	27	26	26	27	24	23	21	22	0	19	16
128 QAM	27	26	26	27	23	23	21	21	0	19	16
256 QAM	27	26	24	27	22	22	20	18	0	17	14
512 QAM	25	24	24	27	22	22	19	18	0	17	14
1024 QAM	25	24	24	25	20	20	18	17	0	16	13
2048 QAM	23	22	22	24	19	20	17	16	0	15	12
4096 QAM	21	20	20	22	17	18	15				

9.4.3.1 Pmin Power with RFU-S

Table 89: Pmin Power for RFU-S

Frequency Band	Pmin	Frequency Band	Pmin
6-15 GHz	2	24 GHz FCC	-20
18-24 GHz	-1	26-42 GHz	-1

[43] For 1ft ant or lower.
Under FCC rules, the transmit power at the antenna port should be limited to 0 dBm.

9.4.4 Transmit Power with RFU-E

Note: The values listed in this section are typical. Actual values may differ in either direction by up to 3 dB.

Table 90: Transmit power specifications for RFU-E (dBm)

Modulation	62.5 MHz	125 MHz	250 MHz	500 MHz
BPSK	18	18	18	15
QPSK	18	18	18	15
8 PSK	18	18	16	11
16 QAM	17	17	15	10
32 QAM	17	17	15	10
64 QAM	16	16	14	9
128 QAM	16	16	14	–
256 QAM	15	15	13	–
512 QAM	14	14	–	–
1024 QAM	13	–	–	–

The Pmin for RFU-E is -2 dBm.

9.5 Receiver Threshold Specifications

Note: The values listed in this section are typical. Actual values may differ in either direction by up to 1dB.

9.5.1 Receiver Thresholds with RFU-D and RFU-S

Note: RSL values for RFU-D and RFU-S are measured at the Antenna Port of the RFU (Port C').

Table 91: Receiver Thresholds with RFU-D and RFU-S (6-18 GHz)

Profile	Modulation	Channel Spacing	6	7-8	10	11	13	15	18
0	BPSK	20 MHz	-91.5	-91.5	-91.0	-92.0	-91.0	-90.0	-91.5
1	QPSK		-88.5	-88.5	-88.5	-89.5	-88.0	-87.5	-88.5
2	8 PSK		-83.5	-83.5	-83.0	-84.0	-83.0	-82.0	-83.5
3	16 QAM		-82.0	-82.0	-81.5	-82.5	-81.5	-80.5	-82.0
4	32 QAM		-78.0	-78.0	-78.0	-79.0	-77.5	-77.0	-78.0
5	64 QAM		-75.5	-75.5	-75.0	-76.0	-75.0	-74.0	-75.5
6	128 QAM		-72.5	-72.5	-72.0	-73.0	-71.5	-71.0	-72.5
7	256 QAM		-69.0	-69.0	-69.0	-70.0	-68.5	-68.0	-69.0
8	512 QAM		-67.0	-67.0	-66.5	-67.5	-66.0	-65.5	-67.0
9	1024 QAM (Strong FEC)		-64.0	-64.0	-64.0	-65.0	-63.5	-63.0	-64.0
10	1024 QAM (Light FEC)		-63.0	-63.0	-63.0	-64.0	-62.5	-62.0	-63.0
0	BPSK	25 MHz	-88.5	-87.5	-87.5	-88.0	-87.0	-86.5	-87.5
1	QPSK		-87.5	-86.5	-86.5	-87	-86.0	-85.5	-86.5
2	8 PSK		-82.5	-82.0	-81.5	-82.5	-81.5	-80.5	-82.0
3	16 QAM		-80.5	-80.0	-79.5	-80.5	-79.5	-78.5	-80.0
4	32 QAM		-77.5	-77.0	-76.5	-77.5	-76.0	-75.5	-77.0
5	64 QAM		-74.5	-74.0	-73.5	-74.5	-73.5	-72.5	-74.0
6	128 QAM		-71.5	-71.0	-70.5	-71.5	-70.5	-69.5	-71.0
7	256 QAM		-68.5	-67.5	-67.5	-68.5	-67.0	-66.5	-67.5
8	512 QAM		-66.0	-65.0	-65.0	-66.0	-64.5	-64.0	-65.0
9	1024 QAM (Strong FEC)		-63.0	-62.5	-62.0	-63.0	-61.5	-61.0	-62.5
10	1024 QAM (Light FEC)		-62.5	-61.5	-61.5	-62.5	-61.0	-60.5	-61.5
11	2048 QAM		-58.5	-58.0	-57.5	-58.5	-57.0	-56.5	-58.0
12	4096 QAM		-55.5	-55.0	-54.5	-55.5	-54.0	-53.5	-55.0

Profile	Modulation	Channel Spacing	6	7-8	10	11	13	15	18
0	BPSK	30 MHz	-88.5	-88.0	-87.5	-88.5	-87.0	-86.5	-88.0
1	QPSK		-87.5	-87.0	-86.5	-87.5	-86.0	-85.5	-87.0
2	8 PSK		-82.5	-81.5	-81.5	-82.5	-81.0	-80.5	-81.5
3	16 QAM		-81.0	-80.0	-80.0	-80.5	-79.5	-79.0	-80.0
4	32 QAM		-77.0	-76.5	-76.0	-77.0	-76.0	-75.0	-76.5
5	64 QAM		-74.5	-73.5	-73.5	-74.0	-73.0	-72.5	-73.5
6	128 QAM		-71.0	-70.5	-70.0	-71.0	-70.0	-69.0	-70.5
7	256 QAM		-68.0	-67.5	-67.0	-68.0	-67.0	-66.0	-67.5
8	512 QAM		-66.0	-65.5	-65.0	-66.0	-64.5	-64.0	-65.5
9	1024 QAM (Strong FEC)		-63.0	-62.0	-62.0	-62.5	-61.5	-61.0	-62.0
10	1024 QAM (Light FEC)		-62.0	-61.0	-61.0	-62.0	-60.5	-60.0	-61.0
11	2048 QAM		-58.0	-57.5	-57.0	-58.0	-56.5	-56.0	-57.5
12	4096 QAM		-55.0	-54.5	-54.0	-55.0	-53.5	-53.0	-54.5
0	BPSK	40 MHz	-87.0	-86.5	-86.0	-87.0	-86.0	-85.0	-86.5
1	QPSK		-86.0	-85.5	-85.0	-86.0	-85.0	-84.0	-85.5
2	8 PSK		-81.0	-80.5	-80.0	-81.0	-79.5	-79.0	-80.5
3	16 QAM		-79.5	-79.0	-78.5	-79.5	-78.0	-77.5	-79.0
4	32 QAM		-76.0	-75.0	-75.0	-75.5	-74.5	-74.0	-75.0
5	64 QAM		-73.0	-72.0	-72.0	-73.0	-71.5	-71.0	-72.0
6	128 QAM		-70.0	-69.0	-69.0	-70.0	-68.5	-68.0	-69.0
7	256 QAM		-67.0	-66.0	-66.0	-66.5	-65.5	-65.0	-66.0
8	512 QAM		-64.0	-63.5	-63.0	-64.0	-62.5	-62.0	-63.5
9	1024 QAM (Strong FEC)		-61.5	-61.0	-60.5	-61.5	-60.0	-59.5	-61.0
10	1024 QAM (Light FEC)		-60.5	-60.0	-59.5	-60.5	-59.5	-58.5	-60.0
11	2048 QAM		-58.0	-57.0	-57.0	-58.0	-56.5	-56.0	-57.0
12	4096 QAM		-55.0	-54.0	-54.0	-55.0	-53.5	-53.0	-54.0

Profile	Modulation	Channel Spacing	6	7-8	10	11	13	15	18
0	BPSK	50 MHz	-86.5	-85.5	-85.5	-86.0	-85.0	-84.5	-85.5
1	QPSK		-85.5	-84.5	-84.5	-85.0	-84.0	-83.5	-84.5
2	8 PSK		-80.0	-79.5	-79.0	-80.0	-79.0	-78.0	-79.5
3	16 QAM		-78.5	-77.5	-77.5	-78.0	-77.0	-76.5	-77.5
4	32 QAM		-74.5	-74.0	-73.5	-74.5	-73.5	-72.5	-74.0
5	64 QAM		-71.5	-70.5	-70.5	-71.5	-70.0	-69.5	-70.5
6	128 QAM		-68.5	-68.0	-67.5	-68.5	-67.5	-66.5	-68.0
7	256 QAM		-66.0	-65.0	-65.0	-66.0	-64.5	-64.0	-65.0
8	512 QAM		-63.5	-63.0	-62.5	-63.5	-62.0	-61.5	-63.0
9	1024 QAM (Strong FEC)		-60.0	-59.5	-59.0	-60.0	-58.5	-58	-59.5
10	1024 QAM (Light FEC)		-59.0	-58.0	-58.0	-59.0	-57.5	-57.0	-58.0
11	2048 QAM		-57.0	-56.0	-56.0	-56.5	-55.5	-55.0	-56.0
12	4096 QAM		-54.0	-53.0	-53.0	-53.5	-52.5	-52.0	-53.0
0	BPSK	60 MHz	-86.0	-85.0	-84.5	-85.5	-84.0	-83.5	-85.0
1	QPSK		-85.0	-84.0	-83.5	-84.5	-83.0	-82.5	-84.0
2	8 PSK		-80.5	-79.0	-79.0	-79.5	-78.5	-78.0	-79.0
3	16 QAM		-78.0	-77.0	-76.5	-77.5	-76.0	-75.5	-77.0
4	32 QAM		-74.5	-73.0	-73.0	-73.5	-72.5	-72.0	-73.0
5	64 QAM		-71.5	-70.0	-69.5	-70.5	-69.5	-68.5	-70.0
6	128 QAM		-69.0	-67.0	-67.0	-67.5	-66.5	-66.0	-67.0
7	256 QAM		-65.5	-64.0	-63.5	-64.5	-63.5	-62.5	-64.0
8	512 QAM		-63.5	-62.0	-61.5	-62.5	-61.5	-60.5	-62.0
9	1024 QAM (Strong FEC)		-60.0	-58.5	-58.0	-59.0	-58.0	-57.0	-58.5
10	1024 QAM (Light FEC)		-59.0	-57.5	-57.0	-58.0	-57.0	-56.0	-57.5
11	2048 QAM		-56.5	-54.5	-54.5	-55.0	-54.0	-53.5	-54.5
12	4096 QAM		-53.5	-51.5	-51.5	-52.0	-51.0	-50.5	-51.5

