

Anti-DDoS System(ADS)

COMPLETE DDoS MITIGATION APPLIANCE

OVERVIEW

Distributed denial-of-service (DDoS) attacks are increasing in complexity, volume, and frequency. There is no doubt that DDoS attacks threatening to overwhelm the bandwidth and application resources of enterprises globally in today's info-security threat landscape.

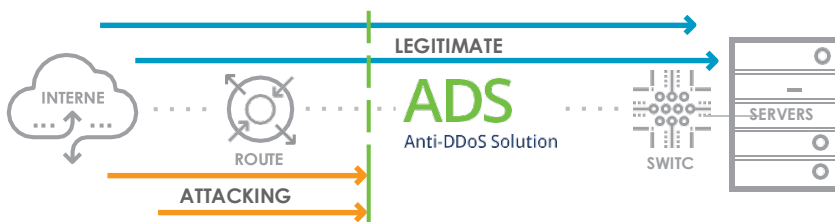
The NSFOCUS Anti-DDoS System (ADS) is the ideal solution for today's advanced and evolving DDoS attacks, which can provide comprehensive, multi-layered DDoS attacks protection. It surgically mitigates DDoS attack traffic, while allowing legitimate traffic to pass downstream. Both inline and out-of-path deployment modes provide extremely low latency and reliable detection and mitigation of attacks while ensuring customers and services are protected from the impact of DDoS.

MONITOR

The ADS provides a complete solution for flexible deployment to meet various customer's business objectives. When the ADS is deployed in L2 or L3 in-line modes, it monitors the incoming traffic for signs of DDoS. When the ADS is deployed in out-of-path modes, the NSFOCUS Network Traffic Analyzer (NTA) performs will take over the monitoring and detection function consuming xFlow data from the border, core, or edge routers. Either mode provides reliable monitoring and detection of DDoS.

DETECT

The ADS provides a multi-stage detection engine with an innovative approach to ensure the full-spectrum DDoS defense. All packets are subjected to a series of analyses, checks, and validations to accurately identify both legitimate and attack traffic. These include RFC Checks, Protocol Analysis, Access Control Lists, IP Reputation, Anti-spoofing, L4-L7 Algorithmic Analysis, User Behavior Analysis, Regular Expressions, Fragmentation Controls, Connection, and Rate Limiting. Together they provide industry-leading accuracy that protects against all DDoS attacks. The detection engine is optimized frequently, so providers always have the most accurate DDoS protection.



MITIGATE

Regardless of the deployment scenario, the ADS can remove DDoS attacks immediately before they reach the enterprise network and affect internet services with the industry-leading DDoS attack mitigation. By utilizing the NSFOCUS Threat Intelligence (NTI), the ADS also can remove the traffic from known botnets immediately and uploads the attack data to NTI for contributing to intelligence. The ADS also provides advanced visibility and reporting of attack mitigation which including attack types, source/ destination IPs, protocols, and more detailed information. An integrated web services API of the ADS can provide additional flexibility to assist with automated configuration, post-incident reporting, and billing operations for customer's unique business needs.

KEY BENEFITS

Defeat DDoS attacks against your customers when deployed in your network

Reduces operating expenses for DDoS mitigation by providing increased levels of automation

KEY FEATURES

Multi-Tenant Design

Domain specific configurations, learning algorithms, automated mitigation responses, modular architectures, flexible licensing models, and the lowest total cost of ownership (TCO)

Reliable, Accurate

Algorithmic, multi-filter, rule-based approach provides automated and reliable DDoS mitigation with low false positives and high performance, efficient and intelligent protection from the botnet-based attacks with NTI

Best-in-Class Performance

Provides advanced DDoS mitigation for any size service provider that is easy to integrate with your network

Scalable Architecture

Supports scalable clusters for both In-line and out-of-path deployment scenarios to meet the needs of any size network

Optional product form

Capable to provide both hardware appliance and virtual product

SOFTWARE SPECIFICATIONS

DDoS Protection

- » Comprehensive, multi-layered protection against the volumetric, application, and web application attacks
- » Multi-protocol support and advanced inspection including TCP/UDP/ICMP/ HTTP/HTTPS/DNS/SIP floods, Amplification attacks (NTP/SSDP/SNMP/DNS/CHARGEN/Memcached/NetBIOS), fragments floods, connection exhaustion, header manipulation and more
- » Integrated with NSFOCUS Cloud Security Platform
- » Integrated with NSFOCUS Threat Intelligence

DDoS Mitigation Algorithms

- | | | |
|------------------------------------|----------------------------------|--------------------------------|
| » RFC Checks | » TCP SYN Source IP Rate Limit | » IP Behavior Analysis |
| » Black Filter Lists | » TCP SYN Source Bandwidth Limit | » Trusted Source IP Control |
| » NTI Black Filter Lists | » TCP SYN Time Sequence Check | » Empty Connection Check |
| » White Filter Lists | » TCP Fragment Control | » HTTPS SSL Connection Control |
| » GEOIP Filter Lists | » ICMP Fragment Control | » HTTPS Authentication |
| » Access Control Lists Filtering | » ICMP Traffic Control | » SIP Authentication |
| » TCP Regular Expression Filtering | » DNS Keyword Checking | » UDP Payload Check |
| » UDP Regular Expression Filtering | » DNS Rate-Limiting | » UDP Fragment Control |
| » SYN Check | » DNS TCP-BIT Check | » UDP Packet Length Check |
| » ACK Check | » DNS CNAME Check | » UDP Traffic Control |
| » Reflection Amplification Rules | » DNS Retransmission | » TCP Watermark Check |
| » Port Check | » HTTP Keyword Checking | » UDP Watermark Check |
| » Connection Exhaustion | » HTTP Authentication | » TCP Pattern Matching |
| » URL-ACK Filter Lists | » HTTP Dynamic Script | » UDP Pattern Matching |
| » Anti-spoofing | » HTTP FCS Check | » Protocol ID Check |
| | » HTTP Pattern Matching Check | |
| | » HTTP Slow Attack Check | |

Management

- » Protocols: HTTP, SNMP, Email, Syslog
- » Authentication: Local database, Radius
- » API: web services for reporting and automated configuration

IP Protocols

- » Addressing: IPv4/v6
- » Routing: BGP, OSPF, RIP, IS-IS, static routing, and PBR
- » Datalink and network layer: MPLS, GRE, VLAN (802.1q)

Virtualization

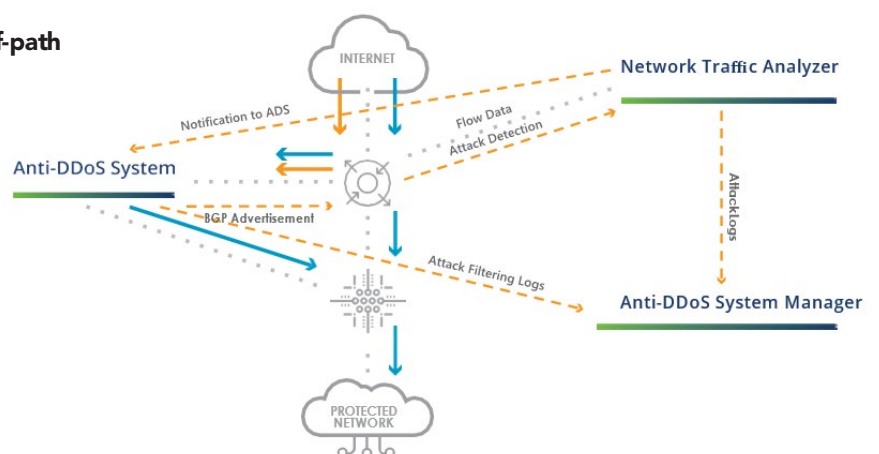
- » Virtual ADS KVM platform available

DEPLOYMENT OPTIONS

Inline Mode Diversion



Out-of-path Traffic



PERFORMANCE – ADS-SERIES

Model	ADSNX5-10000/12000	ADSNX5-HD8500	ADSNX5-8000
Mitigation Capacity	240Gbps/400Gbps 149,942,000pps/297,600,000pps	80Gbps 59,520,000pps	40Gbps 29,760,000pps
Interfaces	1*RJ45 Serial, 1*GE Copper, 1*USB 1*Extension slot	1*RJ45 Serial, 2*GE Copper, 2*USB, 4*Extension Slot	1*RJ45 Serial, 2*GE Copper, 2*USB, 4*Extension Slot
Optional Network Interface Modules for Extension Slot	2-ports 100GE CXP and 20-ports 10GE SFP+ 6-ports 100GE QSFP28 and 4-ports 40GE QSFP+ and 16*10GE SFP+ 16-ports 10GE SFP+ and 4-ports GE Copper	4-ports GE Copper 8-ports GE Copper 4-ports GE SFP 8-ports GE SFP 2-ports 10GE SFP+ 4-ports 10GE SFP+	8-ports GE Copper 8-ports GE SFP 2-ports 10GE SFP+
Dimensions (W*D*H)	19"x27"x10.5" 6 RU	17.4"x24.6"x3.5" 2 RU	17.4"x24.6"x3.5" 2 RU
Weight	121.25 lbs (55 kg)	46.29 lbs (21 kg)	36.38 lbs (16.5 kg)
Environmental	Operating: 32-113° F (0-45° C) Storage: -40-158° F (-40-70° C)	Operating: 32-104° F (0-40° C) Storage: -4-176° F (-20-80° C)	Operating: 41-104° F (5-40° C) Storage: 14-176° F (-10-80° C)
Power	AC/DC Five Power Supply (6000W total)	AC/DC Dual Power Supply (300W total)	AC/DC Dual Power Supply (500W total)
MTBF	52,879 hours	60,000 hours	45,000 hours

Model	ADSNX5-HD6500	ADSNX5-HD4500	ADSNX5-HD2500
Mitigation Capacity	40Gbps 29,760,000pps	20Gbps 14,880,000pps	4Gbps 2,976,000pps
Interfaces	1*RJ45 Serial, 2*GE Copper, 2*USB, 4*Extension Slot	1*RJ45 Serial, 2*GE Copper, 2*USB 4*Extension Slot	1*RJ45 Serial, 2*GE Copper, 2*USB 4*Extension Slot
Optional Network Interface Modules for Extension Slot	4-ports GE Copper 8-ports GE Copper 4-ports GE SFP 8-ports GE SFP 2-ports 10GE SFP+ 4-ports 10GE SFP+	4-ports GE Copper 8-ports GE Copper 4-ports GE SFP 8-ports GE SFP 2-ports 10GE SFP+ 4-ports 10GE SFP+	4-ports GE Copper 8-ports GE Copper 4-ports GE SFP 8-ports GE SFP 2-ports 10GE SFP+ 4-ports 10GE SFP+
Dimensions (W*D*H)	17.4"x20.7"x3.5" 2RU	17.13"x22"x1.7" 1RU	17.13"x22"x1.7" 1RU
Weight	44 lbs (20 kg)	21.2 lbs (9.6 kg)	21.2 lbs (9.6 kg)
Environmental	Operating: 32-104° F (0-40° C) Storage: -4-176° F (-20-80° C)	Operating: 32-104° F (0-40° C) Storage: 14-158° F (-10-70° C)	Operating: 32-104° F (0-40° C) Storage: 14-158° F (-10-70° C)
Power	AC/DC Dual Power Supply (300W total)	AC Dual Power Supply (300W total)	AC Dual Power Supply (300W total)
MTBF	60,000 hours	86,046 hours	86,046 hours

PERFORMANCE – VIRTUAL ADS

Host		Virtual ADS					
Item	Recommended Configuration	Item	Recommended Configuration				
CPU	Intel(R) Xeon(R) CPU E5-2687W v4 @ 3.00GHz	Hypervisor support	QEMU KVM 1.5.3 and above				
Memory	128G (at least 32GB free space)	Mitigation capacity	(@128bytes)	200M-2Gbps	10Gbps	20Gbps	40Gbps
Hard disk	1TB (at least 10GB free space)	Minimum Requirement	CPU Cores	4	6	14	32
Operation system	CentOS		Memory	16G	16G	16G	32G
1000M NIC support	I210, I350, 82571, 82576, 82580 (up to 8)		Storage	10GB at least			
10Gb NIC support	82599, X710/XL710 (up to 4)	License options	200M, 500M, 1G, 2G, 10G, 20G, 40G				
Virtual NIC support	NIC other than those above (cannot guarantee the capacity)						

MANTENHA SUA REDE PROTEGIDA COM QUEM MAIS ENTENDE DE CIBERSEGURANÇA

A **UPX** é uma empresa de tecnologia especialista em redes e segurança da informação. Pioneira na mitigação de **ataques DDoS** no país, possui uma rede global de **ampla conectividade** e **tecnologias próprias** para monitoramento, identificação, tratamento e prevenção de incidentes.

19

anos de
atuação

12 Tbps

capacidade de
mitigação

17

centros de
mitigação

+350

pontos de
presença

+1M

usuários protegidos
em tempo real

EDGE PROTECTION: DDOS DEFENSE **A MELHOR SOLUÇÃO CONTRA ATAQUES DDOS**

O **Edge Protection** é a ferramenta desenvolvida pela **UPX** para proteção de redes, com módulo avançado contra **ataques DDoS**. Confira os diferenciais:

- ▲ Uso de trânsito nacional
- ▲ Ação próxima da origem do ataque
- ▲ Menor latência do mercado
- ▲ Bloqueio de ataques em até 5 segundos
- ▲ Proteção sem limite de banda suja
- ▲ Sem aplicação de blackhole

EMPRESAS QUE CONFIAM NA UPX



BACKBONE ROBUSTO E HIPERCONECTADO

POPs, peerings e scrubbing centers nacionais e internacionais

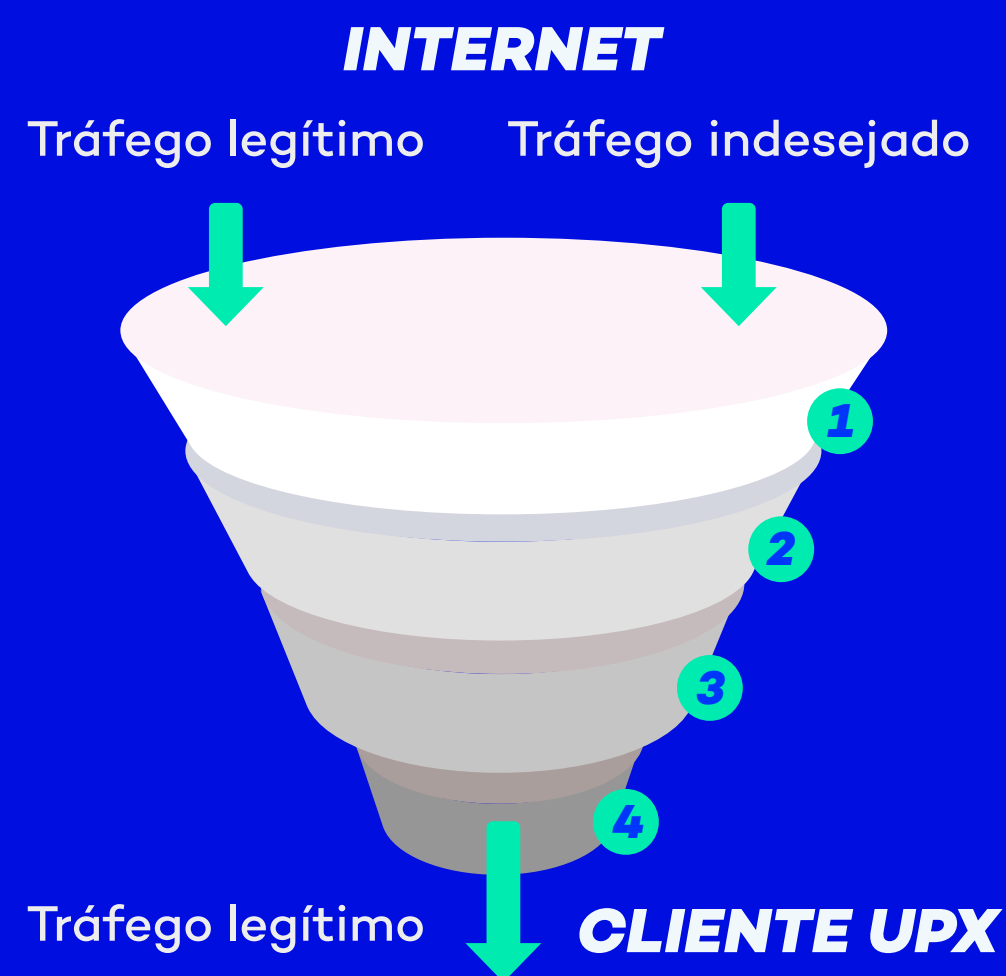


Scrubbing Centers

MELHORES ROTAS E AMPLA CONECTIVIDADE PARA GARANTIR ALTA PERFORMANCE E BAIXA LATÊNCIA

CAMADAS DE MITIGAÇÃO

- 1 Blocklist** Bloqueio baseado no IP de origem
- 2 Bloqueios padrões** Bloqueio baseado em padrões comuns de ataques
- 3 Análise de pacotes e contexto** Bloqueio com base em inspeção profunda de pacotes
- 4 Regras customizadas** Regras de filtragem criadas pelo cliente via dashboard



Mitigação **always-on** e com ação direta nas camadas 3, 4 e 7

Sem necessidade de hardware, toda a mitigação pode ser feita em **nuvem**

Dashboard com tráfego em tempo real, alertas, histórico de ataques e mais

Suporte com especialistas 24/7/365, tempo médio de resposta abaixo de **5 minutos**

**CLIQUE AQUI E FALE AGORA MESMO
COM NOSSOS ESPECIALISTAS**

Miami | São Paulo | Campinas upx.com
 comercial@upx.com + 55 19 3368 0609



Arbor Edge Defense is an Essential On-Premise DDoS Solution

Cloud DDoS services are great for mitigating large-scale volumetric attacks. But with the breadth and depth of today's DDoS attacks (volumetric, state-exhaustion, and application-layer) happening continuously, one single mitigation solution isn't adequate to protect business-critical services. A multi-layered approach combining on-premise surgical mitigation with intelligent signaling to large-scale cloud mitigation combines the best of both techniques, mitigating attacks of all types and ensuring business continuity.

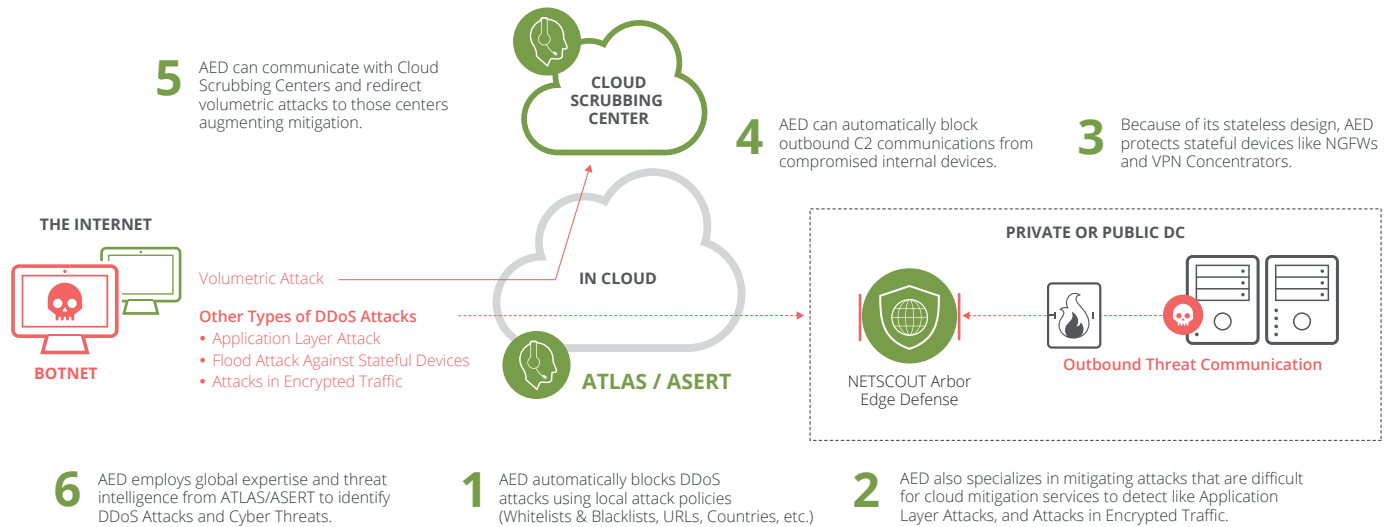
Challenge

As DDoS attacks continually become larger and more prevalent, cloud-based DDoS mitigation services have become popular choices for customers who need protection that can react quickly and scale effectively. These services commonly come from CDN providers, ISPs or ISP-agnostic DDoS protection services providers. Whether it's always-on or on-demand, cloud-based DDoS scrubbing services are a useful and necessary way of protecting your organization. To augment these cloud solutions, it is essential to add on-premise mitigation capacity to effectively combat all DDoS attacks.

Most DDoS attacks combine volume, application-layer, and state-exhaustion techniques to bring down their targets. Although cloud-mitigation solutions are typically used for stopping high-volume and some state-exhaustion attacks, some state-exhaustion and most application-layer DDoS attacks can go completely undetected when the volume is low, or the attack patterns are not identified and stopped by the cloud-based mitigation tools responsible for blocking the high-volume attacks. Beyond DDoS, any attacks actively targeting services, or malicious traffic from a potentially compromised host or other IoT still not only needs to be detected but stopped. On-premise mitigation is a necessary addition to cloud mitigation for protection of business-critical services.

Risk

Dangerous smaller attack traffic is still reaching your business-critical services and networks. That traffic could be state-exhaustion, application-layer attacks, or something even more dangerous such as attempts to compromise hosts or botnet-control messaging. Since cloud mitigation does little in stopping lower-volume attacks and isn't designed to detect or mitigate traffic based on IoTs and threats, your network and services are still vulnerable to both compromise and downtime.



Solution

Arbor Edge Defense® (AED) combines threat detection and DDoS-mitigation techniques to not only keep you informed of malicious traffic but block it. AED is on-premise, always-on, mitigating any attacks, which may not be detected by network-traffic-monitoring tools. With AED, there's no delta between the beginning of an attack and the mitigation. Since cloud-mitigation solutions are designed for high-volume attacks, pre-provisioned redirection might take several minutes while BGP-route updates occur. If you have to provision or manually redirect your traffic during an attack, the window of exposure is much longer. Having an on-premise mitigation solution like AED can assist in the mitigation of attack traffic getting through while redirection is taking place. In the event of a large volumetric attack detected at the network edge, AED's cloud-signaling features can intelligently communicate with a cloud-based mitigation service such as Arbor Cloud or one from your ISP. This feature allows mitigation to rapidly be redirected to the cloud as the volume increases. And everything is easily managed through the same interface.

And while BGP AS-PATH prefixes may direct most of your traffic through the cloud service provider, your ISP may still be sending some traffic straight to you due to BGP pathing preference or local preference configurations. Since AED is always on and on-premise, it sees all attack traffic — even traffic missed by cloud mitigation. Even your GRE endpoint can be protected by AED.

Lastly, AED utilizes threat intelligence from the Atlas Intelligence Feed (AIF) to identify and block IoCs, providing the most mitigation and security available both during an attack and even during peacetime.

By combining cloud mitigation such as Arbor Cloud or your ISP with on-premise mitigation with AED, you have the most comprehensive protection available from massive volumetric attacks, subtle state-exhaustion or application-layer DDoS attacks while blocking hostile traffic with IoCs.

"Yes our Provider Cloud Mitigation is always-on, but not always mitigating based on their model. If an attack is detected there is a time delta between the detection and mitigation. From this point of view NETSCOUT has a critical role to always mitigate and protect during the delta."

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **00546-10-01086**

Validade: **Indeterminada**

Emissão: **26/04/2010**

Requerente:

CNPJ: 00.028.666/0001-58

CISCO DO BRASIL LTDA.

Fabricante:

CISCO SYSTEMS, INC.

170 WEST TASMAN DRIVE

Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC 6293/10, emitido pelo **Associação NCC Certificações do Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Equipamento para Interconexão de Redes - III

Modelo - Nome Comercial (s):

Cisco 1900 Series - (Cisco 1900 Series)

Características técnicas básicas:

Módulos de interfaces disponíveis: **E1 (120 Ohms)**

Observações

Outros módulos de interface e protocolos de sinalização, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Maximiliano Salvadori Martinhao
Gerente Geral de Certificação e Engenharia do Espectro

Cisco 2900 Series Integrated Services Routers

Cisco® 2900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings. The Integrated Services Routers Generation 2 platforms are future-enabled with multi-core CPUs, support for high capacity DSPs (Digital Signal Processors) for future enhanced video capabilities, high powered service modules with improved availability, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS® Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation which can quickly adapt to evolving network requirements. Overall, the Cisco 2900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market leading security, unified communications, wireless, and application services.

Figure 1. Cisco 2900 Series Integrated Services Routers



Product Overview

Cisco 2900 Series builds on the best-in-class offering of the existing Cisco 2800 Series Integrated Services Routers by offering four platforms (Figure 1): the Cisco 2901, 2911, 2921, and 2951 Integrated Services Routers.

All Cisco 2900 Series Integrated Services Routers offer embedded hardware encryption acceleration, voice- and video-capable Digital Signal Processor (DSP) slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. In addition, the platforms support the industries widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper and fiber GE.

Key Business Benefits

The Integrated Services Routers Generation 2 (ISR G2) provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs. Table 1 lists the business benefits of the Cisco 2900 Series.

Table 1. Key Business Benefits of the Cisco 2900 Series Integrated Services Routers

Benefits	Description
Services Integration	• The Cisco 2900 Series ISRs offer increased levels of services integration with voice, video, security, wireless, mobility, and data services, enabling greater efficiencies and cost savings.
Services On Demand	• A single Cisco IOS® Software Universal image is installed on each ISR G2. The Universal image contains all of the Cisco IOS technology sets which can be activated with a software license. This allows your business to quickly deploy advanced features without downloading a new IOS image. Additionally, larger default memory is included to support the new capabilities. • The Cisco Services Ready Engine (SRE) enables a new operational model which allows you to reduce capital expenditures (CapEx) and deploy a variety of application services as needed on a single integrated compute services module.
High Performance with Integrated Services	• The Cisco 2900 Series enables deployment in high speed WAN environments with concurrent services enabled up to 75 Mbps. • A MultiGigabit Fabric (MGF) enables high-bandwidth module-to-module communication without compromising routing performance.
Network Agility	• Designed to address customer business requirements, the Cisco 2900 Series modular architecture offers increased capacity and performance as your network needs grow. • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy Efficiency	• The Cisco 2900 Series architecture provides energy-saving features that include the following: ◦ The Cisco 2900 Series offers intelligent power management and allows the customer to control power to the modules based on the time of day. Cisco EnergyWise technology will be supported in the future. ◦ Services integration and modularity on a single platform performing multiple functions, optimizes raw materials consumption and energy usage. ◦ Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the total cost of ownership, including materials and energy use. ◦ High efficiency power supplies are provided with each platform.
Investment Protection	• The Cisco 2900 Series maximizes investment protection: ◦ Reuse of a broad array of existing modules supported on the original Integrated Services Routers provides a lower cost of ownership. ◦ A rich set of Cisco IOS Software features carried forward from the original Integrated Services Routers and delivered in a single universal image. ◦ Flexibility to adapt as your business needs evolve.

Platform Architecture and Modularity

The Cisco 2900 Series is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support increasing bandwidth requirements, Time-Division Multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 2900 Series.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular Platform	• The Cisco 2900 Series ISRs are highly modular platforms with several types of module slots to add connectivity and services for varied branch-office network requirements. • The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades for future technologies without requiring a platform replacement.
Processors	• The Cisco 2900 Series are powered by high-performance multi-core processors that can support the growing demands of high-speed WAN connections to the branch-office while also running multiple concurrent services.
Embedded IP Security (IPSec) VPN Hardware Acceleration	• Embedded hardware encryption acceleration is enhanced to provide higher scalability, which combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (IPSec acceleration). • The onboard encryption hardware replaces and outperforms the Advanced Integration Modules (AIMs) of previous generations.
Multigigabit Fabric (MGF)	• The Cisco 2900 Series introduces an innovative Multi Gigabit Fabric (MGF) that allows for efficient module-to-module communication, enabling tighter services interactions across modules while reducing the overhead on the route processor.

Architectural Feature	Benefits
TDM Interconnectivity Fabric	Unified communications services in the branch office are significantly enhanced with the use of a TDM interconnectivity fabric in the system architecture, allowing for scaling of DS-0 channel capacity.
Integrated Gigabit Ethernet Ports	- All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN routed ports. - One of the three 10/100/1000 Ethernet WAN ports on the Cisco 2921 and 2951 supports Small Form-Factor Pluggable (SFP)-based connectivity in lieu of a RJ-45 port and enabling fiber connectivity.
Innovative Universal-Serial-Bus (USB)-Based Console Access	- A new, innovative USB console port offers management connectivity for devices without a serial port such as modern laptop computers. - Traditional console and auxiliary ports are also available.
Optional Integrated Power Supply for Distribution of PoE and Universal DC Power Supply	- An optional upgrade to the internal power supply provides inline power (802.3af-compliant PoE and Cisco Inline Power) to integrated switch modules. - On the Cisco 2911, 2921, and 2951, an optional DC power supply is available that extends deployment into central offices and industrial environments. - On the Cisco 2911, an optional DC-PoE power supply is available.
Optional External Redundant Power Supply (RPS)	- The Cisco 2911, 2921, and 2951 allow for power redundancy through the use of an external RPS device, thereby decreasing network downtime and protecting the network from power-supply failures. - Redundant power on the Cisco 2900 Series is supported through the Cisco RPS 2300 Redundant Power System. You can use the Cisco RPS 2300 to provide redundant power for Cisco 2900 Series ISRs as well as Cisco Catalyst® switches. - In order to use the Cisco RPS 2300, an external RPS adapter is required (configurable option) to connect the platform to the external RPS.
PoE Boost	When connected to an external RPS device, the Cisco 2911, 2921, and 2951 can operate in a PoE boost configuration in lieu of redundant power mode - whereby the power capacity of the platform is increased to twice the normal level to power additional PoE ports.
Designed for Flexible Deployments	- The Cisco 2911 and 2951 are designed for NEBS environments. - The 2911 is 12" deep and has an optional fan filter for deployments in a variety of environments. An assembly that provides front-to-back airflow is also available for 23" racks.

Modularity Features and Benefits

The Cisco 2900 Series provides significantly enhanced modular capabilities (refer to Table 3) offering investment protection for customers. Most of the modules available on previous generations of Cisco routers, such as the Cisco 2800 Series, are supported on the Cisco 2900 Series. Additionally, modules can be used on other supported Cisco platforms to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

A complete list of supported modules, including a list of supported SFPs for the Cisco 2900 Series, is available at: <https://www.cisco.com/go/2900>.

Table 3. Modularity Features and Benefits

ISR Modules	Benefits
Cisco Service Module 	- Each service module slot offers high-data-throughput capability: - Up to 4 Gbps aggregate toward the route processor. - Up to 2 Gbps aggregate to other module slots over MGF. - Service Module (SM) slots are highly flexible with support for double-wide service modules (SM-Ds), which are Service Modules that require two SM slots. SM-Ds in the Cisco 2921 and 2951 provide flexibility for higher-density modules. - A service module slot replaces the network module and the extension module for voice/fax (EVM) slots and is offered on Cisco 2911, 2921, and 2951 ISRs. - An adapter module enables backward compatibility with existing network modules, enhanced Network Modules (NMEs), and EVMs. - Service module slots provide twice the power capabilities relative to the network-module slots, allowing for flexibility for higher-scale and better-performance modules. - Power to service module slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.

ISR Modules	Benefits
Cisco Enhanced High-Speed WAN Interface Card (EHWIC) 	• The EHWIC slot provides enhancements to the prior generation's high-speed WAN interface card (HWIC) slots while provide maximum investment protection by natively supporting HWICs, WAN Interface Cards (WICs), Voice Interface Cards (VICs), and Voice/WAN interface cards (VWICs). • Four integrated EHWIC slots on the Cisco 2901, 2911, 2921, and 2951 allow for more flexible configurations. • Each HWIC slot offers high-data-throughput capability: ◦ Up to 1.6 Gbps aggregate toward the route processor. ◦ Up to 2 Gbps aggregate to other module slots over the MGF. • Flexibility to support double-wide modules is enabled by combining two EHWIC slots. Up to 2 doublewide HWIC (HWIC-D) modules are supported.
Cisco Internal Services Module (ISM) 	• A single ISM slot provides flexibility to integrate intelligent service modules on an internal slot within the chassis • Each ISM slot offers high-data-throughput capability: ◦ Up to 4 Gbps aggregate toward the route processor. ◦ Up to 2 Gbps aggregate to other module slots over the MGF. • The ISM replaces the AIM slot; existing AIM modules are not supported in the ISM slot. • Power to ISM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Cisco High-Density Packet Voice Digital Signal Processor (DSP) Module (PVDM3) Slots on Motherboard 	• PVDM3 slots natively support PVDM3 modules, providing support for richer density for rich-media voice and video. • Each PVDM3 slot connects back to the system architecture through a 2 Gbps aggregate link through the MGF. • Investment protection for PVDM2 modules is supported through an adapter module. • Power to the PVDM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Compact Flash Slots	• Two external Compact Flash slots are available on the Cisco 2900 Series Integrated Services Routers. Each slot can support high-speed storage densities upgradeable to 4 GB in density.
USB 2.0 Ports	• Two high-speed USB 2.0 ports are supported. The USB ports enable secure token capabilities and storage.

Cisco IOS Software

Cisco 2900 Series Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, the Integrated Services Routers Generation 2 platforms are supported on Cisco IOS Software releases 15M&T. Release 15.0(1)M is available immediately and provides support for a comprehensive portfolio of Cisco technologies, including the functionality and features delivered in releases 12.4 and 12.4T. New innovations in 15.0(1)M span multiple technology areas, including security, voice, high availability, IP Routing and Multicast, Quality of Service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all IOS technology feature sets is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Four major technology licenses are available on the Cisco 2900 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at <https://www.cisco.com/go/sa>. The four licenses are as follows:

- IP Base: This technology package is available as default.
- Data
- Unified Communications
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

For additional information and details about Cisco IOS Software licensing and packaging on Cisco 2900 Series Integrated Services Routers, please visit <https://www.cisco.com/go/2900l>.

Cisco ONE Software

Cisco ONE™ Software offers a valuable and flexible way to buy software for the WAN, access, and data center domains. At each stage in the product lifecycle, Cisco ONE Software helps make buying, managing, and upgrading your network and infrastructure software easier. Cisco ONE Software provides:

- Flexible licensing models to smoothly distribute customers' software spending over time
- Investment protection for software purchases through software services-enabled license portability
- Access to updates, upgrades, and new technology from Cisco through Cisco® Software Support Services (SWSS)

Cisco ONE for WAN gives organizations broad capabilities for branch offices and the enterprise edge. Cisco ONE Foundation for WAN connects and secures your branch office while optimizing for cost. Cisco ONE WAN Collaboration integrates voice and video into your branch office and network edge.

Key Branch-Office Services

The Cisco Integrated Services Routers are industry-leading platforms that offer unprecedented levels of services integration. Designed to meet the requirements of the branch office, these platforms provide a complete solution with voice, video, security, mobility and application services. Businesses enjoy the benefit of deploying a single device that meets all their needs, reducing capital and operational expenses.

Unified Communications, Collaboration, and Voice-Gateway Services

The Cisco 2900 Integrated Services Router is the foundation for collaboration in the small and midsize branch office, serving as a critical component of a Cisco's video architecture (Medianet) and enterprise Unified Communications solution. With embedded voice services and a wide range of supported telephony interfaces, the Cisco 2900 Series delivers maximum deployment flexibility for the distributed enterprise. Unified communications is enabled through a rich signaling and media-processing infrastructure, including a variety of protocols, media interworking, signal and media security, transcoding, conferencing, and QoS. Cisco Integrated Services Routers also feature a wide range of voice-gateway interfaces, supporting a broad array of signaling and physical network interfaces.

The Cisco 2900 Series enables a full range of existing and emerging video services, with scaling improvements to support Cisco TelePresence® conferencing, security, and session control. The Cisco Unified Border Element extends these capabilities for business-to-business TelePresence communications. The Cisco 2900 Series adds support for the new Cisco High-Density Packet Voice Digital Signal Processor (DSP) Module (PVDM3), which has been optimized for voice and video support. The new PVDM3 modules support all voice-gateway functions of earlier generations of PVDMs and add higher density and more processing power to support emerging rich-media applications. The Cisco 2900 Series provides 2 or 3 onboard PVDM3 slots, depending on the platform.

Cisco Unified Communications Manager Express and Survivable Remote Site Telephony

The Cisco Integrated Services Routers natively provide optional unified communications services within the Cisco IOS Software, minimizing the IT hardware footprint and total cost of ownership at the branch office. Cisco Unified Communications Manager Express (CME) provides a broad range of IP Private-Branch-Exchange (PBX) and key-system features integrated into the router for the small and midsize branch office. Cisco Survivable Remote Site Telephony (SRST), also inherently available in Cisco IOS Software, and an option on the Cisco 2900 Series, helps ensure that branch-office employees have uninterrupted telephony services and features, even if the connection to a centralized Cisco Unified Communications Manager is disrupted.

Coupled with Cisco Unity® Express, the integrated solution for voicemail, Automated Attendant, and Interactive Voice Response (IVR), the Cisco 2900 Series offers the branch office a complete range of unified communications services while delivering industry-leading security within a single platform.

VoiceXML Application Services

The Cisco 2900 Series also supports standards-certified VoiceXML browser services. VoiceXML is an open-standard markup language used to create voice-enabled web browsers and IVR applications. Just as HTML enables you to retrieve data with a PC, VoiceXML enables you to retrieve data using voice or Dual-Tone-Multi-Frequency (DTMF) telephony input. The Cisco 2900 Series can deliver a much higher range of concurrent voice-gateway services combined with VoiceXML browser services, for up to 200 sessions on the Cisco 2951.

Cisco Unified Border Element

The Cisco Unified Border Element capabilities supported on the Cisco 2900 Series address the emerging requirements in an IP-centric interconnect for branch-office unified communications between enterprises and service provider networks. Cisco Unified Border Element provides intelligent border-element functions such as physical and logical ingress and egress demarcation points, signaling and media control, and consolidated security and management features. The Cisco 2900 Series supports higher scale than previously provided on the Cisco 2800 Series, up to three times the number of sessions.

Integrated Network Security for Data, Voice, Video, and Mobility

Security is essential to protect a business' intellectual property while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources. As part of the Cisco' SAFE architectural framework that allows organizations to identify, prevent, and adapt to network security threats, the Cisco 2900 Series Integrated Services Routers facilitate secure business transactions and collaboration.

The Cisco IOS Software Security technology package for the Cisco 2900 Series offers a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks. The Cisco 2900 Series offers onboard hardware-based encryption acceleration to provide greater IPSec throughput with less overhead for the route processor when compared with software-based encryption solutions. Cisco Integrated Services Routers offer a comprehensive and adaptable security solution for branch offices that includes features such as:

- **Secure connectivity:** Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN
- **Integrated threat control:** Responding to sophisticated network attacks and threats using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, Cisco IOS Content Filtering, and Flexible Packet Matching (FPM)
- **Identity management:** Intelligently protecting endpoints using technologies such as Authentication, Authorization, and Accounting (AAA) and Public Key Infrastructure (PKI)

Detailed information about the security features and solutions supported on the Cisco 2900 Series is available at <https://www.cisco.com/go/routersecurity>.

Wireless and Mobility Services

Wireless LAN/WAN

The Cisco Integrated Services Routers supporting the Cisco Unified Wireless Architecture enable deployment of secure, manageable Wireless LANs (WLANs) optimized for remote sites and branch offices, including fast secure mobility, survivable authentication, and simplified management. The Cisco Wireless LAN Controller Module on the Cisco 2900 Series allows Small and Medium-sized Businesses (SMBs) and enterprise branch offices to cost-effectively deploy and manage secure WLANs. Cisco Wireless LAN Controllers work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide WLAN functions, managing up to 6, 12, and 25 access points.

Wireless WAN

Cisco Third-Generation (3G) Wireless WAN (WWAN) modules combine traditional enterprise router functions, such as remote management, advanced IP services such as Voice over IP (VoIP), and security, with mobility capabilities of 3G WAN access. Using high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, Frame Relay, and ISDN. Cisco 3G solutions support 3G standards High-Speed Packet Access (HSPA) and Evolution Data Only/Evolution Data Optimized (EVDO) providing you with a true multipath WAN backup and the ability to rapidly deploy primary WAN connectivity. For more information about 3G solutions on Cisco Integrated Services Routers, please visit <https://www.cisco.com/go/3g>.

Integrated LAN Switching

The Cisco 2900 Integrated Services Routers (Cisco 2911 through Cisco 2951) support the new Cisco Enhanced EtherSwitch® Service Modules, which greatly expand router capabilities by integrating industry-leading Layer 2 or Layer 3 switching with feature sets identical to those found in the Cisco Catalyst 2960 and Catalyst 3650-E Series Switches performing local line-rate switching and routing.

The new Cisco Enhanced EtherSwitch Service Modules take advantage of the increased power capabilities on the Cisco 2900 ISRs. Additionally, the Cisco Enhanced EtherSwitch modules enable the newest Cisco power initiatives, Cisco EnergyWise, Cisco Enhanced Power over Ethernet (ePoE), per-port PoE power monitoring, and RPS-enabled PoE boost. These technologies allow you to meet increased endpoint power requirements without increasing the total power consumption of the branch.

Application Services

As organizations continue to centralize and consolidate their branch-office IT infrastructure in an effort to reduce cost and complexity, they are challenged to provide an excellent user experience, ensure continuous service availability, and deliver business-relevant applications when and where they are needed. To address these challenges, the Cisco 2900 Series provides the capability to host Cisco, third-party, and custom applications on a portfolio of high-performance Cisco Services Ready Engine (SRE) modules that transparently integrate into the router. The modules have their own processors, storage, network interfaces, and memory that operate independently of the host router resources, helping to ensure maximum concurrent routing and application performance while reducing physical space requirements, lowering power consumption, and consolidating management.

Application Acceleration

The Cisco 2900 Series seamlessly combines industry leading security, IOS-based traffic control and visibility, with Cisco application acceleration solutions. Cisco IOS Software features such as NBAR, IP SLA, and NetFlow provide visibility and monitoring of traffic patterns and application performance while IOS features such as QoS, ACLs, and PfR intelligently control the traffic to maximize the quality of the user experience and employee productivity. The user experience can be further enhanced through the addition of a Cisco WAAS Network Module which can be used to securely provide more advanced WAN optimization techniques such as TCP optimization, caching, compression, and application acceleration. Cisco Integrated Services Routers combined with Cisco WAAS Network Modules, provide optimal performance for applications delivered from a central data center to branch-office users. The solution allows you to consolidate costly server, storage, and backup infrastructure into data centers while maintaining LAN-like service levels for remote users.

Cisco Services Ready Engine

The Cisco Services Ready Engine solution is available in a Service Module (SM) and Internal Service Module (ISM) form factor. The Service Module hardware offers up to a seven times performance improvement over the previous generation Network Modules and provides a multi-core x86-64 processor. The SRE modules also support up to 1 terabyte of storage, RAID configurations, hardware-assisted virtualization and cryptography options. The Cisco SRE module enables on-demand provisioning of branch-office applications on the Cisco 2900 Series platforms so that you can deploy the right application, at the right time, in the right place. The hardware and software decoupling provided by the service-ready deployment model enables applications to be provisioned on the module at the time of its installation or remotely anytime thereafter. Supported solutions include Cisco Wide Area Application Services (WAAS), Cisco Unity Express, Cisco Application Extension Platform (AXP), Cisco Wireless LAN Controller (WLC), Cisco Video Surveillance, and other applications under development. The Service Ready Engine enables organizations of various sizes to future-proof their network by allowing them to quickly deploy new branch-office applications without deploying new hardware, reducing the cost of rolling out branch-office services.

WAAS Express

Organizations today face several unique wide area network (WAN) challenges: the need to provide employees with constant access to centrally located information, the requirement to continuously back up and replicate mission-critical data to centrally managed data centers, the desire to provide satisfactory experience for IP phone and video communication, and the mandate to control bandwidth costs without sacrificing application availability and performance.

Cisco WAAS Express is designed to help organizations address these challenges. Cisco WAAS Express extends the [Cisco WAAS product portfolio](#) with a small-footprint, cost-effective IOS-based software solution integrated into the ISR G2 to offer bandwidth optimization and application acceleration capabilities. Cisco WAAS Express increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure. Cisco WAAS Express is unique in providing network transparency, improving deployment flexibility with on-demand service enablement, and integrating with native IOS-based services such as security, NetFlow, and QoS.

Cisco WAAS Express is fully interoperable with WAAS on SM-SRE modules, WAAS appliances and can be managed by a common WAAS Central Manager.

Cisco WAAS Express is available in IOS from version 15.1(2)T1.

Further information on Cisco WAAS Express can be found at <https://www.cisco.com/en/US/products/ps11211/index.html>.

Medianet for 2900 ISRs

As video becomes pervasive in an organization and more video devices are used, new demands are placed on the network. It can be challenging to accommodate video needs while reducing complexity, planning for capacity, and providing the best possible user experience.

Smarter Network, Endpoints, and Services

Traditional IP networks need to evolve to medianets to accommodate these changes. A medianet is an end-to-end IP architecture that helps to enable pervasive media experiences.

The medianet architecture includes a smarter network, smarter endpoints, shared media services, cloud services, and shared media services.

More Medianet Benefits

A medianet reduces total cost of ownership and scales video through features such as auto-configuration and media monitoring. At the same time, it helps to ensure a quality user experience while optimizing bandwidth use and efficiency.

For more information on Medianet for 2900ISR, please go to <https://www.cisco.com/en/US/netsol/ns1094/index.html>.

Managing Your Integrated Services Routers

Network management applications are instrumental in lowering operating expenses (OpEx) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end-to-end network. Day-one device support provides immediate manageability support for the Integrated Services Router, enabling quick and easy deployment, monitoring, and troubleshooting from Cisco and third-party applications.

Organizations rely on Cisco, third-party, and in-house developed network management applications to achieve their OpEx and productivity goals. Underpinning those applications are the embedded management features available in every Integrated Services Router. The new Integrated Services Routers continue a tradition of broad and deep manageability features such as IP Service-Level Agreement (IP SLA), Cisco IOS Embedded Event Manager (EEM), and NetFlow which allow you to know the status of your network at all times. These features, along with Simple Network Management Protocol (SNMP) and syslog, enable your organization's management applications.

Refer to Tables 4 and 5 below for details about network management and manageability support on Cisco 2900 Series Integrated Services Routers.

Table 4. Cisco 2900 ISR G2 Series IOS Software Features and Protocols Support

Feature	Support
Protocols	IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPsec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Encapsulation	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic Management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS software refer to the Feature Navigator tool at <https://www.cisco.com/go/fn>.

Table 5 lists the embedded management features available with Cisco IOS Software.

Table 5. Embedded Management Features Available with Cisco IOS Software

Feature	Description
WSMA	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML-based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
EEM	Cisco IOS Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
IPSLA	Cisco IOS IP Service-Level Agreements (SLAs) enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video in an IP network.
SNMP , RMON , Syslog , NetFlow , and TR-069	Cisco 2900 Series Integrated Services Routers also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.

The Cisco network management applications listed in Table 6 are standalone products that you can download or purchase to manage your Cisco network devices. The applications are built specifically for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Applications

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers. This tool simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through easy-to-use wizards.
Network-wide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco Integrated Services Routers, using new instrumentation such as Cisco IOS EEM Generic Online Diagnostics (GOLD). In addition to supporting basic platform services of the Integrated Services Router, CiscoWorks also provides added-value support for the Cisco Services Ready Engine, enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.
Network-wide staging, configuration, and compliance	CiscoWorks NCM	CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Voice configuration and provisioning	Cisco Unified Provisioning Manager	Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	Easily manage Cisco IOS Software activation and licenses for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager.
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

Summary

As your business strives to lower the total cost of ownership in running your network and increase your overall employee productivity with more centralized and collaborative network applications, you will need more intelligent branch-office solutions. The Cisco 2900 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 2900 Series is designed to consolidate the functions of many separate devices into a single, compact system.

Table 7. Cisco 2900 Integrated Services Router Product Specifications

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Services and Slot Density				
Embedded Hardware-Based Cryptography and Acceleration	Yes	Yes	Yes	Yes
Cisco Unified SRST Sessions	35	50	100	250

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Cisco Unified CCME Sessions	35	50	100	150
Total Onboard WAN 10/100/1000 Ports	2	3	3	3
RJ-45-Based Ports	2	3	3	3
SFP-Based Ports (use of SFP port disables the corresponding RJ-45 port)	0	0	1	1
Service Module Slots	0	1	1	2
Double-Wide Service Module Slots (use of a double-wide slot will occupy all single-wide service module slots in a 2900)	0	0	1	1
EHWIC Slots	4	4	4	4
Double-Wide EHWIC Slots (use of a double-wide EHWIC slot will consume two EHWIC slots)	2	2	2	2
ISM Slots	1	1	1	1
Onboard DSP (PVDM) Slots	2	2	3	3
Memory DDR2 ECC DRAM - Default	512 MB	512 MB	512 MB	512 MB
Memory (DDR2 ECC DRAM) - Maximum	2 GB	2 GB	2 GB	2 GB
Compact Flash (External) - Default	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none
Compact Flash (External) - Maximum	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB
External USB 2.0 Flash Memory Slots (Type A)	2	2	2	2
USB Console Port (Type B) (up to 115.2 kbps)	1	1	1	1
Serial Console Port	1	1	1	1
Serial Auxiliary Port	1	1	1	1
Power-Supply Options	AC and PoE	AC, PoE, and DC	AC, PoE, and DC	AC, PoE, and DC
RPS Support (External)	No	Cisco RPS 2300	Cisco RPS 2300	Cisco RPS 2300
Power Specifications				
AC Input Voltage	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging
AC Input Frequency	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz
AC Input Current Range AC Power Supply (Maximum)	1.5 to 0.6A	2.2 to 1.0A	3.4 to 1.4A	3.4 to 1.4A
AC Input Surge Current	<50A	<50A	<50A	<50A
Typical Power (No Modules) (Watts)	40	50	60	70
Maximum Power with AC Power Supply (Watts)	150	210	320	340
Maximum Power with PoE Power Supply (Platform Only) (Watts)	175	250	370	405
Maximum Power with DC-PoE Power Supply (Platform Only) (Watts)	-	140	-	-
Maximum End-Point PoE Power Available from AC PoE Power Supply (Watts)	130	200	280	370

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Maximum End-Point PoE Power Available from DC PoE Power Supply (Watts)	-	160	-	-
Maximum End-Point PoE Power Capacity with PoE Boost (Watts)	N/A	750	750	750
DC Input Voltage	N/A	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative
DC Input Current	N/A	(MAX) 8A (24V) 3.5A (60V)	(MAX) 12A (24V) 5A (60V)	(MAX) 12A (24V) 5A (60V)
Physical Specifications				
Dimensions (H x W x D)	1.75 x 17.25 x 17.3 in. (44.5 x 438.2 x 439.4 mm)	3.5 x 17.25 x 12 in. (88.9 x 438.2 x 304.8 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)
Rack Height	1RU (rack unit)	2RU	2RU	2RU
Rack-Mount 19 in. (48.3 cm) EIA	Included	Included	Included	Included
Rack-Mount 23 in. (58.4 cm) EIA	Optional	Optional	Optional	Optional
Wall-Mount (refer to installation guide for approved orientation)	Yes	Yes	No	No
Weight with AC Power Supply (No Modules)	13.4 lb (6.1 kg)	18 lb (8.2 kg)	29 lb (13.2 kg)	29 lb (13.2 kg)
Weight with AC PoE Power Supply (No Modules)	14.3 lb (6.5 kg)	19 lb (8.6 kg)	30 lb (13.6 kg)	30 lb (13.6 kg)
Typical Weight Fully Configured	16 lb (7.3 kg)	21 lb (9.5 kg)	34 lb (15.5 kg)	34 lb (15.5 kg)
Airflow	Front to side	Side to side	Back and Side to Front	Back and Side to Front
Optional Airflow Kit	N/A	Front to back	N/A	N/A
Environmental Specifications				
Operating Conditions				
Temperature: 5,906 feet (1,800m) Maximum Altitude	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: 9,843 feet (3,000m) Maximum Altitude	32 to 77°F (0 to 25°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: 13,123 feet (4,000m) Maximum Altitude	N/A	32 to 86°F (0 to 30°C)	32 to 86°F (0 to 30°C)	32 to 86°F (0 to 30°C)
Temperature: Short-Term (per NEBS) 5906 feet (1,800m) Maximum Altitude	N/A	23°F to 122°F (-5 to 50°C)	N/A	23°F to 122°F (-5 to 50°C)
Altitude	10,000 ft (3,000m)	13,000 ft (4,000m)	10,000 ft (3,000m)	13,000 ft (4,000m)
Relative Humidity	10 to 85%	5 to 85%	10 to 85%	5 to 85%
Short-Term (per NEBS) Humidity	N/A	5% to 90%, but not to exceed 0.024 kg water/kg of dry air	N/A	N/A
Acoustic: Sound Pressure (Typical/Maximum)	41/53 dBA	51.8/62.9 dBA	54.4/67.4 dBA	54.4/67.4 dBA
Acoustic: Sound Power (Typical/Maximum)	49/61 dBA	58.5/70.3 dBA	62.6/74.5 dBA	62.6/74.5 dBA
Non-Operating Conditions				
Temperature	-40 to 158°F (-40 to 70°C)	-40 to 176°F (-40 to 80°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)
Relative Humidity	5 to 95%	5 to 95%	5 to 95%	5 to 95%
Altitude	15,000 ft (4,570m)	15,000 ft (4,570m)	15,000 ft (4,570m)	15,000 ft (4,570m)

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Regulatory Compliance				
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive

Supported Modules

The Cisco 2900 Series supports a wide range of modules that span industry-leading breadth of services at the branch office. For a list of modules supported on the Cisco 2900 Series, please visit:

https://www.cisco.com/en/US/products/ps10537/products_relevant_interfaces_and_modules.html

Ordering Information

The Cisco 2900 Series Integrated Services Routers are orderable and shipping. For information about how to order the Cisco 2900 Series, please visit the Cisco 2900 Series Ordering Guide. To place an order, visit the [Cisco Ordering Home Page](#) and refer to Table 8, which provides basic ordering information. For additional product numbers, including the Cisco 2900 Series bundle offerings, please check the [Cisco 2900 Series Integrated Services Router Price List](#) or contact your local Cisco account representative.

Table 8. Cisco 2900 Series Basic Ordering Information

Product Name	Product Description
CISCO2901/K9	Cisco 2901 with 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
CISCO2911/K9	Cisco 2911 with 3 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
CISCO2921/K9	Cisco 2921 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
CISCO2951/K9	Cisco 2951 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
SL-29-DATA-K9	Data License for Cisco 2901-2951
SL-29-UC-K9	Unified Communications License for Cisco 2901-2951
SL-29-SEC-K9	Security License for Cisco 2901-2951

[Cisco ONE Software for WAN](#) is available for the ISR 2900.

Cisco ONE Software offers a complete solution that delivers an optimal experience over any connection while helping you get the most from your WAN investment with secure, fault-tolerant connectivity.

Benefits:

- Connect branch offices and your campus securely at an optimal cost by improving application performance through application protocol acceleration and optimization techniques that offload the WAN.
- Integrate voice and video across branch offices and your campus to increase productivity.

For ordering information for Cisco ONE Software for the ISR 2900, go to

<https://www.cisco.com/c/en/us/products/software/one-wan/wan-part-numbers.html>.

Cisco Integrated Services Router Migration Options

Cisco 2900 Series Integrated Services Routers are included in the standard Cisco Technology Migration Program (TMP). Refer to <https://www.cisco.com/go/tmp> and contact your local Cisco account representative for program details.

Warranty Information

The Cisco 2900 Series Integrated Services Routers have a ninety (90) day limited liability warranty.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, please visit <https://www.cisco.com/go/services>.

Cisco SMARTnet[®] technical support for the Cisco 2900 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- 24-hour access to the industry's largest dedicated technical support staff

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº 00547-10-01086

Validade: Indeterminada

Emissão: 12/06/2012

Requerente:

CNPJ: 00.028.666/0001-58

CISCO DO BRASIL LTDA.

Fabricante:

CISCO SYSTEMS, INC.

170 WEST TASMAN DRIVE

Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC 6298/10, emitido pelo **Associação NCC Certificações do Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Equipamento para Interconexão de Redes - III

Modelo - Nome Comercial (s):

Cisco 2900 Series - (Cisco 2900 Series)

Características técnicas básicas:

Módulos de interfaces disponíveis: E1 (120 Ohms), FXO e FXS.

Observações

Outros módulos de interface e protocolos de sinalização, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.
Este certificado substitui o de mesmo número emitido em 26/04/2010.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente Geral de Certificação e Engenharia do Espectro

Overview

The Cisco 3925 router, modular Services Performance Engine (SPE) 100, which can be upgraded for even higher performance as next-generation WAN environments evolve.

Quick Specs

Figure 1 shows the appearance of the CISCO3925/K9.



Table 1 shows the Quick Specs of the CISCO3925/K9.

Product Code	CISCO3925/K9
Services Performance Engine module	w/SPE 100
Rack Units	3U
Interfaces	3 integrated 10/100/1000 Ethernet ports with 2 ports capable of RJ-45 or SFP connectivity
Expansion Slot(s)	2 service module slots 1 Internal Services Module slot 4 onboard digital signal processor (DSP) slots 4 Enhanced High-Speed WAN Interface Card (EHWIC) slots
RAM	1 GB (installed) / 2 GB (max)
Flash Memory	256 MB (installed) / 8 GB (max)
Dimensions	47.6 cm x 43.8 cm x 13.3 cm
Package Weight	27.78 Kg

Product Details

Figure 2 shows the front panel of the Cisco 3925 router.



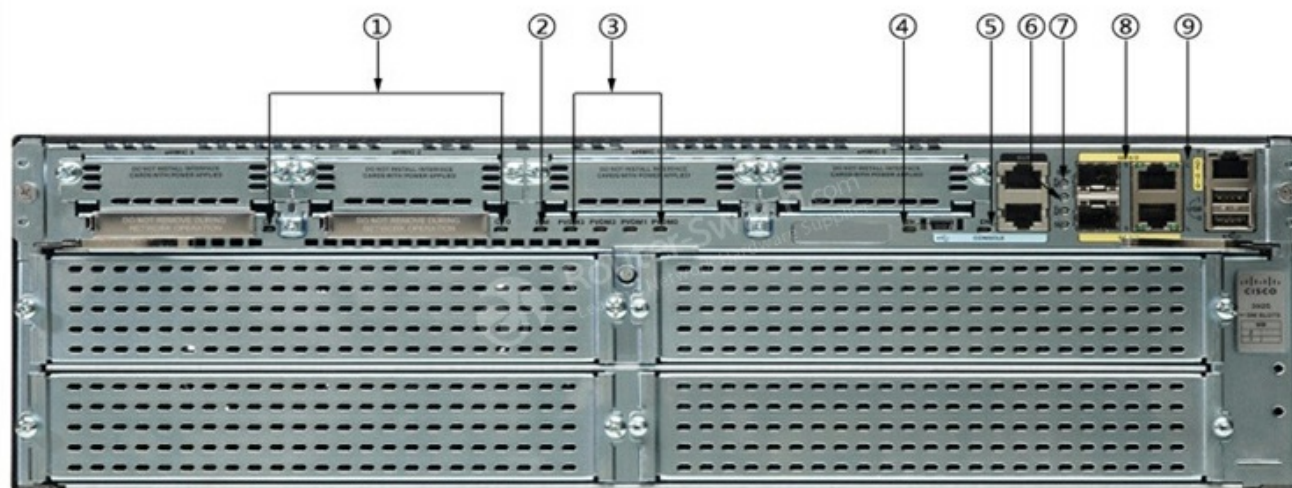
Note:

(1) On/Off switch (2) Power connector (3) LEDs area

Table 2 shows the LEDs area description.

LED	Description	
SYS status LED	Solid green	Solid green indicates normal operation.
	Blinking green	System is booting or is in ROM monitor mode.
	Amber	System error.
	Off	Power is off or system board is faulty.
ACT status LED	Solid or blinking green	Solid or blinking indicates packet activity between the forwarding and routing engine and any I/O port.
	Off	No packet transfers are occurring.
POE	Green	IP phone power is on.
	Amber	IP phone power is not on.
PS1 / PS2	Green	System is running.
	Amber	System is not running.

Figure 3 shows the back panel of the Cisco router 3925/K9 with LEDs.



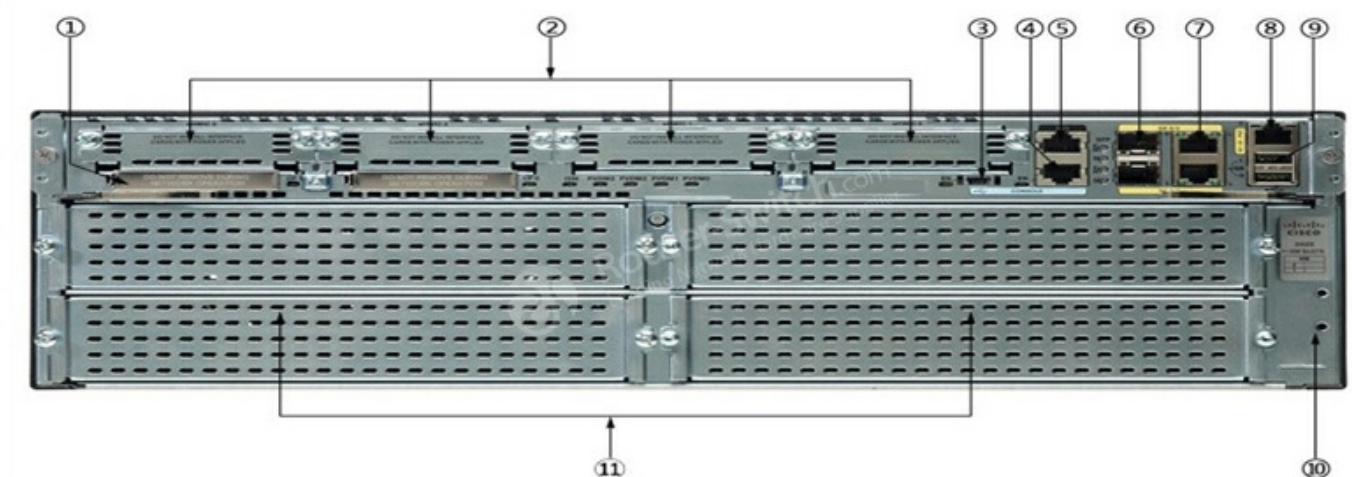
Note:

(1) Compact flash 0 and 1 (0, right) (2) ISM (3) PVDMA 0,1,2 and 3 (0, far right) (4) EN (Enable USB console) (5) EN (Enable RJ-45 console) (6) SFP S (7) SFP EN (8) S (Speed) (9) L (Link)

Table 3 shows the description of these LEDs on the back panel.

LED	Color	Description	Location
CompactFlash 1	Green	Flash memory is busy.	Back Panel
	Amber	Initialized with error.	
	Blinking Green then turns off	CompactFlash is ready for removal.	
CompactFlash 0	Green	Flash memory is busy.	Back Panel
	Amber	Initialized with error.	
	Blinking Green then turns off	CompactFlash is ready for removal.	
S (Speed)	1 blink + pause	GE port operating at 10 Mb/s.	Back Panel
	2 blink + pause	GE port operating at 100 Mb/s.	
	3 blink + pause	GE port operating at 1000 Mb/s.	
L (Link)	Green	GE link is established.	Back Panel
	Off	No GE link is established.	
EN (RJ-45 console port)	Green	The RJ-45 console port is active.	Back Panel
EN (USB serial console port)	Green	The USB console port is active.	Back Panel
ISM	Green	Initialized.	Back Panel
	Amber	Initialized with error.	
	Off	Not installed.	
PVDM3 0,1,2 and 3	Green	PVDM is initialized.	Back Panel
	Amber	PVDM is detected but not initialized.	
	Off	No PVDM installed.	
SFP S	Blinking green	Blinking frequency indicates port speed.	Back Panel
SFP EN	Off	Not present.	Back Panel
	Green	Present and enabled.	
	Amber	Present with failure.	

Figure 4 shows the back panel of the Cisco 3925 router with slots and ports.



Note:

(1) Compact flash 0 and 1 (0, right) (2) EHWIC 0,1,2 and 3 (0, far right) (3) USB serial port (4) RJ-45 serial console port (5) AUX port (6) SFP 1 and SFP 2 (2, top)

(7) 10/100/1000 Ethernet port GE 0/1 and GE 0/2 (GE 0/1, down) (8) 10/100/1000 Ethernet port GE 0/0 (9) USB 0 and USB 1 (1,top) (10) Ground (11) Service module slots

Figure 5 shows the SPE area and you can upgrade these slots and ports directly by one SPE module.

The Cisco 3900 Series offers field-replaceable SPEs which allow you to protect your initial investment in the Cisco 3900 platform for a longer time period and scale router performance as your network and branch-office needs grow.



Modules and License

Table 4 shows modules and licenses for this router.

Models	Description
C3900-SPE100/K9	Cisco Services Performance Engine 100 for Cisco 3925 ISR. (It's a configured item in the CISCO3925/K9.)
SM-ES3G-16-P	Enhanced EtherSwitch Service Module, L2/L3 switching, 16* 10/100/1000 GE ports, Enhanced POE, Cisco EnergyWise technology
SM-ES3G-24-P	Enhanced EtherSwitch Service Module, L2/L3 switching, 24 * 10/100/1000 GE ports, Enhanced POE, Cisco EnergyWise technology
VVIC3-2MFT-G703	Cisco Voice/WAN Card VVIC3-2MFT-G703
HWIC-2T	2-Port Serial WAN Interface Card Cisco Router High-Speed WAN Interface card
EHWIC-1GE-SFP-CU	Cisco 1900, 2900, 3900 Router EHWIC WAN Card EHWIC-1GE-SFP-CU
EHWIC-4ESG	Four port 10/100/1000 Base-TX Gigabit Ethernet switch interface card for Cisco 1900 2900 3900 Routers
ISM-SRE-300-K9	Internal Services Module (ISM) with Services Ready Engine
PVDM3-16	16-channel high-density voice DSP module
MEM-CF-256U1GB	256MB to 1GB Compact Flash Upgrade for Cisco 1900,2900,3900
MEM-CF-256U2GB	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900
MEM-CF-256U512MB	256MB to 512MB CF Upgrade for Cisco 1900,2900,3900 ISR
MEM-CF-256U4GB	256MB to 4GB Compact Flash Upgrade for Cisco 1900,2900,3900
MEMUSB-1024FT	1GB USB Flash Token
Licenses	Description

L-FL-39-HSEC-K9=	Cisco 3900 License L-FL-39-HSEC-K9 U.S. Export Restriction Compliance license for 3900 series
L-FL-39-SNA=	Cisco 3900 Router License - FL-39-SNA= SNA E-Delivery License for Cisco 3925/3945 for Cisco 3900 Series
L-SL-39-APP-K9=	Cisco Application Experience License ISR 3900 series - includes licenses for: AppX, DATA and WAASX.
L-SL-39-SEC-K9=	Cisco 3900 License L-SL-39-SEC-K9 Security E-Delivery PAK for Cisco 3900 Series
L-SL-39-UC-K9=	Cisco 3900 License L-SL-39-UC-K9 Unified Communication E-Delivery PAK for Cisco 3900 Series

Get more information

Do you have any question about the Cisco 3925/K9 router?

Contact us now via [Live Chat](#) or sales@router-switch.com.

Specification

CISCO3925/K9 Specification	
General	
Manufacturer	Cisco Systems, Inc
Manufacturer Part Number	CISCO3925/K9
Product Type	Router
Form Factor	Desktop - modular - 3U
Connectivity Technology	Wired
Data Link Protocol	Ethernet, Fast Ethernet, Gigabit Ethernet
Capacity	Cisco Unified Communications Manager Express sessions : 250 Cisco Unified SRST sessions : 730
Network / Transport Protocol	IPSec, PPPoE, L2TPv3
Routing Protocol	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing, policy-based routing (PBR)
Remote Management Protocol	SNMP, RMON
Encryption Algorithm	SSL
Features	Firewall protection, VPN support, MPLS support, Syslog support, content filtering, IPv6 support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Quality of Service (QoS), Dynamic Multipoint VPN (DMVPN)
Compliant Standards	IEEE 802.3, IEEE 802.1Q, IEEE 802.1ah, IEEE 802.1ag
DRAM Memory	1 GB (installed) / 2 GB (max)
Flash Memory	256 MB (installed) / 8 GB (max)
LED Status Lights Indicators	Link activity, power
Connectivity Slots	

Router Interfaces	3 x 10Base-T/100Base-TX/1000Base-T - RJ-45 Management : 1 x console - RJ-45 Management : 1 x console - mini-USB Type B Serial : 1 x auxiliary - RJ-45 Hi-Speed USB : 2 x 4 PIN USB Type A 2 x SFP (mini-GBIC)
Expansion Slots Total (Free)	4 (4) x EHWIC 4 (4) x PVDM 2 (1) x CompactFlash Card 1 (1) x Expansion Slot 2 (2) x service module (SM)
Power Supply	
Power Device	Power supply - internal
Voltage Required	AC 120/230 V (47/63 Hz)
Dimensions / Weight / Miscellaneous	
Dimensions (W x D x H)	18.74 x 17.24 x 5.24 in (47.6 x 43.8 x 13.3 cm)
Package Wight	61.3 lbs (27.78 Kg)
Weight	39 lbs (17.7 kg)
Compliant Standards	CISPR 22 Class A, CISPR 24, EN55024, EN55022 Class A, EN50082-1, AS/NZS 60950-1, AS/NZ 3548 Class A, CAN/CSA-E60065-00, ICES- 003 Class A, CS-03, FCC CFR47 Part 15, EN300-386, UL 60950-1, IEC 60950-1, EN 60950-1, CSA C22.2 No. 60065, BSMI CNS 13438
System Software	
IOS Software Included	Cisco IOS IP Base

Download Resource

Support and Resources

-  [Cisco Router 3900 Series Datasheet](#)
-  [Cisco ISR 4451-X vs. ISR 3900 vs. ISR 2900 vs. ISR 1900](#)

Transition Guide

-  [Guide to Upgrade Your ISR G1 and ISR G2 Routers to ISR 4000](#)

Want to Buy

- Order Now
- Get a Quote

Why Router-switch.com

As a leading network hardware supplier, Router-switch.com focuses on original new ICT equipment of [Cisco](#), [Huawei](#), [HPE](#), [Dell](#), [Hikvision](#), [Juniper](#), [Fortinet](#), etc.


200+


18,000+


\$20,000,000


50%-98%


100%

Contact Us

- Tel: +1-626-239-8066 (USA) +852-3050-1066 / +852-3174-6166
- Fax: +852-3050-1066 (Hong Kong)
- Email: sales@router-switch.com



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **00548-10-01086**

Validade: Indeterminada

Emissão: 13/06/2013

Requerente:

CNPJ: 00.028.666/0001-58

CISCO DO BRASIL LTDA.

Fabricante:

CISCO SYSTEMS, INC.

170 WEST TASMAN DRIVE

Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC 6301/10, emitido pelo **Associação NCC Certificações do Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Equipamento para Interconexão de Redes - III

Modelo - Nome Comercial (s):

Cisco 3900 Series - (Cisco 3900 Series)

Características técnicas básicas:

Módulos de interfaces disponíveis: E1 (120 Ohms), FXO e FXS.

Observações

Modelos disponíveis na série Cisco 3900 series: CISCO3945/K9 V01, CISCO3925/K9 V01, CISCO3925E/K9 e CISCO3945E/K9.

Outros módulos de interface e protocolos de sinalização, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados. Este certificado substitui o de mesmo número emitido em 26/04/2010.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente de Certificação e Numeração



CABO OPTICO CFOA-AS (ABNT), AUTOSUSTENTADO PARA VÃO ATÉ 200m



Construção	ROHS Compliant	
	Dielétrico	
	Núcleo Seco ou Geleado	
	Tubos Loose	
	SM, MM e NZD	
Descrição	Cabos óptico dielétricos auto sustentados de 02 (duas) a 144 (cento e quarenta e quatro) fibras ópticas com revestimento em acrilato curado com UV, protegidas por tubo de proteção preenchidos com geleia (tubo loose) com núcleo resistente a penetração de umidade e revestimento externo de material termoplástico, sendo indicados para instalações aéreas em vãos com até 200m.	
Aplicação	Ambiente de Instalação	Externo
	Ambiente de Operação	Aéreo Auto-suportado
Normas	• ABNT NBR 14160 Cabo óptico dielétrico aéreo auto-sustentado • ITU-T Recomendación G.652: "Characteristics of a single-mode optical fibre and cable" • ITU-T Recomendación G.651: "Characteristics of a 50/125µm multimode graded index optical fibre cable" • ITU-T Recomendación G.655: "Characteristics of a non-zero dispersion-shifted single-mode optical fibre and cable"	
Certificações	Anatel	
Fibra Óptica	Monomodo (SM), Multimodo (MM)* ou Monomodo com Dispersão Não Nula (NZD)** * Disponível apenas para cabos Geleados(AS-G) ** Disponível apenas para cabos Secos (AS-S)	
Características Ópticas	Fibra	Características
	Monomodo	De acordo com especificação técnica 2000 (Anexo A)
	Multimodo (OM1, OM2, OM3 e OM4)	De acordo com especificação técnica 1999 (Anexo B)
	NZD	De acordo com especificação técnica 1902 (Anexo C)
Revestimento Primário da Fibra	Fibras ópticas revestidas em acrilato curado com UV.	

Identificação da Fibra	Fibra	Cor
	01	Verde
	02	Amarela
	03	Branca
	04	Azul
	05	Vermelha
	06	Violeta
	07	Marrom
	08	Rosa
	09	Preta
	10	Cinza
	11	Laranja
	12	Azul claro

Identificação das Unidades Básicas	Unidade Básica	Referência	Código de Cores
	01	Piloto	Verde
	02	Direcional	Amarelo
	03 em diante	Normal	Branco ou Natural

Unidade Básica As fibras ópticas são agrupadas entre si de forma não aderente e protegidas por um tubo de material termoplástico, preenchendo seu interior com um composto para evitar a penetração de umidade proporcionando proteção mecânica às fibras.

Elemento Central Elemento de material dielétrico posicionado no centro do núcleo para prevenir os esforços de contração do cabo. Como membro central se emprega um elemento em FRP (Fiber Reinforced Plastic).

Núcleo As unidades básicas serão trançados ao redor do membro central para formar o núcleo do cabo. O núcleo deve ser protegido por um composto de geléia (núcleo geleado) ou materias hidro-expansíveis (núcleo seco) para prevenir a entrada de umidade. Se necessário, poderão ser usados tubos de material termoplástico para manter o núcleo cilíndrico.

Elemento de Tração Fibras dielétricas de aramidas aplicadas sobre o núcleo do cabo ou sobre a capa interna, quando existir, para fornecer ao cabo resistência contra os esforços de tração, de modo que este tenha o desempenho previsto nesta norma.

Formação do Núcleo	Quantidade de fibras ópticas no cabo	Quantidade de Tubos de Proteção	Número de fibras por Tubo de Proteção
	02 a 12	01 a 06	02
	18 a 36	03 a 06	06
	48 a 144	04 a 12	12

Capa Interna Para cabos de núcleo geleados será aplicada uma capa interna de material termoplástico. Deverá conter um cordão de rasgamento (RIP CORD) sob a capa interna.
Para cabos de núcleo seco a capa interna será opcional.

Capa Externa Camada de material termoplástico resistente a intempéries e a luz solar na cor preta (NR). Quando solicitado pode ser do tipo Retardante a Chamas (RC). Deverá conter um cordão de rasgamento (RIP CORD) sob a capa externa.

**Características
Físicas**
CABOS AEREOS AUTOSSUPORTADOS COM NÚCLEO SECO

Quantidade total de fibras ópticas	Massa nominal (kg/km) vão máximo 80m - AS80-S		Massa nominal (kg/km) vão máximo 120m – AS120-S		Massa nominal (kg/km) vão máximo 200m – AS200-S	
	Revestimento externo NR	Revestimento externo RC	Revestimento externo NR	Revestimento externo RC	Revestimento externo NR	Revestimento externo RC
2 a 12	81	91	83	94	86	99
18 a 36	98	105	97	106	106	113
48	123	130	123	130	130	136
72	124	132	126	134	131	139
96	143	163	145	165	147	167
120	176	198	179	200	188	210
144	234	260	234	260	242	267

CABOS AEREOS AUTOSSUPORTADOS COM NÚCLEO GELEADO

Quantidade total de fibras ópticas	Massa nominal (kg/km) vão máximo 80m - AS80-G		Massa nominal (kg/km) vão máximo 120m – AS120-G		Massa nominal (kg/km) vão máximo 200m – AS200-G	
	Revestimento externo NR	Revestimento externo RC	Revestimento externo NR	Revestimento externo RC	Revestimento externo NR	Revestimento externo RC
2 a 12	100	112	100	112	106	115
18 a 36	100	112	100	112	109	118
48 a 72	128	142	133	147	141	154
96	175	185	172	188	188	194
120	207	224	210	229	222	237
144	260	276	260	281	269	291

Carga de
Fluência
Raio Mínimo de Curvatura

Força de Tração sem Acréscimo de Atenuação (N)		Compressão (N)	projetada após 20 anos de instalação (%)	(mm)			
Vão (m)	Carga Máxima de Operação			Durante instalação	Após instalação		
80	1,5 x Peso do cabo /km			1 x Peso do cabo /km (Mínimo 1000)	Máxima 0,2	20 x Diâmetro Externo do Cabo	10 x Diâmetro Externo do Cabo
120	2 x Peso do cabo /km						
200	3 x Peso do cabo /km						
Temperatura de instalação		-10 °C a 50 °C					
Temperatura de armazenamento		-20 °C a 65 °C					
Temperatura de operação		-20 °C a 65 °C					

Dimensionais

CABOS AEREOS AUTOSSUPORTADOS COM NÚCLEO SECO			
Quantidade total de fibras ópticas	Diâmetro externo (mm) vão máximo 80m - AS80-S	Diâmetro externo (mm) vão máximo 120m - AS120-S	Diâmetro externo (mm) vão máximo 200m - AS200-S
2 a 12	9.3 ± 0,2	9.3 ± 0,2	9.3 ± 0,2
18 a 36	9.3 ± 0,2	9.3 ± 0,2	9.3 ± 0,2
48 a 60	9.5 ± 0,2	9.5 ± 0,2	10.7 ± 0,2

72	9.8 ± 0,2	9.8 ± 0,2	10.7 ± 0,2
96	14.0 ± 0,2	14.0 ± 0,2	14.7 ± 0,2
120	15.8 ± 0,2	16.0 ± 0,2	16.4 ± 0,2
144	18.2 ± 0,2	18.2 ± 0,2	18.8 ± 0,2
CABOS AEREOS AUTOSSUPORTADOS COM NÚCLEO GELEADO			
Quantidade total de fibras ópticas	Diâmetro externo (mm) vão máximo 80m - AS80-G	Diâmetro externo (mm) vão máximo 120m - AS120-G	Diâmetro externo (mm) vão máximo 200m - AS200-G
2 a 12	9.9 ± 0,2	9.9 ± 0,2	10.8 ± 0,2
18 a 36	10.6 ± 0,2	10.6 ± 0,2	10.9 ± 0,2
48 a 72	11.7 ± 0,2	11.7 ± 0,2	12.0 ± 0,2
96	14.8 ± 0,2	14.8 ± 0,2	15.6 ± 0,2
120	16.4 ± 0,2	16.4 ± 0,2	17.2 ± 0,2
144	18.2 ± 0,2	18.4 ± 0,2	19.0 ± 0,2

Gravação

FURUKAWA CFOA-x-ASz-w yF v k mês/ano "Nome do Cliente" ANATEL nº do certificado ()**
LOTE nL"

Onde:

x = tipo da fibra

SM (fibra monomodo)

MM (fibra multimodo)

NZD (fibra monomodo com dispersão não nula)

z = Vão (80, 120 ou 200)

w = Preenchimento do núcleo (S ou G)

y = número de fibras

v = Denominação extra para fibras especiais

G-652D = para fibras SM G.652.D

(50) = para fibras multimodo - 50µm

(62.5) = para fibras multimodo - 62.5µm

(50) OM3 = para fibras MM50 OM3

(50) OM4 = para fibras MM50 OM4

k = Denominação para material de capa

RC: retardante à chama

NR: não retardante

mês/ano = data de fabricação (MM/AAAA)

"Nome do Cliente" = quando solicitado no Pedido de Compra*

*Sob consulta prévia para análise de viabilidade

nº do certificado = número da certificação ANATEL para o respectivo produto

()** = marcação seqüencial métrica xxxxxx m

nL = número do lote

CABOS MISTOS:

Obrigatoriamente adotam a seguinte ordenação de distribuição conforme tipo de fibra óptica:
As primeiras unidades básicas serão compostas por fibras tipo NZD.

As demais unidades básicas serão compostas por fibras SM.

Ex. FURUKAWA CFOA-NZD/SM AS200-G 36F (24F NZD+12F SM) RC

Tubos 1 a 4: fibras NZD

Tubos 5 a 6: fibras SM

Tipo de Embalagem	Bobina de madeira
Comprimento Padrão	Comprimento nominal por bobina: 4000m Sobre o valor nominal de cada lance é permitida uma tolerância de até $\pm 1\%$ sobre o comprimento do lance
Observações	Demais características conforme ABNT NBR 14160. Utilize somente acessórios pré-formados na ancoragem dos cabos cobertos por esta proposta. A Furukawa não recomenda outros tipos de acessórios para este fim. Para maiores informações, favor contactar a Furukawa.

[Codificação](#)



REPÚBLICA FEDERATIVA DO BRASIL
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

Certificado de Homologação
(Intransferível)

Nº **1626-06-0256**

Validade: **Indeterminada**

Emissão: **13/07/2007**

Fabricante:

FURUKAWA INDUSTRIAL S/A PRODUTOS ELÉTRICOS
RUA HASDRUBAL BELLEGARD 820 CIDADE INDUSTRIAL
81460-120 - CURITIBA - PR

Este documento homologa, nos termos do Regulamento para Certificação e Homologação de Produtos para Telecomunicações, aprovado pela Resolução Anatel nº 242, de 30 de novembro de 2000, o Certificado de Conformidade nº 0844, emitido pelo **OCD - Fundação CPqD**. Esta homologação é expedida em nome do fabricante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação do serviço ou aplicação a que se destina.

Tipo:

Cabo de Fibras Ópticas - Categoria III

Modelo(s):

CFOA-SM-ASU-120-S 2 a 12F RC
CFOA-SM-ASU-120-S 2 a 12F NR

Serviço/Aplicação:

Serviço Telefônico Fixo Comutado - STFC

Características técnicas básicas:

Cabo óptico tipo "loose" para aplicação aérea em vãos de até 120m, com capacidade de até 12 fibras ópticas monomodo de fabricação própria, testado nos comprimentos de onda de 1310nm e 1550nm e agrupadas em uma unidade básica, núcleo seco e revestimento normal (NR) ou retardante à chama (RC)

Observações:

Este certificado substitui o de mesmo número emitido em 09/02/2007.
O produto poderá ser comercializado com o nome fantasia CFOA-SM-AS120-RA.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos do art. 39 do Regulamento anexo à Resolução Anatel nº 242, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SGCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Maximiliano Salvadori Martinhão
Gerente Geral de Certificação e
Engenharia do Espectro



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **01535-17-08867**

Validade: Indeterminada

Emissão: 20/04/2017

Requerente:

CNPJ: 23.664.260/0001-67

FORTINET NETWORK SECURITY BRASIL LTDA

Fabricante:

FORTINET, INC.

899 KIFER ROAD

Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº 5493, emitido pelo **FUNDACAO CENTRO DE PESQUISA E DESENVOLVIMENTO DE TELECOMUNICACOES- CPQD**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Equipamento de Rede de Dados - III

Modelo - Nome Comercial (s):

FG-30E - (FORTIGATE-30E)

Características técnicas básicas:

Equipamento utilizado em redes Ethernet.

Observações

Este produto destina-se ao uso profissional, manuseado por pessoal devidamente qualificado, não sendo destinado ao uso do público em geral para acesso a serviço de telecomunicações de interesse coletivo.

Modulos de interface e protocolos de sinalizacao, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente de Certificação e Numeração

DATA SHEET

FortiWiFi® 30E

FWF-30E

Secure SD-WAN
Next Generation Firewall



The FortiWiFi 30E series provides an application-centric, scalable and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

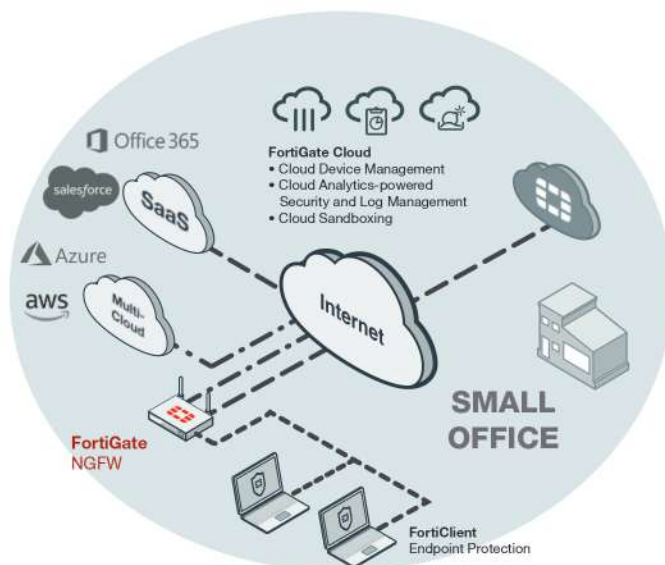
Firewall	IPS	NGFW	Threat Protection	Interfaces
950 Mbps	300 Mbps	200 Mbps	150 Mbps	Multiple GE RJ45 WiFi variants

DEPLOYMENT



Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

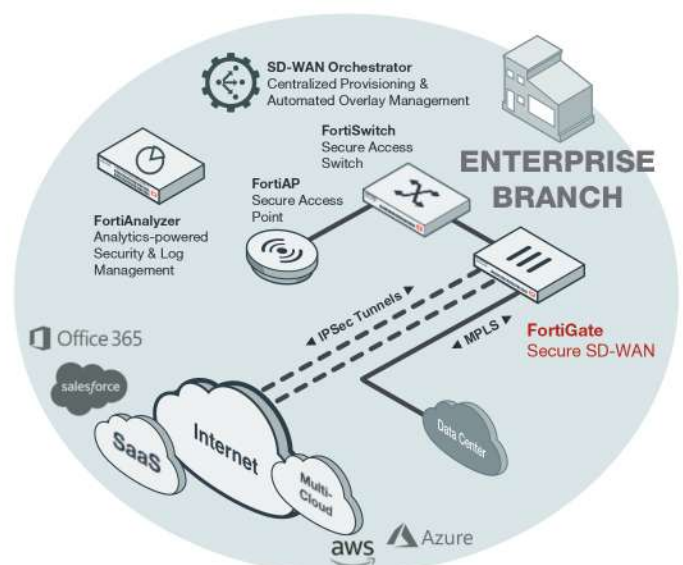


Small Office Deployment
(NGFW)



Secure SD-WAN

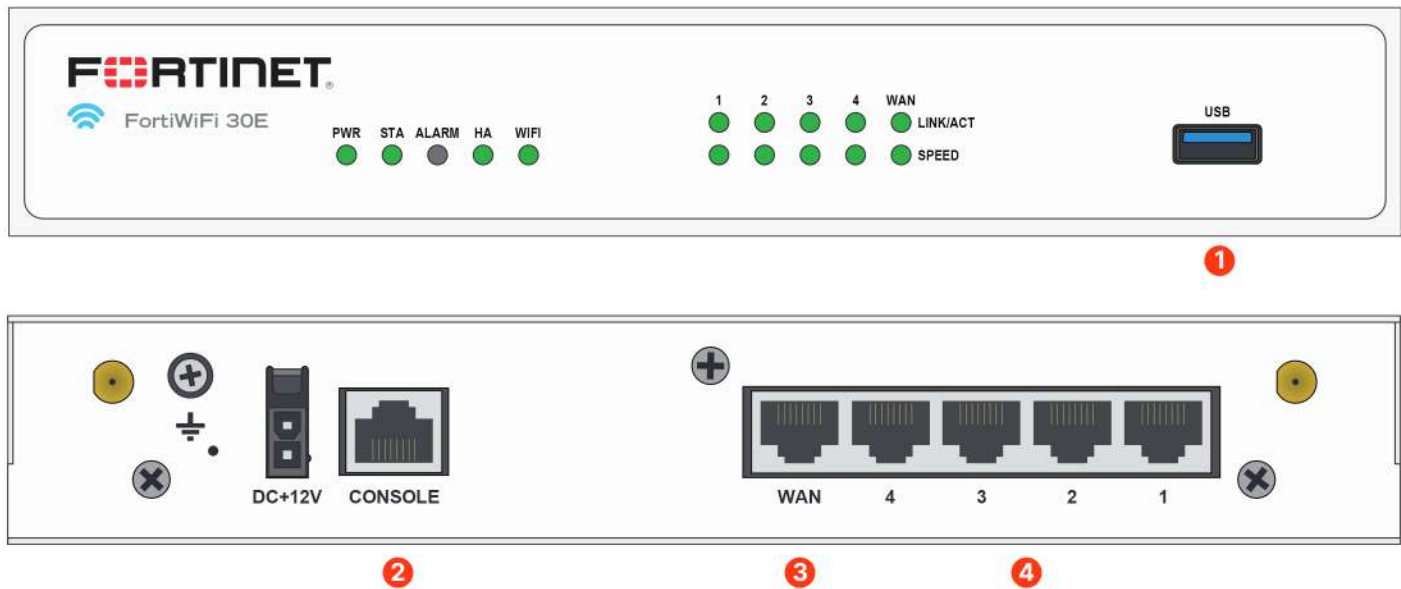
- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated Overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with SD-WAN Orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real-time threat protection



Enterprise Branch Deployment
(Secure SD-WAN)

HARDWARE

FortiWiFi 30E



Interfaces

1. USB Port
2. Console Port
3. 1x GE RJ45 WAN Port
4. 4x GE RJ45 Switch Ports

Hardware Features



Install in Minutes with FortiExplorer

The FortiExplorer wizard enables easy setup and configuration coupled with easy-to-follow instructions. FortiExplorer runs on popular iOS devices. Using FortiExplorer is as simple as starting the application and connecting to the appropriate USB port on the FortiGate. By using FortiExplorer, you can be up and running and protected in minutes.