Profile	Modulation	Channel Spacing	6	7-8	10	11	13	15	18
0	BPSK	80 MHz	-85.0	-85.0	-84.5	-85.5	-84.5	-83.5	-85.0
1	QPSK		-82.5	-82.5	-82.5	-83.0	-82.0	-81.5	-82.5
2	8 PSK		-79.0	-79.0	-78.5	-79.5	-78.5	-77.5	-79.0
3	16 QAM		-76.0	-76.0	-75.5	-76.5	-75.0	-74.5	-76.0
4	32 QAM		-72.5	-72.5	-72.0	-73.0	-71.5	-71.0	-72.5
5	64 QAM		-69.0	-69.0	-69.0	-70.0	-68.5	-68.0	-69.0
6	128 QAM		-66.5	-66.5	-66.0	-67.0	-66.0	-65.0	-66.5
7	256 QAM		-63.5	-63.5	-63.0	-64.0	-63.0	-62.0	-63.5
8	512 QAM		-61.0	-61.0	-61.0	-62.0	-60.5	-60.0	-61.0
9	1024 QAM (Strong FEC)		-58.0	-58.0	-57.5	-58.5	-57.5	-56.5	-58.0
10	1024 QAM (Light FEC)		-57.0	-57.0	-57.0	-58.0	-56.5	-56.0	-57.0
11	2048 QAM		-54.5	-54.5	-54.5	-55.5	-54.0	-53.5	-54.5

Table 92: Receiver Thresholds with RFU-D and RFU-S (23-42 GHz)

Profile	Modulation	Channel Spacing	23	24[44]	26	28-31	32	38
0	BPSK	20 MHz	-90.5	-87.0	-90.0	-90.0	-89.5	-89.0
1	QPSK		-88.0	-84.0	-87.5	-87.0	-87.0	-86.5
2	8 PSK		-82.5	-79.0	-82.0	-82.0	-81.5	-81.0
3	16 QAM		-81.0	-77.5	-80.5	-80.5	-80.0	-79.5
4	32 QAM		-77.5	-73.5	-77.0	-76.5	-76.5	-76.0
5	64 QAM		-74.5	-71.0	-74.0	-74.0	-73.5	-73.0
6	128 QAM		-71.5	-68.0	-71.0	-71.0	-70.5	-70.0
7	256 QAM		-68.5	-64.5	-68.0	-67.5	-67.5	-67.0
8	512 QAM		-66.0	-62.5	-65.5	-65.5	-65.0	-64.5
9	1024 QAM (Strong FEC)		-63.5	-59.5	-63.0	-62.5	-62.5	-62.0
10	1024 QAM (Light FEC)		-62.5	-58.5	-62.0	-61.5	-61.5	-61.0
0	BPSK	25 MHz	-86.5	-83.0	-86.5	-86.0	-86.0	-85.0
1	QPSK		-85.5	-82.0	-85.5	-85.0	-85.0	-84.0
2	8 PSK		-81.0	-77.5	-80.5	-80.5	-80.0	-79.5
3	16 QAM		-79.0	-75.5	-78.5	-78.5	-78.0	-77.5
4	32 QAM		-76.0	-72.5	-75.5	-75.5	-75.0	-74.5
5	64 QAM		-73.0	-69.5	-72.5	-72.5	-72.0	-71.5
6	128 QAM		-70.0	-66.5	-69.5	-69.5	-69.0	-68.5
7	256 QAM		-67.0	-63.0	-66.5	-66.0	-66.0	-65.5
8	512 QAM		-64.5	-60.5	-64.0	-63.5	-63.5	-63.0
9	1024 QAM (Strong FEC)		-61.5	-58.0	-61.0	-61.0	-60.5	-60.0
10	1024 QAM (Light FEC)		-61.0	-57.0	-60.5	-60.0	-60.0	-59.5
11	2048 QAM		-57.0	-53.5	-56.5	-56.5	-56.0	-55.5

[44] Customers in countries following EC Directive 2006/771/EC (incl. amendments) must observe the 100mW EIRP obligation by adjusting transmit power according to antenna gain and RF line losses.

Profile	Modulation	Channel Spacing	23	24[44]	26	28-31	32	38
0	BPSK	30 MHz	-87.0	-83.5	-86.5	-86.5	-86.5	-86.0
1	QPSK		-86.0	-82.5	-85.5	-85.5	-85.5	-85.0
2	8 PSK		-81.0	-77.0	-80.5	-80.0	-80.0	-79.5
3	16 QAM		-79.0	-75.5	-79.0	-78.5	-78.5	-78.0
4	32 QAM		-75.5	-72.0	-75.0	-75.0	-75.0	-74.5
5	64 QAM		-72.5	-69.0	-72.5	-72.0	-72.0	-71.5
6	128 QAM		-69.5	-66.0	-69.0	-69.0	-69.0	-68.5
7	256 QAM		-66.5	-63.0	-66.0	-66.0	-66.0	-65.5
8	512 QAM		-64.5	-61.0	-64.0	-64.0	-64.0	-63.5
9	1024 QAM (Strong FEC)		-61.0	-57.5	-61.0	-60.5	-60.5	-60.0
10	1024 QAM (Light FEC)		-60.5	-56.5	-60.0	-59.5	-59.5	-59.0
11	2048 QAM		-56.5	-53.0	-56.0	-56.0	-56.0	-55.5
0	BPSK	40 MHz	-85.5	-82.0	-85.0	-85.0	-85.0	-84.5
1	QPSK		-84.5	-81.0	-84.0	-84.0	-84.0	-83.5
2	8 PSK		-79.5	-76.0	-79.0	-79.0	-79.0	-78.5
3	16 QAM		-78.0	-74.5	-77.5	-77.5	-77.5	-77.0
4	32 QAM		-74.0	-70.5	-74.0	-73.5	-73.5	-73.0
5	64 QAM		-71.5	-67.5	-71.0	-70.5	-70.5	-70.0
6	128 QAM		-68.5	-64.5	-68.0	-67.5	-67.5	-67.0
7	256 QAM		-65.0	-61.5	-65.0	-64.5	-64.5	-64.0
8	512 QAM		-62.5	-59.0	-62.0	-62.0	-62.0	-61.5
9	1024 QAM (Strong FEC)		-60.0	-56.5	-59.5	-59.5	-59.5	-59.0
10	1024 QAM (Light FEC)		-59.0	-55.5	-58.5	-58.5	-58.5	-58.0
11	2048 QAM		-56.5	-52.5	-56.0	-55.5	-55.5	-55.0

Profile	Modulation	Channel Spacing	23	24[44]	26	28-31	32	38
0	BPSK	50 MHz	-84.5	-81.0	-84.5	-84.0	-84.0	-83.5
1	QPSK		-83.5	-80.0	-83.5	-83.0	-83.0	-82.5
2	8 PSK		-78.5	-75.0	-78.0	-78.0	-78.0	-77.5
3	16 QAM		-76.5	-73.0	-76.5	-76.0	-76.0	-75.5
4	32 QAM		-73.0	-69.5	-72.5	-72.5	-72.5	-72v
5	64 QAM		-70.0	-66.0	-69.5	-69.0	-69.0	-68.5
6	128 QAM		-67.0	-63.5	-66.5	-66.5	-66.5	-66.0
7	256 QAM		-64.5	-60.5	-64.0	-63.5	-63.5	-63.0
8	512 QAM		-62.0	-58.5	-61.5	-61.5	-61.5	-61.0
9	1024 QAM (Strong FEC)		-58.5	-55.0	-58.0	-58.0	-58.0	-57.5
10	1024 QAM (Light FEC)		-57.5	-53.5	-57.0	-56.5	-56.5	-56.0
11	2048 QAM		-55.0	-51.5	-55.0	-54.5	-54.5	-54.0
0	BPSK	60 MHz	-84.0	-83.5	-83.5	-83.5	-83.0	-82.5
1	QPSK		-83.0	-82.5	-82.5	-82.5	-82.0	-81.5
2	8 PSK		-78.0	-77.5	-78.0	-77.5	-77.5	-77.0
3	16 QAM		-76.0	-75.5	-75.5	-75.5	-75.0	-74.5
4	32 QAM		-72.0	-71.5	-72.0	-71.5	-71.5	-71.0
5	64 QAM		-69.0	-68.5	-68.5	-68.5	-68.0	-68.0
6	128 QAM		-66.0	-65.5	-66.0	-65.5	-65.5	-65.0
7	256 QAM		-63.0	-62.5	-62.5	-62.5	-62.0	-62.0
8	512 QAM		-61.0	-60.5	-60.5	-60.5	-60.0	-60.0
9	1024 QAM (Strong FEC)		-57.5	-57.0	-57.0	-57.0	-56.5	-56.5
10	1024 QAM (Light FEC)		-56.5	-56.0	-56.0	-56.0	-55.5	-55.5
11	2048 QAM		-53.5	-53.0	-53.5	-53.0	-53.0	-52.5

Profile	Modulation	Channel Spacing	23	24[44]	26	28-31	32	38
0	BPSK	80 MHz	-84.0	-83.5	-83.5	-83.5	-83.0	-83.5
1	QPSK		-81.5	-81.0	-81.5	-81.0	-81.0	-81.0
2	8 PSK		-78.0	-77.5	-77.5	-77.5	-77.0	-77.5
3	16 QAM		-75.0	-74.5	-74.5	-74.5	-74.0	-74.0
4	32 QAM		-71.5	-71.0	-71.0	-71.0	-70.5	-70.5
5	64 QAM		-68.5	-68.0	-68.0	-67.5	-67.5	-67.5
6	128 QAM		-65.5	-65.0	-65.0	-65.0	-64.5	-65.0
7	256 QAM		-62.5	-62.0	-62.0	-62.0	-61.5	-62.0
8	512 QAM		-60.5	-60.0	-60.0	-59.5	-59.5	-59.5
9	1024 QAM (Strong FEC)		-57.0	-56.5	-56.5	-56.5	-56.0	-56.5
10	1024 QAM (Light FEC)		-56.5	-56.0	-56.0	-55.5	-55.5	-55.5
11	2048 QAM		-54.0	-53.5	-53.5	-53.0	-53.0	

9.5.2 Receiver Thresholds with RFU-D-HP

Note: The RSL values shown in the tables below are at the radio port (Port A') of the RFU-D-HP. To determine the RSL at the antenna port of the radio and branching system (Port C'), diplexer losses, branching losses, and mediation devices losses must also be considered. See *Diplexer Unit Typical Losses with RFU-D-HP* on page 279, *RFU-D and RFU-D-HP Mediation Device Losses* on page 311, and *RFU-D-HP Branching Losses* on page 313.