Wireless and 3G/4G WAN Extensions

The FortiGate supports external 3G/4G modems that allow additional or redundant WAN connectivity for maximum reliability. The FortiGate can also operate as a wireless access point controller to further extend wireless capabilities.

Compact and Reliable Form Factor

Designed for small environments, you can simply place the FortiWiFi 30E on a desktop. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Superior Wireless Coverage

A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 30E and provides speedy 802.11n coverage on 2.4 GHz or 5 GHz bands. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

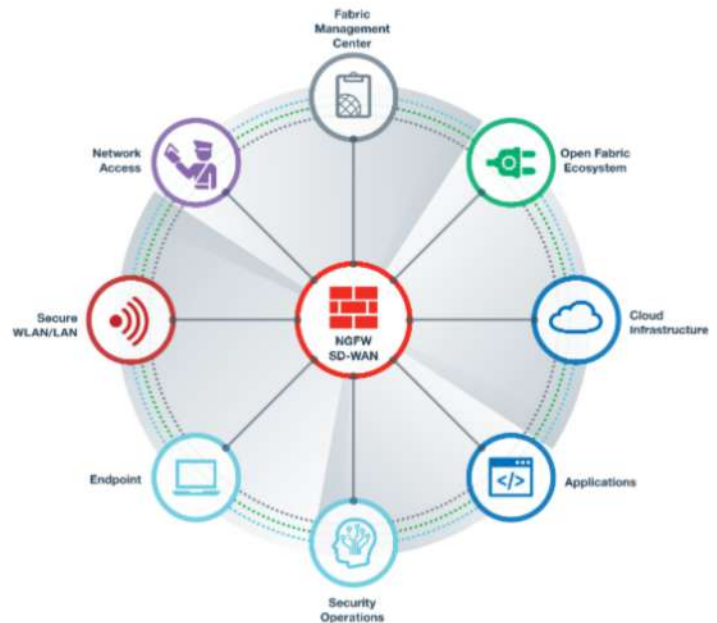


FORTINET SECURITY FABRIC

Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



FortiOS

FortiGate is the foundation of the Fortinet Security Fabric — the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance
- Leverage the latest technologies such as deception-based security

- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation
- Utilize SPU hardware acceleration to boost network security performance

Services



FortiGuard™ Security Services

FortiGuard Labs offer real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.



FortiCare™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.



For more information, please refer to forti.net/fortiguard and forti.net/forticare



SPECIFICATIONS

FORTIWIFI 30E	
Hardware Specifications	
GE RJ45 Switch Ports	4
GE RJ45 WAN Port	1
USB Port	1
Console (RJ45)	1
Wireless Interface	802.11 a/b/g/n
System Performance — Enterprise Traffic Mix	
IPS Throughput ²	300 Mbps
NGFW Throughput ^{2,4}	200 Mbps
Threat Protection Throughput ^{2,5}	150 Mbps
System Performance	
Firewall Throughput	950 Mbps
Firewall Latency (64 byte UDP packets)	130 µs
Firewall Throughput (Packets Per Second)	180 Kpps
Concurrent Sessions (TCP)	900,000
New Sessions/Second (TCP)	15,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte) ¹	75 Mbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	250
SSL-VPN Throughput	35 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	100
SSL Inspection Throughput (IPS, avg. HTTPS) ³	125 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	120
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	45,000
Application Control Throughput (HTTP 64K) ²	400 Mbps
CAPWAP Throughput (HTTP 64K)	850 Mbps
Virtual Domains (Default / Maximum)	5 / 5
Maximum Number of FortiSwitches Supported	8
Maximum Number of FortiAPs (Total / Tunnel Mode)	2 / 2
Maximum Number of FortiTokens	500
High Availability Configurations	Active/Active, Active/Passive, Clustering

FORTIWIFI 30E	
Dimensions and Power	
Height x Width x Length (inches)	1.61 × 8.27 × 5.24
Height x Width x Length (mm)	41 × 210 × 133
Weight	2.008 lbs (0.911 kg)
Form Factor	Desktop
Input Rating	12Vdc, 2A
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz
Maximum Current	100V / 0.6A, 240V / 0.4A
Power Consumption (Average / Maximum)	16 / 19 W
Heat Dissipation	66 BTU/h
Operating Environment	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	–31–158°F (–35–70°C)
Humidity	10–90% non-condensing
Noise Level	Fan-less 0 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	
Regulatory Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Certifications	
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN
Radio Specifications	
MIMO	2×2
Maximum Wi-Fi Speeds	300 Mbps
Maximum Tx Power	21 dBm
Antenna Gain	2 dBi @ 5 GHz 2.4 dBi @ 2.4 GHz

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



ORDERING INFORMATION

Product	SKU	Description
FortiWiFi 30E	FWF-30E	5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports), Wireless (802.11a/b/g/n)
Optional Accessory		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for supported products.

BUNDLES



FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiCASB SaaS-only Service	•	•		
FortiConverter Service	•			
SD-WAN Cloud Assisted Monitoring ²	•			
SD-WAN Overlay Controller VPN Service ²	•			
FortiAnalyzer Cloud ²	•			
FortiManager Cloud ²	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2



www.fortinet.com

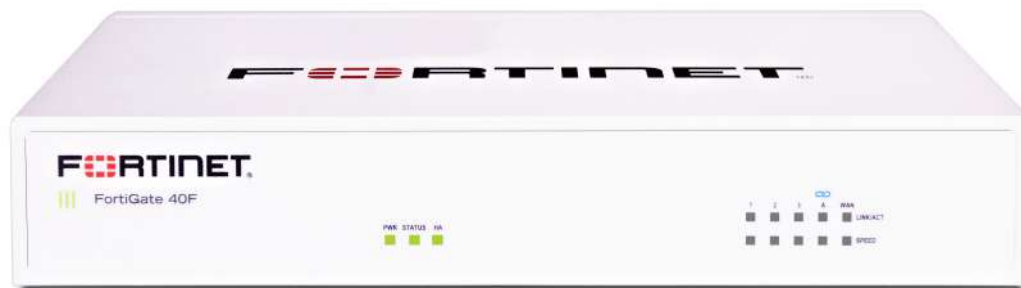
Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

DATA SHEET

FortiGate® FortiWiFi 40F Series

FG-40F and FWF-40F

Next Generation Firewall
Secure SD-WAN



The FortiGate/FortiWiFi 40F series provides a fast and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

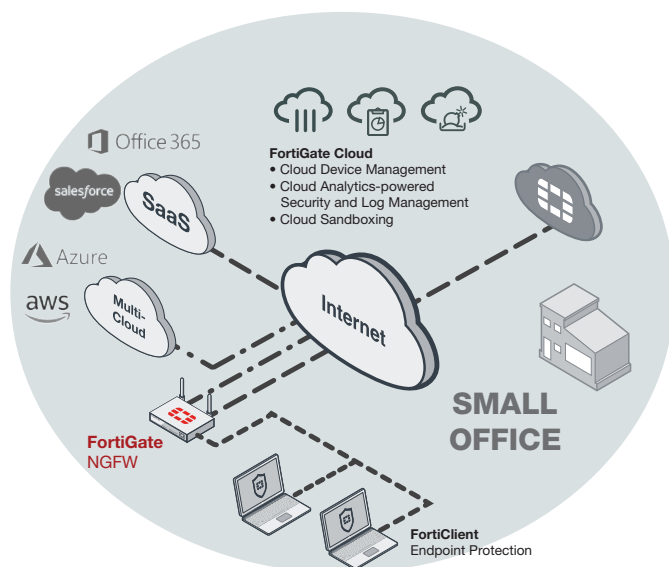
Firewall	IPS	NGFW	Threat Protection	Interfaces
5 Gbps	1 Gbps	800 Mbps	600 Mbps	Multiple GE RJ45 WiFi variants

DEPLOYMENT



Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, and applications across the entire attack surface, and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

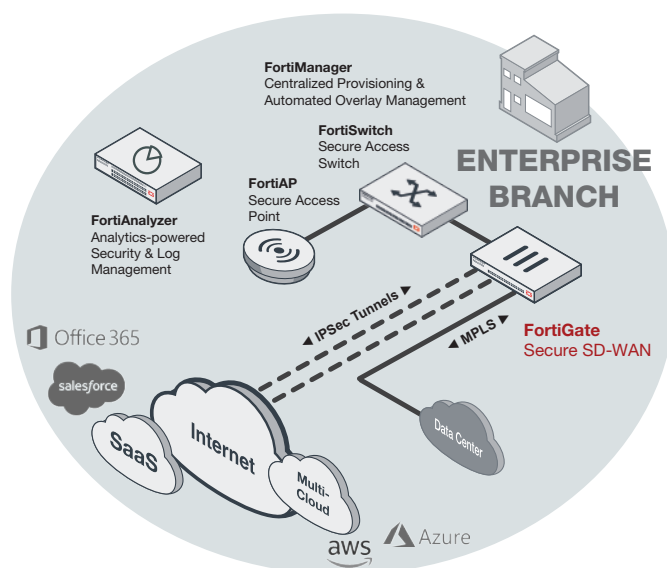


**Small Office Deployment
(NGFW)**



Secure SD-WAN

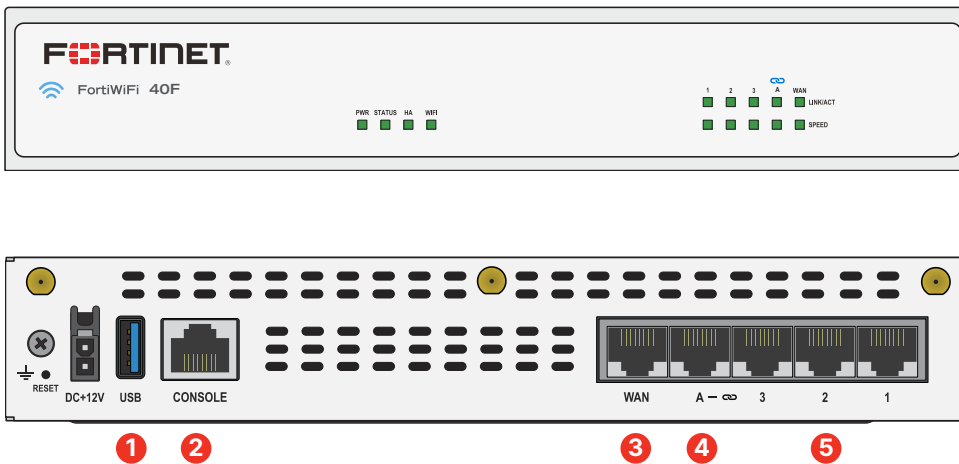
- Consistent business application performance with accurate detection and dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated Overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage
- Simplified and intuitive workflow with FortiManager for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real-time threat protection



**Enterprise Branch Deployment
(Secure SD-WAN)**

HARDWARE

FortiGate/FortiWiFi 40F Series



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 1x GE RJ45 WAN Port
4. 1x GE RJ45 FortiLink Port
5. 3x GE RJ45 Ethernet Ports

Hardware Features



Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables the best of breed NGFW Security and Deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

3G/4G WAN Connectivity

The FortiGate 40F Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Secure Access Layer

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.



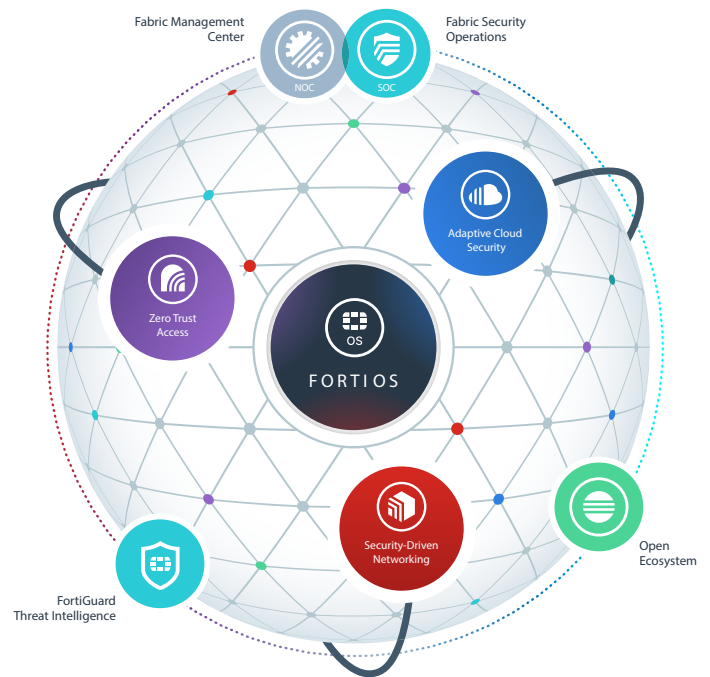
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SPECIFICATIONS

	FORTIGATE 40F	FORTIWIFI 40F
Interfaces and Modules		
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	
Hardware Accelerated GE RJ45 Internal Ports	3	
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	
Hardware Accelerated GE RJ45 PoE/+ Ports	0	
Wireless Interface	0	Single Radio (2.4GHz/5GHz) 802.11 /a/b/g/n/ac-W2
USB Ports	1	
Console Port (RJ45)	1	
Onboard Storage	0	
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	1 Gbps	
NGFW Throughput ^{2,4}	800 Mbps	
Threat Protection Throughput ^{2,5}	600 Mbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps	
Firewall Latency (64 byte, UDP)	2.97 µs	
Firewall Throughput (Packet per Second)	7.5 Mpps	
Concurrent Sessions (TCP)	700 000	
New Sessions/Second (TCP)	35 000	
Firewall Policies	5000	
IPsec VPN Throughput (512 byte) ¹	4.4 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	250	
SSL-VPN Throughput	490 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	310 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	320	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	55 000	
Application Control Throughput (HTTP 64K) ²	990 Mbps	
CAPWAP Throughput (HTTP 64K)	3.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	8	
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 40F	FORTIWIFI 40F
Dimensions and Power		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160	
Weight	2.2 lbs (1 kg)	
Form Factor (supports EIA/non-EIA standards)	Desktop	
Input Rating	12Vdc, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	13.4 W / 15.4 W	14.6 W / 16.6 W
Current (Maximum)	100V AC / 0.2A, 240V AC / 0.1A	
Heat Dissipation	52.55 BTU/h	56.64 BTU/h
Redundant Power Supplies		
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	
Radio Specifications		
Multiple (MU) MIMO	0	3 × 3
Maximum Wi-Fi Speeds	0	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	0	20 dBm
Antenna Gain	0	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz

Note: All performance values are “up to” and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



ORDERING INFORMATION

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports).
FortiWiFi 40F	FWF-40F-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2).
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FG/FWF-40F, come with interchangeable power plugs. (XX=various countries code).
Wall Mount Kits	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

BUNDLES



FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24x7	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video' Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•			
FortiGuard IoT Detection Service	•			
FortiGuard Industrial Service	•			
FortiConverter Service	•			
FortiGate Cloud Subscription		•		

1. Available when running FortiOS 7.0



Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **03515-20-08867**

Validade: Indeterminada

Emissão: 31/03/2020

Requerente:

CNPJ: 23.664.260/0001-67

FORTINET NETWORK SECURITY BRASIL LTDA

Fabricante:

FORTINET, INC.

899 KIFER ROAD

Nº

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº 00122692, emitido pelo **Instituto Brasileiro de Certificação para produtos de Telecomunicações**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações:

Tipo - Categoria:

Equipamento de Rede de Dados - III

Modelo - Nome Comercial (s):

FG-40F

Características técnicas básicas:

Equipamento utilizado em redes Ethernet.

Observações

Não estão cobertos por este certificado módulos de interface, de emissão de RF e outros protocolos de sinalização passíveis de homologação, ainda que especificados em documentos técnicos do produto. Caso estes venham a ser fornecidos ou utilizados será obrigatória sua certificação e homologação.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Davison Gonzaga da Silva
Gerente de Certificação e Numeração



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **01269-16-08867**

Validade: Indeterminada

Emissão: 19/05/2016

Requerente:

**CNPJ: 28.268.233/0006-01
WESTCON BRASIL LTDA.**

Fabricante:

**FORTINET, INC.
899 KIFER ROAD
Nº**

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº 5127, emitido pelo **FUNDACAO CENTRO DE PESQUISA E DESENVOLVIMENTO DE TELECOMUNICACOES- CPQD**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Equipamento de Rede de Dados - III

Modelo - Nome Comercial (s):

FORTIGATE-51E (FG-51E) - (FORTIGATE-51E (FG-51E)) / FORTIGATE-50E (FG-50E) - (FORTIGATE-50E (FG-50E))

Características técnicas básicas:

Equipamento utilizado em redes Ethernet.

Observações

Este produto destina-se ao uso profissional, manuseado por pessoal devidamente qualificado, não sendo destinado ao uso do público em geral para acesso a serviço de telecomunicações de interesse coletivo.

Módulos de interface e protocolos de sinalização, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente de Certificação e Numeração



airFiber® 5

5 GHz Full Duplex Point-to-Point
Gigabit Radio

Models: AF-5, AF-5U

USER GUIDE

Table of Contents

Chapter 1: Overview	1
Introduction	1
Package Contents	1
airFiber Configuration Interface System Requirements	1
Hardware Overview	1
Chapter 2: Installation	3
Link Planning	3
Installation Requirements	3
Installation Overview	4
Connecting Power over Ethernet	4
airFiber Configuration	5
Hardware Installation	7
Connecting Ethernet	10
Alignment	12
Chapter 3: Navigation	18
Accessing the airFiber Configuration Interface	18
Product Verification	19
Interface Tabs	19
Chapter 4: Main Tab	20
Status	20
Monitor	22
Chapter 5: Wireless Tab	23
Basic Wireless Settings	24
Frequency Settings	25
Wireless Security	25
Chapter 6: Network Tab	26
Management Network Settings	26
Chapter 7: Advanced Tab	28
Wireless Settings	28
DATA Port Ethernet Settings	28
MGMT Port Ethernet Settings	30

Chapter 8: Services Tab	31
Ping Watchdog	31
SNMP Agent	32
Telnet Server	33
NTP Client	33
Dynamic DNS	33
System Log	34
Device Discovery	34
Chapter 9: System Tab	35
Firmware Update	35
Device	36
Date Settings	36
System Accounts	36
Miscellaneous	37
Location	37
Device Maintenance	37
Configuration Management	37
Chapter 10: Tools	38
Align Antenna	38
Discovery	39
Ping	39
Traceroute	39
Appendix A: Specifications	40
Appendix B: Safety Notices	42
Electrical Safety Information	42
Appendix C: Warranty	43
Limited Warranty	43
Appendix D: Compliance Information	45
Installer Compliance Responsibility	45
FCC	45
Industry Canada	45
RF Exposure Warning	45
Australia and New Zealand	45
CE Marking	45
Frequency Ranges and Power Levels per Country/Region	46
RoHS/WEEE Compliance Statement	48
Appendix E: Declaration of Conformity	49
Appendix F: Contact Information	50
Ubiquiti Networks Support	50

Chapter 1: Overview

Introduction

Thank you for purchasing the Ubiquiti Networks® airFiber® 5 GHz Full Duplex Point-to-Point Gigabit Radio. This User Guide is for use with the following models:

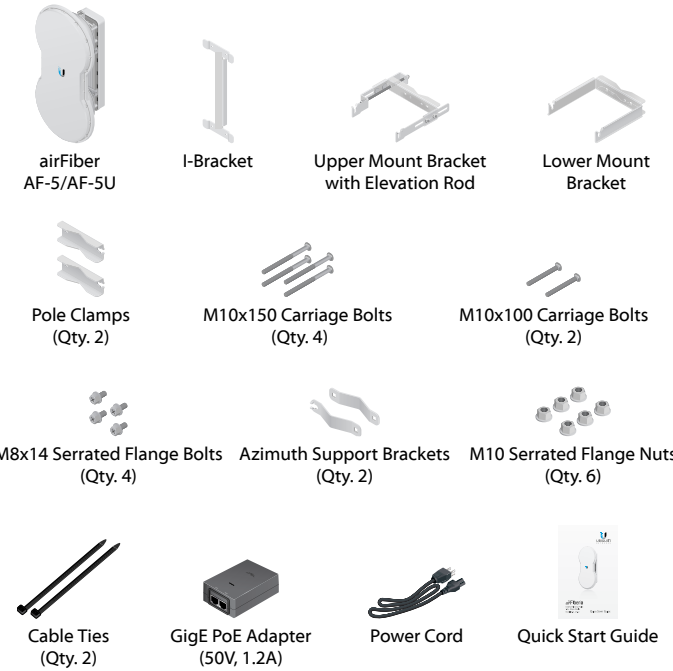
Model	Description	Operating Frequency*
AF-5	Supports mid-band frequencies	5470 - 5950 MHz
AF-5U	Supports high-band frequencies	5725 - 6200 MHz

*Refer to **“Specifications” on page 40** for more information.

The mid-band model, AF-5, features the popular mid-band frequencies, which are freely used in many parts of the world. The high-band model, AF-5U, which can operate in the 5.7 - 6.2 GHz bands, has robust filtering to enable co-location with devices operating in the lower 5 GHz bands while allowing operation at a higher output power in many areas of the world.

The same instructions apply to both models, and the User Guide will refer to both models as the airFiber AF-5.

Package Contents



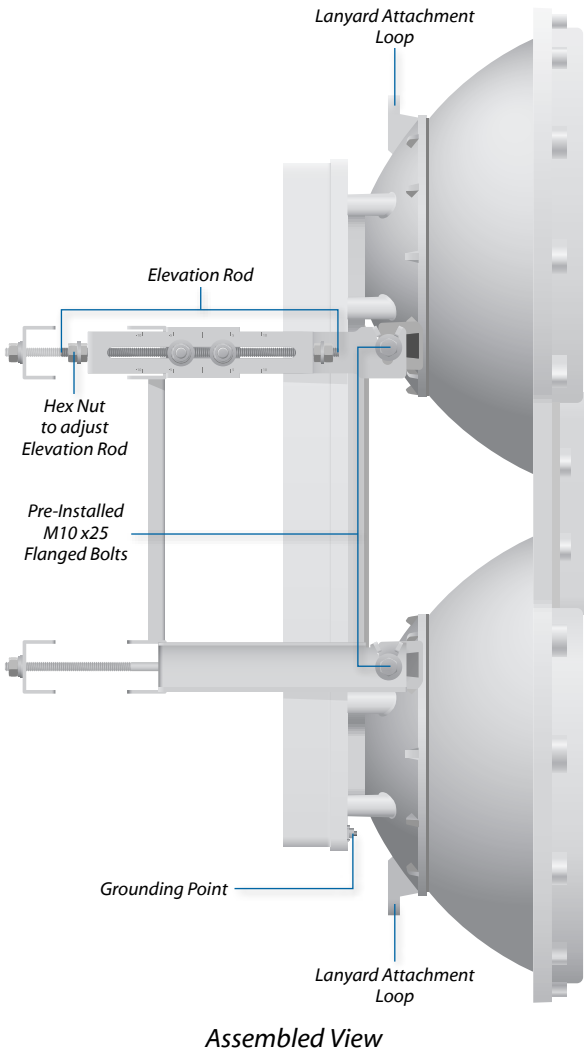
TERMS OF USE: Ubiquiti radio devices must be professionally installed. Shielded Ethernet cable and earth grounding must be used as conditions of product warranty. TOUGH Cable™ is designed for outdoor installations. It is the customer's responsibility to follow local country regulations, including operation within legal frequency channels, output power, and Dynamic Frequency Selection (DFS) requirements.

airFiber Configuration Interface System Requirements

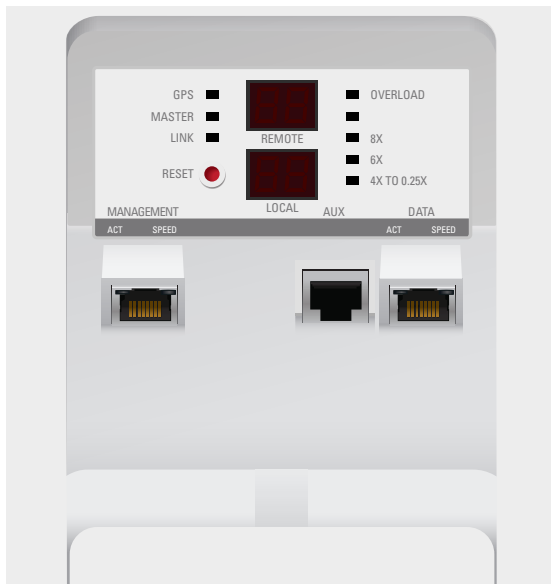
- Microsoft Windows Vista, Windows 7, Windows 8, Linux, or Mac OS X
- Java Runtime Environment 1.6 (or above)
- Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Internet Explorer 8 (or above)

Hardware Overview

Side

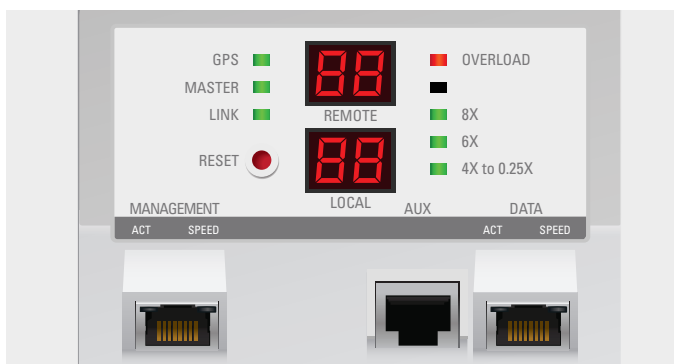


Interfaces



Interface	Description
Reset Button	To reset to factory defaults, press and hold the Reset button for more than five seconds while the unit is already powered on.
Remote Display	Displays the received signal strength in dBm of the remote airFiber radio.
Local Display	Displays the received signal strength in dBm of the local airFiber radio.
Management Port	10/100 Mbps, secured port for configuration. By default, this is the only port that can monitor, configure, and/or update firmware.
Aux Port	Port for audio tone aiming.
Data Port	10/100/1000 Mbps port handles all user traffic.

LEDs



LED	State	Status
GPS	Off	No GPS Synchronization
	On	Operational (Strong Signal)
	Normal Flash*	Non-Operational (Weak Signal)
Master	Off	Slave mode
	On	Master mode
Link Status	Off	RF Off
	Short Flash*	Syncing DFS countries only: • DFS CAC • RADAR Detected
	Normal Flash*	Beaconing
	Long Flash*	Registering
	On	Operational
Remote	On	Displays the received signal strength in dBm of the remote airFiber radio.
Local	On	Displays the received signal strength in dBm of the local airFiber radio.
Overload	Fast Flash	Overload Condition (Identify and eliminate any source of strong in-band interference.)
(Unlabeled)	On	10x (1024QAM MIMO)
8x	On	256QAM MIMO
6x	On	64QAM MIMO
4x to 0.25x	On	16QAM MIMO
	Long Flash*	QPSK MIMO
	Normal Flash*	1x QPSK xRT**
	Short Flash*	1/4x QPSK xRT**

* Short Flash (1:3 on/off cycle)

Normal Flash (1:1 on/off cycle)

Long Flash (3:1 on/off cycle)

** xtreme Range Technology

Port LEDs

LED		State	Status
Management	Act	Off	No Ethernet Link
		On	Ethernet Link Established
		Random Flashing	Ethernet Activity
	Speed	Off	10 Mbps
		On	100 Mbps
Data	Act	Off	No Ethernet Link
		On	Ethernet Link Established
		Random Flashing	Ethernet Activity
	Speed	Off	10/100 Mbps
		On	1000 Mbps

Chapter 2: Installation

Link Planning

Before you install the airFiber AF-5, consider the following:

- Point-to-Point (PtP), daisy chain, or ring configuration
- Co-Location

Configuration

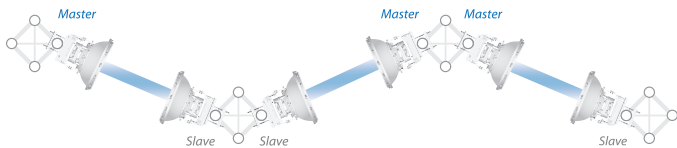
There are three typical configurations:

- **PtP backhaul** Uses two airFiber radios, one configured as *Master* and the other configured as *Slave*.



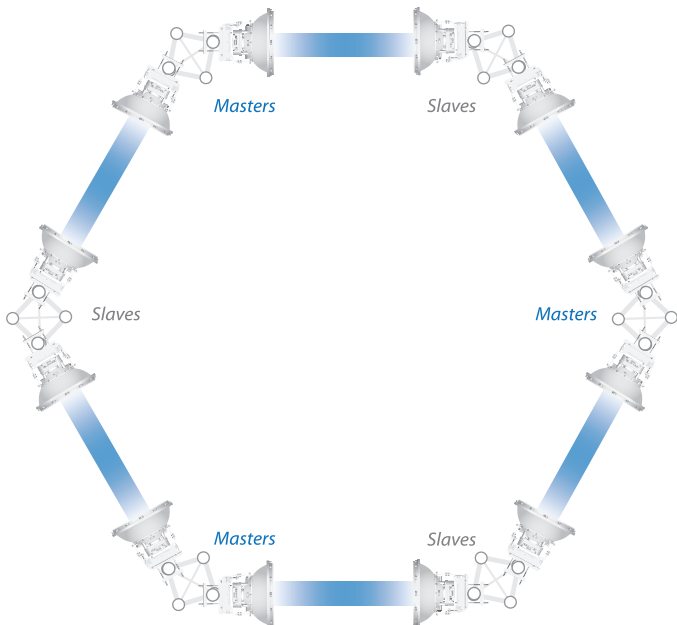
Point-to-Point Backhaul

- **Daisy chain** Uses multiple airFiber radios to extend the distance of a link, like a relay from point to point to point. The airFiber radios in the same node must use the same *Wireless Mode (Master or Slave)*.



Daisy Chain Configuration

- **Ring** Uses multiple airFiber radios to form redundant paths. If one link goes down, the other links have an alternate route available. For each link, configure one airFiber radio as *Master*, and configure the other as *Slave*.



Ring Configuration

Co-Location

You can co-locate multiple airFiber radios if they are pointed in different directions. Co-located airFiber radios must use the same *Wireless Mode (Master or Slave)*. Back-to-back airFiber radios can use the same frequency. We recommend that you use different frequencies for adjacent airFiber radios; however, this is not a strict requirement.

Installation Requirements

Pre-Assembly Tool

- 13 mm (½") wrench

Pole-Mounting Tool

- 17 mm (⅝") wrench

Other Requirements

- Clear line of sight between airFiber radios
- Clear view of the sky for proper GPS operation
- Vertical mounting orientation
- Mounting location with < 0.5° displacement due to twist and sway under wind loading
- Mounting point:
 - At least 1 m (3.28 ft) below the highest point on the structure
 - For tower installations, at least 3 m (9.84 ft) below the top of the tower
- Ground wires – min. 10 AWG (5 mm²) and max. length: 1 m (3.28 ft). As a safety precaution, ground the airFiber radios to grounded masts, poles, towers, or grounding bars.



WARNING: Failure to properly ground your airFiber units will void your warranty.

- (Recommended) 2 Outdoor GigE PoE surge protectors



Note: For guidelines about grounding and lightning protection, follow your local electrical regulatory codes.

- Outdoor, shielded Category 6 (or above) cabling and shielded RJ-45 connectors are required for all wired Ethernet connections.

Installation Overview

We recommend that you configure your paired airFiber radios before mounting. Below is an overview of the installation with specific details in the following instructions:

- Connect Power over Ethernet to the Data port, and connect an Ethernet cable between your computer and the Management port.
- Configure the device settings in the airFiber Configuration Interface.
- Once configuration is complete, disconnect the cables to move the airFiber radios.
- Pre-assemble the mounting hardware.
- Install the airFiber radios at the site.
- Establish and optimize the RF link.



Note: The AF-5 and AF-5U models share the same installation and configuration instructions.

Connecting Power over Ethernet

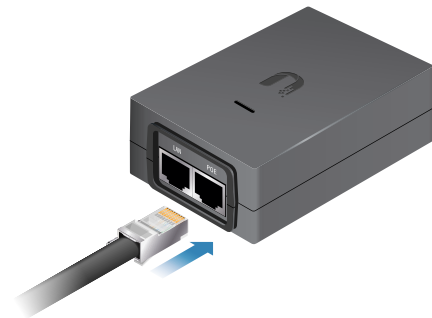
1. Push the button and slide the port cover down to access cable ports. (The port cover cannot be completely removed.)



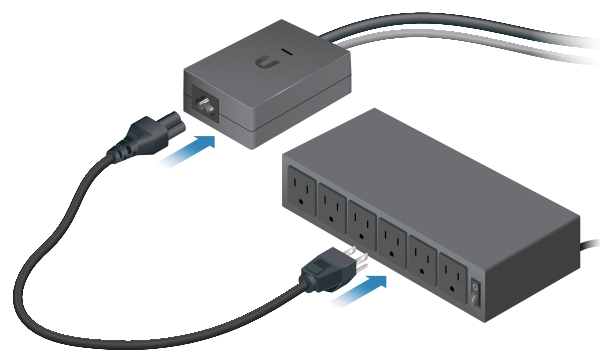
2. Connect an Ethernet cable to the *Data* port.



3. Connect the other end of the Ethernet cable from the *Data* port to the Ethernet port labeled **POE** on the *GigE PoE Adapter*.



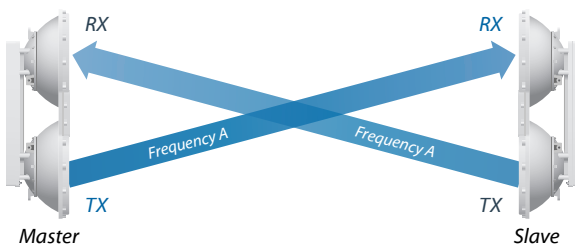
4. Connect the *Power Cord* to the power port on the *GigE PoE Adapter*. Connect the other end of the *Power Cord* to a power source.



airFiber Configuration

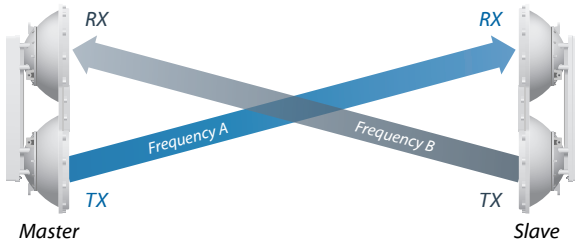
The instructions in this section explain how to access the airFiber Configuration Interface and configure the following settings:

- **Wireless Mode** Configure one airFiber radio as the *Master* and the other as the *Slave*.
- **Duplex** The airFiber radio supports both half-duplex and full-duplex operation. Half-duplex operation provides more frequency planning options at the cost of higher latency and throughput. Full-duplex operation provides the highest throughput and lowest latency; however, you have fewer frequency management options.
 - **Half Duplex (default)** The *TX* and *RX* Frequencies can be the same or different to suit local interference.



Half-Duplex Diagram

- **Full Duplex** The *TX* and *RX* Frequencies should be different.



Full-Duplex Diagram

- **TX and RX Frequencies** The *TX* Frequency on the Master must match the *RX* Frequency on the Slave, and vice versa.

1. Connect an Ethernet cable from your computer to the *Management* port on the airFiber radio.



2. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.1.x subnet.
3. Launch your web browser. Type **http://192.168.1.20** in the address field and press enter (PC) or return (Mac).



4. The login screen will appear. Enter **ubnt** in the *Username* and *Password* fields. Select your *Country* and *Language*. You must agree to the *Terms of Use* to use the product. Click **Login**.



Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

5. The *Main* tab will appear. Click the **Tools** drop-down and select **Link Calculator**. This tool will guide you on how to best minimize bandwidth and power/interference issues.



Note: If you do not see the *Link Calculator*, then upgrade the firmware on your airFiber radios. Download the firmware at:

downloads.ubnt.com/airfiber

6. Enter the requirements of your link, and then click **Calculate**. Adjust the values as needed to get the optimal result, and then write down the settings needed for your configuration.

7. Click the **Wireless** tab.8. Enter the *Basic Wireless Settings*:

- a. For one airFiber radio, select **Master** from the *Wireless Mode* drop-down. For the other airFiber radio, keep the default, *Slave*.
- b. Enter a name in the *Link Name* field. This should be the same on both the Master and the Slave.
- c. For the *Duplex* drop-down:
 - **Half Duplex** The default mode. The *TX* and *RX Frequencies* can be the same or different to suit local interference.
 - **Full Duplex** The *TX* and *RX Frequencies* should be different.
- d. Select a *TX Frequency*. This must match the *RX Frequency* on your other airFiber radio.
- e. Select a *RX Frequency*. This must match the *TX Frequency* of your other airFiber radio.
- f. If needed, change the *Output Power* and/or *Maximum Modulation Rate* settings.

9. Configure the *Wireless Security*:

- a. Select the *AES Key Type*, **HEX** or **ASCII**.
- b. For the *Key* field:
 - **HEX** Enter 16 bytes (eight, 16-bit HEX values: 0-9, A-F, or a-f). You can omit zeroes and use colons, similar to the IPv6 format.



Note: The airFiber Configuration Interface supports IPv6 formats excluding dotted quad and ":::" (double-colon) notation.

- **ASCII** Enter a combination of alphanumeric characters (0-9, A-Z, or a-z).

10. Click **Change** and then click **Apply**.

11. *In-Band Management* is enabled by default, so each airFiber radio must have a unique *IP Address*. (If the airFiber radios use the same *IP Address*, then you may lose access to the airFiber radios via the Data ports.) Click the **Network** tab.

a. For the *Management IP Address* option:

- **DHCP** Keep the default, *DHCP*, to use DHCP reservation on your router to assign a unique *IP Address*.
- **Static** Change the *IP Address*, *Netmask*, and other settings to make them compatible with your network.

b. Click **Change** and then click **Apply**.

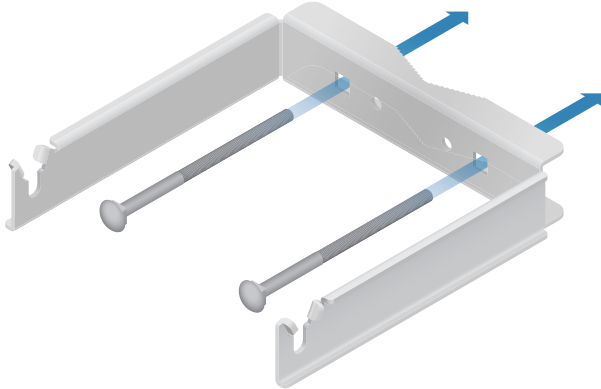
Repeat the instructions in the *airFiber Configuration* section on your other airFiber radio. After you have configured the airFiber radios, disconnect them and move them to your installation site.

Hardware Installation

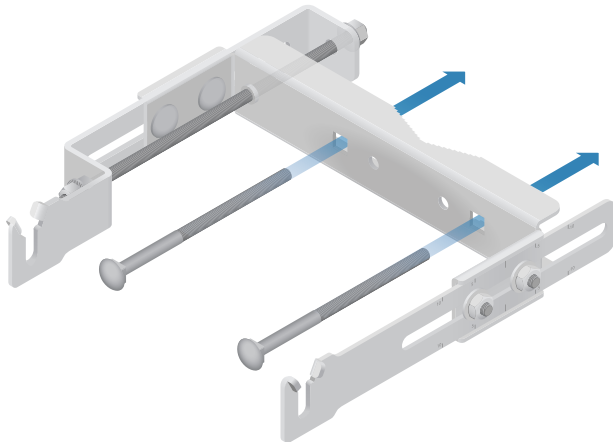
The mounting hardware of the airFiber radio can be pre-assembled before pole-mounting.

Mounting Hardware Pre-Assembly

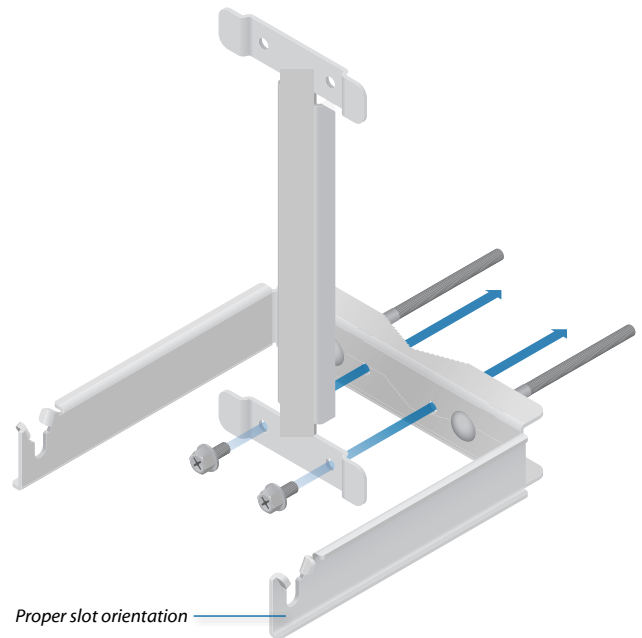
1. Insert two *M10x150 Carriage Bolts* into the *Lower Mount Bracket*.