Table 93: Receiver Thresholds with RFU-D-HP – 20 MHz to 40 MHz

	Channel Spacing	20 MHz			25 MHz			30 MHz			40 MHz		
Modulation	**Frequency (GHz)**	**4-6**	**7-8**	**11**	**4-6**	**7-8**	**11**	**4-6**	**7-8**	**11**	**4-6**	**7-8**	**11**
BPSK		-94.5	-92.5	-92.5	-88.5	-87.5	-88.0	-88.5	-88.0	-88.5	-86.5	-85.5	-86.0
QPSK		-92.0	-90.0	-90.0	-87.5	-86.5	-87.0	-87.5	-87.0	-87.5	-85.5	-84.5	-85.0
8 QAM		-86.5	-84.5	-84.5	-82.5	-82.0	-82.5	-82.5	-81.5	-82.5	-80.0	-79.5	-80.0
16 QAM		-85.0	-83.5	-83.5	-80.5	-80.0	-80.5	-81.0	-80.0	-80.5	-78.5	-77.5	-78.0
32 QAM		-81.5	-79.5	-79.5	-77.5	-77.0	-77.5	-77.0	-76.5	-77.0	-74.5	-74.0	-74.5
64 QAM		-78.5	-76.5	-76.5	-74.5	-74.0	-74.5	-74.5	-73.5	-74.0	-71.5	-70.5	-71.5
128 QAM		-75.5	-73.5	-73.5	-71.5	-71.0	-71.5	-71.0	-70.5	-71.0	-68.5	-68.0	-68.5
256 QAM		-72.5	-70.5	-70.5	-68.5	-67.5	-68.5	-68.0	-67.5	-68.0	-66.0	-65.0	-66.0
512 QAM		-70.0	-68.0	-68.0	-66.0	-65.0	-66.0	-66.0	-65.5	-66.0	-63.5	-63.0	-63.5
1024 QAM		-67.5	-65.5	-65.5	-63.0	-62.5	-63.0	-63.0	-62.0	-62.5	-60.0	-59.5	-60.0
2048 QAM					-58.5	-58.0	-58.5	-58.0	-57.5	-58.0	-57.0	-56.0	-56.5
4096 QAM					-55.5	-55.0	-55.5	-55.0	-54.5	-55.0	-54.0	-53.0	-53.5

Table 94: Receiver Thresholds with RFU-D-HP – 50 MHz to 80 MHz

	Channel Spacing	50 MHz			60 MHz			80 MHz		
Modulation	**Frequency (GHz)**	**4-6**	**7-8**	**11**	**4-6**	**7-8**	**11**	**4-6**	**7-8**	**11**
BPSK		-86.5	-85.5	-86.0	-85.5	-84.5	-85.0	-88.0	-86.0	-86.0
QPSK		-85.5	-84.5	-85.0	-84.5	-83.5	-84.0	-86.0	-84.0	-84.0
8 QAM		-80.0	-79.5	-80.0	-79.0	-78.5	-79.0	-82.0	-80.0	-80.0
16 QAM		-78.5	-77.5	-78.0	-77.5	-76.5	-77.0	-79.0	-77.0	-77.0
32 QAM		-74.5	-74.0	-74.5	-73.5	-73.0	-73.5	-75.5	-73.5	-73.5
64 QAM		-71.5	-70.5	-71.5	-70.5	-69.5	-70.5	-72.5	-70.5	-70.5
128 QAM		-68.5	-68.0	-68.5	-67.5	-67.0	-67.5	-69.5	-67.5	-67.5
256 QAM		-66.0	-65.0	-66.0	-65.0	-64.0	-65.0	-66.5	-64.5	-64.5
512 QAM		-63.5	-63.0	-63.5	-62.5	-62.0	-62.5	-64.5	-62.5	-62.5
1024 QAM		-60.0	-59.5	-60.0	-59.0	-58.5	-59.0	-61.0	-59.5	-59.5
2048 QAM		-57.0	-56.0	-56.5	-56.0	-55.0	-55.5	-58.0	-56.0	-56.0
4096 QAM		-54.0	-53.0	-53.5	-53.0	-52.0	-52.5			

9.5.3 Receiver Thresholds with RFU-E

Note: The values listed in this section are typical. Actual values may differ in either direction by up to 3dB.

Table 95: Receiver Thresholds with RFU-E

	Channel Spacing [MHz]			
Modulation	**62.5**	**125**	**250**	**500**
BPSK	-83.0	-80.0	-77.0	-74.0
4 QAM	-79.5	-76.5	-73.5	-70.5
8 QAM	-75.5	-72.5	-70.0	-67.0
16 QAM	-73.0	-69.5	-67.0	-64.0
32 QAM	-69.0	-66.0	-63.0	-60.0
64 QAM	-66.0	-63.0	-60.0	-57.0
128 QAM	-63.0	-60.0	-57.0	–
256 QAM	-59.5	-57.0	-54.0	–
512 QAM	-57.0	-54.0	–	–
1024 QAM	-54.0	–	–	–

9.6 Frequency Bands

This section outlines the supported tuning range of each RFU unit.

9.6.1 Frequency Bands – RFU-D, RFU-D-HP, and RFU-S

Table 96: Frequency Bands – RFU-D, RFU-D-HP, and RFU-S

Note: The 4-5.8 GHz bands are only relevant for RFU-D-HP. Bands above 11 GHz are not relevant for RFU-D-HP.

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
4 GHz	3810-3984	4023-4197	213
	3702.5-3926.5	3968.5-4192.5	266
	3600-3880	3920-4200	320

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
U4(5) GHz	4400.5-4653.5	4500.5-4753.5	100
	4395-4685 4400-4680 4410-4690	4695-4985 4700-4980 4710-4990	300
	4404-4684	4716-4996	312

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
5.8 GHz	5725-5785	5790-5850	65
	5725-5765	5810-5850	85

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
6L GHz	6332.5-6393	5972-6093	300A
	5972-6093	6332.5-6393	
	6191.5-6306.5	5925.5-6040.5	266A
	5925.5-6040.5	6191.5-6306.5	
	6303.5-6418.5	6037.5-6152.5	
	6037.5-6152.5	6303.5-6418.5	
	6245-6290.5	5939.5-6030.5	260A
	5939.5-6030.5	6245-6290.5	
	6365-6410.5	6059.5-6150.5	
	6059.5-6150.5	6365-6410.5	
	6226.89-6286.865	5914.875-6034.825	252B

	5914.875-6034.825	6226.89-6286.865	
	6345.49-6405.465	6033.475-6153.425	
	6033.475-6153.425	6345.49-6405.465	
	6181.74-6301.69	5929.7-6049.65	252A
	5929.7-6049.65	6181.74-6301.69	
	6241.04-6360.99	5989-6108.95	
	5989-6108.95	6241.04-6360.99	
	6300.34-6420.29	6048.3-6168.25	
	6048.3-6168.25	6300.34-6420.29	
	6235-6290.5	5939.5-6050.5	240A
	5939.5-6050.5	6235-6290.5	
	6355-6410.5	6059.5-6170.5	
	6059.5-6170.5	6355-6410.5	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
6H GHz	6924.5-7075.5	6424.5-6575.5	500
	6424.5-6575.5	6924.5-7075.5	
	7032.5-7091.5	6692.5-6751.5	340C
	6692.5-6751.5	7032.5-7091.5	
	6764.5-6915.5	6424.5-6575.5	340B
	6424.5-6575.5	6764.5-6915.5	
	6924.5-7075.5	6584.5-6735.5	
	6584.5-6735.5	6924.5-7075.5	
	6781-6939	6441-6599	340A
	6441-6599	6781-6939	
	6941-7099	6601-6759	
	6601-6759	6941-7099	
	6707.5-6772.5	6537.5-6612.5	160A
	6537.5-6612.5	6707.5-6772.5	
	6767.5-6832.5	6607.5-6672.5	
	6607.5-6672.5	6767.5-6832.5	
	6827.5-6872.5	6667.5-6712.5	
	6667.5-6712.5	6827.5-6872.5	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
7 GHz	7783.5-7898.5	7538.5-7653.5	
	7538.5-7653.5	7783.5-7898.5	
	7301.5-7388.5	7105.5-7192.5	196A
	7105.5-7192.5	7301.5-7388.5	
	7357.5-7444.5	7161.5-7248.5	
	7161.5-7248.5	7357.5-7444.5	
	7440.5-7499.5	7622.5-7681.5	
	7678.5-7737.5	7496.5-7555.5	
	7496.5-7555.5	7678.5-7737.5	
	7580.5-7639.5	7412.5-7471.5	168C
	7412.5-7471.5	7580.5-7639.5	
	7608.5-7667.5	7440.5-7499.5	
	7440.5-7499.5	7608.5-7667.5	
	7664.5-7723.5	7496.5-7555.5	
	7496.5-7555.5	7664.5-7723.5	
	7609.5-7668.5	7441.5-7500.5	168B
	7441.5-7500.5	7609.5-7668.5	
	7637.5-7696.5	7469.5-7528.5	
	7469.5-7528.5	7637.5-7696.5	
	7693.5-7752.5	7525.5-7584.5	
	7525.5-7584.5	7693.5-7752.5	
	7273.5-7332.5	7105.5-7164.5	168A
	7105.5-7164.5	7273.5-7332.5	
	7301.5-7360.5	7133.5-7192.5	
	7133.5-7192.5	7301.5-7360.5	
	7357.5-7416.5	7189.5-7248.5	
	7189.5-7248.5	7357.5-7416.5	
	7280.5-7339.5	7119.5-7178.5	161P
	7119.5-7178.5	7280.5-7339.5	
	7308.5-7367.5	7147.5-7206.5	
	7147.5-7206.5	7308.5-7367.5	
	7336.5-7395.5	7175.5-7234.5	
	7175.5-7234.5	7336.5-7395.5	