2. Insert two *M10x150 Carriage Bolts* into the *Upper Mount Bracket with Elevation Rod*.



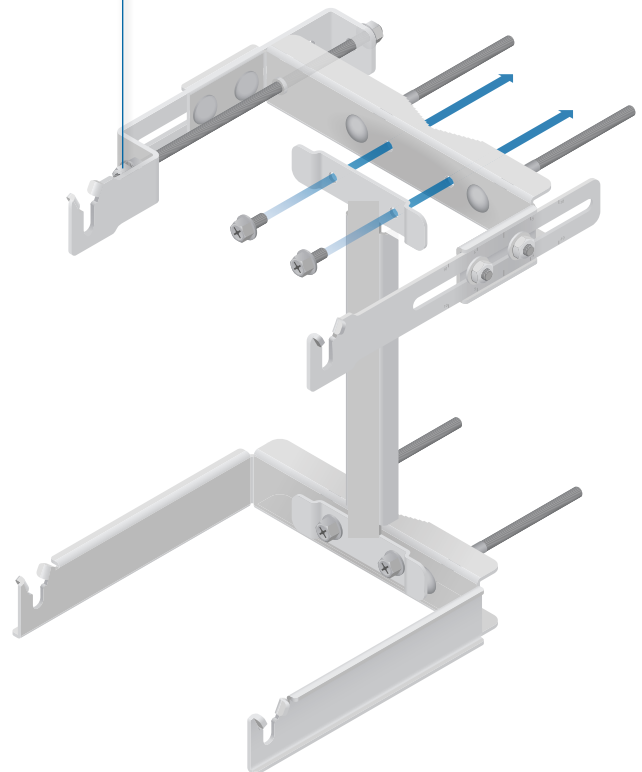
3. Attach the *Lower Mount Bracket* to the *I-Bracket* using two *M8x14 Serrated Flange Bolts*. Ensure that the slots face up and securely tighten the bolts.



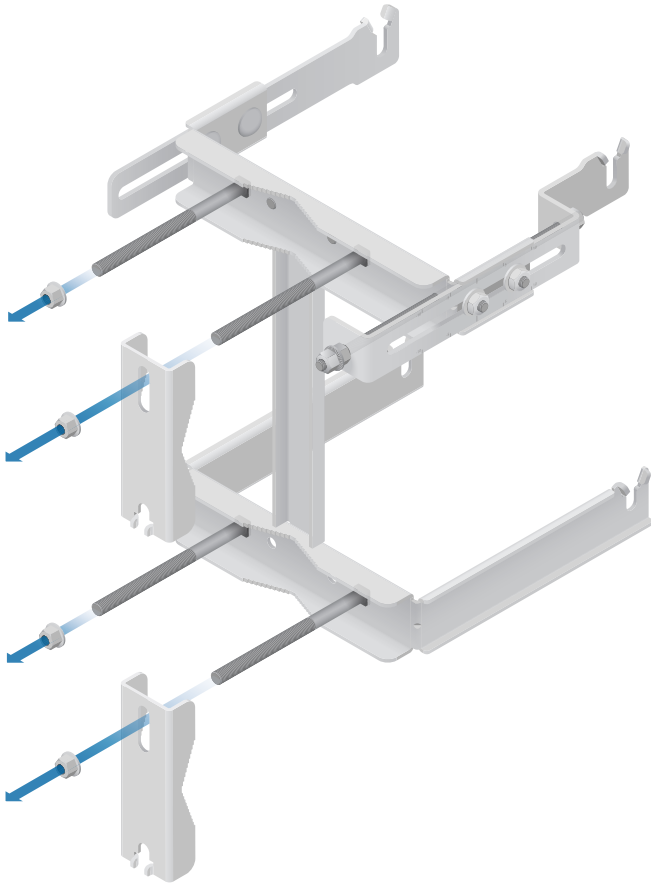
4. Attach the *Upper Mount Bracket with Elevation Rod* to the *I-Bracket* using two *M8x14 Serrated Flange Bolts*.



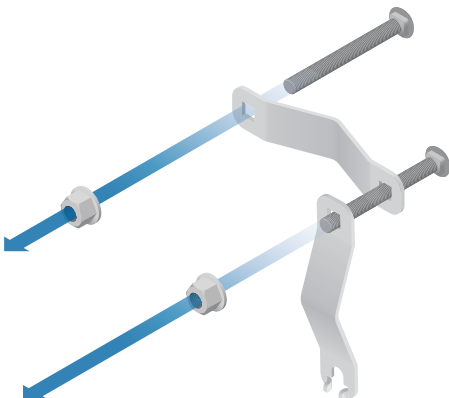
Note: Ensure that the orientation of the *Upper Mount Bracket* matches the illustration below, with the *Elevation Rod* on the correct side.



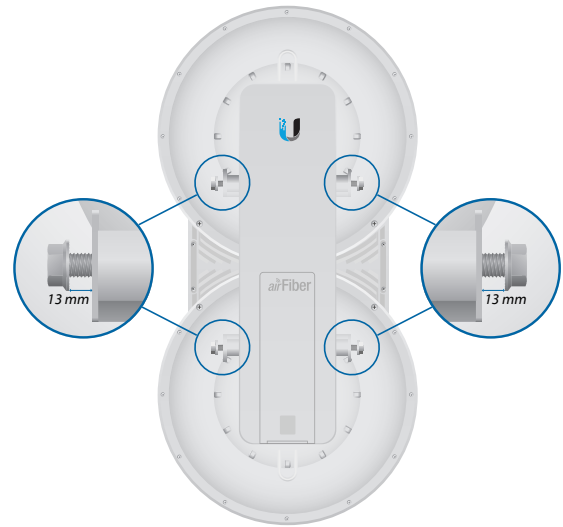
5. Attach the *Pole Clamps* to the *Mount Brackets*.
 - a. Slide the slotted hole of each *Pole Clamp* over one upper and one lower *M10x150 Carriage Bolt*.
 - b. Place one *M10 Serrated Flange Nut* on each *M10x150 Carriage Bolt*.



6. Attach the *Azimuth Support Brackets* together.
 - a. Insert the two *M10x100 Carriage Bolts* into the *Azimuth Support Bracket* that has two slotted holes.
 - b. Slide the slotted hole of the other *Azimuth Support Bracket* over one *M10x100 Carriage Bolt*.
 - c. Place one *M10 Serrated Flange Nut* on each *M10x100 Carriage Bolt*.



7. Ensure that there is a 13 mm gap between the head of each *Pre-Installed M10x25 Flanged Bolt* and the corresponding trunnion on the airFiber radio.



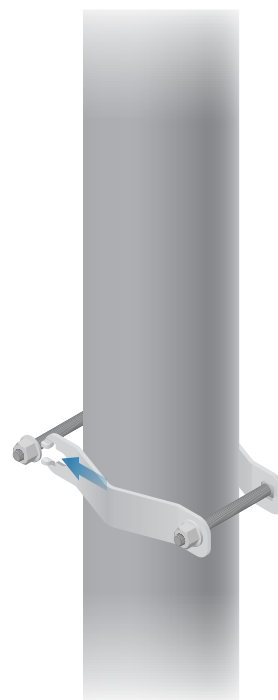
Pole-Mounting

1. Attach the *Azimuth Support Brackets* to the pole just beneath the area where the airFiber radio will be attached.

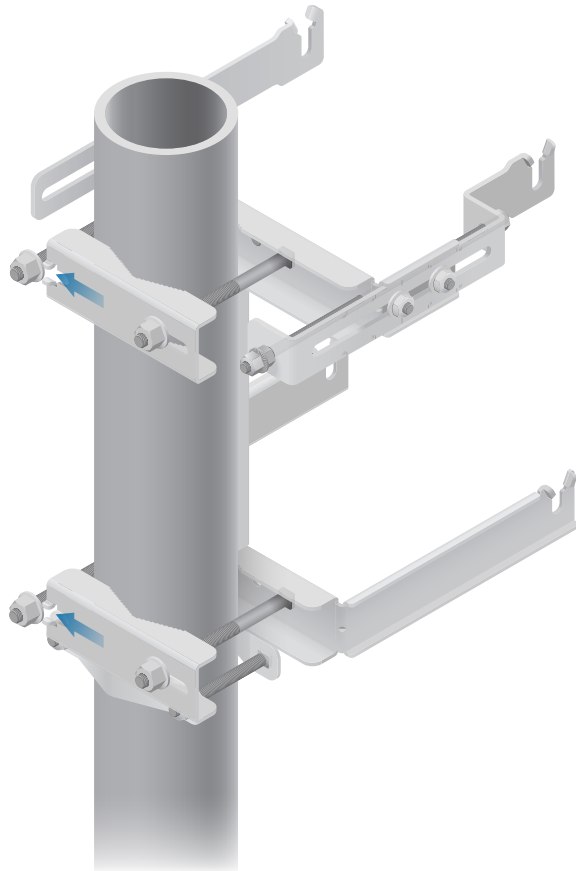


Note: The mounting assembly can accommodate a $\varnothing$ 38.1 - 101.6 mm (1.5" - 4.0") pole.

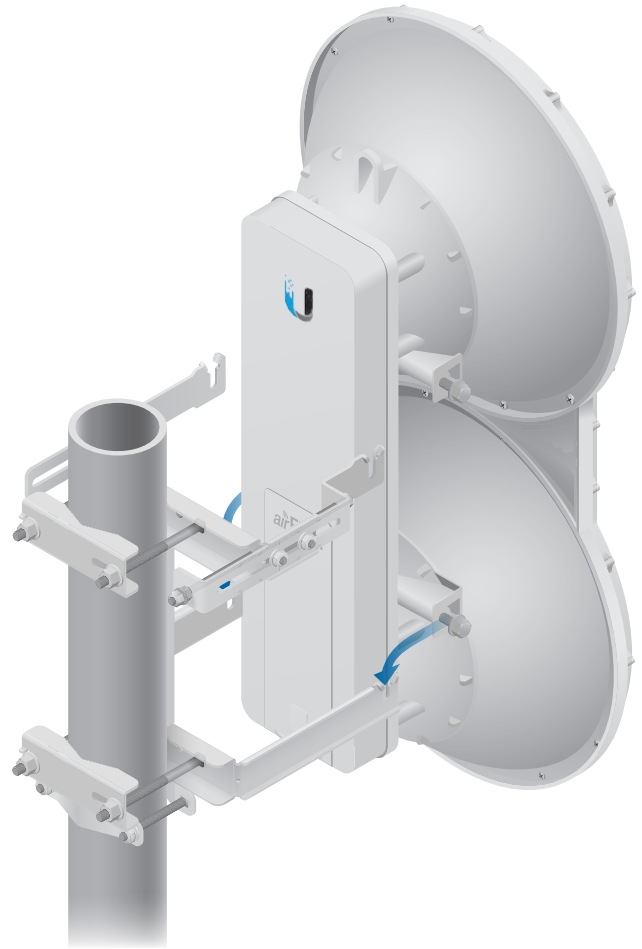
- a. Orient the *Azimuth Support Brackets* around the pole so it is aimed in the direction of the other airFiber radio.
- b. Slide the open slot of the *Azimuth Support Bracket* over the corresponding *M10x100 Carriage Bolt*.
- c. Tighten the *M10 Serrated Flange Nuts* to approximately 50 N-m.



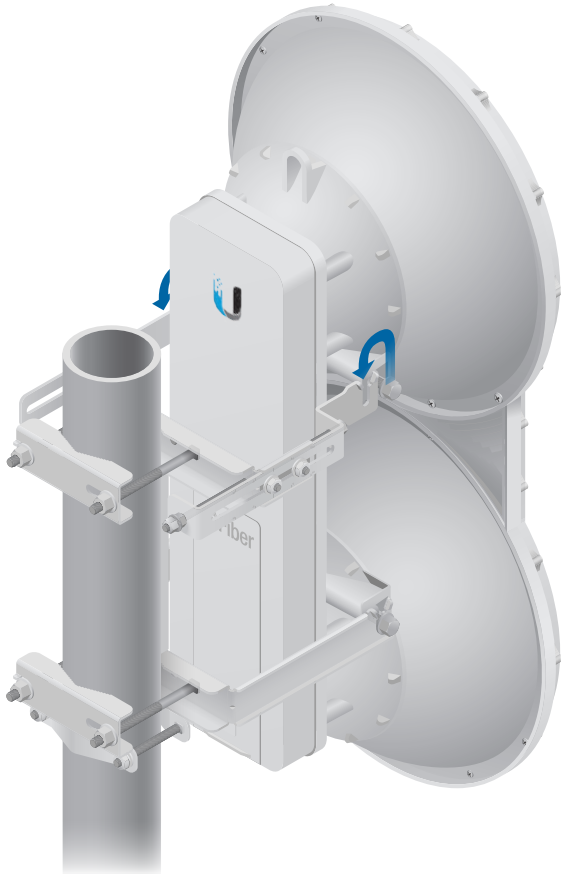
2. Attach the mounting assembly to a pole.
 - a. Orient the mounting assembly around the pole so it is aimed in the direction of the other airFiber radio.
 - b. Slide the open slot of each *Pole Clamp* over the corresponding *M10x150 Carriage Bolt*.
 - c. Tighten the *M10 Serrated Flange Nuts* of the *M10x150 Carriage Bolts* to secure the mounting assembly to the pole.



3. Lift the airFiber radio and align the two lower *Pre-Installed M10x25 Flanged Bolts* with the slots on the *Lower Mount Bracket*. Seat the bolts in the slots.



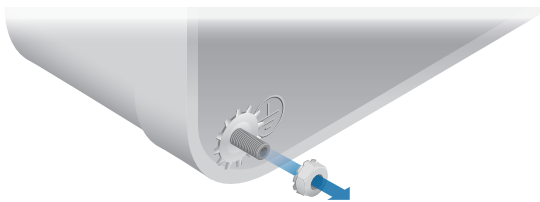
- Align the two upper *Pre-Installed M10x25 Flanged Bolts* of the airFiber radio next to the slots on the *Upper Mount Bracket*. Lift the airFiber radio and seat the bolts in the slots.



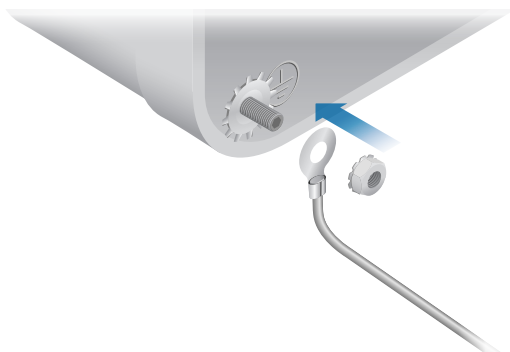
Grounding

To attach a ground wire:

- Remove the nut from the *Grounding Point*.



- Attach a ground wire (min. 8 AWG or 10 mm²) to the lug and replace the nut to secure the wire.



- Secure the other end of the ground wire to a grounded mast, pole, tower, or grounding bar.



WARNING: Failure to properly ground your airFiber units will void your warranty.



Note: The ground wire should be as short as possible and no longer than one meter in length.

Connecting Ethernet

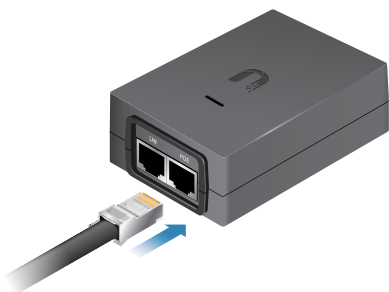
- Push the button and slide the port cover down to access cable ports. (The port cover cannot be completely removed.)



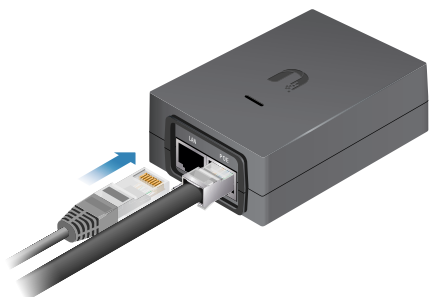
- Connect the Data/PoE Ethernet cable:
 - Feed an outdoor, shielded CAT6 cable up through the rightmost cable feed slot on the bottom of the port cover.
 - Connect the cable to the *Data* port.
 - Create a strain relief for the Ethernet cable by feeding a *Cable Tie* through the tie slot to the side of the cable.
 - Wrap the *Cable Tie* around the cable and tighten.



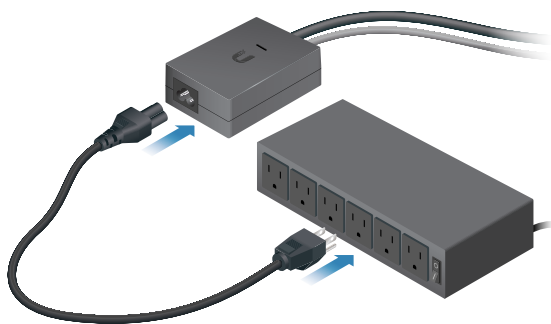
3. Connect the other end of the Ethernet cable from the *Data* port to the Ethernet port labeled **POE** on the *GigE PoE Adapter*.



4. Connect an Ethernet cable from your network to the Ethernet port labeled **LAN** on the *GigE PoE Adapter*.

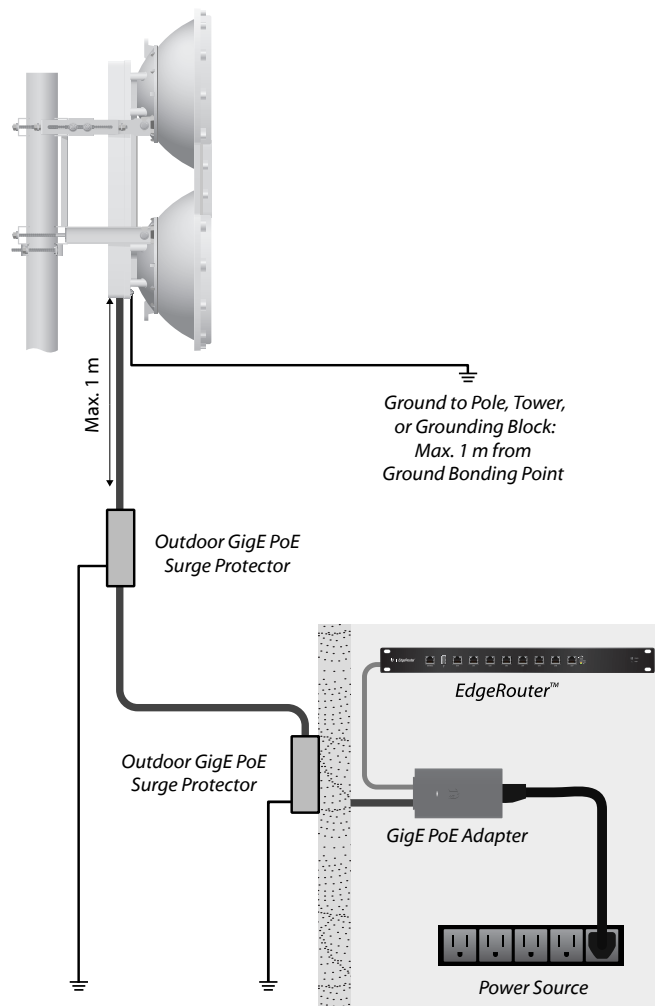


5. Connect the *Power Cord* to the power port on the *GigE PoE Adapter*. Connect the other end of the *Power Cord* to a power source.



Note: For added protection, we recommend installing two GigE PoE surge protectors. Install the first surge protector within one meter of the airFiber *Data* port, and install the second surge protector at the ingress point of the location housing the wired network equipment.

Below is a diagram of a finished installation with recommended surge protectors installed.



Alignment

Tips

- To accurately align the airFiber radios for best performance, you **MUST** align only one end of the link at a time.
- For more convenient alignment, you may consider using long-range scopes (not included) temporarily attached to your airFiber radios.
- You may need to use additional hardware to compensate for issues such as the improper orientation of a mounting pole or significant elevation differences between airFiber radios.

Determining the Received Signal Level

There are three methods for determining the received signal level:

- LED Displays (See the next column.)
- airFiber Configuration Interface (See [“Using the airFiber Configuration Interface” on page 14.](#))
- Audio tone (Optional equipment required. See [“Using the Audio Tone” on page 16.](#))

Using the LED Displays

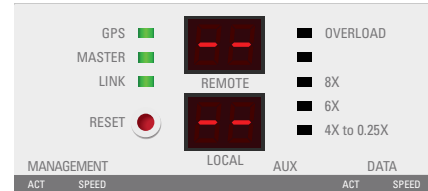
Before a link is established, the *Master's LED Display* looks like this:

- GPS and *Master* LEDs are solidly lit



Note: The GPS LED may not be lit if there is a weak GPS signal. A GPS signal is not required for alignment.

- *Link Status* LED flashes (Normal Flash 1:1)
- *Remote* and *Local LED Displays* show a double dash



Note: The *Local LED Display* may briefly flash a large number (such as 95) when there is no link.

Establishing a Link

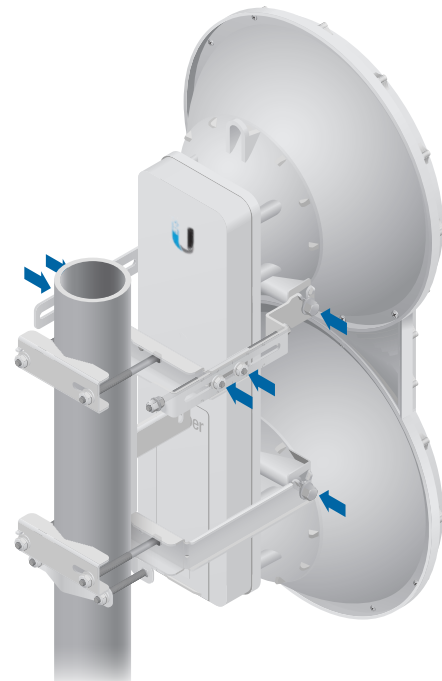
Adjust the positions of the *Master* and the *Slave* to establish a link.



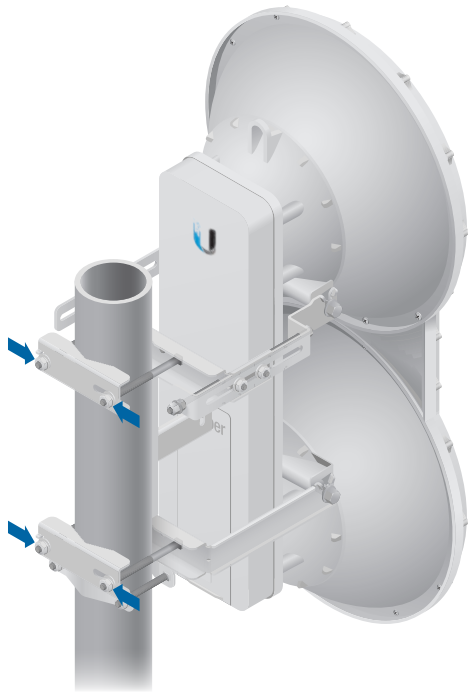
Note: The *Master* must be aimed first at the *Slave* because the *Slave* does not transmit any RF signal until it detects transmissions from the *Master*.

1. Ensure that the following bolts and nuts are loose:

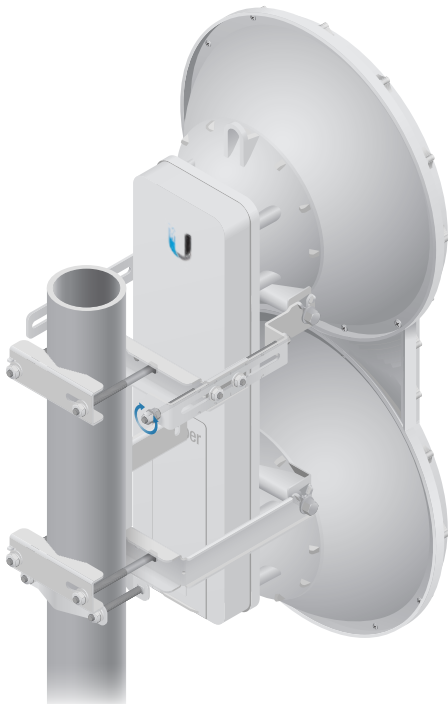
- Four *Pre-Installed M10x25 Flanged Bolts* on the airFiber radio (two on each side)
- Four *M10 Hex Nuts* used to lock the elevation alignment on the *Upper Mount Bracket* (two on each side)



2. Ensure that the pole mount is snug yet the four *M10 Hex Nuts* attaching the *Pole Clamps* are loose enough to allow rotation around the pole for azimuth alignment.

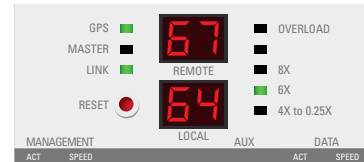


3. **Master** Visually aim the *Master* at the *Slave*. To adjust the *Master's* position:
 - a. Rotate the airFiber radio on the pole to align the azimuth.
 - b. Use the hex nut on the *Elevation Rod* to adjust the elevation.



Note: Do NOT make simultaneous adjustments on the *Master* and *Slave*.

4. **Slave** Visually aim the *Slave* at the *Master*. To adjust the *Slave's* position:
 - a. Rotate the airFiber radio on the pole to align the azimuth.
 - b. Use the hex nut on the *Elevation Rod* to adjust the elevation.
5. Check to see if a link is established. Ensure that the *Link Status* LED is solidly lit green and the *Remote* and *Local* LED Displays of the *Slave* are displaying signal levels.



6. **Slave** Aim the *Slave* at the *Master* to achieve the strongest signal level on the *Remote LED Display* of the *Slave*.



Note: Values on the *LED Displays* are displayed in negative (-) dBm. For example, 67 represents a received signal level of -67 dBm. Smaller numerical values indicate stronger received signal levels. For example, a reading of 49 is stronger than a reading of 55.



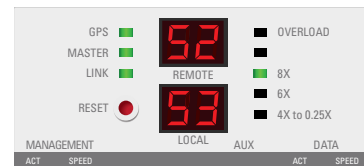
Note: Maximum signal strength can best be achieved by iteratively sweeping through both azimuth and elevation.

7. **Master** Aim the *Master* at the *Slave* to achieve the strongest signal level on the *Remote LED Display* of the *Master*.



Note: If the *Overload* LED lights up, identify and eliminate any source of strong in-band interference.

8. Repeat steps 6 and 7 until you achieve a symmetric link, with the signal levels within 1 dB of each other. This ensures the best possible data rate between the airFiber radios.



9. Lock the alignment on both airFiber radios by tightening the nuts and bolts.
10. Observe the *Local* and *Remote LED Displays* of each airFiber radio to ensure that the values remain constant while tightening the nuts and bolts. If any LED value changes during the locking process, loosen the nuts and bolts, finalize the alignment of each airFiber radio again, and retighten the nuts and bolts.
11. For each airFiber radio, close the port cover and ensure that the Ethernet cable stays in the cable feed slot.

Using the airFiber Configuration Interface

Before You Begin



Note: The instructions in this section assume that you are viewing the *Antenna Alignment* screen of the *Master*; however, you can also use the *Antenna Alignment* screen of the *Slave*.

To access the airFiber Configuration Interface:

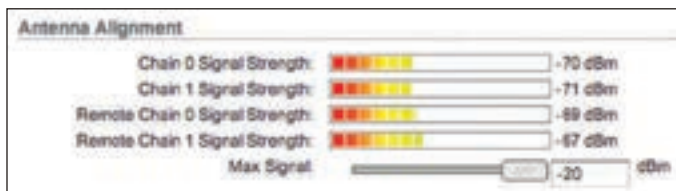
1. Make sure that your computer is connected to the *Management* port on the airFiber AF-5.
2. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.1.x subnet.
3. Launch your web browser. Type **http://192.168.1.20** in the address field and press **enter** (PC) or **return** (Mac).



4. The login screen will appear. Enter **ubnt** in the *Username* and *Password* fields. Click **Login**.



5. The *Main* tab of the airFiber Configuration Interface appears. Click the **Tools** drop-down list at the top right corner of the page.
6. Click **Align Antenna**. You will use the *Align Antenna* tool to point and optimize the antenna in the direction of maximum link signal. (The *Antenna Alignment* window is designed to refresh every 250 milliseconds. See **“Align Antenna” on page 38** for more details.)
7. The *Antenna Alignment* window appears, displaying the *Signal Strengths* for both airFiber radios. The *Chain Signal Strength* bar graphs display the *Signal Strengths* for the local airFiber AF-5 you have accessed, while the *Remote Signal Strength* bar graphs display the *Signal Strengths* for the remote airFiber AF-5.



Establishing a Link

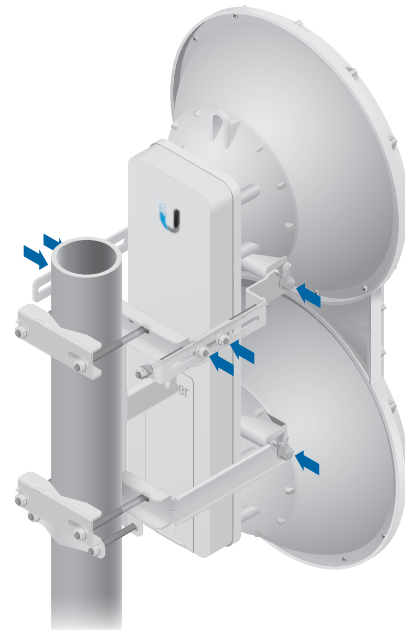
Adjust the positions of the *Master* and the *Slave* to establish a link.



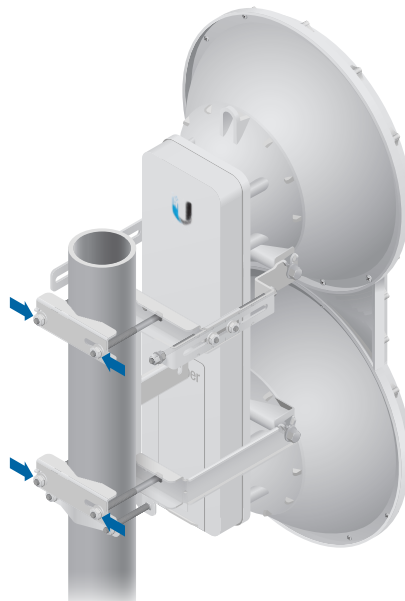
Note: The *Master* must be aimed first at the *Slave* because the *Slave* does not transmit any RF signal until it detects transmissions from the *Master*.

1. Ensure that the following bolts and nuts are loose:

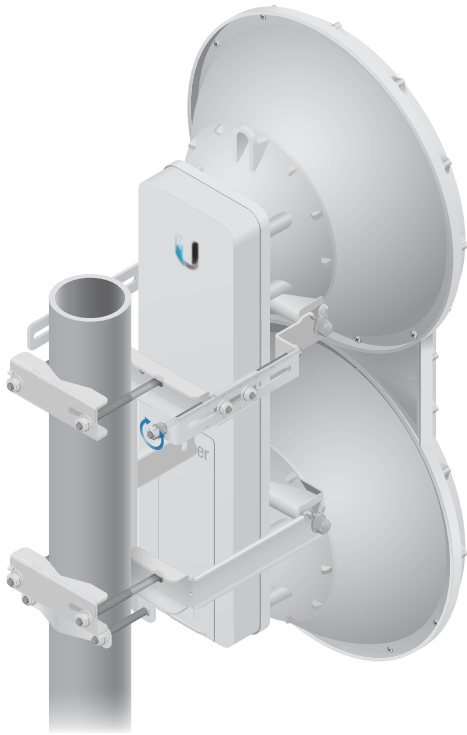
- Four *Pre-Installed M10x25 Flanged Bolts* on the airFiber radio (two on each side)
- Four *M10 Hex Nuts* used to lock the elevation alignment on the *Upper Mount Bracket* (two on each side)



2. Ensure that the pole mount is snug yet the four *M10 Hex Nuts* attaching the *Pole Clamps* are loose enough to allow rotation around the pole for azimuth alignment.

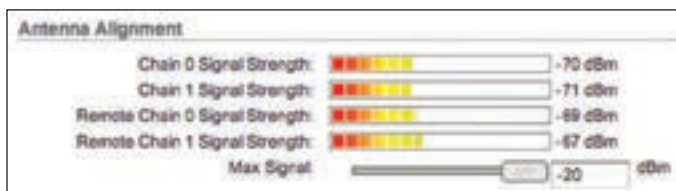


3. **Master** Visually aim the *Master* at the *Slave*. To adjust the *Master's* position:
 - a. Rotate the airFiber radio on the pole to align the azimuth.
 - b. Use the hex nut on the *Elevation Rod* to adjust the elevation.



Note: Do NOT make simultaneous adjustments on the *Master* and *Slave*.

4. **Slave** Visually aim the *Slave* at the *Master*. To adjust the *Slave's* position:
 - a. Rotate the airFiber radio on the pole to align the azimuth.
 - b. Use the hex nut on the *Elevation Rod* to adjust the elevation.
5. Check to see if a link is established. Ensure that the local and *Remote Signal Strength* bar graphs are displaying signal levels.



6. **Slave** Aim the *Slave* at the *Master* to achieve the strongest signal level on the *Remote Signal Strength* bar graph of the *Slave*.



Note: The *Signal Strength* bar graphs display the absolute power level (in dBm) of the received signal for each chain. Smaller numerical values indicate stronger received signal levels. For example, a reading of -49 dBm is stronger than a reading of -55 dBm.



Note: Maximum signal strength can best be achieved by iteratively sweeping through both azimuth and elevation.

7. **Master** Aim the *Master* at the *Slave* to achieve the strongest signal level on the local *Signal Strength* bar graph of the *Master*.



Note: If the Overload LED lights up, identify and eliminate any source of strong in-band interference.

8. Repeat steps 6 and 7 until you achieve a symmetric link, with the signal levels within 1 dB of each other. This ensures the best possible data rate between the airFiber radios.



9. Lock the alignment on both airFiber radios by tightening the nuts and bolts.
10. Observe the *Antenna Alignment* window to ensure that the values remain constant while tightening the nuts and bolts. If the values change during the locking process, loosen the nuts and bolts, finalize the alignment of each airFiber radio again, and retighten the nuts and bolts.
11. For each airFiber radio, close the port cover and ensure that the Ethernet cable stays in the cable feed slot.

Using the Audio Tone

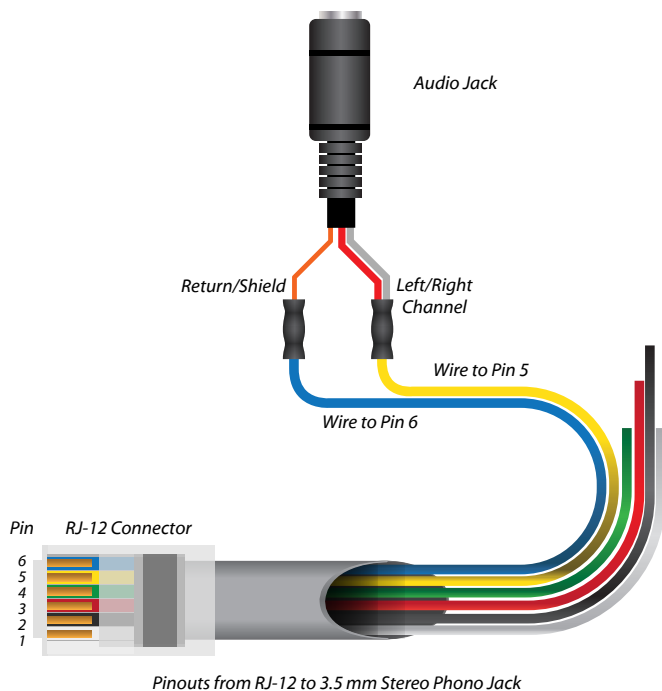
Before You Begin

Create your own cable adapter to connect the *Aux* port to your headphones or other listening device. The cable adapter requires two items:

- An RJ-12 cable with an RJ-12 connector
 - A cable with a 3.5 mm, female, stereo phono jack (mono jack is acceptable)
1. Attach the wire from pin 6 of the RJ-12 cable to the return or shield wire of the 3.5 mm jack.
 2. Attach the wire from pin 5 of the RJ-12 cable to both the left and right channel wires of the 3.5 mm stereo phono jack.



Note: For a mono jack, connect the wire from pin 5 to the + wire of the mono jack.



Note: Wire colors may vary on RJ-12 cables.

Establishing a Link

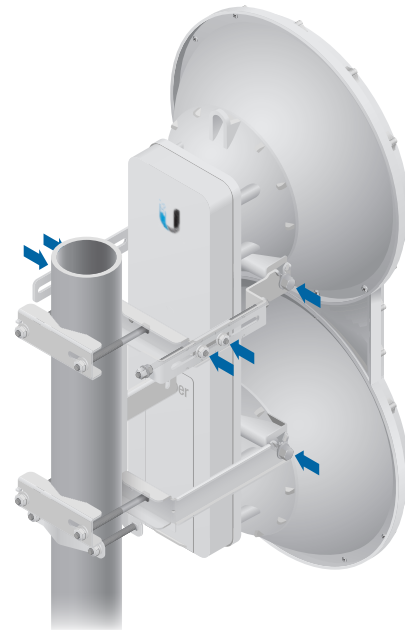
Adjust the positions of the *Master* and the *Slave* to establish a link.



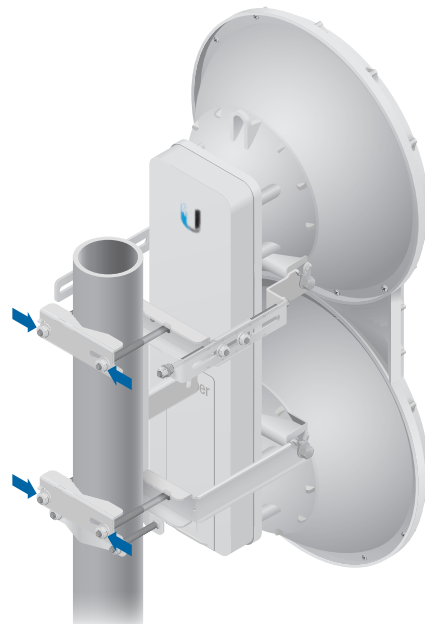
Note: The *Master* must be aimed first at the *Slave* because the *Slave* does not transmit any RF signal until it detects transmissions from the *Master*.

1. Ensure that the following bolts and nuts are loose:

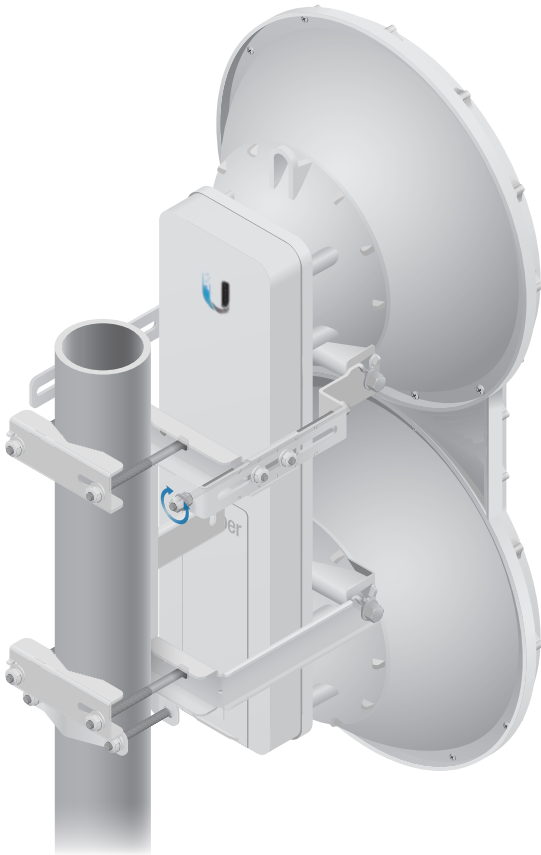
- Four *Pre-Installed M10x25 Flanged Bolts* on the airFiber radio (two on each side)
- Four *M10 Hex Nuts* used to lock the elevation alignment on the *Upper Mount Bracket* (two on each side)



2. Ensure that the pole mount is snug yet the four *M10 Hex Nuts* attaching the *Pole Clamps* are loose enough to allow rotation around the pole for azimuth alignment.



3. **Master** Visually aim the *Master* at the *Slave*. To adjust the *Master's* position:
 - a. Rotate the airFiber radio on the pole to align the azimuth.
 - b. Use the hex nut on the *Elevation Rod* to adjust the elevation.



Note: Do NOT make simultaneous adjustments on the *Master* and *Slave*.

4. **Slave** Visually aim the *Slave* at the *Master*. To adjust the *Slave's* position:
 - a. Rotate the airFiber radio on the pole to align the azimuth.
 - b. Use the hex nut on the *Elevation Rod* to adjust the elevation.
5. **Slave** Listen to the audio tone of the *Slave* – the higher the pitch, the stronger the signal strength. Aim the *Slave* at the *Master* to achieve the strongest signal level on the *Slave*.



Note: Maximum signal strength can best be achieved by iteratively sweeping through both azimuth and elevation.

6. **Master** Aim the *Master* at the *Slave* to achieve the strongest signal level on the *Master*.



Note: If the Overload LED lights up, identify and eliminate any source of strong in-band interference.

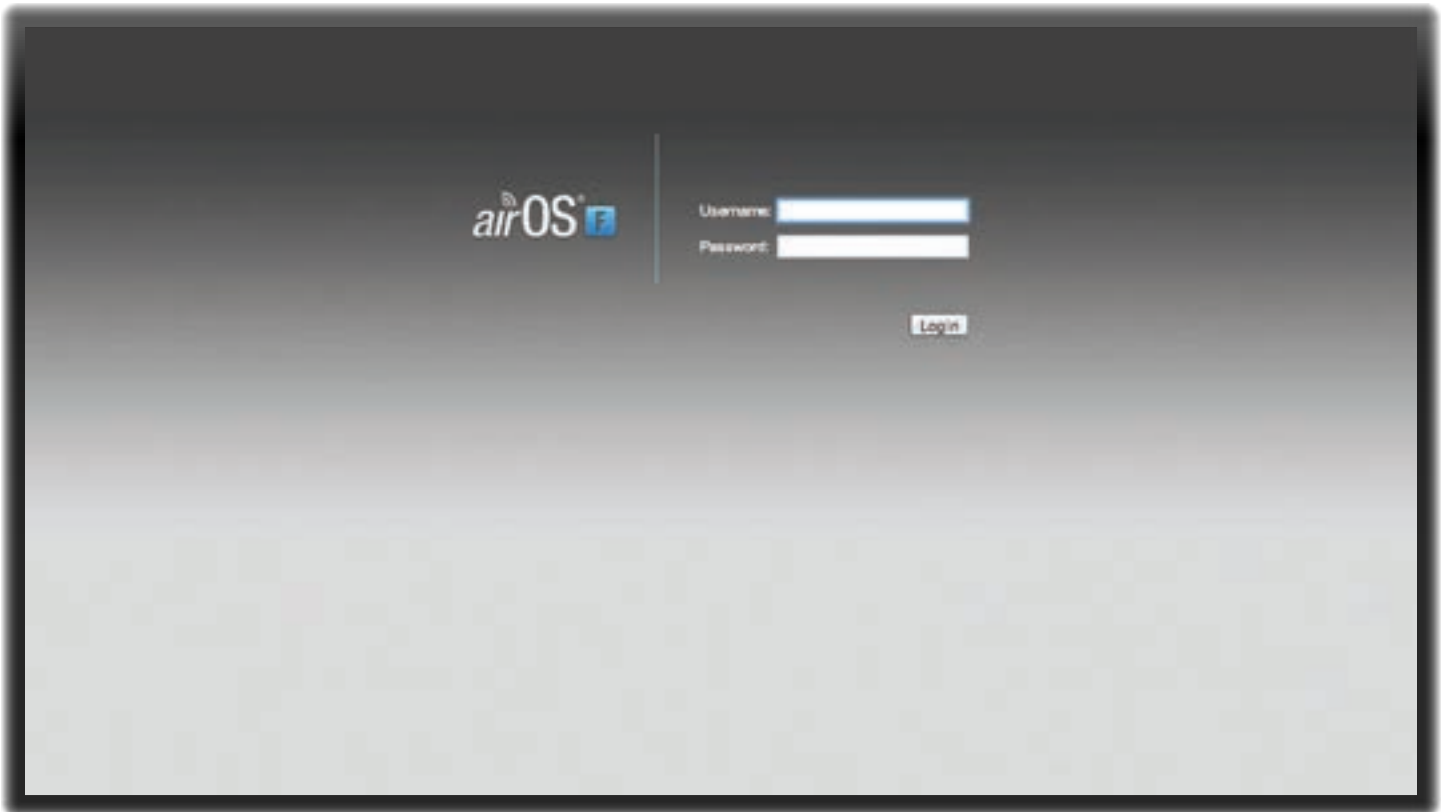
7. Repeat steps 6 and 7 until you achieve a symmetric link, with the signal levels within 1 dB of each other. This ensures the best possible data rate between the airFiber radios.