7364.5-7423.5	7203.5-7262.5	
7203.5-7262.5	7364.5-7423.5	
7597.5-7622.5	7436.5-7461.5	161O
7436.5-7461.5	7597.5-7622.5	
7681.5-7706.5	7520.5-7545.5	
7520.5-7545.5	7681.5-7706.5	
7587.5-7646.5	7426.5-7485.5	161M
7426.5-7485.5	7587.5-7646.5	
7615.5-7674.5	7454.5-7513.5	
7454.5-7513.5	7615.5-7674.5	
7643.5-7702.5	7482.5-7541.5	161K
7482.5-7541.5	7643.5-7702.5	
7671.5-7730.5	7510.5-7569.5	
7510.5-7569.5	7671.5-7730.5	
7580.5-7639.5	7419.5-7478.5	161J
7419.5-7478.5	7580.5-7639.5	
7608.5-7667.5	7447.5-7506.5	
7447.5-7506.5	7608.5-7667.5	
7664.5-7723.5	7503.5-7562.5	
7503.5-7562.5	7664.5-7723.5	
7580.5-7639.5	7419.5-7478.5	161I
7419.5-7478.5	7580.5-7639.5	
7608.5-7667.5	7447.5-7506.5	
7447.5-7506.5	7608.5-7667.5	
7664.5-7723.5	7503.5-7562.5	
7503.5-7562.5	7664.5-7723.5	
7273.5-7353.5	7112.5-7192.5	161F
7112.5-7192.5	7273.5-7353.5	
7322.5-7402.5	7161.5-7241.5	
7161.5-7241.5	7322.5-7402.5	
7573.5-7653.5	7412.5-7492.5	
7412.5-7492.5	7573.5-7653.5	
7622.5-7702.5	7461.5-7541.5	
7461.5-7541.5	7622.5-7702.5	

7709-7768	7548-7607	161D
7548-7607	7709-7768	
7737-7796	7576-7635	
7576-7635	7737-7796	
7765-7824	7604-7663	
7604-7663	7765-7824	
7793-7852	7632-7691	
7632-7691	7793-7852	
7584-7643	7423-7482	161C
7423-7482	7584-7643	
7612-7671	7451-7510	
7451-7510	7612-7671	
7640-7699	7479-7538	
7479-7538	7640-7699	
7668-7727	7507-7566	
7507-7566	7668-7727	
7409-7468	7248-7307	161B
7248-7307	7409-7468	
7437-7496	7276-7335	
7276-7335	7437-7496	
7465-7524	7304-7363	
7304-7363	7465-7524	
7493-7552	7332-7391	
7332-7391	7493-7552	
7284-7343	7123-7182	161A
7123-7182	7284-7343	
7312-7371	7151-7210	
7151-7210	7312-7371	
7340-7399	7179-7238	
7179-7238	7340-7399	
7368-7427	7207-7266	
7207-7266	7368-7427	
7280.5-7339.5	7126.5-7185.5	154C
7126.5-7185.5	7280.5-7339.5	

	7308.5-7367.5	7154.5-7213.5	
	7154.5-7213.5	7308.5-7367.5	
	7336.5-7395.5	7182.5-7241.5	
	7182.5-7241.5	7336.5-7395.5	
	7364.5-7423.5	7210.5-7269.5	
	7210.5-7269.5	7364.5-7423.5	
	7594.5-7653.5	7440.5-7499.5	154B
	7440.5-7499.5	7594.5-7653.5	
	7622.5-7681.5	7468.5-7527.5	
	7468.5-7527.5	7622.5-7681.5	
	7678.5-7737.5	7524.5-7583.5	
	7524.5-7583.5	7678.5-7737.5	
	7580.5-7639.5	7426.5-7485.5	154A
	7426.5-7485.5	7580.5-7639.5	
	7608.5-7667.5	7454.5-7513.5	
	7454.5-7513.5	7608.5-7667.5	
	7636.5-7695.5	7482.5-7541.5	
	7482.5-7541.5	7636.5-7695.5	
	7664.5-7723.5	7510.5-7569.5	
	7510.5-7569.5	7664.5-7723.5	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
8 GHz	8396.5-8455.5	8277.5-8336.5	119A
	8277.5-8336.5	8396.5-8455.5	
	8438.5 – 8497.5	8319.5 – 8378.5	
	8319.5 – 8378.5	8438.5 – 8497.5	
	8274.5-8305.5	7744.5-7775.5	530A
	7744.5-7775.5	8274.5-8305.5	
	8304.5-8395.5	7804.5-7895.5	500A
	7804.5-7895.5	8304.5-8395.5	
	8023-8186.32	7711.68-7875	311C-J
	7711.68-7875	8023-8186.32	
	8028.695-8148.645	7717.375-7837.325	311B
	7717.375-7837.325	8028.695-8148.645	

8147.295-8267.245	7835.975-7955.925	
7835.975-7955.925	8147.295-8267.245	
8043.52-8163.47	7732.2-7852.15	311A
7732.2-7852.15	8043.52-8163.47	
8162.12-8282.07	7850.8-7970.75	
7850.8-7970.75	8162.12-8282.07	
8212-8302	7902-7992	310D
7902-7992	8212-8302	
8240-8330	7930-8020	
7930-8020	8240-8330	
8296-8386	7986-8076	
7986-8076	8296-8386	
8212-8302	7902-7992	310C
7902-7992	8212-8302	
8240-8330	7930-8020	
7930-8020	8240-8330	
8296-8386	7986-8076	
7986-8076	8296-8386	
8380-8470	8070-8160	
8070-8160	8380-8470	
8408-8498	8098-8188	
8098-8188	8408-8498	
8039.5-8150.5	7729.5-7840.5	310A
7729.5-7840.5	8039.5-8150.5	
8159.5-8270.5	7849.5-7960.5	
7849.5-7960.5	8159.5-8270.5	
8024.5-8145.5	7724.5-7845.5	300A
7724.5-7845.5	8024.5-8145.5	
8144.5-8265.5	7844.5-7965.5	
7844.5-7965.5	8144.5-8265.5	
8302.5-8389.5	8036.5-8123.5	266C
8036.5-8123.5	8302.5-8389.5	
8190.5-8277.5	7924.5-8011.5	266B
7924.5-8011.5	8190.5-8277.5	

	8176.5-8291.5	7910.5-8025.5	266A
	7910.5-8025.5	8176.5-8291.5	
	8288.5-8403.5	8022.5-8137.5	
	8022.5-8137.5	8288.5-8403.5	
	8226.52-8287.52	7974.5-8035.5	252A
	7974.5-8035.5	8226.52-8287.52	
	8270.5-8349.5	8020.5-8099.5	250A

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
10 GHz	10501-10563	10333-10395	168A
	10333-10395	10501-10563	
	10529-10591	10361-10423	
	10361-10423	10529-10591	
	10585-10647	10417-10479	
	10417-10479	10585-10647	
	10501-10647	10151-10297	350A
	10151-10297	10501-10647	
	10498-10652	10148-10302	350B
	10148-10302	10498-10652	
	10561-10707	10011-10157	550A
	10011-10157	10561-10707	
	10701-10847	10151-10297	
	10151-10297	10701-10847	
	10590-10622	10499-10531	91A
	10499-10531	10590-10622	
	10618-10649	10527-10558	
	10527-10558	10618-10649	
	10646-10677	10555-10586	
	10555-10586	10646-10677	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
11 GHz	11425-11725	10915-11207	All
	10915-11207	11425-11725	
	11185-11485	10695-10955	
	10695-10955	11185-11485	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
13 GHz	13002-13141	12747-12866	266
	12747-12866	13002-13141	
	13127-13246	12858-12990	
	12858-12990	13127-13246	
	12807-12919	13073-13185	266A
	13073-13185	12807-12919	
	12700-12775	12900-13000	200
	12900-13000	12700-12775	
	12750-12825	12950-13050	
	12950-13050	12750-12825	
	12800-12870	13000-13100	
	13000-13100	12800-12870	
	12850-12925	13050-13150	
	13050-13150	12850-12925	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
15 GHz	15110-15348	14620-14858	490
	14620-14858	15110-15348	
	14887-15117	14397-14627	
	14397-14627	14887-15117	
	15144-15341	14500-14697	644
	14500-14697	15144-15341	
	14975-15135	14500-14660	475
	14500-14660	14975-15135	
	15135-15295	14660-14820	
	14660-14820	15135-15295	
	14921-15145	14501-14725	420

	14501-14725	14921-15145	
	15117-15341	14697-14921	
	14697-14921	15117-15341	
	14963-15075	14648-14760	315
	14648-14760	14963-15075	
	15047-15159	14732-14844	
	14732-14844	15047-15159	
	15229-15375	14500-14647	728
	14500-14647	15229-15375	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
18 GHz	19160-19700	18126-18690	1010
	18126-18690	19160-19700	
	18710-19220	17700-18200	
	17700-18200	18710-19220	
	19260-19700	17700-18140	1560
	17700-18140	19260-19700	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
23 GHz	23000-23600	22000-22600	1008
	22000-22600	23000-23600	
	22400-23000	21200-21800	1232 /1200
	21200-21800	22400-23000	
	23000-23600	21800-22400	
	21800-22400	23000-23600	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
24UL GHz	24000 - 24250	24000 - 24250	All

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
26 GHz	25530-26030	24520-25030	1008
	24520-25030	25530-26030	
	25980-26480	24970-25480	
	24970-25480	25980-26480	

	25266-25350	24466-24550	800
	24466-24550	25266-25350	
	25050-25250	24250-24450	
	24250-24450	25050-25250	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
28 GHz	28150-28350	27700-27900	450
	27700-27900	28150-28350	
	27950-28150	27500-27700	
	27500-27700	27950-28150	
	28050-28200	27700-27850	350
	27700-27850	28050-28200	
	27960-28110	27610-27760	
	27610-27760	27960-28110	
	28090-28315	27600-27825	490
	27600-27825	28090-28315	
	29004-29453	27996-28445	1008
	27996-28445	29004-29453	
	28556-29005	27548-27997	
	27548-27997	28556-29005	
	29100-29125	29225-29250	125
	29225-29250	29100-29125	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
31 GHz	31000-31085	31215-31300	175
	31215-31300	31000-31085	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
32 GHz	31815-32207	32627-33019	812
	32627-33019	31815-32207	
	32179-32571	32991-33383	
	32991-33383	32179-32571	

Frequency Band	Lower Channels Range	High Channels Range	Tx/Rx Spacing
38 GHz	39500-39600	38240-38340	1260
	38240-38340	39500-39600	
	38820-39440	37560-38180	
	37560-38180	38820-39440	
	38316-38936	37045-37676	
	37045-37676	38316-38936	
	39650-40000	38950-39300	700
	38950-39300	39500-40000	
	39300-39650	38600-38950	
	38600-38950	39300-39650	
	37700-38050	37000-37350	
	37000-37350	37700-38050	
	38050-38400	37350-37700	
	37350-37700	38050-38400	

9.6.2 Frequency Bands – RFU-E

Table 97: Frequency Bands – RFU-E

Frequency Band (GHz)	Frequency range (GHz)	Recommendations ITU-R F Series	Tx/Rx Spacing (MHz)
70/80	71-76 GHz/81-86 GHz	F.2006	125 MHz (pattern)
	71-76 GHz/81-86 GHz	F.2006, Annex 1	n × 250 MHz blocks (n = 1, …, 20)
	71-76 GHz/81-86 GHz	F.2006, Annex 2	n × 250 MHz channels (n = 1, …, 18)
	74-76 GHz/84-86 GHz	F.2006, Annex 2	n × 250 MHz channels (n = 1, …, 7)

9.7 Ethernet Latency Specifications

The specifications in this section are for 1+0 configurations.

9.7.1 Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S

9.7.1.1 Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 25 MHz Channel Bandwidth

Table 98: Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 25 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		975	1011	1086	1236	1537	1830
1	QPSK		476	496	529	597	737	873
2	8 QAM		342	355	379	426	521	612
3	16 QAM		261	271	289	325	396	468
4	32 QAM		219	226	241	270	328	383
5	64 QAM		192	199	212	236	286	333
6	128 QAM		173	179	190	212	255	297
7	256 QAM		158	163	174	193	233	271
8	512 QAM		162	168	177	196	233	268
9	1024 QAM (Strong FEC)		153	158	167	185	220	255
10	1024 QAM (Light FEC)		151	156	165	182	216	249
11	2048 QAM		144	149	158	174	207	238
12	4096 QAM		144	149	158	174	207	238

9.7.1.2 Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 30 MHz Channel Bandwidth

Table 99: Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 30 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		796	823	881	1002	1248	1487
1	QPSK		400	415	444	502	618	732
2	8 QAM		289	299	321	361	444	524
3	16 QAM		221	230	246	276	338	399
4	32 QAM		188	194	208	232	282	330
5	64 QAM		165	171	182	204	247	288
6	128 QAM		150	155	165	184	222	259
7	256 QAM		141	146	156	173	207	241
8	512 QAM		141	146	155	172	205	237
9	1024 QAM (Strong FEC)		133	138	146	162	194	224
10	1024 QAM (Light FEC)		131	136	144	159	190	219
11	2048 QAM		124	129	137	151	180	208
12	4096 QAM		124	129	137	151	180	208

9.7.1.3 Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 40 MHz Channel Bandwidth

Table 100: Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 40 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		575	597	642	729	900	1069
1	QPSK		303	313	335	379	467	552
2	8 QAM		223	231	248	278	341	402
3	16 QAM		173	181	194	218	267	314
4	32 QAM		148	154	165	185	225	264
5	64 QAM		132	137	147	164	200	234
6	128 QAM		120	125	134	149	181	211
7	256 QAM		110	115	123	138	168	197
8	512 QAM		113	118	125	139	168	196
9	1024 QAM (Strong FEC)		108	113	120	133	160	186
10	1024 QAM (Light FEC)		107	111	118	131	157	183
11	2048 QAM		102	106	113	126	151	175
12	4096 QAM		102	106	113	126	151	175

9.7.1.4 Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 50 MHz Channel Bandwidth

Table 101: Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 50 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		457	475	509	576	714	848
1	QPSK		251	262	281	317	390	463
2	8 QAM		182	189	203	228	281	330
3	16 QAM		144	150	161	182	224	264
4	32 QAM		124	129	138	156	192	227
5	64 QAM		111	116	124	140	170	200
6	128 QAM		101	106	113	127	155	183
7	256 QAM		94	98	105	118	144	169
8	512 QAM		97	101	108	120	145	169
9	1024 QAM (Strong FEC)		92	96	103	114	138	162
10	1024 QAM (Light FEC)		91	95	101	113	136	158
11	2048 QAM		88	91	97	109	131	153
12	4096 QAM		88	91	97	109	131	153

9.7.1.5 Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 60 MHz Channel Bandwidth

Table 102: Ethernet Latency with RFU-D, RFU-D-HP, and RFU-S – 60 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		387	402	431	488	604	717
1	QPSK		211	219	235	266	328	388
2	8 QAM		174	180	193	216	262	307
3	16 QAM		127	132	142	161	198	233
4	32 QAM		110	115	123	139	171	200
5	64 QAM		100	104	111	125	153	180
6	128 QAM		92	96	103	115	141	165
7	256 QAM		88	92	98	110	134	157
8	512 QAM		88	91	98	109	132	154
9	1024 QAM (Strong FEC)		84	87	93	105	127	148
10	1024 QAM (Light FEC)		83	86	92	103	125	146
11	2048 QAM		83	86	92	103	125	146
12	4096 QAM		83	86	92	103	125	146

9.7.2 Ethernet Latency with RFU-E

9.7.2.1 Ethernet Latency with RFU-E – 62.5 MHz Channel Bandwidth

Table 103: Ethernet Latency with RFU-E – 62.5 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface					
	Frame Size	64	128	256	512	1024	1518
0	BPSK	411	424	454	513	630	741
1	QPSK	214	222	237	265	322	377
2	8 QAM	165	171	182	203	245	286
3	16 QAM	134	140	149	166	200	233
4	32 QAM	119	123	131	146	174	202
5	64 QAM	109	113	120	133	159	183
6	128 QAM	102	106	112	124	147	170
7	256 QAM	96	100	106	116	138	159
8	512 QAM	98	102	108	118	139	159
9	1024 QAM	95	98	104	114	134	153

9.7.2.2 Ethernet Latency with RFU-E – 125 MHz Channel Bandwidth

Table 104: Ethernet Latency with RFU-E – 125 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface					
	Frame Size	64	128	256	512	1024	1518
0	BPSK	215	223	238	267	326	384
1	QPSK	128	133	143	160	194	227
2	8 QAM	105	109	117	130	157	182
3	16 QAM	90	94	100	111	134	156
4	32 QAM	82	86	92	102	122	141
5	64 QAM	78	81	86	95	114	132
6	128 QAM	75	77	82	91	109	125
7	256 QAM	72	75	79	88	104	120
8	512 QAM	74	76	81	89	105	120

9.7.2.3 Ethernet Latency with RFU-E – 250 MHz Channel Bandwidth

Table 105: Ethernet Latency with RFU-E – 250 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface					
	Frame Size	64	128	256	512	1024	1518
0	BPSK	129	134	144	161	196	230
1	QPSK	87	91	97	109	132	153
2	8 QAM	76	79	85	94	113	132
3	16 QAM	69	72	77	85	102	119
4	32 QAM	66	68	73	81	97	112
5	64 QAM	63	66	70	78	93	107
6	128 QAM	62	64	68	76	90	104
7	256 QAM	61	64	68	75	89	103

9.7.2.4 Ethernet Latency with RFU-E – 500 MHz Channel Bandwidth

Table 106: Ethernet Latency with RFU-E – 500 MHz Channel Bandwidth

ACM Working Point	Modulation	Latency (µsec) with GbE Interface		
	Frame Size	64	512	1518
0	BPSK	85	103	140
1	QPSK	52	65	89
2	8 QAM	43	54	75
3	16 QAM	37	47	66
4	32 QAM	34	44	61
5	64 QAM	32	40	57

9.8 Mediation Device and Branching Network Losses

Note: In general, the mediation devices per RFU are available for the frequency bands in which the RFU is available.

9.8.1 RFU-D and RFU-D-HP Mediation Device Losses

Note: The 4-5 GHz bands are only relevant for RFU-D-HP. Bands above 11 GHz are not relevant for RFU-D-HP.

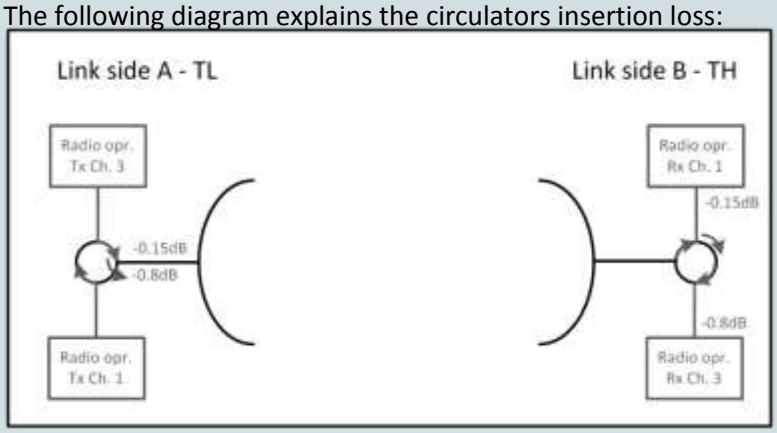
Table 107: RFU-D and RFU-D-HP Mediation Device Losses

Mediation Devices	Signal Path / Remarks	Maximum Insertion Loss [dB]						
		4-5 GHz	6-8 GHz	11 GHz	13-15 GHz	18 GHz	23-26 GHz	28-38 GHz
Flex WG	Size varies per frequency.	0.5	0.5	0.5	1.2	1.2	1.5	1.8
OMT	Radio to antenna ports (V or H)	n/a	0.3	0.3	0.3	0.3	0.5	0.5
Splitter[45]	Radio to antenna port	3.6	3.6	3.7	3.7	3.7	3.7	4.0
Dual Coupler	Main Paths	1.4	1.6	1.6	1.6	1.8	1.8	2.0
	Secondary Paths	6±0.7	6±0.7	6±0.7	6±0.7	6±0.8	6±0.8	6±1.0
Dual Splitter	Radio to antenna port	3.6	3.6	3.7	3.7	3.7	3.7	4.0
Dual Circulator	High Ch radio to antenna port	0.2	0.2	0.2	0.2	0.5	0.5	0.5
	Low Ch radio to antenna port	0.2	0.2	0.2	0.2	0.5	0.5	0.5

Notes:
- The antenna interface is always the RFU interface.
- If other antennas are to be used, an adaptor with a 0.1 dB loss should be considered.
- The numbers above represent the typical loss per component.

[45] The RFU-D-HP splitter is planned for future release.

The following diagram explains the circulators insertion loss:



9.8.2 RFU-D-HP Branching Losses – Filter-Based Branching

When designing a link budget calculation, the branching loss (dB) should be considered as per specific configuration, frequency, and channel bandwidth. This section contains tables that list the typical branching losses for the following split-mount configurations.