Note: If you have difficulty discerning whether the link is symmetric, you can use one of the following methods to determine more precise, received signal level readings.

- LED Display (See [“Using the LED Displays” on page 12.](#))
- airFiber Configuration Interface (See [“Using the airFiber Configuration Interface” on page 14.](#))

8. Lock the alignment on both airFiber radios by tightening the nuts and bolts.
9. Listen to the audio tone for each airFiber radio to ensure that the values remains constant while tightening the nuts and bolts. If the audio tones change during the locking process, loosen the nuts and bolts, finalize the alignment of each airFiber radio again, and retighten the nuts and bolts.
10. For each airFiber radio, close the port cover and ensure that the Ethernet cable stays in the cable feed slot.



Chapter 3: Navigation

The airFiber Configuration Interface is an advanced operating system capable of powerful wireless and routing features, built upon a simple and intuitive user interface foundation.

The airFiber AF-5 uses the airFiber Configuration Interface for easy configuration and management via a web browser.

There are two ways to access the airFiber Configuration Interface:

- **Management Port** Enabled by default. Use a direct connection to the *Management* port for out-of-band management.
- **In-Band Management** Enabled by default. In-band management is available through the local *Data* port or the *Data* port at the other end of the link. You can disable it on the *Network* tab. (See **“Management Network Settings”** on page 26 for more details.)

Accessing the airFiber Configuration Interface

Connect to the airFiber Configuration Interface.

1. Make sure that your host machine is connected to the LAN that is connected to the *Management* port on the airFiber AF-5.
2. Configure the Ethernet adapter on your host system with a static IP address on the 192.168.1.x subnet (for example, 192.168.1.100).

3. Launch your web browser. Type **http://192.168.1.20** in the address field and press **enter** (PC) or **return** (Mac).



4. Upon initial login, the *Terms of Use* appear on the login screen. Enter **ubnt** in the *Username* and *Password* fields, and select the appropriate choices from the *Country* and *Language* drop-down lists. Check the box next to *I agree to these terms of use*, and click **Login**.



Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

5. The airFiber Configuration Interface will appear, allowing you to customize your settings as needed.

Product Verification

The airFiber Configuration Interface will verify whether a product is genuine or counterfeit.

For a genuine airFiber AF-5, the airFiber Configuration Interface will display a Genuine Product logo in the lower left corner of the screen.



For any product that is not an official Ubiquiti product, the airFiber Configuration Interface will display a counterfeit warning. Please contact Ubiquiti at support@ubnt.com regarding this product.



Note: For product models introduced prior to 2012, the airFiber Configuration Interface will NOT display any logo in the lower left corner of the screen.

Interface Tabs

The airFiber Configuration Interface contains six main tabs, each of which provides a web-based management page to configure a specific aspect of the airFiber AF-5. This User Guide covers each tab with a chapter. For details on a specific tab, refer to the appropriate chapter.

- **Main** The **“Main Tab” on page 20** displays device status, statistics, and network monitoring links.
- **Wireless** The **“Wireless Tab” on page 23** configures basic wireless settings, including the wireless mode, link name, frequency, output power, speed, and wireless security.
- **Network** The **“Network Tab” on page 26** configures the management network settings, Internet Protocol (IP) settings, management VLAN, and automatic IP aliasing.
- **Advanced** The **“Advanced Tab” on page 28** provides more precise wireless interface controls, including advanced wireless settings and advanced Ethernet settings.
- **Services** The **“Services Tab” on page 31** configures system management services: Ping Watchdog, Simple Network Management Protocol (SNMP), servers (web, SSH, telnet), Network Time Protocol (NTP) client, Dynamic Domain Name System (DDNS) client, system log, and device discovery.
- **System** The **“System Tab” on page 35** controls system maintenance routines, administrator account management, location management, device customization, firmware update, and configuration backup. You can also change the language of the web management interface.

Each page also contains network administration and monitoring tools:

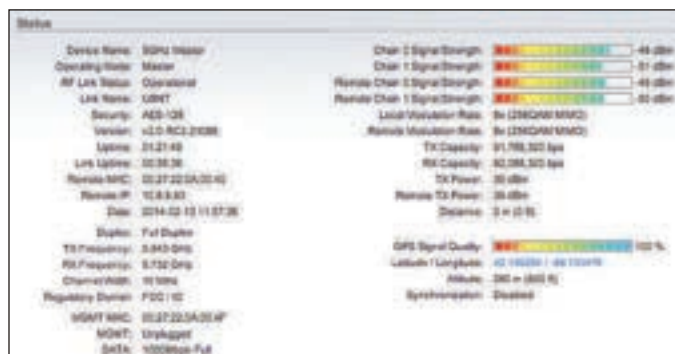
- **“Align Antenna” on page 38**
- **“Discovery” on page 39**
- **“Ping” on page 39**
- **“Traceroute” on page 39**



Chapter 4: Main Tab

The *Main* tab displays a summary of the link status information, current values of the basic configuration settings, network settings and information, and traffic statistics.

Status



Device Name Displays the customizable name or identifier of the device. The Device Name (also known as host name) is displayed in registration screens and discovery tools.

Operating Mode Displays the mode of the airFiber AF-5: *Slave*, *Master*, or *Reset*.

RF Link Status Displays the status of the airFiber AF-5: *RF Off*, *Syncing*, *Beaconing*, *Registering*, *Enabling*, *Listening*, *Operational*, *DFS CAC*, or *RADAR Detected*.



Note: Most of the RF Link Statuses map to specific flash rates of the *Link Status* LED (See **“LEDs” on page 2** for more details.)

Status	Flash Rate of LED
RF Off	Off
Syncing	Short Flash (1:3 on/off cycle)
DFS countries only:	
• DFS CAC	
• RADAR Detected	Normal Flash (1:1 on/off cycle)
Beaconing	
Registering	Long Flash (3:1 on/off cycle)
Operational	On

When the airFiber AF-5 operates in a DFS country, it performs a Channel Availability Check (CAC) before operating. The rules vary by country and frequency, but in general:

- **FCC domains** If the airFiber AF-5 operates in the DFS band (5.4 GHz band), then the following rule applies:
 - If the *TX* and *RX Frequencies* are the same, then the airFiber AF-5 performs a 60-second check on the *Master* only.
 - If the *TX* and *RX Frequencies* are different, then the airFiber AF-5 performs a 60-second check on both the *Master* and *Slave*.
- **ETSI domains** For most frequencies, the airFiber AF-5 performs a 60-second check on the *Master* and *Slave*; however, if it operates in the 5600-5650 MHz range, then the airFiber AF-5 performs a 10-minute check.

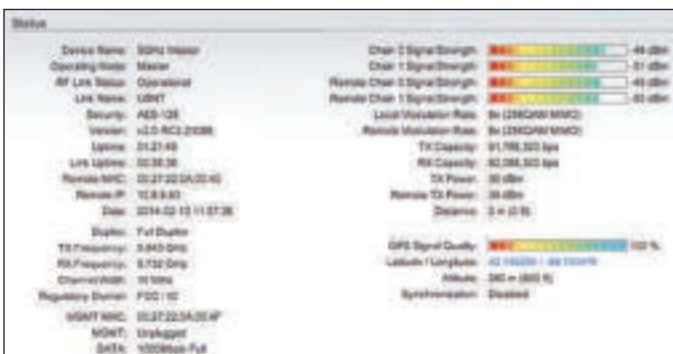
While the airFiber AF-5 is performing this check, the *RF Link Status* displays *DFS CAC*, and the *RF Link Timeout* is displayed.

If radar is detected, the *RF Link Status* displays *RADAR Detected*, and the *RF Link Timeout* is displayed.

RF Link Timeout (Available only if the *RF Link Status* is *DFS CAC* or *RADAR Detected*.) During the *DFS CAC* or *RADAR Detected* state, the *RF Link Timeout* counts down the time remaining before the airFiber AF-5 can move to the next RF link state.

Link Name Displays the name of your link.

Security AES-128 is enabled at all times.



Version Displays the airFiber Configuration Interface software version.

Uptime This is the total time the device has been running since the latest reboot (when the device was powered up) or software upgrade. The time is displayed in days, hours, minutes, and seconds.

Link Uptime This is the total time the airFiber link has been continuously operational. The time is displayed in days, hours, minutes, and seconds.

Remote MAC Displays the Management Ethernet MAC address of the remote airFiber AF-5.

Remote IP Displays the Management Ethernet IP address of the remote airFiber AF-5.

Date Displays the current system date and time. The date and time are displayed in YEAR-MONTH-DAY HOURS:MINUTES:SECONDS format. The system date and time is retrieved from the Internet using NTP (Network Time Protocol). The NTP Client is enabled by default on the *Services* tab. The airFiber AF-5 doesn't have an internal clock, and the date and time may be inaccurate if the NTP Client is disabled or the device isn't connected to the Internet.

Duplex Displays *Full Duplex* or *Half Duplex*. Full-duplex mode allows communication in both directions simultaneously. Half-duplex mode allows communication in one direction at a time, alternating between transmission and reception.

TX Frequency Displays the current transmit frequency. The airFiber AF-5 uses the radio frequency specified to transmit data.

RX Frequency Displays the current receive frequency. The airFiber AF-5 uses the radio frequency specified to receive data.

Channel Width Size of the channel in MHz.

Regulatory Domain Displays the regulatory domain (*FCC/IC*, *ETSI*, or *Other*), as determined by country selection.

MGMT MAC Displays the MAC address of the *Management* port.

MGMT Displays the speed and duplex of the *Management* port.

DATA Displays the speed and duplex of the *Data* port.

Chain 0/1 Signal Strength Displays the absolute power level (in dBm) of the received signal for each chain.

The software calculates the proper signal strength based on the measured distance and power levels, and then it scales the *Signal Strength* bar graphs so that when the link is aimed correctly, the bar graphs are full-scale. If the bar graphs are not full-scale, then they indicate that your link is not optimally aimed.

Remote Chain 0/1 Signal Strength Displays the absolute power level (in dBm) of the received signal for each chain of the remote airFiber AF-5. The bar graphs will display as full-scale once the link is aimed correctly.

Local Modulation Rate Displays the modulation rate:

- 10x (1024QAM MIMO)
- 8x (256QAM MIMO)
- 6x (64QAM MIMO)
- 4x (16QAM MIMO)
- 2x (QPSK MIMO)
- 1x (½ Rate QPSK xRT)
- ¼x (¼ Rate QPSK xRT)

If *Automatic Rate Adaptation* is enabled on the *Wireless* tab, then *Local Modulation Rate* displays the current speed in use and depends on the *Maximum Modulation Rate* specified on the *Wireless* tab and current link conditions.

Remote Modulation Rate Displays the modulation rate of the remote airFiber AF-5:

- 10x (1024QAM MIMO)
- 8x (256QAM MIMO)
- 6x (64QAM MIMO)
- 4x (16QAM MIMO)
- 2x (QPSK MIMO)
- 1x (½ Rate QPSK xRT)
- ¼x (¼ Rate QPSK xRT)

TX Capacity Displays the potential TX throughput, how much the airFiber AF-5 can send, after accounting for the modulation and error rates.

RX Capacity Displays the potential RX throughput, how much the airFiber AF-5 can receive, after accounting for the modulation and error rates.

TX Power Displays the maximum average transmit output power (in dBm) of the airFiber AF-5.

Remote TX Power Displays the maximum average transmit output power (in dBm) of the remote airFiber AF-5.

Distance Displays the distance between the airFiber radios.

GPS Signal Quality Displays Global Positioning System (GPS) signal quality as a percentage value on a scale of 0-100%.

Latitude/Longitude Based on GPS tracking, reports the device's current latitude and longitude. Clicking the link opens the reported latitude and longitude in a browser using Google Maps™ (<http://maps.google.com>).

Altitude Based on GPS tracking, reports the device's current altitude relative to sea level.

Synchronization airFiber uses GPS to synchronize the timing of its transmissions. By default, this option is disabled.

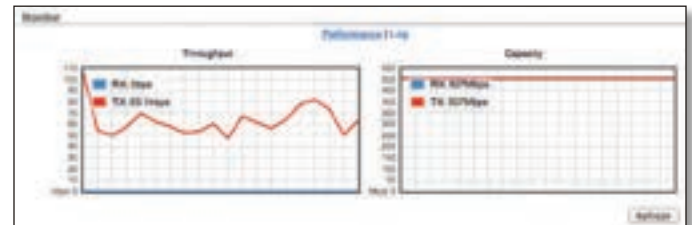
Monitor

There are two monitoring tools accessible via the links on the *Main* tab. The default is *Performance*, which is displayed when you first open the *Main* tab.

Performance

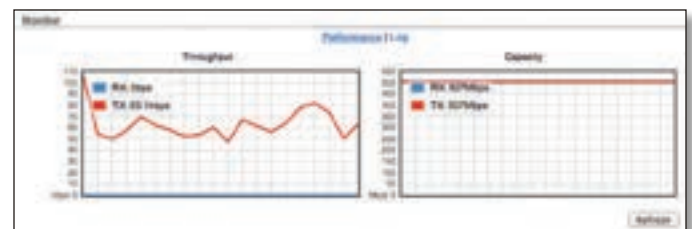
Throughput and *Capacity* charts display the current and potential data traffic.

Throughput



Throughput displays the current data traffic on the *Data* port in both graphical and numerical form. The chart scale and throughput dimension (Bps, Kbps, Mbps) change dynamically depending on the mean throughput value. The statistics are updated automatically.

Capacity



Capacity displays the potential data traffic on the *Data* port in both graphical and numerical form. The chart scale and throughput dimension (Bps, Kbps, Mbps) change dynamically depending on the mean throughput value. The statistics are updated automatically.

Refresh If there is a delay in the automatic update, click **Refresh** to manually update the statistics.

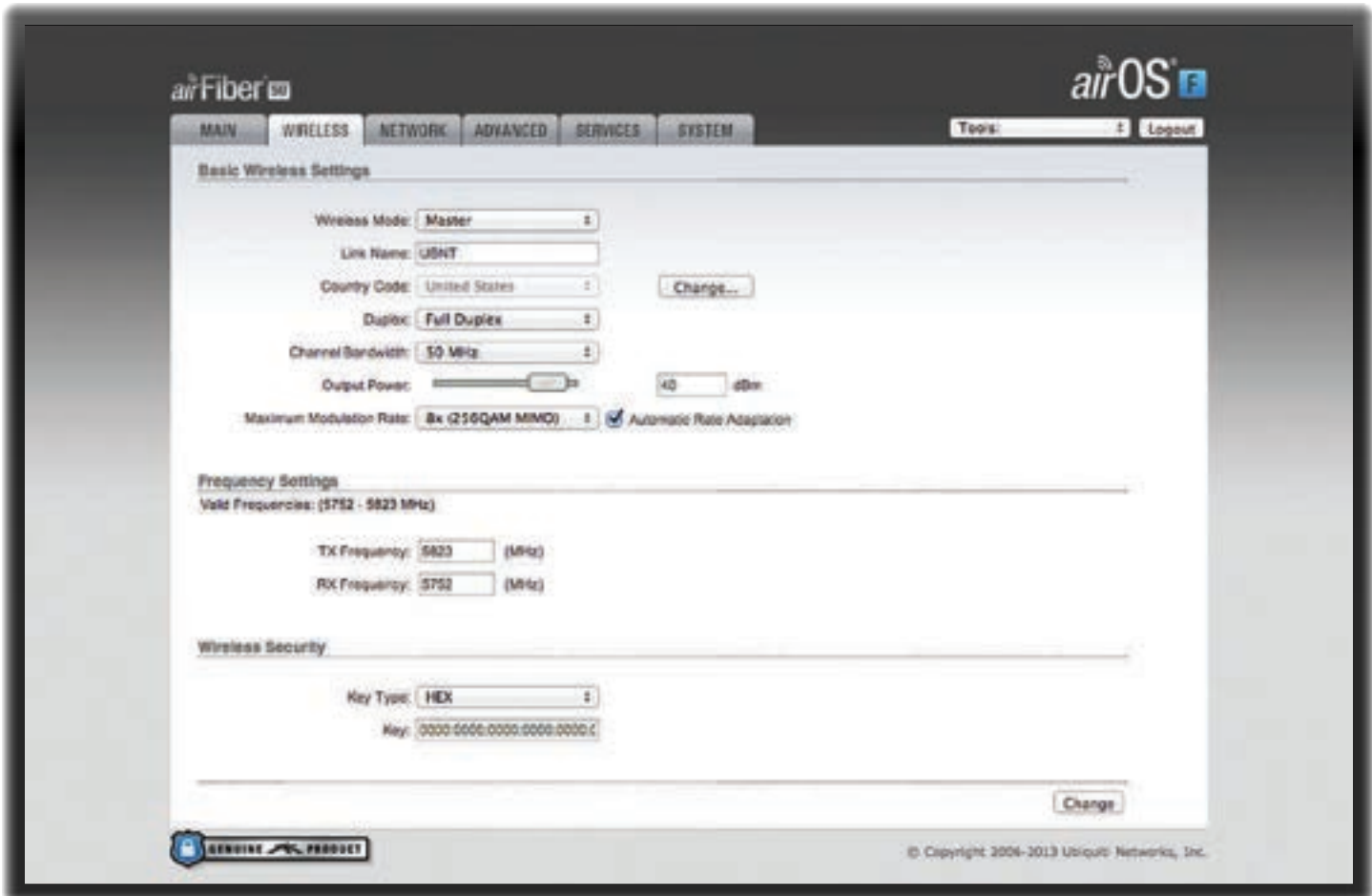
Log

When logging is enabled (see **“System Log” on page 34** to enable logging), this option lists all registered system events. By default, logging is not enabled.



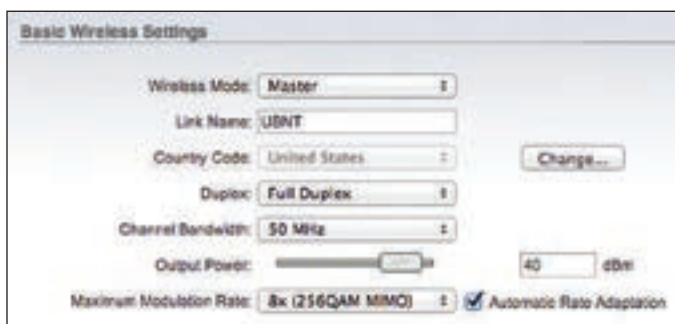
Clear To delete all entries in the system log, click **Clear**.

Refresh To update the log content, click **Refresh**.



Chapter 5: Wireless Tab

The *Wireless* tab contains options to set up the wireless part of the link. This includes wireless mode, link name, frequencies, output power, speed, and wireless security.



Change To save or test your changes, click **Change**.

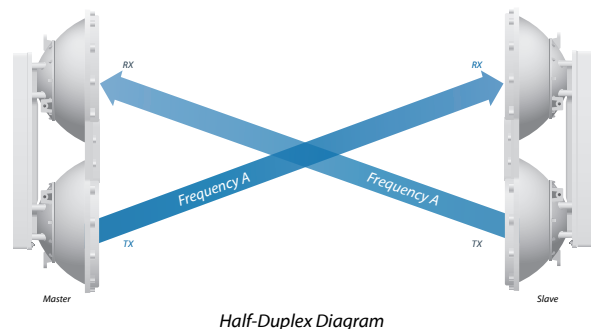
A new message appears. You have three options:

- **Apply** To immediately save your changes, click **Apply**.
- **Test** To try the changes without saving them, click **Test**. To keep the changes, click **Apply**. If you do not click **Apply** within 180 seconds (the countdown is displayed), the airFiber AF-5 times out and resumes its earlier configuration.
- **Discard** To cancel your changes, click **Discard**.

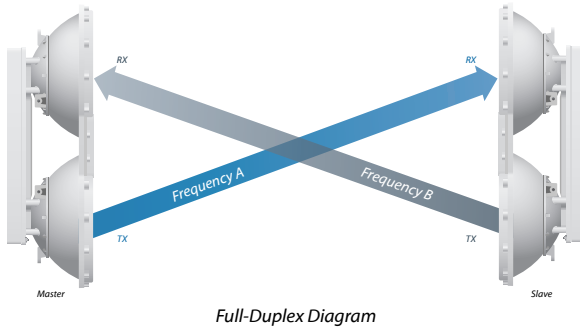
Write down the settings you configure on the *Wireless* tab. You will need to enter the same settings on the airFiber AF-5 at the other end of your PtP link. The exceptions are as follows:

- **Wireless Mode** Configure one airFiber AF-5 as the *Master* and the other as the *Slave*.
- **TX and RX Frequencies** The *TX Frequency* on the Master should be used as the *RX Frequency* on the Slave, and vice versa.

For *Half Duplex* mode (default), the *TX* and *RX Frequencies* can be the same or different to suit local interference.



For **Full Duplex** mode, the **TX** and **RX Frequencies** should be different.



Basic Wireless Settings

In this section, configure the basic wireless settings, such as wireless mode, link name, country code, frequencies, output power, speed, and gain.

Wireless Mode By default, the Wireless Mode is *Slave*. You must configure one airFiber AF-5 to **Master** because each PtP link must have one *Master*.

Link Name Enter a name for your PtP link.

Country Code Each country has its own power level and frequency regulations. *To ensure the airFiber AF-5 operates under the necessary regulatory compliance rules, you must select the country where your device will be used.* The frequency settings and output power limits will be tuned according to the regulations of the selected country. For details, refer to this table, **“Frequency Ranges and Power Levels per Country/Region” on page 46.**

This radio is restricted to use with a license and to use only in certain EU countries or geographical areas of EU countries.

- **Change** To select a new country, click **Change**.



Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

- **Country** Select the new country.
- **I agree to these terms of use** Check this box; you must agree to the *Terms of Use* to use the product.
- **Accept** Saves your change.
- **Cancel** Discards your change.

Duplex Select **Half Duplex** or **Full Duplex**. Half-duplex operation provides more frequency planning options at the cost of higher latency and throughput. (Half-duplex mode allows communication in one direction at a time, alternating between transmission and reception.) Full-duplex operation provides the highest throughput and lowest latency; however, you have fewer frequency management options. (Full-duplex mode allows communication in both directions simultaneously.)



Note: For *Half Duplex* mode (default), the **TX** and **RX Frequencies** on the same airFiber AF-5 can be the same or different to suit local interference. For *Full Duplex* mode, the **TX** and **RX Frequencies** on the same airFiber AF-5 should be different.

Channel Bandwidth Select the appropriate channel size: **10, 20, 30, 40, or 50 MHz.**

Output Power Defines the maximum average transmit output power (in dBm) of the airFiber AF-5. To specify the output power, use the slider or manually enter the output power value. The transmit power level maximum is limited according to country regulations.

Maximum Modulation Rate or Modulation Rate Higher modulations support greater throughput but generally require stronger RF signals and a higher Signal-to-Noise Ratio (SNR). By default, *Automatic Rate Adaptation* is enabled, and *Maximum Modulation Rate* is displayed. This allows the airFiber AF-5 to automatically adjust the modulation rate to changing RF signal conditions. Under certain conditions, you may prefer to lock the *Maximum Modulation Rate* to a lower setting to improve link performance.

When *Automatic Rate Adaptation* is disabled, *Modulation Rate* is displayed. Lock the *Modulation Rate* to the setting of your choice.

Select one of the available modulation rates:

- **10x (1024QAM MIMO)**
- **8x (256QAM MIMO)**
- **6x (64QAM MIMO)**
- **4x (16QAM MIMO)**
- **2x (QPSK MIMO)**
- **1x (½ Rate QPSK xRT)**
- **¼x (¼ Rate QPSK xRT)**

Frequency Settings

The *Valid Frequencies* for your *Country Code* selection are displayed. Ensure that you use frequencies that comply with the local country regulations.

TX Frequency Enter a valid transmit frequency. The *Current State* is displayed.



Note: The *TX Frequency* on the Master should be used as the *RX Frequency* on the Slave, and vice versa.

RX Frequency Enter a valid receive frequency.

DFS Frequencies

If you have Dynamic Frequency Selection (DFS) frequencies, then you have three sets of *TX* and *RX Frequency* options. The airFiber radio will shut down on the current TX frequency if it detects certain radar pulses.

You can configure alternative TX frequencies as fallback options in case of a radar-induced shutdown. For example, if radar is detected on *TX Frequency 1*, then the airFiber radio will switch to *TX Frequency 2*.

The three *TX Frequencies* of the local airFiber radio should match the three *RX Frequencies* of the remote airFiber radio, and vice versa. This ensures that in the case of radar detection at the remote end, the local airFiber radio will scan all *RX Frequencies* until it finds the *TX Frequency* used by the remote airFiber radio.



Note: If you set *TX Frequency 2* or *3* to *0*, then they will not be used. If there is a DFS event, then the airFiber AF-5 will wait 30 minutes and then use *TX Frequency 1* again.

TX Frequency 1-3 Enter a valid transmit frequency. The *Current State* is displayed.



Note: The *TX Frequency* on the Master should be used as the *RX Frequency* on the Slave, and vice versa.

RX Frequency 1-3 Enter a valid receive frequency.

Wireless Security

airFiber uses 128-bit, AES (Advanced Encryption Standard) encryption at all times.

Key Type Specifies the character format.

- **HEX** By default, this option uses hexadecimal characters. 0-9, A-F, or a-f are valid characters.
- **ASCII** ASCII uses the standard English alphabet and numeric characters (0-9, A-Z, or a-z).

Key Select the format of the MAC address.

- **HEX** Enter 16 bytes (eight, 16-bit HEX values). You can omit zeroes and use colons, similar to the IPv6 format. The default is:

0000:0000:0000:0000:0000:0000:0000:0000.



Note: The airFiber Configuration Interface supports IPv6 formats excluding dotted quad and "::<" (double-colon) notation.

- **ASCII** Enter a combination of alphanumeric characters. Using 128-bit, SHA1 (Secure Hash Algorithm 1), the airFiber AF-5 hashes the ASCII key to create a 128-bit key for AES.



Chapter 6: Network Tab

The *Network* tab allows you to configure settings for the management network.

There are two ways to access the airFiber Configuration Interface:

- **Management Port** Enabled by default. Use a direct connection to the *Management* port for out-of-band management.
- **In-Band Management** Enabled by default. In-band management is available through the local *Data* port or the *Data* port at the other end of the link.

The *Management* port and in-band management share the default IP address of 192.168.1.20.

Change To save or test your changes, click **Change**.

A new message appears. You have three options:

- **Apply** To immediately save your changes, click **Apply**.
- **Test** To try the changes without saving them, click **Test**. To keep the changes, click **Apply**. If you do not click **Apply** within 180 seconds (the countdown is displayed), the airFiber AF-5 times out and resumes its earlier configuration.
- **Discard** To cancel your changes, click **Discard**.

Management Network Settings

In-Band Management Enabled by default. In-band management is available through the local *Data* port or the *Data* port at the other end of the link.



Note: If *In-Band Management* is enabled, ensure that each airFiber radio of a link has a unique *IP Address*. If the airFiber radios use the same *IP Address*, then you may lose access via the *Data* ports.

Management IP Address The airFiber AF-5 can use a static IP address or obtain an IP address from its DHCP server.

- **DHCP** Keep the default, *DHCP*, to use DHCP reservation on your router to assign a unique *IP Address*. The local DHCP server assigns a reserved IP address, gateway IP address, and DNS address to the airFiber AF-5.



Note: If you select the *DHCP* option, ensure that you use DHCP reservation because if you do not know the IP address, then the only way to manage the airFiber AF-5 is to reset the airFiber AF-5 to its factory default settings. (Press and hold the **Reset** button for more than five seconds.) Its default *Management IP Address* is reset to 192.168.1.20.



- **DHCP Fallback IP** Specify the IP address the airFiber AF-5 should use if a DHCP server is not found.
- **DHCP Fallback Netmask** Specify the netmask the airFiber AF-5 should use if a DHCP server is not found.

- **Static** Assign static IP settings to the airFiber AF-5.



Note: IP settings should be consistent with the address space of the airFiber AF-5's network segment.

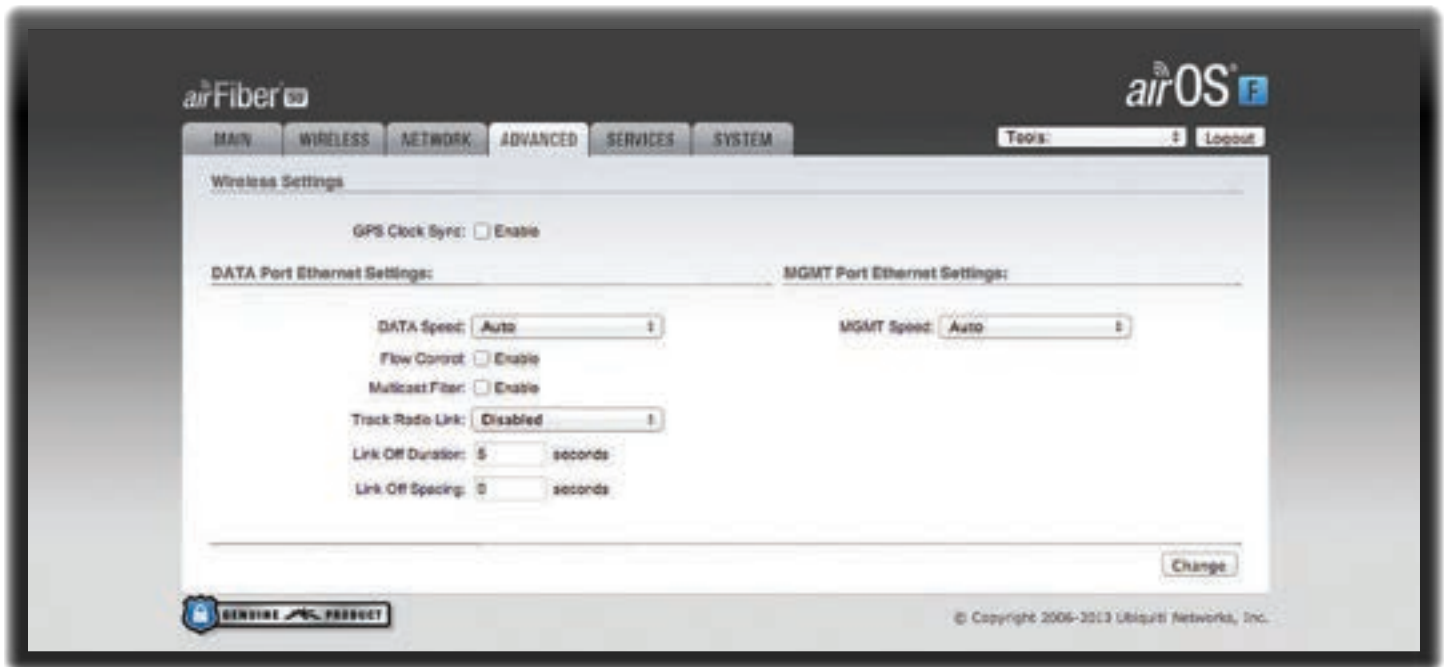
The Auto IP Aliasing setting can be useful because you can still access and manage devices even if you lose, misconfigure, or forget their IP addresses. Because an Auto IP address is based on the last two octets of the MAC address, you can determine the IP address of a device if you know its MAC address.

- **IP Address** Specify the IP address of the airFiber AF-5. This IP will be used for device management purposes.
- **Netmask** When the netmask is expanded into its binary form, it provides a mapping to define which portions of the IP address range are used for the network devices and which portions are used for host devices. The netmask defines the address space of the airFiber AF-5's network segment. The 255.255.255.0 (or "/24") netmask is commonly used on many Class C IP networks.
- **Gateway IP** Typically, this is the IP address of the host router, which provides the point of connection to the Internet. This can be a DSL modem, cable modem, or WISP gateway router. The airFiber AF-5 directs data packets to the gateway if the destination host is not within the local network.
- **Primary DNS IP** Specify the IP address of the primary DNS (Domain Name System) server.
- **Secondary DNS IP** Specify the IP address of the secondary DNS server. This entry is optional and used only if the primary DNS server is not responding.

Management VLAN If enabled, automatically creates a management Virtual Local Area Network (VLAN).

- **VLAN ID** Enter a unique VLAN ID from 2 to 4094.

Auto IP Aliasing If enabled, automatically generates an IP address for the corresponding WLAN/LAN interface. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (netmask 255.255.0.0), which is intended for use within the same network segment only. The Auto IP always starts with 169.254.X.Y, with X and Y as the last two octets from the MAC address of the airFiber AF-5. For example, if the MAC address is 00:15:6D:A3:04:FB, then the generated unique Auto IP will be 169.254.4.251. (The hexadecimal value, *FB*, converts to the decimal value, *251*.)



Chapter 7: Advanced Tab

The *Advanced* tab handles advanced wireless and Ethernet settings. These settings should not be changed unless you know the effects the changes will have on the airFiber AF-5.

Change To save or test your changes, click **Change**.

A new message appears. You have three options:

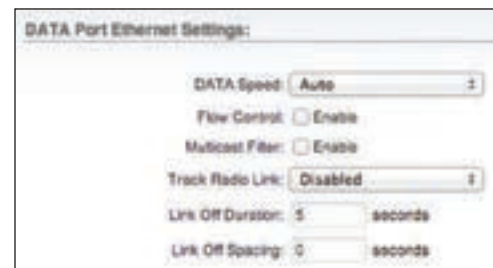
- **Apply** To immediately save your changes, click **Apply**.
- **Test** To try the changes without saving them, click **Test**. To keep the changes, click **Apply**. If you do not click **Apply** within 180 seconds (the countdown is displayed), the airFiber AF-5 times out and resumes its earlier configuration.
- **Discard** To cancel your changes, click **Discard**.

Wireless Settings



GPS Clock Sync The airFiber uses GPS to synchronize the timing of its transmissions. By default, this option is disabled.

DATA Port Ethernet Settings



DATA Speed This is the speed of the *Data* port. By default, the option is **Auto**. The airFiber AF-5 automatically negotiates transmission parameters, such as speed and duplex, with its counterpart. In this process, the networked devices first share their capabilities and then choose the fastest transmission mode they both support.

To manually specify the maximum transmission link speed and duplex mode, select one of the following options: **100 Mbps-Full**, **100 Mbps-Half**, **10 Mbps-Full**, or **10 Mbps-Half**.

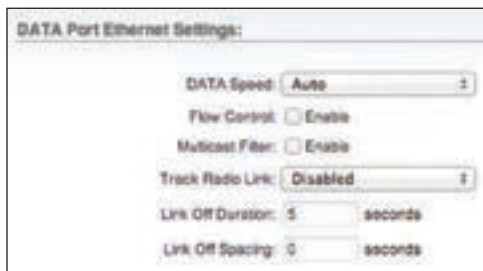
Full-duplex mode allows communication in both directions simultaneously. Half-duplex mode allows communication in one direction at a time, alternating between transmission and reception.

Flow Control If enabled, the airFiber AF-5 generates and responds to Ethernet layer PAUSE frames. The airFiber AF-5 regulates inbound traffic from the customer's network to avoid buffer overflows within the airFiber AF-5. Flow

control has the effect of controlling the inter-packet spacing of packets headed into the airFiber Data interface.

Multicast Filter If enabled, the filter blocks multicast traffic from overloading the CPU when in-band management is enabled. This allows the airFiber AF-5 to be managed in-band when the customer's network is carrying large volumes of multicast traffic, such as IPTV. The filter does not block multicast traffic going over the radio; it simply blocks it from reaching the airFiber's management interface CPU.

Track Radio Link If this option is enabled, the airFiber AF-5 disconnects the Data port's Ethernet link when the RF link is lost (The Management port is never disabled by this option). The *Track Radio Link* option is useful because it quickly indicates a "link lost" condition to the customer's routing equipment (such as a direct connection to OSPF-enabled routers).



- **Disabled** The *Track Radio Link* option is disabled by default. The Data port's Ethernet link will always remain up regardless of the RF link state.
- **Use Timeout Duration** This option is designed for use by operators who are using in-band management. Two timers control the Data port's Ethernet link.

RF Link	Ethernet Link	Notes
Goes down for the first time	The Ethernet link goes down and remains down for the number of seconds specified by the <i>Link Off Duration</i> timer. The Ethernet link will then come back up so that the airFiber AF-5 can be managed even when the RF link is down.	Even if the RF link goes back up before the <i>Link Off Duration</i> timer elapses, the Ethernet link remains down. The Ethernet link's downtime is long enough to signal to the customer's routing equipment that the path is lost.

RF Link	Ethernet Link	Notes
Goes down for the second time	The Ethernet link remains up as long as time remains on the <i>Link Off Spacing</i> timer. When the <i>Link Off Spacing</i> timer elapses, then the Ethernet link goes down again for the number of seconds specified by the <i>Link Off Duration</i> timer. (This happens only if the RF link is still down.)	The Ethernet link's uptime is long enough so the operator has enough time to access the airFiber AF-5, make configuration changes, and save those changes. Sufficient Ethernet link uptime is vital when a RF link is constantly up and down.

When the *Use Timeout Duration* option is enabled, then the *Track Radio Link* option and the following timers are enabled:

- **Link Off Duration** The *Link Off Duration* timer controls the length of time the Data port's Ethernet link will be down if the RF link goes down. Enter the number of seconds that the Ethernet link should be offline. For example, if this is set to 10 seconds, then when the RF link goes down, the Ethernet link will go down and remain down for 10 seconds (regardless of the RF link state), and then it will go back up.
- **Link Off Spacing** The *Link Off Spacing* timer controls the length of time the airFiber AF-5 will wait before allowing the Data port's Ethernet link to go down for a second time if the RF link goes down again. Enter the minimum interval (in seconds) between offline events of the Ethernet link, regardless of the RF link status. The value for *Link Off Spacing* should be larger than the value for *Link Off Duration*, and it should be enough time for the operator to access the airFiber AF-5, make any configuration changes, and apply those changes.



Note: If the *Link Off Spacing* timer is set to 0 seconds, then the Ethernet link will only use the *Link Off Duration* timer. If the *Link Off Duration* timer is set to 10 seconds and the RF link goes down, then the Ethernet link will go down for 10 seconds and then go back up regardless of the RF link state. If the RF link is still down, then the Ethernet link will not go down again until the RF link goes back up and then down again.

Here are a couple of examples involving the use of the *Use Timeout Duration* option.

- Example #1
 - **Link Off Duration** 5 seconds
 - **Link Off Spacing** 60 seconds

The Data port's Ethernet link will be initially disconnected when the RF link first goes down. That event will start a 60-second timer. The Ethernet link will remain offline for 5 seconds (regardless of the RF link status) and then come back online. The Ethernet link will remain online (regardless of the RF link state) until the 60-second timer expires.

- Example #2

- **Link Off Duration** 20 seconds
- **Link Off Spacing** 120 seconds

The Data port's Ethernet link will be initially disconnected when the RF link first goes down. That event will start a 120-second timer. The RF link goes back up after 10 seconds; however, that does not affect the Ethernet link. The Ethernet link will remain offline for 20 seconds and then come back online. The RF link goes down again after 60 seconds; however, that does not affect the Ethernet link. The Ethernet link will then remain online until the 120-second timer expires.

- **Enabled** This option is designed for use by operators who are not using in-band management. The *Track Radio Link* option is enabled without timers, so the Data port's Ethernet link follows the RF link state exactly. If the RF link goes down, then the Ethernet link goes down and remains down until the RF link goes back up.

MGMT Port Ethernet Settings



MGMT Speed This is the speed of the *Management* port. By default, the option is **Auto**. The airFiber AF-5 automatically negotiates transmission parameters, such as speed and duplex, with its counterpart. In this process, the networked devices first share their capabilities and then choose the fastest transmission mode they both support.

To manually specify the maximum transmission link speed and duplex mode, select one of the following options: **100 Mbps-Full**, **100 Mbps-Half**, **10 Mbps-Full**, or **10 Mbps-Half**. If you are running extra long Ethernet cables, a link speed of 10 Mbps could help to achieve better stability.

Full-duplex mode allows communication in both directions simultaneously. Half-duplex mode allows communication in one direction at a time, alternating between transmission and reception.

The screenshot shows the 'Services' tab in the airOS configuration interface. The top navigation bar includes 'MAIN', 'WIRELESS', 'NETWORK', 'ADVANCED', 'SERVICES', and 'SYSTEM'. The 'SERVICES' tab is selected. The interface is divided into two columns. The left column contains sections for 'Ping Watchdog', 'Web Server', 'Telnet Server', 'Dynamic DNS', and 'Device Discovery'. The right column contains sections for 'SNMP Agent', 'SSH Server', 'NTP Client', and 'System Log'. Each section has various configuration options, many of which are checked by default. A 'Change' button is located at the bottom right of the configuration area.

Chapter 8: Services Tab

The *Services* tab configures system management services: *Ping Watchdog*, *SNMP Agent*, *Web Server*, *SSH Server*, *Telnet Server*, *NTP Client*, *Dynamic DNS*, *System Log*, and *Device Discovery*.

Change To save or test your changes, click **Change**.

A new message appears. You have three options:

- **Apply** To immediately save your changes, click **Apply**.
- **Test** To try the changes without saving them, click **Test**. To keep the changes, click **Apply**. If you do not click *Apply* within 180 seconds (the countdown is displayed), the airFiber AF-5 times out and resumes its earlier configuration.
- **Discard** To cancel your changes, click **Discard**.

Ping Watchdog

Ping Watchdog sets the airFiber AF-5 to continuously ping a user-defined IP address (it can be the Internet gateway, for example). If it is unable to ping under the user-defined constraints, then the airFiber AF-5 will automatically reboot. This option creates a kind of “fail-proof” mechanism.

Ping Watchdog is dedicated to continuous monitoring of the specific connection to the remote host using the *Ping* tool. The *Ping* tool works by sending ICMP echo request packets to the target host and listening for ICMP echo response replies. If the defined number of replies is not received, the tool reboots the airFiber AF-5.

Ping Watchdog

Ping Watchdog: ☐ Enable

IP Address To Ping:

Ping Interval: 300 seconds

Startup Delay: 300 seconds

Failure Count To Reboot: 3

Save Support Info: ☐

Ping Watchdog Enables use of *Ping Watchdog*.

- **IP Address To Ping** Specify the IP address of the target host to be monitored by *Ping Watchdog*.
- **Ping Interval** Specify the time interval (in seconds) between the ICMP echo requests that are sent by *Ping Watchdog*. The default value is 300 seconds.
- **Startup Delay** Specify the initial time delay (in seconds) until the first ICMP echo requests are sent by *Ping Watchdog*. The default value is 300 seconds.
The Startup Delay value should be at least 60 seconds as the network interface and wireless connection initialization takes a considerable amount of time if the airFiber AF-5 is rebooted.
- **Failure Count to Reboot** Specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, *Ping Watchdog* will reboot the airFiber AF-5. The default value is 3.
- **Save Support Info** This generates a support information file.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Network administrators use SNMP to monitor network-attached devices for issues that warrant attention.

The airFiber AF-5 contains an *SNMP Agent*, which does the following:

- Provides an interface for device monitoring using SNMP
- Communicates with SNMP management applications for network provisioning
- Allows network administrators to monitor network performance and troubleshoot network problems

SNMP Agent

SNMP Agent: ☐ Enable

SNMP Community: public

Contact:

Location:

For the purpose of equipment identification, configure the *SNMP Agent* with contact and location information:

SNMP Agent Enables the *SNMP Agent*.

- **SNMP Community** Specify the SNMP community string. It is required to authenticate access to Management Information Base (MIB) objects and functions as an embedded password. The airFiber AF-5 also supports a read-only community string; authorized management stations have read access to all the objects in the MIB except the community strings, but do not have write access. The airFiber AF-5 supports SNMP v1. The default SNMP Community is *public*.
- **Contact** Specify the contact who should be notified in case of emergency.
- **Location** Specify the physical location of the airFiber AF-5.