Table 108: RFU-D-HP Branching Network Losses

	6-8 GHz					11 GHz				
Configuration	**30 MHz**	**40 MHz**	**60 MHz**	**80 MHz**	**112 MHz**	**30 MHz**	**40 MHz**	**60 MHz**	**80 MHz**	**112 MHz**
2+0 XPIC (CCDP)	1.8	1.8	2.3	2.6	1.8	2.3	2.3	2.3	2.6	1.8
4+0 XPIC (CCDP)	2.0	2.0	2.5	2.8	2.0	2.5	2.5	2.5	2.8	2.0
4+0 XPIC (ACCP)[46]	5.3	5.3	5.8	6.1	5.3	5.8	5.8	5.8	6.1	5.3
2+0 SP	2.2	2.2	2.7	3	2.2	2.7	2.7	2.7	3.0	2.2
3+0 SP	2.4	2.4	2.9	3.2	2.4	2.9	2.9	2.9	3.2	2.4
4+0 SP	2.7	2.7	3.2	3.5	2.7	3.2	3.2	3.2	3.5	2.7
2+0 SP (ACCP)[46]	5.3	5.3	5.8	6.1	5.3	5.8	5.8	5.8	6.1	5.3
4+0 SP (ACCP)[46]	5.7	5.7	6.2	6.5	5.7	6.2	6.2	6.2	6.5	5.7

Notes:

- (c) – Radio Carrier
- **CCDP** – Co-channel dual polarization
- **SP** – Single pole antenna
- **DP** – Dual pole antenna

In addition, the following losses will be added when using these items:

Table 109: Added Losses

Item	Where to Use	Loss (dB)
Flex WG	All configurations	0.5
15m Coax cable	Diversity path 6-8/11 GHz	5/6.5
Symmetrical Coupler	Adjacent channel configuration.	3.5
Asymmetrical coupler	1+1 HSB configurations	Main: 1.6 Coupled: 6.5

[46] Planned for future release.

9.8.3 RFU-E Mediation Device Losses

Table 110: RFU-E Mediation Device Losses

Device Type	Maximum Insertion Loss (Main/Secondary)
OMT	2dB
Splitter 1:2	4.5dB
Coupler 1:4	2.2dB/ 6.5±1dB

9.8.4 RFU-S Mediation Device Losses

Table 111: RFU-S Mediation Device Losses

Configuration	Interfaces		5.7-8 GHz	11 GHz	13-15 GHz	18 GHz	23-26 GHz	28-38 GHz
Flex WG	Remote Mount antenna	Added on remote mount configurations	0.5	0.5	1.2	1.2	1.5	1.8
1+0	Direct Mount	Integrated antenna	0.2	0.2	0.4	0.5	0.5	0.5
OMT	Direct Mount	Integrated antenna	0.3	0.3	0.3	0.3	0.5	0.5
Splitter	Direct Mount	Integrated antenna	3.6	3.7	3.7	3.7	3.7	4.0

Notes:
The antenna interface is always the RFU interface.

If other antennas are to be used, an adaptor with a 0.1 dB loss should be considered.

9.9 Ethernet Specifications

9.9.1 Ethernet Interface Specifications

Table 112: Ethernet Interface Specifications

Supported Ethernet Interfaces for Traffic	Up to 6 x 10/100/1000Base-T (RJ-45) or 1000base-X (SFP)
Supported Ethernet Interfaces for Management	2 x 10/100 Base-T (RJ-45)
Supported SFP Types	See *Approved SFP Modules* on page 316

9.9.2 Carrier Ethernet Functionality

Table 113: Carrier Ethernet Functionality

Switching capacity	5 Gbps
"Jumbo" Frame Support	Up to 9600 Bytes
General	Header De-Duplication
Integrated Carrier Ethernet Switch	MAC address learning with 128K MAC addresses 802.1ad provider bridges (QinQ) 802.3ad link aggregation
QoS	Advanced CoS classification and remarking Per interface CoS based packet queuing/buffering (8 queues) Per queue statistics Tail-drop and WRED with CIR/EIR support Flexible scheduling schemes (SP/WFQ/Hierarchical) Per interface and per queue traffic shaping Hierarchical-QoS (H-QoS) – Up to 2.5K service level queues[47] 2 Gbit packet buffer
Network resiliency	MSTP ERP (G.8032)
Service OAM	FM (Y.1731) PM (Y.1731) [48]
Performance Monitoring	Per port Ethernet counters (RMON/RMON2) Radio ACM statistics Enhanced radio Ethernet statistics (Frame Error Rate, Throughput, Capacity, Utilization)

[47] Planned for future release.

[48] Planned for future release.

9.9.3 Approved SFP Modules

Table 114: Approved GbE SFP Modules

Part Number	Marketing Model	Marketing Description	Item Description
AO-0058-0	SFP-GE-ZX	SFP optical interface 1000Base-ZX	XCVR,SFP,1550nm,2.125G,SM,80km,W.DDM
AO-0226-0	SFP-GE-CWDM-120km-1510nm	SFP GE CWDM, 120Km, 1510nm	XCVR,SFP,1510nm,GE,SM,CWDM,120km,W.DDM,COMMERCIAL TEMP
ER-8000-0	SFP-GE-SX	SFP optical interface 1000Base-SX	XCVR,SFP,850nm,MM,1.0625 Gbit/s FC/ 1.25 GBE,PACKED
ER-1002-0	SFP-GE-LX	SFP optical interface 1000Base-LX*ROHS	XCVR,SFP,1310nm,1.25Gb,SM,10km,W.DDM, SINGLE PACK KIT

Table 115: Approved 2.5 GbE SFP Modules

Part Number	Marketing Model	Marketing Description	Item Description
AO-0165-0	SFP-3.7G-SX-EXT-TEMP	SFP-3.7G-SX-EXT-TEMP	XCVR,SFP,850nm,MM,3.7 Gbit/s, INDUSTRIAL GRADE
AO-0265-0	SFP-3.7G-LX-EXT-TEMP	SFP-3.7G-LX-EXT-TEMP	XCVR,SFP,1310nm,SM,10km,3.7 Gbit/s, INDUSTRIAL GRADE

Note: Ceragon recommends the use of SFP and SFP+ modules certified by Ceragon, as listed above.

9.10 TDM Specifications

9.10.1 DS1 Cross Connect

Table 116: DS1 Cross Connect

DS1 Cross Connect Capacity	256 DS1 Trails (VCs)
DS1 Trails Protection	1+1 / 1:1

9.10.2 DS1 Interface Specifications

Interface Type	DS1
Number of Ports	16 x DS1s
Connector Type	MDR 69-pin
Framing	Framed / Unframed
Coding	HDB3
Line Impedance	120 ohm/100 ohm balanced. Optional 75 ohm unbalanced supported using panel with integrated impedance adaption.
Compatible Standards	ITU-T G.703, G.736, G.775, G.823, G.824, G.828, ITU-T I.432, ETSI ETS 300 147, ETS 300 417, Bellcore GR-253-core, TR-NWT-000499

9.10.3 Pseudowire Specifications

Table 117: Pseudowire Specifications

Circuit-Emulation Modes	RFC 4553 – SAToP RFC 5086 – CESoP[49]
Circuit-Emulation Encapsulations	Ethernet (MEF-8) IP/UDP[50] MPLS (MFA-8)[51]
Frame payload size	Configurable – 1 DS1 frame (256 bytes) to 64 frames (8192 bytes)
De-Jitter buffer size	Configurable – 1 ms to 32 ms

[49] CESoP mode is planned for future release.

[50] IP/MPLS encapsulation is planned for future release.

[51] MFA-8 encapsulation is planned for future release.

9.10.4 Electrical OC-3 SFP Interface Specifications

Table 118: Electrical OC-3 SFP Interface Specifications

Interface Type	**OC-3**
Number of Ports	1 x OC-3 per LIC
Connector Type	1.0/2.3 on SFP
Framing	Framed carrying up to 84 x VC11
Coding	CMI
Line Impedance	75ohms
Compatible Standards	ITU-T G.703, G.775, G.813, G.825, EN 300 386 V1.2.1, ES 201 468 V1.1.1 :2000-03, ES 201 468 V1.2.1 :2002-09, EN 61000 4-3

9.10.5 Optical OC-3 SFP Interface Specifications

Transceiver Name	SH1310	LH1310	LH1550
Application Code	S-1.1	L-1.1	L-1.2
Operating Wavelength (nm)	1261-1360	1263-1360	1480-580
Transmitter			
Source Type	MLM	SLM	SLM
Max RMS Width (nm)	7.7	-	-
Min Side Mode Suppression Ratio (dB)	-	30	30
Min Mean Launched Power (dBm)	-15	-5	-5
Max Mean Launched Power (dBm)	-8	0	0
Min Extinction Ratio (dB)	8.2	10	10
Receiver			
Min Sensitivity (BER of 1x10-42 EOL (dBm)	-28	-34	-34
Min Overload (dBm)	-8	-10	-10
Max Receiver Reflectance (dB)	-	-	-25
Optical Path between S and R			
Max Dispersion (ps/nm)	96	-	-
Min Optical Return Loss of Cable (dB)	-	-	-20
Max Discreet Reflectance (dB)	-	-	25
Max Optical Path Penalty (dB)	1	1	1

9.10.6 Approved OC-3 SFP Modules

Part Number	Marketing Model	Marketing Description	Item Description
AO-0096-0	SFP-STM-1-Elec-1.0/2.3-75ohm	SFP STM-1 Module Elec, 1.0/2.3, 75ohm	XCVR,SFP,STM1E-SFP 155Mbps 1.0/2.3
AO-0073-0	SFP-STM-1-L1.1	SFP STM-1 Module Long Haul 1310nm	XCVR,SFP,1310nm,OC3,SM,40km,W.DDM
AO-0074-0	SFP-STM-1-L1.2	SFP STM-1 Module Long Haul 1550nm	XCVR,SFP,1550nm,OC3,SM,80km,W.DDM
AO-0118-0	SFP-STM-1-MM_1310	SFP STM-1 Module Multi Mode 1310nm	XCVR,SFP,1310nm,OC3,MM,2km,W.DDM
AO-0072-0	SFP-STM-1-S1.1	SFP STM-1 Module Short Haul 1310nm	XCVR,SFP,1310nm,OC3,SM,15km,W.DDM

Note: Ceragon recommends the use of SFP modules certified by Ceragon, as listed above.

9.11 Mechanical Specifications

Table 119: IDU Mechanical Specifications

IDU Dimensions	Height: 1.73 inches Width: 19 inches Depth: 6.5 inches Weight: 5.3 lbs.

Table 120: RFU-D Mechanical Specifications (including diplexer unit)

RFU-D Dimensions	Height: 9.05 inches Width: 9.17 inches Depth: 3.85 inches Weight: 14.33 lbs.

Table 121: RFU-D-HP Mechanical Specifications (including diplexer or OCU unit)

RFU-D-HP Dimensions	Height: 12.56 inches Width: 11.26 inches Depth: 4.21 inches Weight: 26.5 lbs.

Table 122: RFU-E Mechanical Specifications

RFU-E Dimensions	Height: 8.66 inches Width: 7.8 inches Depth: 3 inches Weight: 6.6 lbs.

Table 123: RFU-S Mechanical Specifications

RFU-S Dimensions	Height: 8.54 inches Width: 8.27 inches Depth: 3.35 inches Weight: 8.82 lbs.

9.12 Environmental Specifications

9.12.1 Environmental Specifications for IDU

- Temperature:
  - **23°F to 131°F** – Temperature range for continuous operating temperature with high reliability.
  - **5°F to 140°F** – Temperature range for exceptional temperatures, tested successfully, with limited margins.

    Note: Cold startup requires at least **23°F**
- Humidity: 5%RH to 95%RH

9.12.2 Environmental Specifications for RFU

- Temperature:
  - **-27°F to +131°F** – Temperature range for continuous operating temperature with high reliability:
  - **-49°F to +140°F** – Temperature range for exceptional temperatures; tested successfully, with limited margins:
- Humidity: 5%RH to 100%RH

9.13 Supported Antenna Types

RFUs can be installed using Direct Mount antennas or Remote Mount antennas, depending on the RFU type and the configuration used.

The following table shows the antenna types supported by the various FibeAir RFUs.

Note: Support of Direct Mount or Remote Mount per RFU is band and configuration dependent.

Table 124: Supported Antenna Types per RFU

	Integrated Antenna	Direct Mount Support	Remote Mount Support
RFU-D	–	All Supported Bands	All Supported Bands
RFU-D-HP	–	All Supported Bands	All Supported Bands
RFU-E	E-Band	E-Band	–
RFU-S	–	All Supported Bands	All Supported Bands

9.13.1.1 Direct Mount Antennas

The RFUs can be mounted directly on the antenna using the following antenna vendors:

- Ceragon
- RFS
- CommScope
- Xian Putian
- Radio Waves

9.13.1.2 Remote Mount Antennas

The RFUs can be used with standard interface antennas using the following antenna vendors:

- Ceragon
- RFS
- CommScope
- Xian Putian
- Radio Waves

9.13.2 RFU-D and RFU-S Waveguide Specifications

Table 125: RFU-D and RFU-S – Waveguide Flanges

Frequency (GHz)	Waveguide Standard	Waveguide Flange	Antenna Flange
6	WR137	PDR70	UDR70
7/8	WR112	PBR84	UBR84
10/11	WR90	PBR100	UBR100
13	WR75	PBR120	UBR120
15	WR62	PBR140	UBR140
18-26	WR42	PBR220	UBR220
28-38	WR28	PBR320	UBR320
42	WR22	UG383/U	UG383/U
60	WR15	UG385/U	UG385/U
80	WR12	UG387/U	UG387/U

9.13.3 RFU-D-HP Waveguide Specifications

Table 126: RFU-D-HP – Waveguide Flanges

Frequency Band	Range (GHz)	Rect. WG Flange Des.	Radio Side (Remote) Flange Des.
4 GHz	3.6-4.2	WR229	UDR40
5 GHz	4.4-5.0	WR187	UDR48
6(L/U) GHz	5.8-7.1	WR137	UDR70[52]
7/8 GHz	7.1-8.5	WR112	UBR84[52]
10/11 GHz	10.0-11.7	WR90	UBR100[52]

[52] There is no direct WG connection. An adaptor is required to connect the RFU to the WG.

9.13.4 RFU-E Antenna Connection

RFU-E uses two types of antennas:

- Integrated 43 dBi Class 2 antenna
- Direct Mount antenna.

9.13.4.1 RFU-E Integrated Antenna

The following table describes the electrical parameters of the RFU-E integrated antenna.

Table 127: RFU-E Integrated Antenna – Electrical Parameters

Frequency coverage	71-76 GHz, 81-86 GHz
Gain	71-76 GHz: 43dBi 81-86 GHz: 44.5dBi
3dB beam width (azimuth and elevation)	1.0°
XPOL	30 dB
Polarization	Single Linear: V or H
Co/cross-polar ratio	>35dB
Front to back ratio	>60dB
Side lobe suppression	ETSI EN 302 217-4 v2.1.1 (2017-05) CLASS 3 FCC 47CFR101.115

9.13.4.2 Direct Mount Antenna

The Direct Mount antenna interface is according to:

Waveguide Standard	Antenna Flange
WR12	UG387/U

9.14 Power Input Specifications

Table 128: Power Input Specifications

IDU Standard Input	-48 VDC
IDU DC Input range	-40 to --60 VDC
RFU-D Operating Range	-40.5 to -59 VDC
RFU-D-HP Operating Range	-40.5 to -59 VDC
RFU-E Operating Range	-40.5 to -59 VDC
RFU-S Operating Range	-40.5 to -59 VDC

9.15 Power Consumption Specifications

The following table shows the maximum power consumption for IP-20F IDU and supported RFUs. The maximum power consumption for the entire system is the sum of the IDU and the RFUs connecting to it.

Table 129: Power Consumption Specifications

Card Type/Configuration	Power (W)	Comments
IDU	48W maximum	
IDU with OC-3 Module	71W maximum	
RFU-D (2+0)	75W	RFU only
RFU-D-HP (2+0)	130W	RFU only
RFU-E	43W	RFU only
RFU-S	43W	RFU only

9.16 IDU-RFU Cable Connection

RFUs can be connected to the IDU via:

- Standard CAT-5e or preferably CAT-6/6a cables, with RJ-45 connectors on the RFU and an RJ-45 RFU interface on the IDU.
- Optical fiber cables via an optical (SFP) RFU interface on the IDU.

For an RFU-D, RFU-E, or RFU-S connecting to an electrical RFU interface, the cable can carry both the data and the DC power required for the RFU.

For an RFU-D, RFU-E, or RFU-S connecting to an optical RFU interface, and for an RFU-D-HP connecting to either an electrical or an optical RFU interface, an external DC power cable is required to supply power to the RFU.

Table 130: IDU-RFU Cable Connection

RFU	Interface	Cable Type	Maximum Length	
			6-11 GHz	13-42 GHz
RFU-D	Optical	Fiber	984 ft.	
	Electrical	CAT-5e (24 AWG)	213 ft.	328 ft.
		CAT-6a (22 AWG)	361 ft.	492 ft.
	DC Power	DC (18 AWG)	328 ft.	
		DC (12 AWG)	331 ft.-984 ft.	
RFU-S	Optical	Fiber	984 ft.	
	Electrical	CAT-5e (24 AWG)	427 ft.	492 ft.
		CAT-6a (22 AWG)	492 ft.	492 ft.
	DC Power	DC (18 AWG)	492 ft.	
		DC (14 AWG)	331 ft. - 984 ft.	
RFU-D-HP	Optical	Fiber	984 ft.	
	Electrical	CAT-5e (24 AWG)	492 ft.	
		CAT-6a (22 AWG)	492 ft.	
	DC Power	DC (14 AWG)	328 ft.	
		DC (10 AWG)	331 ft. - 984 ft.	
RFU-E	Optical	Fiber	984 ft.	
	Electrical	CAT-5e (24 AWG)	427 ft.	
		CAT-6a (22 AWG)	492 ft.	
	DC Power	DC (18 AWG)	492 ft.	
		DC (14 AWG)	331 ft. - 984 ft.	

Network Management

NetMaster NMS

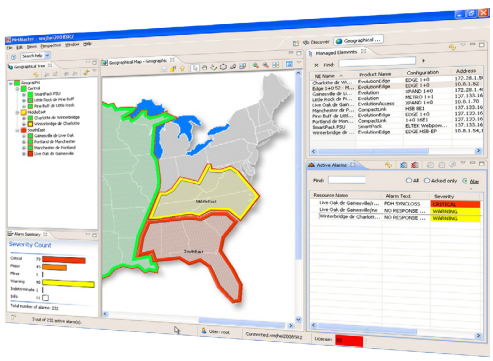
Network availability in focus

NetMaster is a comprehensive Network Management System (NMS) designed for managing large scale microwave networks. With NetMaster, operators get a unified real-time view of the network to provide continuity of service and achieve uninterrupted flows of traffic and revenue. NetMaster is a single point of entry for managing all current and legacy radios, including Evolution Series and FibeAir IP-10 10 radios, as well as 3rd party network elements, such as power supplies, switches, multiplexers and routers.

From small size to large scale networks

NetMaster offers comprehensive integrated management of network elements in a converged network. NetMaster is easily scalable from the smallest network to large scale heterogenous networks. It allows to expand the network on-the-fly, bringing new elements into service and letting operators start generating revenues immediately.

Versatile and flexible, NetMaster allows for various deployments, from a simple single-server installation to high-availability clusters without a single point of failure.



"NetMaster has been an invaluable tool for Conterra to monitor its wireless networks. It gives our Network Operations Center and field operations personnel a complete view of the microwave network in a very intuitive multi-user interface. NetMaster will enable Conterra to continue to scale networks with functionality that automates inventory and maintenance functions, for both new microwave platforms and legacy equipment. NetMaster is, and will continue to be a critical part of our network management strategy."