Web Server

Web Server

Secure Connection (HTTPS): ☐ Enable

Secure Server Port: 443

Server Port: 80

Session Timeout: 15 minutes

The following *Web Server* parameters can be set:

Secure Connection (HTTPS) If enabled, the *Web Server* uses secure HTTPS mode.

- **Secure Server Port** If secure HTTPS mode is used, specify the TCP/IP port of the *Web Server*.

Server Port If HTTP mode is used, specify the TCP/IP port of the *Web Server*.

Session Timeout Specifies the maximum timeout before the session expires. Once a session expires, you must log in again using the username and password.

SSH Server

SSH Server

SSH Server: ☒ Enable

Server Port: 22

Password Authentication: ☒ Enable

Authorized Keys:

The following *SSH Server* parameters can be set:

SSH Server This option enables SSH access to the airFiber AF-5.

- **Server Port** Specify the TCP/IP port of the *SSH Server*.
- **Password Authentication** If enabled, you must authenticate using administrator credentials to grant SSH access to the airFiber AF-5; otherwise, an authorized key is required.

- **Authorized Keys** Click **Edit** to import a public key file for SSH access to the airFiber AF-5 instead of using an admin password.

The SSH Authorized Keys dialog box has a title bar 'SSH Authorized Keys'. Inside, there's a section 'Import Public Key File:' with a 'Choose File' button, the text 'No file chosen', and an 'Import' button. Below this is a table with columns: 'Enabled', 'Type', 'Key', 'Comment', and 'Action'. At the bottom are 'Save' and 'Close' buttons.

- **Choose File** Click **Choose File** to locate the new key file. Select the file and click **Open**.
- **Import** Imports the file for SSH access.
- **Enabled** Enables the specific key. All the added keys are saved in the system configuration file; however, only the enabled keys are active on the airFiber AF-5.
- **Type** Displays the type of key.
- **Key** Displays the key.
- **Comment** You can enter a brief description of the key.
- **Action** You have the following options:
 - **Add** Adds a public key file.
 - **Edit** Make changes to a public key file. Click **Save** to save your changes.
 - **Del** Deletes a public key file.
- **Save** Saves your changes.
- **Close** Discards your changes.

Telnet Server

The Telnet Server dialog box has a title bar 'Telnet Server'. It contains a checkbox labeled 'Telnet Server: Enable' and a text field labeled 'Server Port: 23'.

The following *Telnet Server* parameters can be set:

Telnet Server This option activates Telnet access to the airFiber AF-5.

- **Server Port** Specify the TCP/IP port of the *Telnet Server*.

NTP Client

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. You can use it to set the system time on the airFiber AF-5. If the *Log* option is enabled, then the system time is reported next to every log entry that registers a system event.

The NTP Client dialog box has a title bar 'NTP Client'. It contains a checkbox labeled 'NTP Client: Enable' and a text field labeled 'NTP Server: 0.pool.ntp.org'.

NTP Client Enables the airFiber AF-5 to obtain the system time from a time server on the Internet.

- **NTP Server** Specify the IP address or domain name of the NTP server.

Dynamic DNS

Domain Name System (DNS) translates domain names to IP addresses; Each DNS server on the Internet holds these mappings in its respective DNS database. Dynamic Domain Name System (DDNS) is a network service that notifies the DNS server in real time of any changes in the airFiber AF-5's IP settings. Even if the airFiber AF-5's IP address changes, you can still access the airFiber AF-5 through its domain name.

The Dynamic DNS dialog box has a title bar 'Dynamic DNS'. It contains a checkbox labeled 'Dynamic DNS: Enable', a text field labeled 'Host Name:', a text field labeled 'Username:', a text field labeled 'Password:', and a checkbox labeled 'Show'.

Dynamic DNS If enabled, the airFiber AF-5 allows communications with the DDNS server.

- **Host Name** Enter the host name of the DDNS server.
- **Username** Enter the user name of the DDNS account.
- **Password** Enter the password of the DDNS account.
- **Show** Check the box to display the password characters.

System Log



System Log This option enables the registration routine of system log (syslog) messages. By default it is disabled.

- **Remote Log** Enables the syslog remote sending function. System log messages are sent to a remote server, which is specified in the *Remote Log IP Address* and *Remote Log Port* fields.
 - **Remote Log IP Address** The host IP address that receives syslog messages. Properly configure the remote host to receive syslog protocol messages.
 - **Remote Log Port** The TCP/IP port that receives syslog messages. 514 is the default port for the commonly used system message logging utilities.

Every logged message contains at least a system time and host name. Usually a specific service name that generates the system event is also specified within the message. Messages from different services have different contexts and different levels of detail. Usually error, warning, or informational system service messages are reported; however, more detailed debug level messages can also be reported. The more detailed the system messages reported, the greater the volume of log messages generated.

Device Discovery



Discovery Enables device discovery, so the airFiber AF-5 can be discovered by other Ubiquiti devices through the *Discovery* tool.

CDP Enables Cisco Discovery Protocol (CDP) communications, so the airFiber AF-5 can send out CDP packets to share its information.



Chapter 9: System Tab

The *System* tab contains administrative options. This page enables the administrator to reboot the airFiber AF-5, reset it to factory defaults, upload new firmware, back up or update the configuration, and configure the administrator account.

Change To save or test your changes, click **Change**.

A new message appears. You have three options:

- **Apply** To immediately save your changes, click **Apply**.
- **Test** To try the changes without saving them, click **Test**. To keep the changes, click **Apply**. If you do not click **Apply** within 180 seconds (the countdown is displayed), the airFiber AF-5 times out and resumes its earlier configuration.
- **Discard** To cancel your changes, click **Discard**.

Firmware Update

The controls in this section manage firmware maintenance.



Firmware Version Displays the current firmware version.

Build Number Displays the build number of the firmware version.

Check for Updates By default, the firmware automatically checks for updates. To manually check for an update, click **Check Now**.

Upload Firmware Click this button to update the airFiber AF-5 with new firmware.

The airFiber AF-5 firmware update is compatible with all configuration settings. The system configuration is preserved while the airFiber AF-5 is updated with a new firmware version. However, we recommend that you back up your current system configuration before updating the firmware.

This is a three-step procedure:

1. Click **Choose File** to locate the new firmware file. Select the file and click **Open**.
2. Click **Upload** to upload the new firmware to the airFiber AF-5.
3. The Uploaded Firmware Version is displayed. Click **Update** to confirm.

If the firmware update is in process, you can close the firmware update window, but this does not cancel the firmware update. Please be patient, as the firmware update routine can take three to seven minutes. You cannot access the airFiber AF-5 until the firmware update routine is completed.



WARNING: Do not power off, do not reboot, and do not disconnect the airFiber AF-5 from the power supply during the firmware update process as these actions will damage the airFiber AF-5!

Device

The Device Name (host name) is the system-wide device identifier. The SNMP agent reports it to authorized management stations. The Device Name will be used in popular router operating systems, registration screens, and discovery tools.

Device Name Specifies the host name.

Interface Language Allows you to select the language displayed in the web management interface. *English* is the default language.

Date Settings

Time Zone Specifies the time zone in relation to Greenwich Mean Time (GMT).

Startup Date When enabled, you are able to change the airFiber AF-5's startup date.

- **Startup Date** Specifies the airFiber AF-5's startup date. Click the **Calendar** icon or manually enter the date in the following format: 2-digit month/2-digit day/4-digit year. For example, for January 5, 2014, enter **01/05/2014** in the field.

System Accounts

You can change the administrator password to protect your device from unauthorized changes. We recommend that you change the default administrator password when initially configuring the device.

Administrator Username Specifies the name of the administrator.

Key button Click this button to change the administrator password.

- **Current Password** Enter the current password for the administrator account. It is required to change the *Password* or *Administrator Username*.
- **New Password** Enter the new password for the administrator account.
- **Verify New Password** Re-enter the new password for the administrator account.



Note: The password length is 8 characters maximum; passwords exceeding 8 characters will be truncated.

Read-Only Account Check the box to enable the read-only account, which can only view the *Main* tab. Configure the username and password to protect your device from unauthorized changes.

- **Read-Only Account Name** Specifies the name of the system user.
- **Key button** Click this button to change the read-only password.
 - **New Password** Enter the new password for the read-only account.
 - **Show** Check the box to display the read-only password characters.

Miscellaneous



Reset Button To allow use of the airFiber AF-5's physical reset button, check the box. To prevent an accidental reset to default settings, uncheck the box.



Note: You can reset the airFiber AF-5 to default settings via the airFiber Configuration Interface. Go to the *System* tab > *Reset to Defaults*.

Location

After the on-board GPS determines the location of the airFiber AF-5, its latitude and longitude are displayed. If the GPS does not have a fix on its location, then "Searching for Satellites" will be displayed.



Latitude The latitude of the airFiber AF-5's location is displayed.

Longitude The longitude of the airFiber AF-5's location is displayed.

Device Maintenance

The controls in this section manage the airFiber AF-5 maintenance routines: reboot and support information reports.



Reboot Device Initiates a full reboot cycle of the airFiber AF-5. Reboot is the same as the hardware reboot, which is similar to the power-off and power-on cycle. The system configuration stays the same after the reboot cycle completes. Any changes that have not been applied are lost.

Support Info This generates a support information file that the Ubiquiti support engineers can use when providing customer support. This file only needs to be generated at their request.

Configuration Management

The controls in this section manage the airFiber AF-5 configuration routines and the option to reset the airFiber AF-5 to factory default settings.

The airFiber AF-5 configuration is stored in a plain text file (.cfg file). You can back up, restore, or update the system configuration file:



Back Up Configuration Click **Download** to download the current system configuration file.

Upload Configuration Click **Choose File** to locate the new configuration file. Select the file and click **Open**. We recommend that you back up your current system configuration before uploading the new configuration.

Upload Click this button to upload the new configuration file to the airFiber AF-5. Click **Apply** to confirm.

After the airFiber AF-5 reboots, the settings of the new configuration are displayed in the *Wireless*, *Network*, *Advanced*, *Services*, and *System* tabs of the airFiber Configuration Interface.

Reset to Factory Defaults Resets the airFiber AF-5 to the factory default settings. This option will reboot the airFiber AF-5, and all factory default settings will be restored. We recommend that you back up your current system configuration before resetting the airFiber AF-5 to its defaults.



Chapter 10: Tools

Each tab of the airFiber Configuration Interface contains network administration and monitoring tools. Click the **Tools** drop-down list at the top right corner of the page.

Align Antenna

Use the *Align Antenna* tool to point and optimize the antenna in the direction of maximum link signal. (See **"Using the airFiber Configuration Interface" on page 14** for more details.) The *Antenna Alignment* window is designed to refresh every 250 milliseconds.



Chain 0/1 Signal Strength Displays the absolute power level (in dBm) of the received signal for each chain.



Note: If "Overload" is displayed to indicate an overload condition, identify and eliminate any source of strong in-band interference.

Remote Chain 0/1 Signal Strength Displays the absolute power level (in dBm) of the received signal for each chain of the remote airFiber radio.

Max Signal Displays the maximum signal strength (in dBm). To adjust the range of the *Max Signal* meter, use the slider or manually enter the new value. If you reduce the range, the color change will be more sensitive to signal fluctuations, indicating the offset of the maximum indicator value and the scale itself.

Discovery

The *Device Discovery* tool searches for all Ubiquiti devices on your network. The *Search* field automatically filters devices containing specified names or numbers as you enter them.

Device Discovery

Search:

MAC Address	Device Name	Model	OS	Product	IP Address	IP Netmask
00:07:2D:00:00:00	ArCam	270A	ArCam	ArCam	10.0.0.1	255.255.255.0
00:07:2D:00:00:01	ArCam	270A	ArCam	ArCam	10.0.0.2	255.255.255.0
00:07:2D:00:00:02	ArCam12	270A	ArCam	ArCam	10.0.0.3	255.255.255.0
00:07:2D:00:00:03	Desk Video Reader	Reader	UNNT	arFiber 50	10.0.0.4	255.255.255.0
00:07:2D:00:00:04	Desk Video Reader	Reader	UNNT	arFiber 50	10.0.0.5	255.255.255.0
00:07:2D:00:00:05	Desk Reader	Reader	UNNT	arFiber 240	10.0.0.6	255.255.255.0
00:07:2D:00:00:06	Desk Reader	Reader	UNNT	arFiber 240	10.0.0.7	255.255.255.0
00:07:2D:00:00:07	UNNT	Reader	UNNT	arFiber 300	10.0.0.8	255.255.255.0
00:07:2D:00:00:08	UNNT	Reader	UNNT	arFiber 300	10.0.0.9	255.255.255.0
00:07:2D:00:00:09	UNNT	Reader	UNNT	arFiber 300	10.0.0.10	255.255.255.0
00:07:2D:00:00:10	UNNT	Reader	UNNT	arFiber 300	10.0.0.11	255.255.255.0
00:07:2D:00:00:11	UNNT	Reader	UNNT	arFiber 300	10.0.0.12	255.255.255.0
00:07:2D:00:00:12	UNNT	Reader	UNNT	arFiber 300	10.0.0.13	255.255.255.0
00:07:2D:00:00:13	UNNT	Reader	UNNT	arFiber 300	10.0.0.14	255.255.255.0
00:07:2D:00:00:14	UNNT	Reader	UNNT	arFiber 300	10.0.0.15	255.255.255.0
00:07:2D:00:00:15	UNNT	Reader	UNNT	arFiber 300	10.0.0.16	255.255.255.0
00:07:2D:00:00:16	UNNT	Reader	UNNT	arFiber 300	10.0.0.17	255.255.255.0
00:07:2D:00:00:17	UNNT	Reader	UNNT	arFiber 300	10.0.0.18	255.255.255.0
00:07:2D:00:00:18	UNNT	Reader	UNNT	arFiber 300	10.0.0.19	255.255.255.0
00:07:2D:00:00:19	UNNT	Reader	UNNT	arFiber 300	10.0.0.20	255.255.255.0
00:07:2D:00:00:20	UNNT	Reader	UNNT	arFiber 300	10.0.0.21	255.255.255.0
00:07:2D:00:00:21	UNNT	Reader	UNNT	arFiber 300	10.0.0.22	255.255.255.0
00:07:2D:00:00:22	UNNT	Reader	UNNT	arFiber 300	10.0.0.23	255.255.255.0
00:07:2D:00:00:23	UNNT	Reader	UNNT	arFiber 300	10.0.0.24	255.255.255.0
00:07:2D:00:00:24	UNNT	Reader	UNNT	arFiber 300	10.0.0.25	255.255.255.0
00:07:2D:00:00:25	UNNT	Reader	UNNT	arFiber 300	10.0.0.26	255.255.255.0
00:07:2D:00:00:26	UNNT	Reader	UNNT	arFiber 300	10.0.0.27	255.255.255.0
00:07:2D:00:00:27	UNNT	Reader	UNNT	arFiber 300	10.0.0.28	255.255.255.0
00:07:2D:00:00:28	UNNT	Reader	UNNT	arFiber 300	10.0.0.29	255.255.255.0
00:07:2D:00:00:29	UNNT	Reader	UNNT	arFiber 300	10.0.0.30	255.255.255.0
00:07:2D:00:00:30	UNNT	Reader	UNNT	arFiber 300	10.0.0.31	255.255.255.0
00:07:2D:00:00:31	UNNT	Reader	UNNT	arFiber 300	10.0.0.32	255.255.255.0
00:07:2D:00:00:32	UNNT	Reader	UNNT	arFiber 300	10.0.0.33	255.255.255.0
00:07:2D:00:00:33	UNNT	Reader	UNNT	arFiber 300	10.0.0.34	255.255.255.0
00:07:2D:00:00:34	UNNT	Reader	UNNT	arFiber 300	10.0.0.35	255.255.255.0
00:07:2D:00:00:35	UNNT	Reader	UNNT	arFiber 300	10.0.0.36	255.255.255.0
00:07:2D:00:00:36	UNNT	Reader	UNNT	arFiber 300	10.0.0.37	255.255.255.0
00:07:2D:00:00:37	UNNT	Reader	UNNT	arFiber 300	10.0.0.38	255.255.255.0
00:07:2D:00:00:38	UNNT	Reader	UNNT	arFiber 300	10.0.0.39	255.255.255.0
00:07:2D:00:00:39	UNNT	Reader	UNNT	arFiber 300	10.0.0.40	255.255.255.0

Showing 1 to 40 of 40 entries

[←](#)
[→](#)
[1](#)
[2](#)
[3](#)

Search

It reports the *MAC Address*, *Device Name*, *Mode*, *SSID*, *Product type*, *Firmware version*, and *IP Address* for each Ubiquiti device. To access a device configuration through its web management interface, click the device's IP address.

To refresh the window, click **Scan**.

Ping

You can ping other devices on the network directly from the airFiber AF-5. The *Ping* tool uses ICMP packets to check the preliminary link quality and packet latency estimation between two network devices.

[illegible]

Network Ping

Select Destination IP You have two options:

- Select a remote system IP from the drop-down list, which is generated automatically.
- Select **specify manually** and enter the IP address in the field displayed below.

Packet Count Enter the number of packets to send for the ping test.

Packet Size Specify the size of the packet.

Start Click this button to start the test.

Packet loss statistics and latency time evaluation are displayed after the test is completed.

Traceroute

The *Traceroute* tool traces the hops from the airFiber AF-5 to a specified outgoing IP address. Use this tool to find the route taken by ICMP packets across the network to the destination host.

Network Traceroute

Destination Host ☐ Resolve IP Addresses

#	Host	Response
---	------	----------

Start

Destination Host Enter the IP address of the destination host.

Resolve IP Addresses Select this option to resolve the IP addresses symbolically rather than numerically.

Start Click this button to start the test.

Responses are displayed after the test is completed.

Appendix A: Specifications

airFiber AF-5/AF-5U	
Operating Frequency	
AF-5	5470 - 5600 MHz, 5650 - 5850 MHz
FCC 15.247, 15.407, IC RSS 210	5470 - 5875 MHz
ETSI EN 301 893, EN 302 502	5470 - 5950 MHz
Other Regions	
AF-5U	5725 - 5850 MHz
FCC 15.247, IC RSS 21	5725 - 5875 MHz
ETSI EN 302 502	5725 - 6200 MHz
Other Regions	
Dimensions	938.4 x 468.4 x 281.4 mm (36.94 x 18.44 x 11.08 in)
Weight	
Mount Not Included	11.5 kg (25.35 lb)
Mount Included	16 kg (35.27 lb)
Max. Power Consumption	40 W
Power Supply	50V, 1.2A PoE GigE Adapter (Included)
Power Method	Passive Power over Ethernet (42-58VDC)
Certifications	CE, FCC, IC
Mounting	Pole Mount Kit (Included)
Wind Loading	863 N @ 200 km/hr (194 lbf @ 125 mph)
Wind Survivability	200 km/hr (125 mph)
Operating Temperature	-40 to 55°C (-40 to 131°F)
LEDs	(12) Status LEDs: Data Port Link/Activity Data Port Speed Management Port Link/Activity Management Port Speed GPS Synchronization Master/Slave Link Status Modulation Mode 0.25x to 4x, 6x, 8x, 10x (Unlabeled), Overload Remote and Local Displays (Calibrated Signal Strength)
Interface	
Data Port	(1) 10/100/1000 Ethernet Port
Management Port	(1) 10/100 Ethernet Port
Auxiliary Port	(1) RJ-12, Alignment Tone Port
System	
Maximum Throughput	1.2+ Gbps
Maximum Range	100+ km (62.14+ mi) (Dependent on Regulatory Region)
Packets per Second	1+ Million
Encryption	128-Bit AES
Forward Error Correction	164/205
Cyclic Prefix	1/16 Fixed
Uplink/Downlink Ratio	50% Fixed
Radio Frame Synchronization	GPS
Dynamic Frequency Selection	
AF-5	CE, FCC/IC
AF-5U	CE, (FCC/IC Not Applicable)

airFiber AF-5/AF-5U Receive Sensitivity							
Spatial Streams	Modulation	Sensitivity (10 MHz)	Sensitivity (20 MHz)	Sensitivity (40 MHz)	Sensitivity (50 MHz)	FDD Capacity*	TDD Capacity*
10x	1024QAM	-64 dBm	-61 dBm	-59 dBm	-58 dBm	1280 Mbps	640 Mbps
8x	256QAM	-70 dBm	-67 dBm	-65 dBm	-64 dBm	1024 Mbps	512 Mbps
6x	64QAM	-77 dBm	-74 dBm	-72 dBm	-71 dBm	768 Mbps	384 Mbps
4x	16QAM MIMO	-84 dBm	-81 dBm	-79 dBm	-78 dBm	512 Mbps	256 Mbps
2x	QPSK MIMO	-90 dBm	-87 dBm	-85 dBm	-84 dBm	256 Mbps	128 Mbps
1x	½ Rate QPSK xRT**	-93 dBm	-90 dBm	-88 dBm	-87 dBm	128 Mbps	64 Mbps
¼x	¼ Rate QPSK xRT	-95 dBm	-93 dBm	-92 dBm	-91 dBm	32 Mbps	16 Mbps

* FDD = (2) 50 MHz channels and TDD = (1) 50 MHz channel

** xtreme Range Technology

airFiber AF-5/AF-5U Radio Frequency	
GPS	GPS Clock Synchronization
Transceiver	
EIRP	~50 dBm (Dependent on Regulatory Region and Frequency Band)
Frequency Accuracy	±2.5 ppm without GPS Synchronization ±0.2 ppm with GPS Synchronization
Channel Bandwidth	10/20/30/40/50 MHz
Modulation	1024QAM MIMO 256QAM MIMO 64QAM MIMO 16QAM MIMO QPSK MIMO ½ Rate QPSK xRT ¼ Rate QPSK xRT
Integrated Split Antenna	
TX Gain	23 dBi
RX Gain	23 dBi
Beamwidth	6°
Front-to-Back Ratio	70 dB
Polarity	Dual-Slant Polarization
Cross-Polarity Isolation	> 28 dB

Appendix B: Safety Notices

1. Read, follow, and keep these instructions.
2. Heed all warnings.
3. Only use attachments/accessories specified by the manufacturer.

 **WARNING:** Do not use this product in location that can be submerged by water.

 **WARNING:** Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Electrical Safety Information

1. Compliance is required with respect to voltage, frequency, and current requirements indicated on the manufacturer's label. Connection to a different power source than those specified may result in improper operation, damage to the equipment or pose a fire hazard if the limitations are not followed.
2. There are no operator serviceable parts inside this equipment. Service should be provided only by a qualified service technician.
3. This equipment is provided with a detachable power cord which has an integral safety ground wire intended for connection to a grounded safety outlet.
 - a. Do not substitute the power cord with one that is not the provided approved type. Never use an adapter plug to connect to a 2-wire outlet as this will defeat the continuity of the grounding wire.
 - b. The equipment requires the use of the ground wire as a part of the safety certification, modification or misuse can provide a shock hazard that can result in serious injury or death.
 - c. Contact a qualified electrician or the manufacturer if there are questions about the installation prior to connecting the equipment.
 - d. Protective earthing is provided by Listed AC adapter. Building installation shall provide appropriate short-circuit backup protection.
 - e. Protective bonding must be installed in accordance with local national wiring rules and regulations.

Appendix C: Warranty

Limited Warranty

UBIQUITI NETWORKS, Inc ("UBIQUITI NETWORKS") warrants that the product(s) furnished hereunder (the "Product(s)") shall be free from defects in material and workmanship for a period of one (1) year from the date of shipment by UBIQUITI NETWORKS under normal use and operation. UBIQUITI NETWORKS' sole and exclusive obligation and liability under the foregoing warranty shall be for UBIQUITI NETWORKS, at its discretion, to repair or replace any Product that fails to conform to the above warranty during the above warranty period. The expense of removal and reinstallation of any Product is not included in this warranty. The warranty period of any repaired or replaced Product shall not extend beyond its original term.

Warranty Conditions

The above warranty does not apply if the Product:

- (I) has been modified and/or altered, or an addition made thereto, except by Ubiquiti Networks, or Ubiquiti Networks' authorized representatives, or as approved by Ubiquiti Networks in writing;
- (II) has been painted, rebranded or physically modified in any way;
- (III) has been damaged due to errors or defects in cabling;
- (IV) has been subjected to misuse, abuse, negligence, abnormal physical, electromagnetic or electrical stress, including lightning strikes, or accident;
- (V) has been damaged or impaired as a result of using third party firmware; or
- (VI) has no original Ubiquiti MAC label, or is missing any other original Ubiquiti label(s).
- (VII) has not been received by Ubiquiti within 30 days of issuance of the RMA.

In addition, the above warranty shall apply only if: the product has been properly installed and used at all times in accordance, and in all material respects, with the applicable Product documentation; all Ethernet cabling runs use CAT5 (or above), and for outdoor installations, shielded Ethernet cabling is used, and for indoor installations, indoor cabling requirements are followed.

Returns

No Products will be accepted for replacement or repair without obtaining a Return Materials Authorization (RMA) number from UBIQUITI NETWORKS during the warranty period, and the Products being received at UBIQUITI NETWORKS' facility freight prepaid in accordance with the RMA process of UBIQUITI NETWORKS. Products returned without an RMA number will not be processed and will be returned freight collect or subject to disposal. Information on the RMA process and obtaining an RMA number can be found at: www.ubnt.com/support/warranty.

Disclaimer

EXCEPT FOR ANY EXPRESS WARRANTIES PROVIDED HEREIN, UBIQUITI NETWORKS, ITS AFFILIATES, AND ITS AND THEIR THIRD PARTY DATA, SERVICE, SOFTWARE AND HARDWARE PROVIDERS HEREBY DISCLAIM AND MAKE NO OTHER REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, REPRESENTATIONS, GUARANTEES, OR WARRANTIES OF MERCHANTABILITY, ACCURACY, QUALITY OF SERVICE OR RESULTS, AVAILABILITY, SATISFACTORY QUALITY, LACK OF VIRUSES, QUIET ENJOYMENT, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM ANY COURSE OF DEALING, USAGE OR TRADE PRACTICE IN CONNECTION WITH SUCH PRODUCTS AND SERVICES. BUYER ACKNOWLEDGES THAT NEITHER UBIQUITI NETWORKS NOR ITS THIRD PARTY PROVIDERS CONTROL BUYER'S EQUIPMENT OR THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE PRODUCTS AND SERVICES MAY BE SUBJECT TO LIMITATIONS, INTERRUPTIONS, DELAYS, CANCELLATIONS AND OTHER PROBLEMS INHERENT IN THE USE OF COMMUNICATIONS FACILITIES. UBIQUITI NETWORKS, ITS AFFILIATES AND ITS AND THEIR THIRD PARTY PROVIDERS ARE NOT RESPONSIBLE FOR ANY INTERRUPTIONS, DELAYS, CANCELLATIONS, DELIVERY FAILURES, DATA LOSS, CONTENT CORRUPTION, PACKET LOSS, OR OTHER DAMAGE RESULTING FROM ANY OF THE FOREGOING. In addition, UBIQUITI NETWORKS does not warrant that the operation of the Products will be error-free or that operation will be uninterrupted. In no event shall UBIQUITI NETWORKS be responsible for damages or claims of any nature or description relating to system performance, including coverage, buyer's selection of products (including the Products) for buyer's application and/or failure of products (including the Products) to meet government or regulatory requirements.



WARNING: Failure to properly ground your airFiber units will void your warranty. (Please follow the instructions on "**Grounding**" on page **10** for installation of the ground wires.)

Limitation of Liability

EXCEPT TO THE EXTENT PROHIBITED BY LOCAL LAW, IN NO EVENT WILL UBIQUITI OR ITS SUBSIDIARIES, AFFILIATES OR SUPPLIERS BE LIABLE FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES (INCLUDING LOST PROFIT, LOST DATA, OR DOWNTIME COSTS), ARISING OUT OF THE USE, INABILITY TO USE, OR THE RESULTS OF USE OF THE PRODUCT, WHETHER BASED IN WARRANTY, CONTRACT, TORT OR OTHER LEGAL THEORY, AND WHETHER OR NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Note

Some countries, states and provinces do not allow exclusions of implied warranties or conditions, so the above exclusion may not apply to you. You may have other rights that vary from country to country, state to state, or province to province. Some countries, states and provinces do not allow the exclusion or limitation of liability for incidental or consequential damages, so the above limitation may not apply to you. EXCEPT TO THE EXTENT ALLOWED BY LOCAL LAW, THESE WARRANTY TERMS DO NOT EXCLUDE, RESTRICT OR MODIFY, AND ARE IN ADDITION TO, THE MANDATORY STATUTORY RIGHTS APPLICABLE TO THE LICENSE OF ANY SOFTWARE (EMBEDDED IN THE PRODUCT) TO YOU. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to any transactions regarding the sale of the Products.

Appendix D: Compliance Information

Installer Compliance Responsibility

Devices must be professionally installed and it is the professional installer's responsibility to make sure the device is operated within local country regulatory requirements.

FCC

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operations of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Industry Canada

CAN ICES-3(B)/NMB-3(B)

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-3(B)/NMB-3(B)

Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s). Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

RF Exposure Warning

The antennas used for this transmitter must be installed to provide a separation distance of at least 126 cm (AF-5) or 123 cm (AF-5U) from all persons and must not be located or operating in conjunction with any other antenna or transmitter.

Les antennes utilisées pour ce transmetteur doivent être installées en considérant une distance de séparation de toute personnes d'au moins 126 cm (AF-5) ou 123 cm (AF-5U) et ne doivent pas être localisées ou utilisées en conflit avec tout autre antenne ou transmetteur.

Australia and New Zealand



Warning: This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE Marking

CE marking on this product represents the product is in compliance with all directives that are applicable to it.

Alert sign! follows CE marking

Alert sign must be indicated if a restriction on use applied to the product and it must follow the CE marking.



The product can be operated in the countries and regions listed in this table: **"Frequency Ranges and Power Levels per Country/Region" on page 46**, within the stated frequency ranges and output power (EIRP) limits.

Frequency Ranges and Power Levels per Country/Region

Each country has its own power level and frequency regulations. To ensure the product operates under the necessary regulatory compliance rules, the country where the device will be used must be selected during installation. The frequency settings and output power (EIRP) limits will be tuned according to the regulations of the selected country/region:

Country/Region	Model	5.4 GHz Frequency Range (Band Edges in MHz)	Max. EIRP (dBm)	5.8 GHz Frequency Range (Band Edges in MHz)	Max. EIRP for 5.7 GHz (dBm)
Argentina	AF5/AF5U	5470-5725	30	5725-5850	36
Australia	AF5/AF5U	5470-5600, 5650-5725	30	5725-5855	36
Bahrain	AF5U			5735-5835	20
Barbados	AF5U			5725-5850	36
Belize	AF5U			5735-5835	30
Bolivia	AF5U			5735-5835	30
Brazil	AF5/AF5U	5470-5725	30	5725-5850	30
Brunei Darussalam	AF5U			5735-5835	20
Canada	AF5/AF5U	5470-5600, 5650-5725	30	5725-5850	50
Chile	AF5U			5735-5835	20
China	AF5U			5735-5835	30
Colombia	AF5U			5735-5835	30
Costa Rica	AF5U			5735-5835	30
Denmark	AF5/AF5U	5470-5725	30	5725-5795, 5815-5850	36
Dominican Republic	AF5U			5735-5835	30
Ecuador	AF5U			5735-5835	30
El Salvador	AF5U			5735-5835	30
Finland	AF5/AF5U	5470-5725	30	5725-5795, 5815-5850	36
Germany	AF5/AF5U	5470-5725	30	5755-5875	36
Greece	AF5/AF5U	5470-5725	30	5725-5795	36
Grenada	AF5/AF5U	5470-5725	30	5725-5850	36
Guatemala	AF5U			5735-5835	30
Honduras	AF5/AF5U	5470-5725	30	5725-5850	36
Hong Kong	AF5/AF5U	5470-5725	30	5725-5850	36
Iceland	AF5/AF5U	5470-5725	30	5725-5875	36
India	AF5U			5825-5875	36
Iraq	AF5U			5735-5835	36
Ireland	AF5/AF5U	5470-5725	30	5725-5875	33
Jamaica	AF5/AF5U	5470-5725	30	5725-5850	36
Kenya	AF5U			5735-5835	30
Korea Republic	AF5/AF5U	5490-5710	30	5735-5815	30
Lebanon	AF5U			5735-5835	30
Liechtenstein	AF5/AF5U	5470-5725	30	5725-5795, 5815-5875	36
Macau	AF5U			5725-5850	36
Malaysia	AF5U			5735-5835	30
Mexico	AF5U			5735-5835	30
Morocco	AF5U			5735-5835	20
Nepal	AF5U			5735-5835	30

Country/Region	Model	5.4 GHz Frequency Range (Band Edges in MHz)	Max. EIRP (dBm)	5.8 GHz Frequency Range (Band Edges in MHz)	Max. EIRP for 5.7 GHz (dBm)
New Zealand	AF5/AF5U	5470-5725	30	5725-5850	36
Norway	AF5/AF5U	5470-5725	30	5725-5795, 5815-5850	50
Oman	AF5/AF5U	5470-5725	30	5725-5850	36
Pakistan	AF5U			5735-5835	30
Panama	AF5U			5735-5835	30
Papua New Guinea	AF5U			5735-5835	30
Peru	AF5/AF5U	5470-5725	30	5725-5850	36
Philippines	AF5/AF5U	5470-5725	30	5725-5850	36
Portugal	AF5/AF5U	5470-5725	30	5725-5875	36
Puerto Rico (U.S. territory)	AF5/AF5U	5470-5600, 5650-5725	30	5725-5850	50
Qatar	AF5U			5735-5835	30
Russia	AF5/AF5U	5470-5725	23	5725-5850	23
Singapore	AF5U			5735-5835	30
South Africa	AF5/AF5U	5470-5725	30	5725-5850	36
Spain	AF5/AF5U	5470-5725	30	5725-5795, 5815-5855	36
Switzerland	AF5/AF5U	5470-5725	30	5725-5795, 5815-5855	36
Taiwan	AF5/AF5U	5490-5710	30	5735-5815	30
Thailand	AF5/AF5U	5470-5725	30	5725-5850	36
Trinidad And Tobago	AF5/AF5U	5470-5725	30	5725-5850	36
United Kingdom	AF5/AF5U	5470-5725	30	5725-5790, 5815-5850	36
United States	AF5/AF5U	5470-5600, 5650-5725	30	5725-5850	50
Uruguay	AF5/AF5U	5470-5725	30	5725-5850	36
Uzbekistan	AF5/AF5U	5470-5725	30	5725-5850	36
Venezuela	AF5U			5735-5835	30

RoHS/WEEE Compliance Statement



English

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Deutsch

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist, nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Español

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Français

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Appendix E: Declaration of Conformity

Česky [Czech]	UBIQUITI NETWORKS tímto prohlašuje, že tento UBIQUITI NETWORKS device, je ve shodě se základními požadavky a dále jím jsou nmi ustanovenými směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede UBIQUITI NETWORKS erklærer herved, at følgende udstyr UBIQUITI NETWORKS device, overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Nederlands [Dutch]	Hierbij verklaart UBIQUITI NETWORKS dat het toestel UBIQUITI NETWORKS device, in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart UBIQUITI NETWORKS dat deze UBIQUITI NETWORKS device, voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, UBIQUITI NETWORKS, declares that this UBIQUITI NETWORKS device, is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Eesti [Estonian]	Käesolevaga kinnitab UBIQUITI NETWORKS seadme UBIQUITI NETWORKS device, vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Suomi [Finnish]	UBIQUITI NETWORKS vakuuttaa täten että UBIQUITI NETWORKS device, tyypin laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Français [French]	Par la présente UBIQUITI NETWORKS déclare que l'appareil UBIQUITI NETWORKS device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, UBIQUITI NETWORKS déclare que ce UBIQUITI NETWORKS device, est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
Deutsch [German]	Hiermit erklärt UBIQUITI NETWORKS, dass sich diese UBIQUITI NETWORKS device, in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet. (BMW) Hiermit erklärt UBIQUITI NETWORKS die Übereinstimmung des Gerätes UBIQUITI NETWORKS device, mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ UBIQUITI NETWORKS ΔΗΛΩΝΕΙ ΟΤΙ UBIQUITI NETWORKS device, ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Magyar [Hungarian]	Alulírott, UBIQUITI NETWORKS nyilatkozom, hogy a UBIQUITI NETWORKS device, megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Íslenska [Icelandic]	Hér með lýsir UBIQUITI NETWORKS yfir við a UBIQUITI NETWORKS device, er í samræmi við grunnkröfur og a rar kröfur, sem gerar eru í tilskipun 1999/5/EC.
Italiano [Italian]	Con la presente UBIQUITI NETWORKS dichiara che questo UBIQUITI NETWORKS device, è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar o UBIQUITI NETWORKS deklar, ka UBIQUITI NETWORKS device, atbilst Direkt vās 1999/5/EK b tiskaj m pras b m un citiem ar to saist tajiem noteikumiem.
Lietuviškai [Lithuanian]	UBIQUITI NETWORKS deklaruoja, kad šis UBIQUITI NETWORKS įrenginys atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Malti [Maltese]	Hawnhekk, UBIQUITI NETWORKS, jiddikjara li dan UBIQUITI NETWORKS device, jikkonforma mal- ti ijjiet essenzjali u ma provvedimenti o rajn relevanti li hemm fid-Direttiva 1999/5/EC.
Norsk [Norwegian]	UBIQUITI NETWORKS erklærer herved at utstyret UBIQUITI NETWORKS device, er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Slovensky [Slovak]	UBIQUITI NETWORKS týmto vyhlasuje, že UBIQUITI NETWORKS device, spĺa základné požiadavky a v etky príslušné ustanovenia Smernice 1999/5/ES.
Svenska [Swedish]	Härmed intygar UBIQUITI NETWORKS att denna UBIQUITI NETWORKS device, står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Español [Spanish]	Por medio de la presente UBIQUITI NETWORKS declara que el UBIQUITI NETWORKS device, cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Polski [Polish]	Niniejszym, firma UBIQUITI NETWORKS o wiadcza, że produkt serii UBIQUITI NETWORKS device, spełnia zasadnicze wymagania i inne istotne postanowienia Dyrektywy 1999/5/EC.
Português [Portuguese]	UBIQUITI NETWORKS declara que este UBIQUITI NETWORKS device, está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Română [Romanian]	Prin prezenta, UBIQUITI NETWORKS declară că acest dispozitiv UBIQUITI NETWORKS este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/CE.

Appendix F: Contact Information

Ubiquiti Networks Support

Ubiquiti Support Engineers are located around the world and are dedicated to helping customers resolve software, hardware compatibility, or field issues as quickly as possible. We strive to respond to support inquiries within a 24-hour period.

Online Resources

Support: support.ubnt.com

Community: community.ubnt.com

Downloads: downloads.ubnt.com



2580 Orchard Parkway
San Jose, CA 95131
www.ubnt.com

©2013- 2015 Ubiquiti Networks, Inc. All rights reserved. Ubiquiti, Ubiquiti Networks, the Ubiquiti U logo, the Ubiquiti beam logo, airFiber, and TOUGH Cable are trademarks or registered trademarks of Ubiquiti Networks, Inc. in the United States and in other countries. All other trademarks are the property of their respective owners.



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **00994-15-08356**

Validade: **Indeterminada**

Emissão: **24/06/2019**

Requerente:

CNPJ: 04.679.642/0001-10

CH INTERNATIONAL DO BRASIL LTDA

Fabricante:

UBIQUITI INC.

685 THIRD AVENUE, 27TH FLOOR

Nº

10017

ESTADOS UNIDOS DA AMÉRICA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC-11886/15, emitido pelo **Associação NCC Certificações do Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Transceptor de Radiação Restrita - II

Modelo - Nome Comercial (s):

AF-5U

Características técnicas básicas:

Faixa de Frequências Tx (MHz)	Potência Máxima de Saída (W)	Designação de Emissões	Tecnologias	Tipo de Modulação
5.725,0 a 5.850,0	0,0689	9M65X9D	OFDM	QPSK/16-64-256-1024-QAM
5.725,0 a 5.850,0	0,0755	19M3X9D	OFDM	QPSK/16-64-256-1024-QAM
5.725,0 a 5.850,0	0,0655	38M6X9D	OFDM	QPSK/16-64-256-1024-QAM
5.725,0 a 5.850,0	0,0622	48M2X9D	OFDM	QPSK/16-64-256-1024-QAM

O produto incorpora Antena Ponto a Ponto com as seguintes características:

Faixa de Frequências Tx (MHz)	Ganho Mínimo (dBi)	Polarização	Classe Horizontal	Classe Cruzada
5.470,0 a 5.850,0	22,79	+45°/-45°	Classe 1A	XPD1

Ensaio de SAR não aplicável.

Observações

Este produto destina-se ao uso profissional, manuseado por pessoal devidamente qualificado, não sendo destinado ao uso do público em geral para acesso a serviço de telecomunicações de interesse coletivo.

Na instalação do produto devem ser observadas as condições de uso conforme estabelecido no Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita.

Este certificado substitui o de mesmo número emitido em 24/06/2019

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Davison Gonzaga da Silva

Gerente de Certificação e Numeração

CCR1009-7G-1C-1S+

The new updated revision of CCR1009 is here. We attempted to combine all the customer feedback and best practice in CCR device manufacturing that we learned over the last three years, since the first CCR1009 devices were launched.

Important changes

No switch-chip - the device now features only fully independent Ethernet ports each with a direct connection to the CPU, allowing to overcome previous shared 1Gbit limitation from switch-chip ports and utilize full potential of CPU processing power on those ports.

Combo-port - a single 1Gbit software interface that has two hardware interfaces - a SFP cage and a Gigabit Ethernet port, allowing you to use any type of connection available to you. Port also allows to switch from one to another interface from software, or in event of disconnect, providing new, unique hardware fail-over feature.

100Mbps SFP support - this is our first device that supports 100BASE-LX/100BASE-SX/100BASE-BX fiber modules, as well as standard 1.25G SFP modules.

More throughput - due to how ports are connected to CPU, new CCR1009 models can achieve higher theoretical throughput.



The unit is equipped with dual power supplies built in for redundancy (if one power line fails, the other one will take over automatically).

Unit comes with the 1U rackmount case and supports a Smart card, to store your private key for use in all features that support Certificate based authentication. It also includes LCD touchscreen, microSD and a SFP+ port for 10G connections.



Specifications

Product code	CCR1009-7G-1C-1S+
CPU nominal frequency	TILE-Gx9, 9 cores, 1.2 GHz
Size of RAM	2 GB
Storage type	NAND
Storage size	128 MB
10/100/1000 Ethernet ports	7
Number of USB ports	1
Power jack	2
PoE in	Yes
Supported input voltage	15 V - 57 V
Voltage monitor	Yes
PCB temperature monitor	Yes
CPU temperature monitor	Yes
LCD	Yes
Dimensions	444 x 175 x 47mm
Operating system	RouterOS, level 6 license
Max Power consumption	34W
Ethernet/SFP combo port	1
SFP+ ports	1
USB slot type	microUSB type AB
Smart card	Yes
Storage expansion	microSD
Serial port	RS232
Suggested price	\$495

Included



USB cable



Rack ears



2x IEC cord



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **07657-17-03817**

Validade: Indeterminada

Emissão: 12/12/2017

Requerente:

CNPJ: 07.212.549/0002-70

OIW INDÚSTRIA ELETRÔNICA S/A

Fabricante:

MIKROTIKLS, SIA

AIZKRAUKLES

Nº

LETÔNIA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº 00104358, emitido pelo **Instituto Brasileiro de Certificação para produtos de Telecomunicações**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações:

Tipo - Categoria:

Equipamento de Rede de Dados - III

Modelo - Nome Comercial (s):

CCR1009-7G-1C-1S+

Características técnicas básicas:

Equipamento utilizado em redes Ethernet.

Observações

Este produto destina-se ao uso profissional, manuseado por pessoal devidamente qualificado, não sendo destinado ao uso do público em geral para acesso a serviço de telecomunicações de interesse coletivo.