Anthony Good,
VP Information Technology &
Data Network Engineering
Conterra Telecom Services, USA

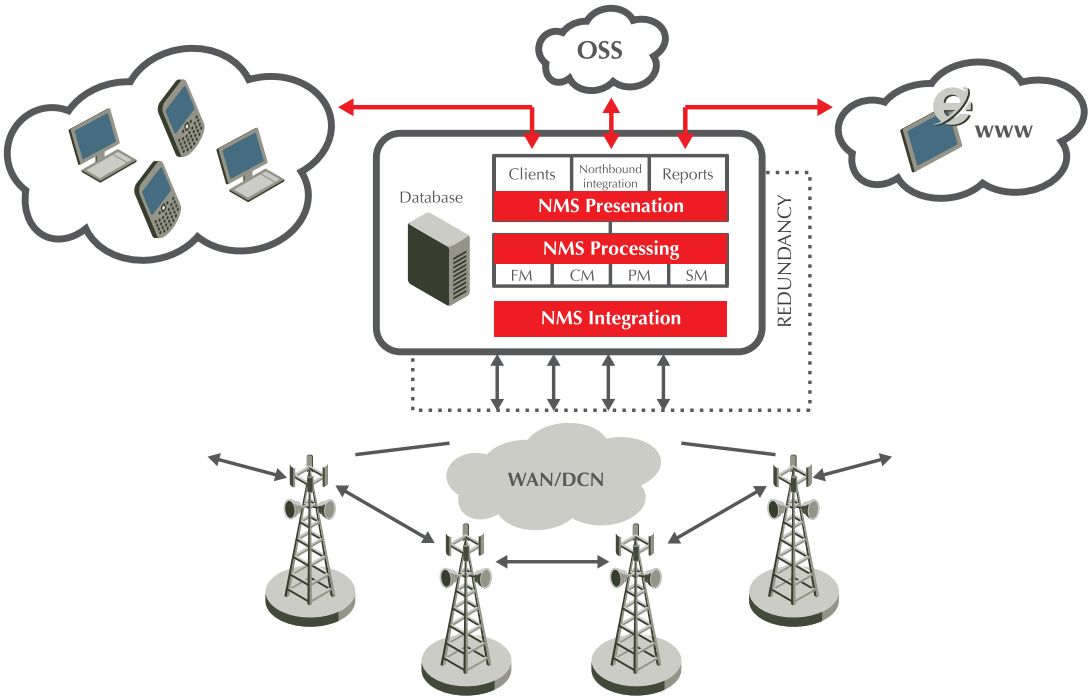
"The ability to visualize and monitor our radio network in a simple and effective way was key factor to the choice of NetMaster. Using NetMaster we can reduce our maintenance costs by ensuring a greater degree of assertiveness in our network interventions."

Marco Antônio Pereira Gomes,
Senior Operations Analyst
VALE, Brazil

CERAGON

NetMaster Architecture - Modular and Future-Proof Design

Based on a modular and future-proof architecture, NetMaster cost-effectively manages thousands of network elements. Network supervisors, field engineers and network maintenance staff can easily supervise the network from the view of the bird's eye down to the single network element level – from any location, from any device.



Platform Independent Application Server

The application server manages the interaction of all NetMaster system components. It runs continuously in the background as a service. The application server is based on JAVA/J2EE technology, which makes it platform independent.

Database Server

The database server stores all configuration data and traffic related information collected from the network. The database server can be configured with redundancy and automated replication to increase system availability.

NetMaster Client

The client provides the user interface to the NetMaster features and services. Multiple clients can be logged on to the server simultaneously. Clients can be installed separately and are launched on demand and connected to the NetMaster application server.

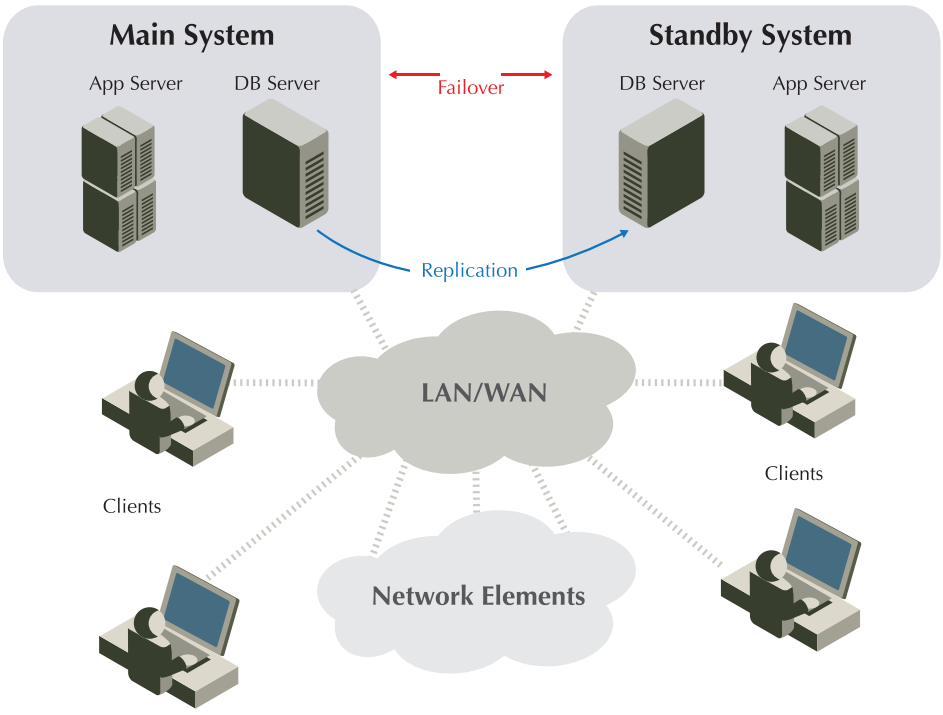
The NetMaster client can be installed on various Microsoft Windows and Sun Solaris platforms.

Northbound Interface to Higher Order OSS

The NetMaster architecture supports open interfaces to higher order management network systems or other business operations components.

Network Availability in Focus

Network downtime means lost revenues. NetMaster is the key to reducing time to recovery so that such failures minimally affect your customers. Easy scalability and fault tolerance of the network management system itself are no less important - NetMaster offers both to ensure continuous network uptime.



Scalability

The modular structure of both Evolution Series and NetMaster allows the entire system to scale in size and functionality. For small networks, the application and database server can be hosted on the same platform. As the network grows, NetMaster can be scaled accordingly, from a small compact single-server configuration to a large distributed system, supporting thousands of deployed network elements.

NetMaster takes care of both the network expansion and easy upgrade to new technologies - it allows for easy migration to new all-IP equipment with minimal effort and zero downtime.

Real-time Network Awareness

NetMaster allows network operators to get a clear, real-time view of traffic and network performance, manage and monitor every network element and entire network as a whole. It discovers faults and traces them down to their root causes, enabling network operators recover network failures before they significantly affect the user.

Redundancy

NetMaster can be configured to achieve co-located hardware redundancy as well as geographical system redundancy for disaster recovery:

- Hot and cold standby systems
- Data integrity through automated database replication

With redundancy and failover capabilities, NetMaster provides continuity of service even when faults occur.

Key Features

Managing wireless backhaul networks

- Unified view of the network
- Intuitive, easy-to-use workflow
- Redundancy and scalability
- Manages different elements and networks
- Network availability in focus
- Rapid deployment
- Fast root cause identification and repair
- Lowers life cycle costs

Fault management

- Alarm acquisition and verification
- Current and historical alarm views
- Alarm reports
- Template based alarm handling
- Audible notifications upon status change
- Email notifications to remote users

Configuration management

- Configuration of elements and sub-networks
- Complete network inventory reports
- Software and license distribution
- Clock synchronization
- Backup/restore of element configuration

Performance management

- Collection of traffic statistics, quality metrics and analogue measurements
- Threshold crossing alarms
- Powerful analysis and presentation tools
- Configurable pre-defined reports

Network awareness

- Auto-discovery of new network elements
- Drag-and-drop of network elements into any logical or geographical domain
- System self-monitoring and diagnosis
- Fast fault recognition

Tailored to your business

- Pay-as-you-grow with Mini/Basic Server/Premium editions
- 24-hour customer support

Ceragon Comprehensive Network Offering:

Product Portfolio

Network Management

Professional Services

Strategic Partnerships

ref: NetMaster NMS, Feb. 2011

www.ceragon.com

CERAGON

EU Declaration of Conformity

We,

Ceragon Networks Ltd.

Espehaugen, 32, Entrance B N-5258 Blomsterdalen

Norway

Hereby declare under our own responsibility that the following products

Model Identifier
FibeAir IP-20F

to which this declaration relates, are in conformity with the essential requirements set out in the Radio Equipment Directive - RED (2014/53/EU), the Restriction of the use of certain Hazardous Substances Directive - RoHS 2011/65/EU and the Directive 2015/863/EU - Amendment Annex II to Directive 2011/65/EU.

For the evaluation of the compliance with these Directives and Regulations, the following standards, requirements and other normative documents were applied:

Directive RED 2014/53/ EU

Article 3.1a – Product safety:

EN 62368-1:2020

IEC 62368-1:2018

Article 3.1b – Product Electromagnetic Compatibility:

EN 301 489-1 V2.1.1:2017

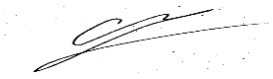
EN 301 489-4 V3.1.1:2017

Directive RoHS 2011/65/EU

EN 50581:2012

2 May 2021

Sergey Shkolnik
Regulatory Affairs Manager, R&D



Identification marking:

CE

EU Declaration of Conformity

We,

Ceragon Networks Ltd.

Espehaugen, 37, N-5258 Blomsterdalen

Norway

Hereby declare under our own responsibility that the following products

Model Identifier: RFU-D	
RFU-D-06	RFU-D-E-18-H-L
RFU-D-07	RFU-D-E-18-H-H
RFU-D-08	RFU-D-E-23-L
RFU-D-11	RFU-D-E-23-H
RFU-D-13	RFU-D-E-26-L-L
RFU-D-15	RFU-D-E-26-L-H
RFU-D-E-18-L-L	RFU-D-E-26-H-L
RFU-D-E-18-L-H	RFU-D-E-26-H-H
Diplexer Unit variants	
DXDff-xxxY-ccWdd-eeWgg-t *ff - Frequency Band { L6/U6/07/08/11/13/15}* *xxxY - TRS Block, ccWdd - {Start ch}W{End ch}, (eeWgg is optional when using different diplexers)* *t - Tx Low/High {L/H}*	

to which this declaration relates, are in conformity with the essential requirements set out in the Radio Equipment Directive - RED 2014/53/EU, the Restriction of the use of certain Hazardous Substances Directive - RoHS 2011/65/EU and the Directive 2015/863/EU - Amendment Annex II to Directive 2011/65/EU.

For the evaluation of the compliance with these Directives and Regulations, the following standards, requirements and other normative documents were applied:

Directive RED 2014/53/ EU

Article 3.1a – Product safety:

EN 62368-1:2020

IEC 62368-1:2018

EN 50385:2017

Article 3.1b – Product Electromagnetic Compatibility:

EN 301 489-1 V2.1.1:2017

EN 301 489-4 V3.1.1:2017

Article 3.2 – The effective usage of the spectrum allocated to radio communication:

EN 302 217-2 V3.1.1:2017

Directive RoHS 2011/65/EU

EN 50581:2012

2 May 2021

Sergey Shkolnik
Regulatory Affairs Manager, R&D

Identification marking:

CE