Módulos de interface e protocolos de sinalização, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

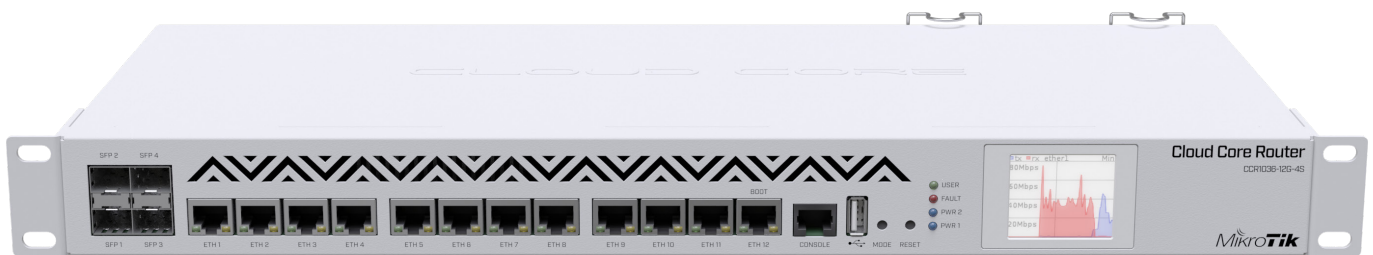
As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente de Certificação e Numeração

CCR1036-12G-4S

CCR1036-12G-4S is an industrial grade router with cutting edge 36 core CPU. If your network requires to operate with millions of packets per second - Cloud Core Router with 36 cores is your best choice.

The device comes in a 1U rackmount case, has four SFP ports, twelve Gigabit Ethernet ports, a serial console cable and a USB port.



- 36 core CPU
- 1.2 GHz clock per core
- 12 Mbytes total on-chip cache
- State of the art TILE GX architecture
- 28.8 mpps fastpath forwarding (wire speed for all ports)
- Up to 16 Gbit/s throughput
- 1U rackmount case
- 12 Gigabit Ethernet ports
- 4 SFP ports
- Color touchscreen LCD
- Ports directly connected to CPU



The new r2 version has onboard 4 GB of RAM (8 GB for CCR1036-12G-4S-EM model), onboard M.2 slot, full size USB slot and dual PSU for redundancy.

Specifications

Product code	CCR1036-12G-4S	CCR1036-12G-4S-EM
CPU	Tilera Tile-Gx36 CPU, 36 cores, 1.2 GHz per core	
Size of RAM	4 GB	8 GB
Storage	1 GB NAND, 512 KB flash	
10/100/1000 Ethernet ports	12	
Supported input voltage	AC power supply 100 - 240 V	
1G SFP ports	4	
Redundant supply	Yes	
USB port	USB type A	
Serial port	RJ45	
Dimensions	443 x 193 x 44 mm	
Operating temperature	-20°C .. +60°C	
Operating system	RouterOS, License level 6	
Max power consumption	60 W	

Included parts



2 IEC cords



Screw and feet
kit (K10)



Rack ears



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **00991-14-03817**

Validade: Indeterminada

Emissão: 24/04/2014

Requerente:

CNPJ: 05.917.486/0001-40

LIVETECH DA BAHIA INDÚSTRIA E COMÉRCIO LTDA

Fabricante:

MIKROTIKLS, SIA

AIZKRAUKLES

Nº

LETÔNIA

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº NCC-10486/14, emitido pelo **Associação NCC Certificações do Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Equipamento de Rede de Dados - III

Modelo - Nome Comercial (s):

CCR1016-12G - (CCR1016-12G) / CCR1036-12G-4S - (CCR1036-12G-4S) / CCR1036-12G-4S-EM - (CCR1036-12G-4S-EM)

Características técnicas básicas:

Equipamento utilizado em redes Ethernet.

Observações

Este produto destina-se ao uso em ambientes corporativos, não sendo sua utilização destinada ao uso do público em geral para acesso a serviço de telecomunicações de interesse coletivo.

Módulos de interface e protocolos de sinalização, especificados em documentos técnicos do produto, não estão cobertos por este certificado, sendo obrigatória sua certificação e homologação, caso venham a ser fornecidos ou utilizados.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH - Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Marcos de Souza Oliveira
Gerente de Certificação e Numeração



FibeAir® IP-10G

Installation Guide

Doc-00023199 Rev E
June 2012

Notice

This document contains information that is proprietary to Ceragon Networks Ltd. No part of this publication may be reproduced, modified, or distributed without prior written authorization of Ceragon Networks Ltd. This document is provided as is, without warranty of any kind.

Registered Trademarks

Ceragon Networks® is a registered trademark of Ceragon Networks Ltd. FibeAir® is a registered trademark of Ceragon Networks Ltd. CeraView® is a registered trademark of Ceragon Networks Ltd. Other names mentioned in this publication are owned by their respective holders.

Trademarks

CeraMap™, PolyView™, EncryptAir™, ConfigAir™, CeraMon™, EtherAir™, and MicroWave Fiber™, are trademarks of Ceragon Networks Ltd. Other names mentioned in this publication are owned by their respective holders.

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 incidental or consequential 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 ("GPL License"). Inasmuch that such software is being used, it is released under the GPL License, accordingly. Some software might have changed. The complete list of the software being used in this product including their respective license and the aforementioned public available changes is accessible on <http://www.gnu.org/licenses/>.

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.

Revision History

Rev	Date	Author	Description	Approved by	Date
D	September 7, 2011	Baruch Gitlin	System installation guide for IP-10G.	Tomer Aizenberg, Amit Stark, Ilan Benoliel, Rami Lerner, Uri Sela, Ari Bachman	September 6, 2011
E	June 14, 2012	Baruch Gitlin	Update initial configuration instructions and acceptance and commissioning procedures.	Erez Aviv	June 14, 2012

Table of Contents

1. About This Guide.....	9
2. What You Should Know	9
3. Target Audience	9
4. Related Documents	9
5. Section Summary	10
6. Preparing for Installation	11
6.1 Packing.....	11
6.2 Transportation	11
6.3 Inspection.....	11
6.4 Unpacking Equipment at the Site.....	11
7. Installing the IDU	12
7.1 Required Tools for IDU Installation	12
7.2 Cables	12
7.3 Special Requirements for North America.....	12
7.4 Site Requirements.....	13
7.4.1 IDU Dimensions	13
7.5 Configuration Options	14
7.6 Installing the IDU in a 19"/ETSI Rack	14
7.7 Installing the IDU in a Nodal Enclosure	15
7.7.1 Nodal Enclosure Design.....	15
7.7.2 List of Kits Needed to Install an IDU in a Nodal Configuration	16
7.7.3 Procedure for IDU Installation in a Nodal Configuration	16
7.8 Grounding the IDU and Electrical Information	20
7.8.1 Dual DC Feed	22
8. RFU Overview	23
8.1 Installing an RFU.....	23
8.2 RFU Selection Guide	24
9. Connecting an IDU to an RFU.....	25
10. Initial System Configuration	27
10.1 Establishing a Connection with the IDU	28
10.2 Launching the Web EMS	29
10.3 Configuring IP Addresses	30
10.4 Upgrading the IDU Software	31
10.4.1 Viewing IDU Version Information	32
10.4.2 Downloading IDU Software Files	33

10.4.3 Upgrading the IDU Software Version	34
10.5 Loading the License Key	36
10.6 Configuring XPIC	38
10.7 Conditions for XPIC	39
10.8 Configuring the Antenna and RFU for XPIC	39
10.8.1 IDU-RFU Cable Installation	39
10.8.2 Antenna Alignment	39
10.8.3 Polarization Alignment	40
10.9 Displaying XPI Values	40
11. Acceptance and Commissioning Procedures	42
11.1 Site Acceptance Procedure	43
11.2 Site Acceptance Checklist Notes	46
11.2.1 Antenna Mounting	46
11.2.2 Antenna	47
11.2.3 RFU (Radio Frequency Unit)	47
11.3 IDU (Indoor Unit)	47
11.4 1+0 Commissioning Procedure	48
11.4.1 Commissioning Test	48
11.4.1.1 Link Verification	48
11.4.1.2 Line Interfaces Test	48
11.4.1.3 Interoperability Verification	48
11.4.1.4 Management Verification	49
11.4.1.5 Loopback Operation	49
11.5 1+1 Commissioning Procedure	50
11.5.1 Commissioning Tests	50
11.5.1.1 Link Verification	50
11.5.1.2 Line Interfaces Test	50
11.5.1.3 Switching Tests	51
11.5.1.4 Interoperability Verification	51
11.5.1.5 Management Verification	52
11.6 2+0 XPIC Commissioning Procedure	53
11.6.1 XPIC Commissioning Tests	55
11.6.1.1 Individual Link Verification	55
11.6.1.2 XPIC Configuration Verification	55
11.6.1.3 XPIC Recovery Verification	55
11.7 FibeAir IP-10 Commissioning Log	56
12. Appendix A: Line Interfaces	60
12.1 Main Channel Interfaces	60
12.2 Wayside Channel Interface	62
12.3 Protection Channel Interface	62
12.4 Management Channel Interface	62
12.5 Order Wire Channel Interface	63
12.6 User Channel Interface	63

13. Appendix B: Connector Pin-Outs 64

13.1 External Alarms Connector Pin-Out..... 64

13.2 Protection/Wayside/Management Connector Pin-Out..... 65

13.3 Power Connector Pin-Out 65

13.4 16 x E1/DS1Connector 66

13.5 Ethernet 10/100/1000 Connector Pin-Out..... 68

13.6 Ethernet 10/100 Connector Pin-Out..... 69

13.7 User Channel Connector Pin-Out 69

13.8 Craft Terminal Connector Pin-Out 70

14. Appendix C: Fan Tray Replacement..... 71

Safety Precautions & Declared Material

General Equipment Precautions



Use of controls, adjustments, or performing procedures other than those specified herein, may result in hazardous radiation exposure.



When working with a FibeAir IDU, note the following risk of electric shock and energy hazard: Disconnecting one power supply disconnects only one power supply module. To isolate the unit completely, disconnect all power supplies.



Machine noise information order - 3. GPSGV, the highest sound pressure level amounts to 70 dB (A) or less, in accordance with ISO EN 7779.

Static electricity may cause body harm, as well as harm to electronic components inside the device.



Anyone responsible for the installation or maintenance of the FibeAir IDU must use an ESD Wrist Strap.

ESD protection measures must be observed when touching the IDU.

To prevent damage, before touching components inside the device, all electrostatic must be discharged from both personnel and tools.



In Norway and Sweden:

Equipment connected to the protective earthing of the building installation through the mains connection or through other equipment with a connection to protective earthing – and to a cable distribution system using coaxial cable, may in some circumstances create a fire hazard. Connection to a cable distribution system has therefore to be provided through a device providing electrical isolation below a certain frequency range (galvanic isolator, see EN 60728-11).

Utstyr som er koplet til beskyttelsesjord via nettplugg og/eller via annet jordtilkoplet utstyr – og er tilkoplet et kabel-TV nett, kan forårsake brannfare. For å unngå dette skal det ved tilkopling av utstyret til kabel-TV nettet installeres en galvanisk isolator mellom utstyret og kabel-TV nettet.

Utrustning som är kopplad till skyddsjord via jordat vägguttag och/eller via annan utrustning och samtidigt är kopplad till kabel-TV nät kan i vissa fall medföra risk för brand. För att undvika detta skall vid anslutning av utrustningen till kabel-TV nät galvanisk isolator finnas mellan utrustningen och kabel-TV nätet.

Précautions générales relatives à l'équipement



L'utilisation de commandes ou de réglages ou l'exécution de procédures autres que celles spécifiées dans les présentes peut engendrer une exposition dangereuse aux rayonnements.



L'usage de FibeAir IDU s'accompagne du risque suivant d'électrocution et de danger électrique : le débranchement d'une alimentation électrique ne déconnecte qu'un module d'alimentation électrique. Pour isoler complètement l'unité, il faut débrancher toutes les alimentations électriques.



Bruit de machine d'ordre - 3. GPSGV, le plus haut niveau de pression sonore s'élève à 70 dB (A) au maximum, dans le respect de la norme ISO EN 7779.

Allgemeine Vorsichtsmaßnahmen für die Anlage



Wenn andere Steuerelemente verwendet, Einstellungen vorgenommen oder Verfahren durchgeführt werden als die hier angegebenen, kann dies gefährliche Strahlung verursachen.



Beachten Sie beim Arbeiten mit FibeAir IDU das folgende Stromschlag- und Gefahrenrisiko: Durch Abtrennen einer Stromquelle wird nur ein Stromversorgungsmodul abgetrennt. Um die Einheit vollständig zu isolieren, trennen Sie alle Stromversorgungen ab.



Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 70 dB(A) oder weniger gemäß EN ISO 7779.

RoHS Compliance Declaration*Electronic Information Products Declaration of Hazardous/Toxic Substances*

Component	Hazardous Substance					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr VI)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB/Circuit Modules	Comply	Comply	Comply	Comply	Comply	Comply
Mechanical Parts	Comply	Comply	Comply	Comply	Comply	Comply
Cables	Comply	Comply	Comply	Comply	Comply	Comply

1. About This Guide

This guide describes the installation procedures for an IP-10 system using an IP-10 G-Series IDU and any of the supported RFUs. This guide also provides additional information concerning system configuration and verification once the installation is complete.

2. What You Should Know

An IP-10 system includes one or more FibeAir IP-10 G-Series or E-Series IDUs and any of several types of Ceragon RFUs. This manual provides instructions for the installation of a complete IP-10 system, including an IP-10 G-Series or E-Series IDU and an RFU.

3. Target Audience

This guide contains technical information about installation of an IP-10 system, and is intended for use by personnel of all levels certified by Ceragon personnel such as system engineers, technicians, or supervisors.

4. Related Documents

- FibeAir IP-10G and IP-10E User Guide, DOC-00034612
- FibeAir IP-10G Product Description
- FibeAir IP-10 MIB Reference - DOC-00015446
- FibeAir IP-10 License Management System - DOC-00019183
- FibeAir CeraBuild Commission Reports Guide, DOC-00028133
- FibeAir RFU-HP Product Description
- FibeAir RFU-HP Installation Guide - DOC-00015514
- FibeAir RFU-C Product Description
- FibeAir RFU-C Installation Guide - DOC-00017708
- FibeAir RFU-HS Product Description
- FibeAir RFU-HS Installation Guide - DOC-00022617
- FibeAir RFU-SP Product Description
- FibeAir RFU-SP Installation Guide - DOC-00015515
- 1500P Installation Guide - DOC-00015520

5. Section Summary

This manual includes the following sections:

Section Summary

Section	Summary of Contents
Preparing for Installation	Provides guidelines for transporting, inspecting, and unpacking the equipment for an IP-10 system.
Installing the IDU	Provides instructions for installing IDU units, including instructions for rack and nodal configurations, and special instructions for 1+1, 2+0, and 2+2 configurations.
RFU Overview	Describes the Ceragon RFU models that can be used in an IP-10 system, including a comparison guide.
Connecting an IDU to an RFU	Provides instructions for connecting an IDU to an RFU.
Initial System Configuration	Describes the basic configuration steps for an IP-10 radio link, including how to connect a PC or laptop to the IDU and launch Ceragon Web-Based Management, upgrade the IDU software, activate the license key, and configure basic IDU parameters.
Acceptance and Commissioning Procedures	Provides Ceragon's recommended Acceptance and Commissioning Procedure for a FibeAir IP-10 system, to be performed after initial setup is complete.
Appendix A: Line Interfaces	Describes the FibeAir main channel, wayside channel, and order wire channel interfaces.
Appendix B: Connector Pin-Outs	Provides pin-outs for FibeAir IDU connectors.
Appendix C: Fan Tray Replacement	Explains how to replace the fan tray in an IP-10 IDU.

6. Preparing for Installation

This section provides instructions for transporting, inspecting, and unpacking the equipment for an IP-10 system prior to installation.

6.1 Packing

The equipment is packed at the factory, and sealed moisture-absorbing bags are inserted.

6.2 Transportation

- The equipment is prepared for public transportation. The cargo must be kept dry during transportation, in accordance with ETS 300 019-1-2, Class 2.3.
- It is recommended to transport the equipment to the installation site in its original packing case.
- If intermediate storage is required, the packed equipment must be stored in dry and cool conditions and out of direct sunlight, in accordance with ETS 300 019-1-1, Class 1.2.

6.3 Inspection

Check the packing lists, and ensure that the correct part numbers and quantities of components arrived.

6.4 Unpacking Equipment at the Site

A single FibeAir system (1+0) is shipped in 4 crates. Upon delivery, make sure that the following items are included:

- Two indoor units (IDUs) and accessories
- Two radio frequency units (RFUs)

Unpack the contents and check for damaged or missing parts. If any part is damaged or missing, contact your local Ceragon distributor.

7. Installing the IDU

This section provides instructions for installing a FibeAir IP-10 IDU at a customer site.

Note: For full functionality and feature availability, upgrade the IDU to the latest released software version. You can obtain the latest software version and release notes at Ceragon's FTP site. For access to the site, contact support@ceragon.com. For additional details, refer to *Initial System Configuration* on page 27.

7.1 Required Tools for IDU Installation

The following tools are required to install an IDU:

- Philips screwdriver (for mounting the IDU to the rack and grounding screw)
- Flathead small screwdriver (for PSU connector)
- Sharp cutting knife (for wire stripping)
- Crimping tool for ground cable lug crimping (optional: if alternative grounding cable is used).

7.2 Cables

In addition to the tools mentioned above, the interface connectors and their pin-outs are described in the following sections in this guide:

- Appendix A: Line Interfaces
- Appendix B: Connector Pin-Outs

7.3 Special Requirements for North America

Restricted Access Area: DC powered equipment should only be installed in a Restricted Access Area.

Installation Codes: The equipment must be installed according to country national electrical codes. For North America, equipment must be installed in accordance to the US National Electrical Code, Articles 110-16, 110-17 and 110-18, and the Canadian Electrical Code, Section 12.

Overcurrent Protection: A readily accessible listed branch circuit overcurrent protective device, rated 15 A, must be incorporated in the building wiring.

CAUTION: This equipment is designed to permit connection between the earthed conductor of the DC supply circuit and the earthing conductor at the equipment.

Grounded Supply System: The equipment shall be connected to a properly grounded supply system. All equipment in the immediate vicinity shall be grounded the same way, and shall not be grounded elsewhere.

Local Supply System: The DC supply system is to be local, i.e. within the same premises as the equipment.

Disconnect Device: A disconnect device is not allowed in the grounded circuit between the DC supply source and the frame/grounded circuit connection.

7.4 Site Requirements

- Must be located indoors.
- The environment temperature must be between -5 C and +45 C.
- Easily accessible, but only by authorized personnel.
- Available power source of -48 VDC, and the site must comply with National Electric Code (NEC) standards.
- Available management connection (Ethernet).

In addition, since the IDU will be connected to the RFU, when considering a site, it is important to check for current and future obstacles on the roof or tower. Possible future obstacles may include trees, new buildings, and window cleaners on the roof, and snow that may accumulate in front of the antenna. The site should be accessible, but only by certified personnel.

Note about Heat Dissipation: The IP-10 IDU overall heat dissipation is 25W max (~85 BTU/h). The RFU heat dissipation is 100W max.

Note about Antenna Location: As with any type of construction, a local permit may be required before installing an antenna. It is the owner's responsibility to obtain any and all permits.

7.4.1 IDU Dimensions

The following illustration shows the dimensions (in millimeters) of the FibeAir IP-10 IDU.



7.5 Configuration Options

IP-10 can be installed in a standalone or a nodal configuration. The nodal configuration adds a backplane, which is required for certain functionality such as the TDM Cross-Connect and XPIC.

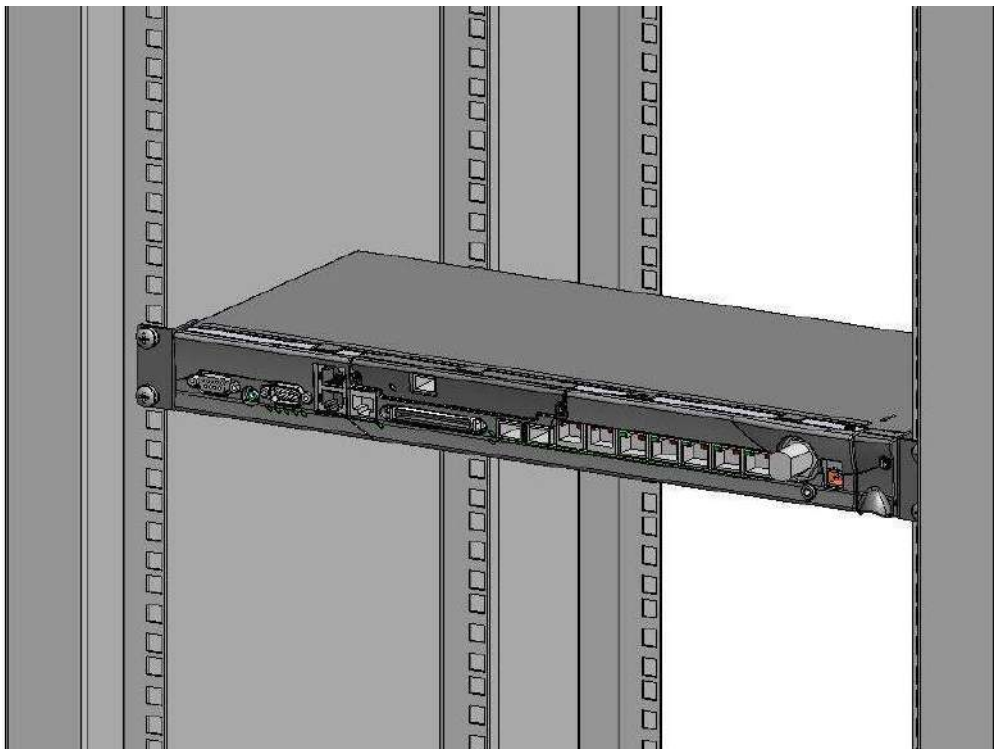
- For instructions on installing an IP-10 IDU in a standalone configuration, refer to *Installing the IDU in a 19"/ETSI Rack* on page 14.
- For instructions on installing an IP-10 IDU in a nodal configuration, refer to *Installing the IDU in a Nodal* on page 15.

7.6 Installing the IDU in a 19"/ETSI Rack



The intra-building port(s) of the equipment or subassembly is suitable for connection to intra-building or exposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metalically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metalically to OSP wiring.

The FibeAir IP-10 IDU can be installed in a standard 19" ETSI rack as shown in the following illustration.



As shown in the illustration, four screws, supplied with the installation kit, are used to secure the IDU to the rack.

7.7 Installing the IDU in a Nodal Enclosure

Each IP-10 IDU in a nodal configuration operates as either the main unit or an extension unit. The IDU's role is determined by its position in the nodal enclosure, with the lowest unit in the enclosure (Unit Number 1) always serving as the main unit.

The main unit performs the following functions:

- Provides a central controller for management
- Provides radio and line interfaces

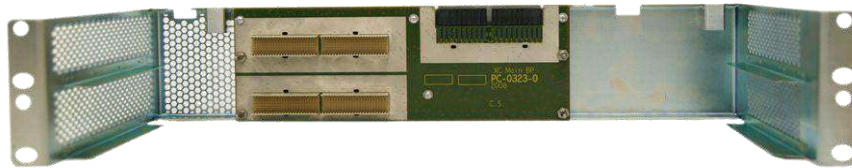
Extension units provide radio and line interfaces, and are accessed through the main unit.

7.7.1 Nodal Enclosure Design

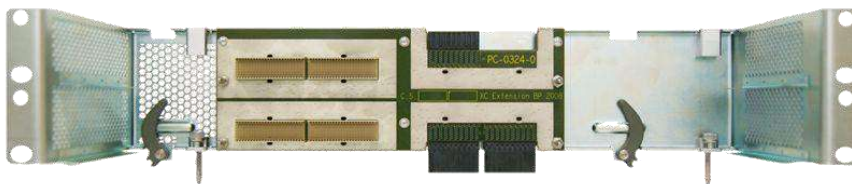
Two types of shelves are available for a nodal configuration:

- **Main Nodal Enclosure** – Each node must have a main nodal enclosure, which can hold two IP-10 IDUs.
- **Extension Nodal Enclosure** – Up to two extension nodal enclosures can be stacked on top of the main nodal enclosure. Each extension nodal enclosure can contain two IP-10 IDUs.

Main Nodal Enclosure



Extension Nodal Enclosure



Each nodal enclosure includes a backplane. The rear panel of an IP-10 IDU includes an extra connector for connection to the backplane. The following interfaces are implemented through the backplane:

- Multi-Radio
- Protection
- XPIC

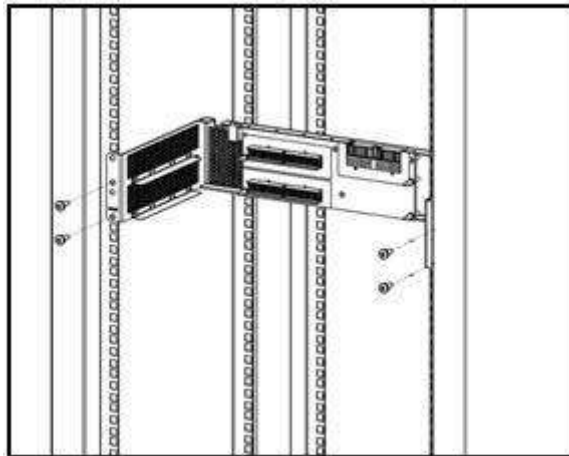
IP-10 IDUs are hot-swappable, and additional extension nodal enclosures and IDUs can be added in the field as required, without affecting traffic.

7.7.2 List of Kits Needed to Install an IDU in a Nodal Configuration

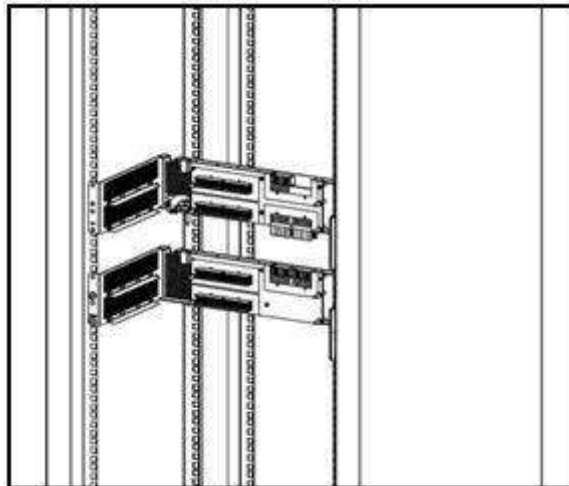
Item	Description	Quantity	Remarks
1	I+MAIN ENCLOSURE	1	
2	I+EXPANSION ENCLOSURE	In accordance with configuration	Optional
3*	I+BLANK	In accordance with configuration	Optional
4	IP-10 G-Series IDU	In accordance with configuration	

* Note that item #3, I+BLANK, is a blank panel that must be installed in each enclosure slot that is not occupied by an IDU.

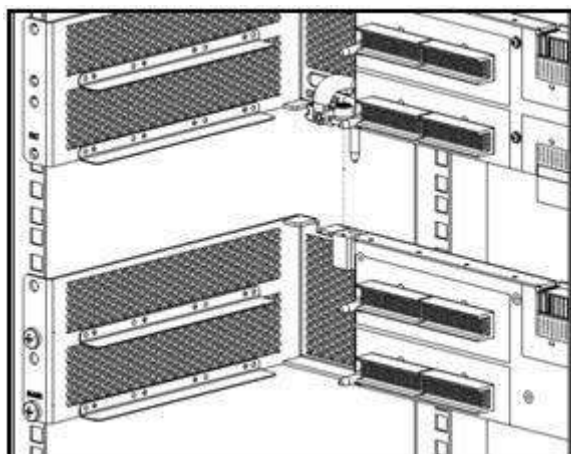
7.7.3 Procedure for IDU Installation in a Nodal Configuration



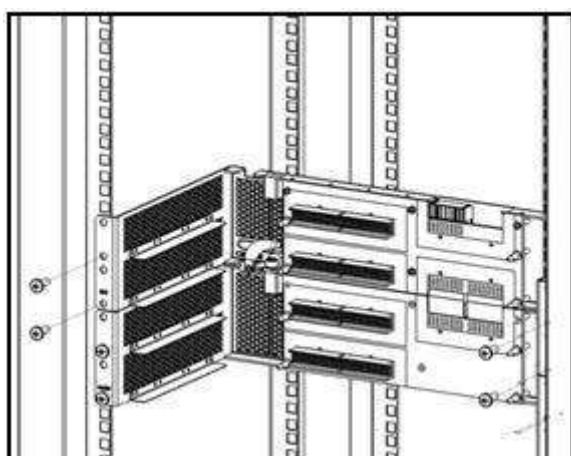
- 1 Install the IP-10 I+Main Enclosure in the 19 inch rack using 4 screws.



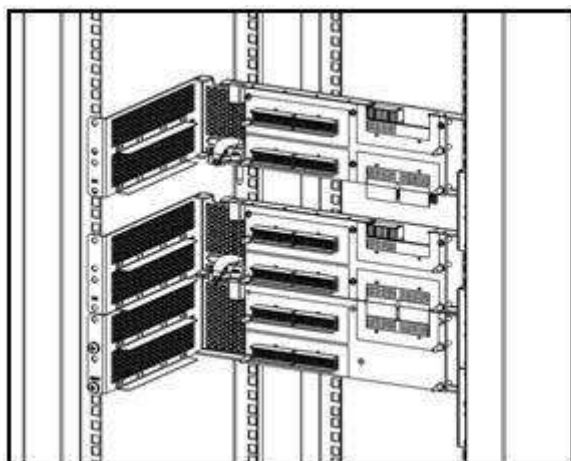
- 2 If an expansion enclosure is required, install the IP-10 I+Expansion Enclosure above the IP-10 I+Main Enclosure, by sliding it down.



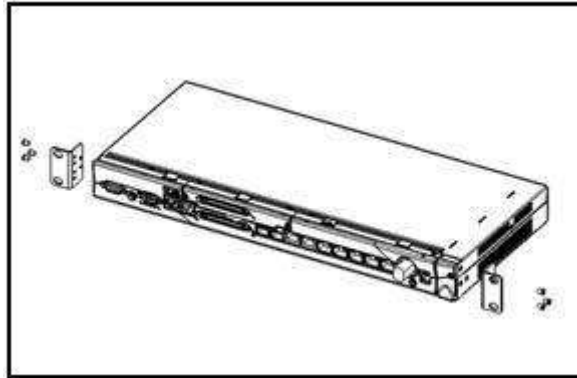
- 3 Fasten the 2 screws at the back of the IP-10 I+Expansion Enclosure.



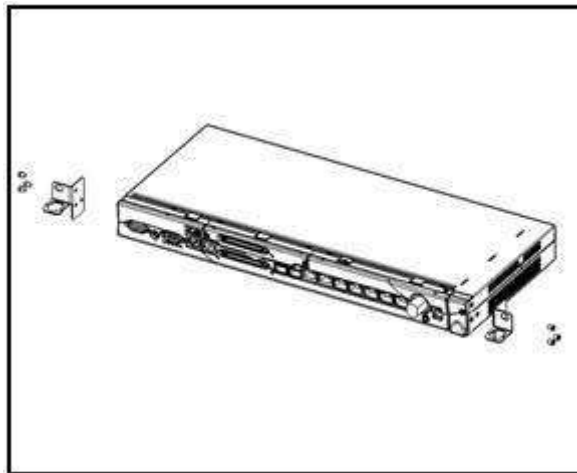
- 4 Install the IP-10 I+Main Enclosure in the 19 inch rack using 4 screws.



- 5 If an additional expansion enclosure is required, perform steps 2-4 again with the second IP-10 I+Expansion Enclosure.

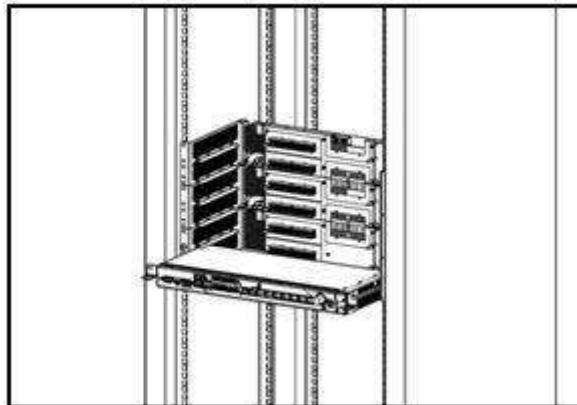


- 6 Remove the two 19" brackets mounted on the IP-10 IDU by unscrewing the 3 screws at each side.

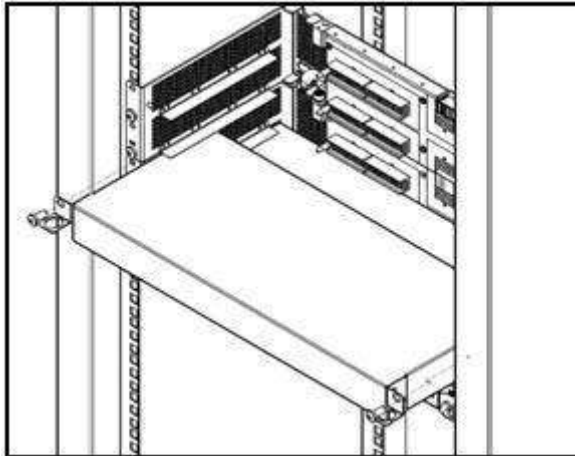


- 7 Install the two special 19" brackets on the IP-10 IDU supplied with the enclosure kit.

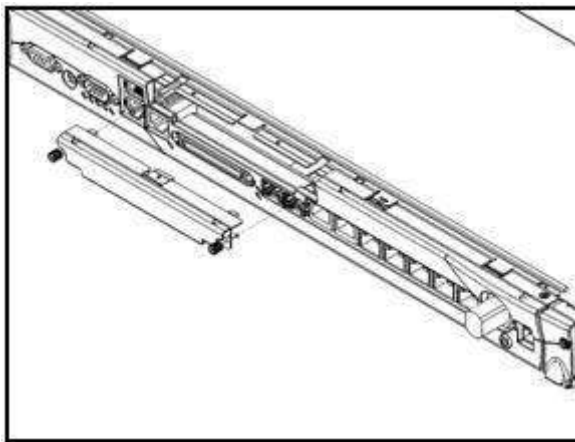
Warning! The 19" ears should be removed from the IP-10 IDU and replaced with the special ears that are used to fasten the IP-10 IDU to the main nodal enclosure (the XC chassis). If this is not done, the unit will not be 100% plugged into the backplane and you may encounter incomprehensible errors.



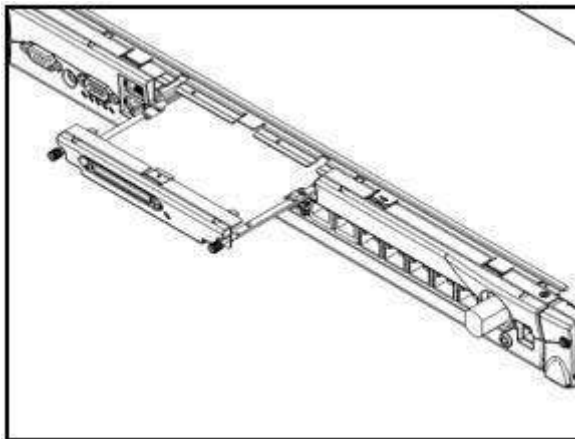
- 8 Slide the IDU into the enclosure and tighten it using 2 screws. Repeat this step for any additional IDUs in your configuration.



- 9 If there are any empty slots in your configuration, slide the IP-10 I+Blank panel into the enclosure, and tighten it using 2 screws.



- 10 In accordance with the configuration, remove the IP-10 T-Card blank panel from the IDU, by releasing 2 side screws.



- 11 In accordance with the configuration, insert the IP-10 T-Card panel into the IDU sliders, and tighten it using 2 side screws.

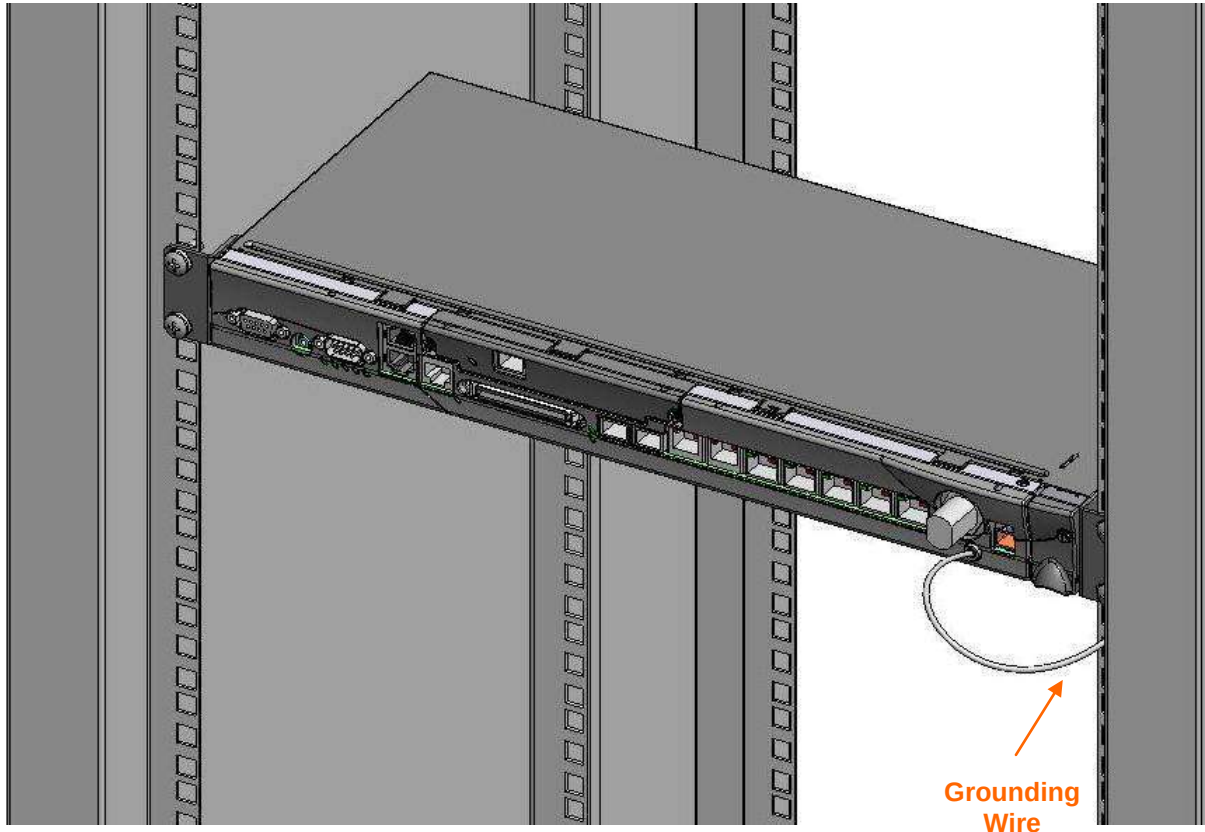
Note If you remove the T-Card, the T-Card blank needs to be put back in the slot.

Important!

For the warranty to be honored, install the unit in accordance with the instructions above.

7.8 Grounding the IDU and Electrical Information

The following illustration shows how the IDU is grounded to the rack.



IDU Grounding Notes

- The IDU is suitable for installation in a Common Bonding Network (CBN).
 - Only copper wire should be used.
 - The wire must be at least 14 AWG.
 - Connector and connection surfaces must be plated. Bare conductors must be coated with antioxidant before crimp connections are made to the screws.
 - FibeAir provides a ground for each IDU, via a one-hole mounted lug onto a single-point stud. The stud must be installed using a UL-listed ring tongue terminal, and two star washers for anti-rotation.
 - For antenna ports, lightning protection is used that does not permit transients of a greater magnitude than the following:
 - Open Circuit: 1.2-50us 600V
 - Short Circuit: 8-20us 300A
 - The ampacity of the conductor connecting the IDU frame to the DC return conductor is equal to, or greater than, the ampacity of the associated DC return conductor.
- 1 On the IDU, connect a grounding wire to the single point stud below the IDU-RFU interface (using the single screw with two washers), and, at its other end, to the rack.

- 2 Connect the power cable to the IDU power connector, and at the other end to the power source.

Note: Connecting the power cable to a live power source will cause the IDU to be powered on.

Important! Make sure to use a circuit breaker to protect the circuit from damage by short or overload.

Power Supply Notes

When selecting a power source, the following must be considered:

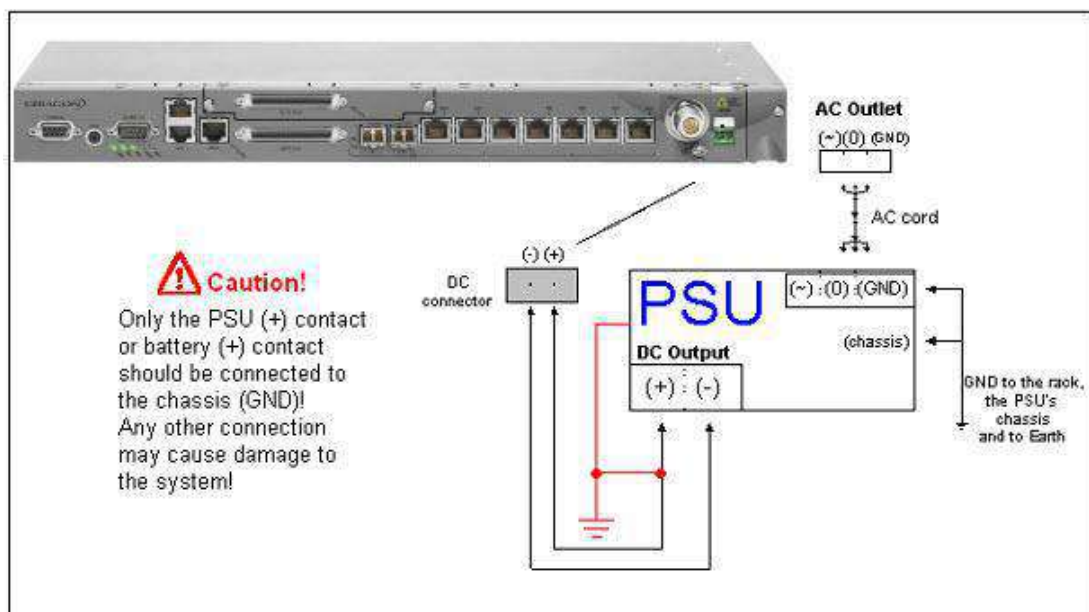
- DC power can be from -40.5 VDC to -60 VDC.
- **Recommended:** Availability of a UPS (Uninterrupted Power Source), battery backup, and emergency power generator.
- Whether or not the power source provides constant power (i.e., power is secured on weekends or is shut off frequently and consistently).
- The power supply must have grounding points on the AC and DC sides.



⚠ Caution!

The user power supply GND must be connected to the positive pole in the IDU power supply. Any other connection may cause damage to the system!

Power supply grounding should be in accordance with the following illustration:



7.8.1 Dual DC Feed



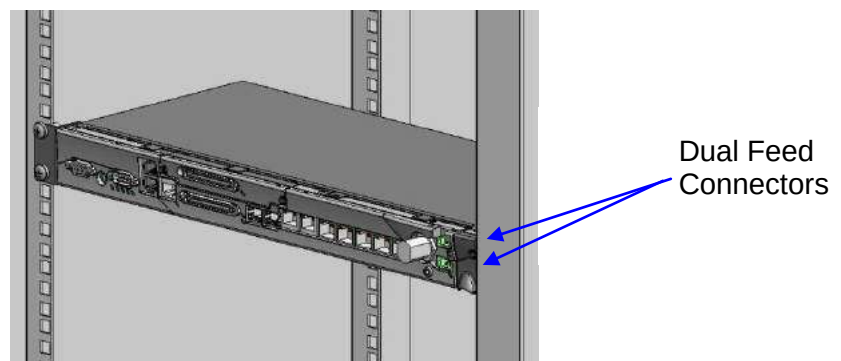
The dual feed IDU supports two DC inputs for power redundancy. Each input can be connected to a separate power source. The lower input is numbered 1, and the upper is numbered 2.

Each input can receive voltage in the range of -40.5V to -60V.

Each power input has a dedicated LED on the front panel which indicates if that input is receiving adequate power. This means that the LED will be off when the input voltage is below -40.5V (absolute value).

In addition, the IDU raises an alarm when the power input is below the minimal level (one alarm per power input). You can mask this alarm using the CLI. This option can be used if you choose to connect only one power input and do not want a permanent alarm in the system.

The power input connectors have built-in screws. Appropriate DC cables should be used, and the screws should be fastened.



8. RFU Overview

This section provides an overview of the radio frequency units (RFUs) that you can install as part of an IP-10G system. Ceragon's RFUs were designed with sturdiness, 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 section can be used in an IP-10G system.

FibeAir RFUs deliver the maximum capacity over 3.5-56 MHz channels with configurable modulation schemes from QPSK to 256QAM, independently of the data interface in use. The RFUs inherently support the use of the XPIC mechanism to double capacity over a specific radio channel.

An IP-10G system can use the following RFUs:

Standard Power

- FibeAir RFU-C
- FibeAir RFU-SP
- FibeAir 1500P

High Power

- FibeAir 1500HP
- FibeAir RFU-HP
- FibeAir RFU-HS

8.1 Installing an RFU

Installation instructions for Ceragon RFUs are provided in separate installation manuals for each type of RFU. For a list of RFU installation manuals and their Ceragon document numbers, refer to *Related Documents* on page 9.

8.2 RFU Selection Guide

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

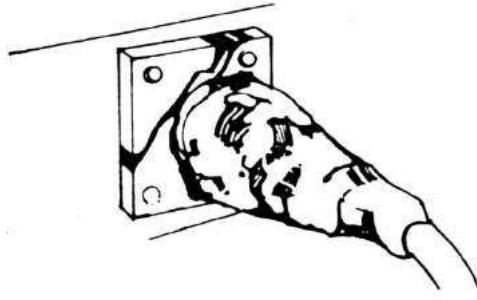
- For the 13-38 GHz frequency range, use FibeAir RFU-C
- For the low frequencies please refer to the options below:

RFU Selection Guide

Character		RFU-C (6 – 38GHz)	1500HP (6 – 11GHz)	RFU-HP (6 – 11GHz)	RFU-HS (6 – 8GHz)	RFU-SP (6 – 8GHz)	1500P (11 – 38GHz)
Installation Type	Split Mount	√	√	√	√	√	√
	All-Indoor	--	√	√	--	--	--
Space Diversity Method	SD (BBS/IFC)	BBS	BBS + IFC ¹	BBS	BBS	BBS	BBS
Frequency Diversity	FD (BBS)	√	√	√	√	√	√
Configuration	1+0/2+0/1+1/2+2	√	√	√	√	√	√
	N+1	--	√	√	--	--	--
	N+0 (N>2)	--	√	√	--	--	--
Tx Power (dBm)	High Power (up to 29 dBm)	--	√	√	√	--	--
	Ultra High Power (up to 32 dBm)	--	√	√	--	--	--
RFU Mounting	Direct Mount Antenna	√	--	--	√	√	√
Bandwidth (BW)	3.5MHz – 56 MHz	√	--	√	--	--	--
	10 MHz – 30 MHz	√	√	√	√	√	√
	56 MHz	√	--	√	√	√	√
Power Saving Mode	Adjustable Power Consumption	--	--	√	--	--	--

¹ 1500 HP (11 GHz) 40 MHz bandwidth does not support IF Combining. For this frequency, space diversity is only available via BBS.

Molding the Coaxial Seal



- iv If more COAX-SEAL is necessary to complete the seal, simply cut the needed amount and add to the existing COAX-SEAL, molding and pressing it into the other material. COAX-SEAL adheres to itself with slight pressure.
- v Carefully inspect the seal to make certain that all joints are covered.

Note:	Make sure you fasten the cable along the ladder!
Important!	Make sure that the inner pin of the connector does not exceed the edge of the connector.

The cable should have a maximum attenuation of 30 dB at 350 MHz.

10. Initial System Configuration

This section describes the basic configuration steps for an IP-10 radio link, including the following main procedures:

- Establishing a Connection with the IDU
- Launching the Web EMS
- Configuring IP Addresses
- Upgrading the IDU Software
- Loading the License Key

For detailed instructions on configuring the IP-10G, refer to the FibeAir IP-10G and IP-10E User Guide, DOC-00034612. The User Guide includes instructions for configuring the IP-10G interfaces, security protocols, management, and all other necessary configurations. The User Guide also includes instructions for setting up the various IP-10G configuration options such as space and frequency diversity, Multi-Radio, XPIC, and 1+1 HSB, 2+2 HSB, and 2+0 configurations.

Note: The instructions in this chapter are written for the Web-Based Element Management System (EMS). However, most of the procedures described in this chapter can also be performed using the CLI or the PolyView and NetMaster NMS.

10.1 Establishing a Connection with the IDU

The default factory configuration of a new IP-10 IDU is:

- IP Address: 192.168.1.1, IP Mask 255.255.255.0.
- Active management ports: ports 6, and 7 (far right RJ45 ports), out-of band management.
- License: Basic – capacity 10Mbps, no ACM, Single Pipe (only GbE ports, ports #1 or #3)
- SW package: Basic – 6.xx.xx.
- Protection: Disabled. 1+0 configuration

To establish a connection with the IDU:

- 1 Verify that no Ethernet traffic (cables or fibers) is connected.
- 2 Power up the IDU.
- 3 Connect your PC or laptop to one of the IDU management ports (ports 6 or 7, far right RJ45 ports).



- 4 Set your PC or laptop to the following configuration:
 - ☐ IP Address: 192.168.1.240
 - ☐ IP Mask 255.255.255.0
 - ☐ No default gateway.
- 5 Verify connectivity to the IDU by pinging 192.168.1.1. If there is no connectivity, verify IDU IP management configuration using the Command Line Interface (CLI).

10.2 Launching the Web EMS

You can use the Web EMS to perform initial IDU configuration. To launch the Web EMS:

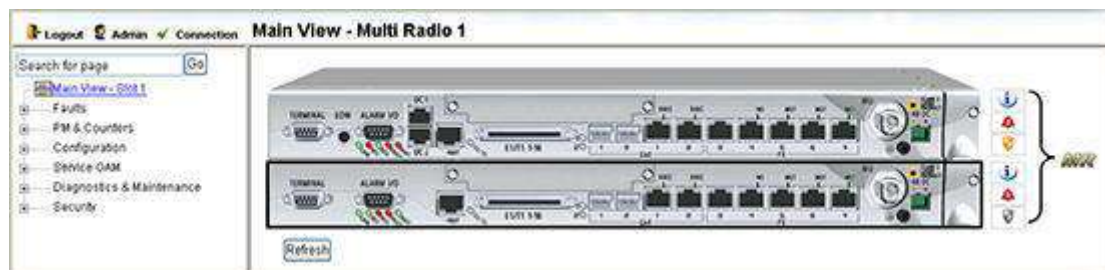
- 1 Start your web browser.
- 2 In the URL address field at the top, type <http://yourIP>, where yourIP is the IP address of the IDU. The default IDU IP address is 192.168.1.1.
- 3 Press **Enter**. The IP-10 Login page is displayed.

The screenshot shows a web browser window titled "Login". It contains two input fields: "User Name" and "Password". Below these fields are two buttons: "Apply" and "Clear".

- 4 Enter the user name and password:
 - ☐ **Default user name:** admin
 - ☐ **Default password:** admin.
- 5 Click **Apply**. The Main View page opens, displaying all the unit's populated slots.

Note: For multi-radio configurations, protection, and extension units, available options will vary according to the available interfaces and configured features for selected slot.

Main View - Multi radio configuration



Main View - Single unit configuration



Configuration and other operations are performed by clicking the menus on the left side of the page.

10.3 Configuring IP Addresses

You can configure the local IDU's IP address in the Local IP Configuration section of the Management page.

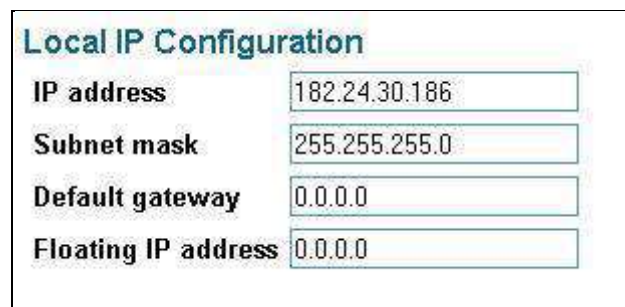
Note: After the link is up and running, you can also configure the remote IDU's IP address, in the Remote IP Configuration section of the Management page.

In protected configurations, the floating IP address feature provides a single IP address that will always provide direct access to the currently active main unit. This is used primarily for web-based management and telnet access.

The user can configure a floating IP address in the active unit, and this IP address will be automatically copied to the standby unit.

To configure local IP settings:

- 1 Select **Configuration > General > Management**. The Management page opens.
- 2 In the Local IP Configuration section of the Management page, enter the IP address of the local unit, its subnet mask, and the default gateway.



The screenshot shows a web form titled "Local IP Configuration". It contains four input fields, each with a label to its left:

Field Label	Value
IP address	182.24.30.186
Subnet mask	255.255.255.0
Default gateway	0.0.0.0
Floating IP address	0.0.0.0

- 3 Optionally, enter a floating IP address. The following limitations apply to a floating IP address:
 - ☐ The floating IP address must be different from the system IP address.
 - ☐ The floating IP address must be in the same subnet as the system IP address.

10.4 Upgrading the IDU Software

New IDUs contain the basic software version (6.xx.xx.), and require a software upgrade in order to support all system features. You must download the new software by FTP.

When downloading software, the IDU functions as an FTP client. You must install FTP server software on the PC or laptop you are using to perform the software upgrade. You may use Windows FTP Server or any other FTP server application to perform the upgrade.

Note: It is recommended to use FileZilla_Server-0_9_26 software that can be downloaded from the web (freeware).

IP-10G/E includes a timed software installation feature that enables you to configure a software upgrade to take place at a later time. This enables you to perform software upgrades during periods of off-peak user traffic.

IP-10G/E software versions are released as zipped Linux RPM (Red Hat Package Manager) files (22 files or more).

10.4.1 Viewing IDU Version Information

To view IDU version information:

- 1 Select **Configuration > General > Versions > IDU**. The IDU Versions window opens.

Package Name	Target Device	Running Version	Installed Version	Upgrade Package	Downgrade Package
aidu	IDC	6.9.0.1.0.33-1	6.9.0.1.0.33-1	6.9.0.1.0.33-1	6.9.0.1.0.33-1
aidu-idc	IDC	6.9.0.1.0.33	6.9.0.1.0.33-1	6.9.0.1.0.33-1	6.9.0.1.0.33-1
aidu-management	IDC	6.9.0.47	6.9.0.47-1	6.9.0.47-1	6.9.0.47-1
aidu-modem-fw	Modem	3.40.2	3.40.2-1	3.40.2-1	3.40.2-1
aidu-fpga-fw	FPGA	N/A	50.6.10-1	50.6.10-1	50.6.10-1
aidu-mrmc-scripts	Modem+FPGA	7.08-1	7.08-1	7.08-1	7.08-1
L2protocols	IDC	7.5.1.aidc.t183.6.9.0.11	7.5.1.aidc.t183.6.9.0.11-1	7.5.1.aidc.t183.6.9.0.11-1	7.5.1.aidc.t183.6.9.0.11-1
kernel	IDC	2.6.14.7-aidc.3.17	2.6.14.7-aidc.3.17	2.6.14.7-aidc.3.17	2.6.14.7-aidc.3.17
kernel-modules	IDC	0.3.16-2.6.14.7_aidc.3.17	0.3.16-2.6.14.7_aidc.3.17	0.3.16-2.6.14.7_aidc.3.17	0.3.16-2.6.14.7_aidc.3.17
aidu-setup	IDC	N/A	6.9.0.14-1	6.9.0.14-1	6.9.0.14-1
aidu-atp	IDC	N/A	3.3.9-1	3.3.9-1	3.3.9-1
aidu-pwc	IDC	0.24	0.24-1	0.24-1	0.24-1

Refresh

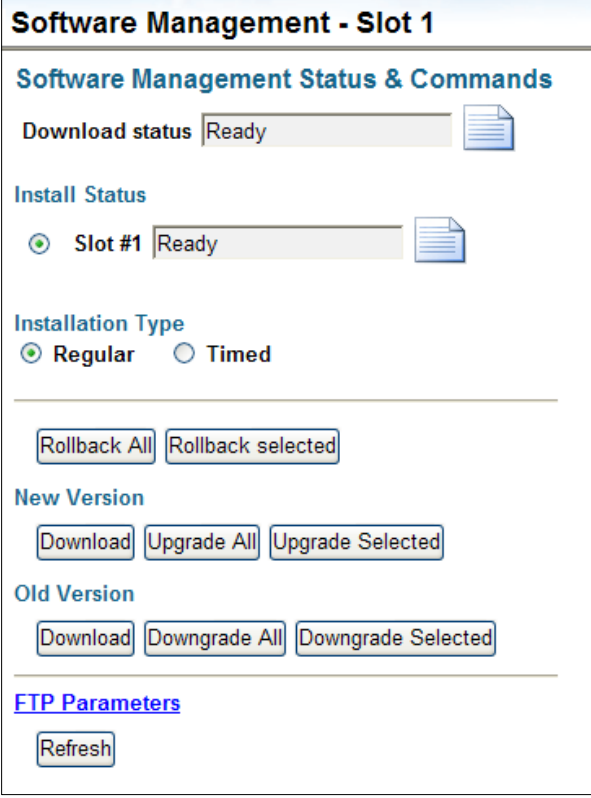
The IDU Versions table includes the following columns:

- **Package Name** – Indicates the name of the software package.
- **Target Device** – Indicates the specific component that contains the version.
- **Running Version** – Indicates the version that is currently running on the IDU.
- **Installed Version** – Displays IDU software files that were successfully installed.
- **Upgrade Package** – Displays IDU software files that were successfully downloaded to the IDU, and are ready to be installed when IDU upgrade is executed.
- **Downgrade Package** – Displays IDU software files that were successfully downloaded to the IDU, and are ready to be installed when IDU downgrade is executed.

10.4.2 Downloading IDU Software Files

To download IDU software files:

- 1 Verify that your Windows firewall is disabled.
- 2 Select **Diagnostics & Maintenance > Software Management**. The Software Management page opens.



Software Management - Slot 1

Software Management Status & Commands

Download status 

Install Status

☒ Slot #1 

Installation Type

☒ Regular ☐ Timed

New Version

Old Version

FTP Parameters

- 3 Verify that your FTP server and remote server are properly configured.
- 4 In the New Version section, click **Download** to download a software upgrade package. This may take a few minutes.



New Version

Note: If you want to install an older version of the software, click **Download** in the Old Version section rather than the New Version section of the Software Management page.

- 5 Download or take the zipped software package (e.g., aidu-6.9.X.X.X.zip) from FTP and save it under C:\updates.
- 6 Extract the files to C;\updates.
- 7 Remove the ZIP file and store it in another location (e.g., C:\IP-10).

The **Download Status** field displays the status of the software download. Options are:

- ☐ Ready
- ☐ In-Progress
- ☐ Success
- ☐ Failure

To view the software download log, click the icon next to the **Download Status** field.



10.4.3 Upgrading the IDU Software Version

If you are upgrading the software in a 1+1 nodal configuration, make sure to perform the following steps:

- 1 Before initiating the upgrade, connect to the active IDU in the local site.
- 2 Select **Configuration > Protection > Protection Parameters**. The Protection Parameters page opens.
- 3 Set **Protection Lockout** to: **On**.
- 4 Click **Apply**.

If you are upgrading the software in a 1+1 standalone configuration, upgrade the standby IDU first, then upgrade the active IDU.

If you are upgrading the software in a 2+2 configuration, upgrade the I ???

To upgrade an IDU's software:

- 1 Select **Diagnostics & Maintenance > Software Management**. The Software Management page opens.
- 2 In the Installation Type section, specify the type of installation:
 - ☐ **Regular – The upgrade will be initiated immediately when you click Upgrade.**
 - ☐ **Timed – The upgrade will be initiated after a defined time interval.**
- 3 For a timed installation, specify the number of minutes in the Timed Install section of the Software Management page. When you click **Upgrade, the upgrade will be initiated after the defined number of minutes.**
- 4 In the New Version section, click **one of the following**:
 - ☐ In a 1+1 nodal configuration, select the standby IDU and click **Upgrade Selected** to upgrade the software in the standby IDU. This may take a few minutes. Once the upgrade is complete, the standby IDU will automatically reboot. Then, select the active IDU and click **Upgrade Selected**. Once the upgrade is complete, verify in the Configuration > General > Versions > IDU page that the new version is installed and running.
 - ☐ In a 2+0 system, click **Upgrade All** to upgrade the software in both IDUs.

- ☐ In a 2+2 configuration, click **Upgrade All** to upgrade the software in both IDUs in the standby enclosure. Once the upgrade is complete in both IDUs, the IDUs will automatically reboot. Then, go to the active enclosure and click **Upgrade All** to upgrade both IDUs in the active enclosure.

Note: If you are downgrading to an older software version, click **Downgrade Selected** or **Download All** in the Old Version section instead of **Upgrade Selected** or **Upgrade All** in the New Version section. Software downgrade requires a special package for downgrade. For example:
`downgrade-aidu-6.9.X.X.X.X.zip.`

- 5 For a 1+1 configuration, select **Configuration > Protection > Protection Parameters**, set **Protection Lockout** to **Off**, and click **Apply**.

The Install Status section indicates the current download status. Options are:

- ☐ Ready
- ☐ In-Progress
- ☐ Success
- ☐ Failure

For a timed installation, the Install Status section indicates the number of remaining minutes until the installation begins.

Note: Cancelling a timed installation operation will not abort an installation that is already in progress.

To view the software installation log, click the icon next to the slot you want to view in the Install Status section.

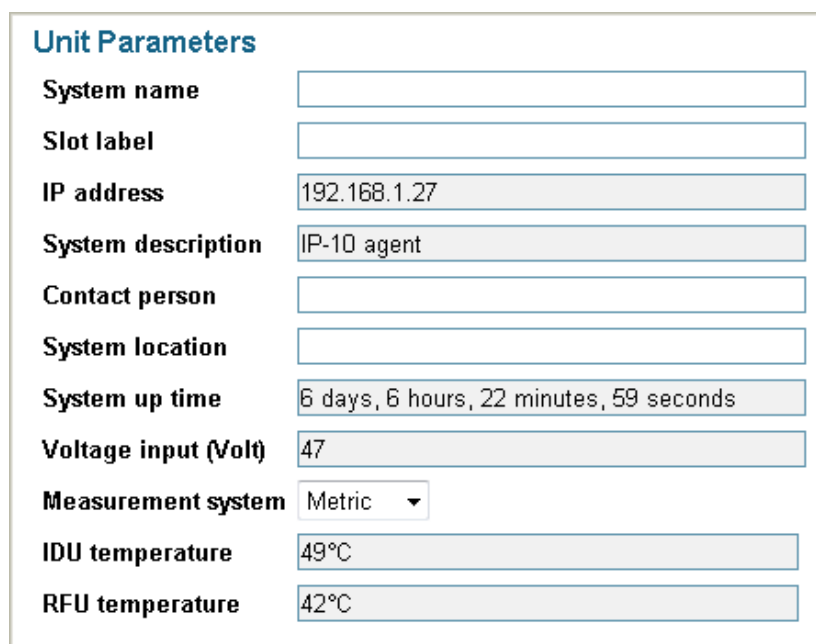
10.5 Loading the License Key

New IDUs are delivered with a basic license:

- License: Basic - capacity 10Mbps, no ACM, Smart Pipe (only GbE ports, ports #1 or #2)

Feature and capacity upgrades are implemented through manual entry of a license key based on the IDU's Serial number. Contact Ceragon in order to obtain your license key. Once you receive a new license key, you must load the new license key into the IDU:

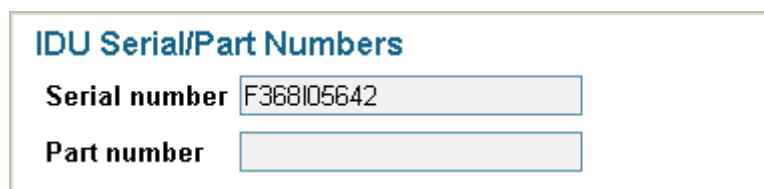
- 1 Select **Configuration > General > Unit Parameters**. The Unit Parameters page opens.



Unit Parameters	
System name	
Slot label	
IP address	192.168.1.27
System description	IP-10 agent
Contact person	
System location	
System up time	6 days, 6 hours, 22 minutes, 59 seconds
Voltage input (Volt)	47
Measurement system	Metric ▼
IDU temperature	49°C
RFU temperature	42°C

- 2 Verify that the three left characters of the license key match the three right characters of the IDU Serial Number, displayed near the bottom of the Unit Parameters page.

Note: You may have to scroll down the Unit Parameters page to display the IDU Serial Number.



IDU Serial/Part Numbers	
Serial number	F368105642
Part number	

- 3 Select **Configuration > General > Licensing**. The Licensing page opens.

Licensing - Slot 1 (Active)

Current License

License type

License code

Demo License

Demo admin

Demo timer

License Features

ACM license	Not allowed
Switch application license	Single pipe
Capacity	10
Network resiliency license	Allowed
TDM-only capacity license	Not allowed
TDM-only capacity value	0
Synchronization Unit License	Allowed
Enhanced Traffic Manger License	Allowed
Asymmetrical scripts license	Allowed
Enhanced compression license	Allowed
Per usage license	Not allowed

- 4 Enter the license key in the **License code** field.
- 5 Click **Apply**.
- 6 Perform a cold reset of the IDU. The new license will take be activated only after a cold reset.
- 7 Select **Configuration > General > Licensing**. The Licensing page opens.
- 8 Verify that the license parameters were updated.

Notes:

If the license key itself is not legal (e.g., a typing mistake or an invalid serial number), a License Violation alarm is raised specific to the problem with the license. In the event of a License Violation alarm, radio port capacity is automatically limited to ~3Mbps, allowing only management channels to the remote end. In order to clear the alarm, you must configure the system to comply with the loaded license, then issue a cold-reset. When the system returns online, it checks the legality of the configuration against the license limits. If no violation is detected, no alarm is raised, and the radio is fully operational.

You may use the Demo license for 60 days for full capacity and a full feature-set.

10.6 Configuring XPIC

Cross Polarization Interference Canceller (XPIC) is a feature that enables two radio carriers to use the same frequency with a polarity separation between them. Since they will never be completely orthogonal, some signal cancelation is required.

In addition, XPIC includes an automatic recovery mechanism that ensures that if one carrier fails, or a false signal is received, the mate carrier will not be affected. This mechanism also assures that when the failure is cleared, both carriers will be operational.

XPIC can be used in a 2+0 or 2+2 configuration. XPIC can be, but does not have to be, used in conjunction with Multi-Radio.

10.7 Conditions for XPIC

XPIC is achieved using two IDUs inserted in a nodal enclosure (main or extension). One IDU is used for the horizontal polarization and the other is used for the vertical polarization.

XPIC IDUs can be placed inside a main node or extension node in any of the following slots: 1 and 2 (main node), 3 and 4 (extension node), and 5 and 6 (second extension node). Slot 1 is the bottom slot in the main node. The data of each polarization is marked by a different value, so the modem cannot lock on the signal of the mate polarization.

When installing an XPIC system, each IDU and each RFU must be the same hardware type. In addition, each IDU on both sides of the link must be set to the same frequency. An appropriate alarm is raised if these requirements are not met.

In order to activate XPIC, an XPIC script should be selected during initial configuration. The same script must be used in all the IDUs on both sides of the link.

After changing a script, the IDU must be reset.

10.8 Configuring the Antenna and RFU for XPIC

- 1 Install the dual polarization antenna and point it in the direction of the other site.
- 2 Following alignment, verify that the link achieves its required RSL.
- 3 The antenna feeders may also need to be aligned (slight rotations) in order to achieve the highest XPI (in absolute value) during installation, and no less than 25dB. Refer to *Displaying XPI Values* on page 40.
- 4 Install the two RFUs on a dual polarization antenna using the appropriate mounting kit, and mark the RFUs as V. and H. respectively.

10.8.1 IDU-RFU Cable Installation

- 1 Install two cables between the RFUs and the IDU. Note that the cable length difference should not exceed 10 meters.
- 2 Mark the cables with V. and H. respectively and connect them respectively to the IDU and RFU.
- 3 It is recommended to connect IP-10G/E units in the lower slots of a pair (slots 1, 3, and 5) to the RFUs with vertical polarization, and the IP-10G/E units in the upper slots of a pair (slots 2, 4, and 6) to the RFUs with horizontal polarization.

10.8.2 Antenna Alignment

- 1 Power up the lower IDU (V) on both ends of the link and configure it to the desired frequency channel, and using the XPIC script with the maximum power.
- 2 Align the antennas, one at a time, until the expected RSL is achieved. Make sure the RSL achieved is no more than +/-2 dB from the expected level.

10.8.3 Polarization Alignment

Polarization alignment is required to verify that the antenna feeds are adjusted, ensuring that the antenna XPD (Cross Polarization Discrimination) is achieved.

Polarization adjustment should only be performed on one antenna.

- 1 Disconnect the V cable from the V RFU and connect it to the H RFU.
- 2 Check the RSL achieved in the H RFU and compare it to the RSL achieved by the V RFU.
- 3 Verify that the XPI (Cross Polarization Interference) is at least 25dB where:

$$XPI = RSL_{POL} - RSL_{XPOL}$$

RSL_{POL} → Link RSL with the same polarization used at both sites.

RSL_{XPOL} → Link RSL with orthogonal polarizations used at both sites.

- 4 If the XPI is less than 25dB, adjust the feed polarization by opening the polarization screw and gently rotating the feed to minimize the RSL_{XPOL} .

Note: Polarization alignment is not always possible since the RSL_{XPOL} might fall below the sensitivity threshold of the RFU.

10.9 Displaying XPI Values

The current XPI value can be displayed in the Web EMS and the CLI (the value is valid only when the modem is locked on a signal).

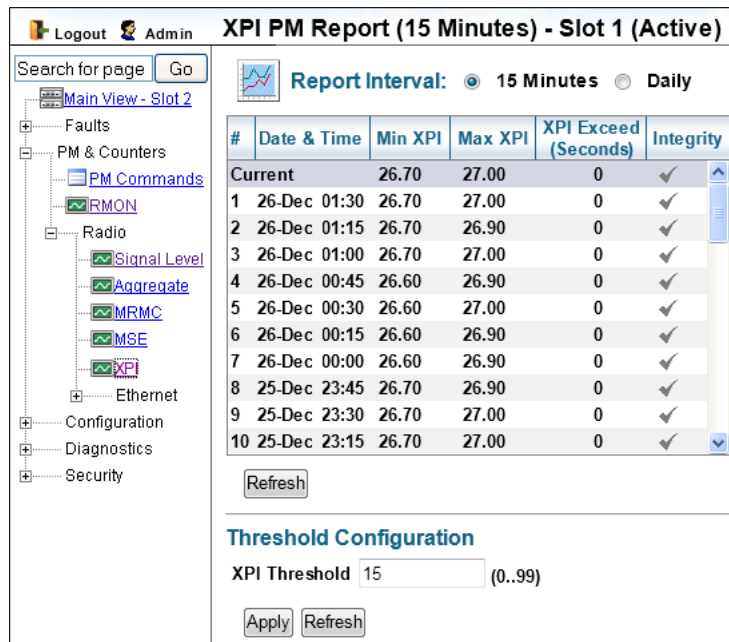
- Using CLI, enter the command `xpi`.
- Using Web-Based Management:
 - ☐ To view the current XPI value, select **Configuration > Radio > Radio Parameters** from the menu bar on the left side of the main management page.



Note: The XPI level field only appears if the IDU is using an XPIC script.

- To view XPI performance for intervals of 15 minutes or daily, select **PM & Counters > Radio > XPI** from the menu bar on the left side of the main management page. The XPI PM Report is displayed.

XPI PM Report



Note: In “clear sky” conditions, a normal XPI level is between 25 and 30dB.

11. Acceptance and Commissioning Procedures

This section provides Ceragon's recommended Acceptance and Commissioning Procedure for a FibeAir IP-10 system. Acceptance and commissioning should be performed after initial setup is complete.

The purpose of this procedure is to verify correct installation and operation of the installed link and the interoperability with customer end equipment.

Ceragon's Acceptance and Commissioning procedure includes the following stages:

- Site Acceptance Procedure
- Commissioning of radio link in a 1+0 configuration
- Commissioning of radio link in a 1+1 configuration
- Commissioning of radio link in a 2+0 or 2+2 XPIC configuration

The Site Acceptance Procedure is a checklist that summarizes the installation requirements of the site at which the products were installed.

The commissioning tests cover the required configuration information that should be recorded, and the tests that should be performed on the radio link in 1+0, 1+1, and 2+0 configurations.

11.1 Site Acceptance Procedure

The purpose of the following procedures is to verify that all installation requirements were noted and checked. Following this procedure will ensure proper, long-lasting, and safe operation of the product.

The checklist below summarizes the installation requirements of the site.

SITE ACCEPTANCE CHECKLIST	
1. SITE INFORMATION	
Customer:	
Radio model:	
Site name:	
Site code:	
Radio link code:	
Site address:	
2. ANTENNA MOUNTING	
Antenna mount type:	
Mount is of sufficient height to clear local obstructions	OK
Mount is safely positioned to not cause a safety hazard	OK
Mount is secure and perpendicular	OK
Mount is grounded as per site specifications	OK
All steelwork is Galvanized or Stainless Steel as appropriate	OK
3. ANTENNA	
Antenna type (model and size):	
Antenna is securely fixed to mount	OK
Antenna is grounded as per site specifications	OK
Antenna sway braces are installed correctly (where applicable)	OK
Antenna Radome is securely fitted (where applicable)	OK
Water drain plugs are fitted and removed, as appropriate	OK
Antenna sealing O-Ring is properly fitted and not damaged	OK
Antenna/Launch unit polarization is as per link requirements	OK

SITE ACCEPTANCE CHECKLIST (continued)	
4. Radio Frequency Unit (RFU)	
Type of RFU mount:	(Direct or Remote mount)
RFU is securely mounted to the antenna or pole	OK
RFU is grounded as per installation instructions	OK
RFU's polarization is as per link requirements	OK
RFU is installed properly and has no physical damage	OK
<i>For Remote-Mount Only:</i>	
Remote mount kit is securely mounted to the pole	OK
Flexible waveguide has no physical damage and connectors are sealed	OK
All flexible waveguide bolts are secured using washers and lock-washers, as appropriate	OK
Flexible waveguide is secured to the pole	OK
6. COAX CABLE	
Overall cable length:	
Cable type:	
N-Type connectors assembled properly on the cable	OK
Cable connected securely to RFU and IDU	OK
Cable connector is weather-proofed (sealed) at the RFU	OK
At the RFU, cable has a service/drip loop to prevent moisture from entering the connector	OK
Cable is secured using suitable restraints to fixed points at regular intervals (0.5 m recommended)	OK
Cable has no sharp bends, kinks, or crushed areas. All bends are per manufacturer specifications	OK
Grounding/lightning protection is as per site specifications	OK
Lightning protection type and model:	
Cable point-of-entry to building/shelter is weather-proof	OK
Cable ends are properly labeled	OK

SITE ACCEPTANCE CHECKLIST (continued)	
7. FLEXIBLE WAVEGUIDE	
Overall flexible WG length:	
Flexible WG type:	
Flexible WG is connected securely to RFU and Antenna	OK
Flexible WG connector is weather-proofed (sealed) at the RFU	OK
At the RFU, the flexible WG has a service/drip loop to prevent moisture from entering the connector	OK
Flexible WG is secured using suitable restraints to fixed points at regular intervals (0.5 m recommended)	OK
Flexible WG has no sharp bends, kinks, or crushed areas. All bends are per manufacturer specifications	OK
Flexible WG point-of-entry to building/shelter is weather-proof	OK
Flexible WG ends are properly labeled	OK
8. INDOOR UNIT (IDU)	
IDU is securely mounted to the rack	OK
IDU is located in a properly ventilated environment	OK
IDU fans are functional and air flow to the fans is not disrupted	OK
IDU and rack are grounded as per site specifications	OK
Traffic cables and connections are properly terminated as per manufacturer/cable instructions	OK
All cabling is secured, tidy, and visibly labeled	OK
9. DC POWER SUPPLY	
Measured DC voltage input to the IDU:	(-40.5 to -60 VDC)
Power-Supply maximum current:	(at least 3 Ampere in 1 +0 site)
Power-Supply is properly grounded	OK
DC power backup type:	
IDU DC connector is secure and the DC input leads are correctly terminated (no bare wires are visible)	OK
IDU DC connector (+) and (GND) leads are shorted and GND is grounded	OK
10. RACK INSTALLATION	
Rack is mounted to the shelter floor with four screws	OK
Rack is mounted to the shelter wall with two screws	OK

SITE ACCEPTANCE CHECKLIST (continued)	
11. REMARKS/NOTES	
12. GENERAL INFORMATION	
Site accepted by:	Name:
	Title:
	Company:
	Signature:
	Date:
Site approved by:	Name:
	Title:
	Company:
	Signature:
	Date:

11.2 Site Acceptance Checklist Notes

The following notes provide important additional information about the Site Acceptance Checklist.

11.2.1 Antenna Mounting

- Mounting pole is of sufficient height to clear local obstructions, such as parapets, window cleaning gantries, and lift housings.
- Mounting Pole is of sufficient height, and is safely positioned, so as not to cause a safety hazard. No person should be able to walk in front of, or look directly into the path of the microwave radio beam. Where possible, the pole should be away from the edge of the building.
- Mounting pole is secure and perpendicular. A pole that is not perpendicular may cause problems during antenna alignment.
- Mounting pole is grounded as per site specifications. All operators and site owners have specific requirements regarding the grounding of installations. As a minimum, typical requirements are such that any metal structure must be connected to the existing lightning protection ground of the building. Where it extends beyond the 45 degree cone of protection of existing lightning conductors, additional lightning protectors should be installed.
- All steelwork is Galvanized or Stainless Steel, as appropriate to prevent corrosion.

11.2.2 Antenna

- Antenna is grounded as per site specifications. See the third point in the Antenna Mounting section above.
- Antenna sway braces are fitted and installed correctly, where applicable. Typically, for an antenna of 1.2 m or larger, an extra sway brace is fitted to the mounting frame of the antenna. This sway brace should not be mounted to the same pole as the antenna, but should be installed directly back to the tower or an alternative point.
- Antenna Water Drain Plugs are fitted and removed, where appropriate. Some antennas have moisture drain plugs installed at various points around the antenna. The purpose of these plugs is to allow any moisture that forms on the inside of the antenna or radome to drip out and prevent a pool within the antenna. Only the plugs at the bottom of the antenna, after installation, should be removed. All other plugs should be left in position.

11.2.3 RFU (Radio Frequency Unit)

- The RFU is grounded as per installation instructions. See the third point in the Antenna Mounting section above.
- The RFU polarization is as per link requirements and matches the polarization of the antenna.

11.3 IDU (Indoor Unit)

- The main traffic connections are correctly terminated and crimped as per cable and connector manufacturer instructions. All fiber optic patch leads should be routed carefully and efficiently, using conduits to prevent damage to the cables.
- All other user terminations are secure and correctly terminated.
- All labeling is complete as per site requirements. Labeling is specific to each customer. At a site with only one installation, labeling may be unnecessary. However, at sites with multiple installations, correct and adequate labeling is essential for future maintenance operations. Typical labeling requirements include:
 - ☐ **Antenna labels** - for link identity and bearing
 - ☐ **RFU labels** - for link identity, frequency, and polarization
 - ☐ **Coax cable labels** - for link identity, close to the RFU, IDU, and either end of any joint
 - ☐ **IDU labels** - for link identity

11.4 1+0 Commissioning Procedure

This section describes the recommended commissioning tests for a FibeAir radio link in a 1+0 configuration.

The purpose of the commissioning tests is to verify correct and proper operation of the product.

11.4.1 Commissioning Test

The following tests should be performed on each installed link.

11.4.1.1 Link Verification

- “Link” LED and RFU LED on the IDU front panel are green, indicating the radio link is up.
- Received Signal Level (RSL) is up to +/- 2dB from the expected (calculated) level at both ends of the link.
- Radio Bit Error Rate (BER) is $10E^{-11}$ or higher.
- If working with ATPC, ATPC is operating as expected (RSL = reference level).
- After connecting test equipment or end equipment to the line interfaces, all LEDs on the front panel of the IDU are green.

11.4.1.2 Line Interfaces Test

- 50/100/200 Mbps, GbE Interface - connect a Packet Analyzer to GbE Ethernet interface and verify error-free operation (no packet loss) for at least 1 hour. Use an Ethernet loop on the remote site.
- 45 Mbps Interface - connect PDH test equipment to the DS3 interface and verify error-free operation for at least 1 hour. Use a physical or software loop at the far end.
- 2 Mbps/1.5 Mbps - connect PDH test equipment to the E1/DS1 interface and verify error-free operation for at least 1 hour. Use a physical or software loop at the far end.

11.4.1.3 Interoperability Verification

- Connect customer end equipment to the line interfaces, and verify correct operation.
- Further interoperability tests should be performed in accordance with the specific requirements of the connected end equipment.

11.4.1.4 Management Verification

- Launch the Web EMS on your laptop browser.
- Verify that you can manage the link and that you are able to perform changes to the link configuration (frequency channel, Tx power, system name, time and date, etc.) via the Web EMS.
- Verify that the Web EMS reports the correct parameters when performing the above.
- Verify that there are no active alarms on the link.
- If the management station is located at a remote site (Network Operation Center), verify that the management station can manage the link and receive traps.

11.4.1.5 Loopback Operation

- Perform, IDU-IF loopback, RFU loopback, and remote loopback, and verify that the system operates accordingly.

11.5 1+1 Commissioning Procedure

This section describes the recommended commissioning tests for a FibeAir radio link in 1+1 HSB (Hot Standby) configurations (internal protection).

The purpose of the commissioning tests is to verify correct and proper operation of the product.

Note that in this section:

Primary refers to the RFUs connected to the main path of the directional coupler in a 1+1 HSB configuration.

Secondary refers to the RFUs connected to the secondary path of the directional coupler in a 1+1 HSB configuration.

11.5.1 Commissioning Tests

The following tests should be performed on each installed link.

11.5.1.1 Link Verification

The following steps should be repeated for each of the four RFU combinations (Primary-Primary, Primary-Secondary, Secondary-Primary, Secondary-Secondary).

- “Link” LED and RFU LED on the IDU front panel are green, indicating the radio link is up.
- Received Signal Level (RSL) is up to +/- 2 dB from the expected (calculated) level at both ends of the link.
- Radio Bit Error Rate (BER) is $10E^{-11}$ or higher.
- If working with ATPC, ATPC is operating as expected (RSL = reference level).
- After connecting test equipment or end equipment to the line interfaces, all LEDs on the front panel of the IDU are green.

11.5.1.2 Line Interfaces Test

- 10/100/200/300/400 Mbps, GbE interface - Connect a Packet Analyzer to the GbE interfaces using an Fiber optic splitter, and verify error-free operation (no packet loss) for at least 1 hour. Use an Ethernet loop at the far end.
- 45 Mbps interface - connect PDH test equipment to the DS3 interfaces using splitters, and verify error-free operation for at least 1 hour. Use a physical loop between the splitters at the far end.
- 2 Mbps/1.5 Mbps - connect PDH test equipment to the E1/DS1 interfaces using splitters, and verify error-free operation for at least 1 hour. Use a physical loop between the splitters at the far end.

11.5.1.3 Switching Tests

Define each of the N channels as preferred (one at a time) for errorless switching to the +1 channel. The regular channel supports hitless switching to the +1 channel.

- Perform the following switching tests from one IDU to the other, and verify the system switches automatically.
 - ☐ Power: power off the active IDU
 - ☐ Radio: disconnect the coax cable of the active IDU
 - ☐ Line: disconnect the GbE line input of the active IDU
 - ☐ Management: perform manual switchover using the Web EMS
 - ☐ Management: force a switchover using the Web EMS
- For diversity configurations, verify that each receiver is receiving its own signal, and then mute the active RFU. Verify that the receiver at the far end still receives from the diversity path. Verify that there are no errors in the test equipment.

50/100/200 Mbps, GbE Interface

- Connect a Packet Analyzer to the GbE interfaces using optical splitters. Use an Ethernet loop between the splitters at the far end. Verify no alarms exist.
- Perform the following switching tests from one IDU to the other, and verify the system switches automatically.
 - ☐ Power: power off the active IDU
 - ☐ Radio: disconnect the coax cable of the active IDU
 - ☐ Line: disconnect the GbE line input of the active IDU
 - ☐ Management: perform manual switchover using the Web EMS.
 - ☐ Management: force a switchover using the Web EMS.

45/2/1.5/2 Mbps Interface

- Connect PDH test equipment to the interfaces using splitters. Use a physical loop between the splitters at the far end. Verify no alarms exist.
- Perform the following switching tests from one IDU to the other, and verify the system switches automatically.
 - ☐ Power: power off the active IDU
 - ☐ Radio: disconnect the coax cable of the active IDU
 - ☐ Management: force a switchover using the Web EMS.

11.5.1.4 Interoperability Verification

- Connect the customer end equipment to the line interfaces and verify correct operation.
- Further interoperability tests should be performed in accordance with the specific requirements of the connected end equipment.

11.5.1.5 Management Verification

- Launch the Web EMS on your laptop browser.
- Verify that you can manage the link and that you are able to perform changes to the link configuration (frequency channel, Tx power, system name, time and date, etc.) via the Web EMS.
- Verify that the Web EMS reports the correct parameters when performing the above.
- Verify that there are no active alarms on the link.
- If the management station is located at a remote site (Network Operation Center), verify that the management station can manage the link and receive traps.

11.6 2+0 XPIC Commissioning Procedure

This section describes the recommended commissioning tests for a FibeAir radio link in a 2+0 XPIC Co-Channel-Dual-Polarization configuration.

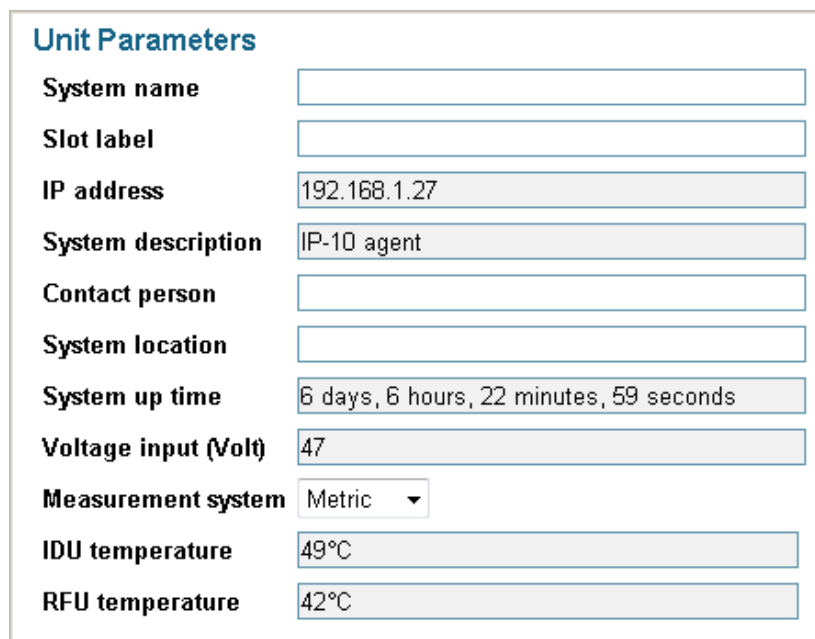
The purpose of the commissioning tests is to verify correct and proper operation of the product.

Important! Since operation of the XPIC system depends on correct installation, make sure the guidelines for XPIC system installation provided in *New IDUs* are delivered with a basic license:

- License: Basic - capacity 10Mbps, no ACM, Smart Pipe (only GbE ports, ports #1 or #2)

Feature and capacity upgrades are implemented through manual entry of a license key based on the IDU's Serial number. Contact Ceragon in order to obtain your license key. Once you receive a new license key, you must load the new license key into the IDU:

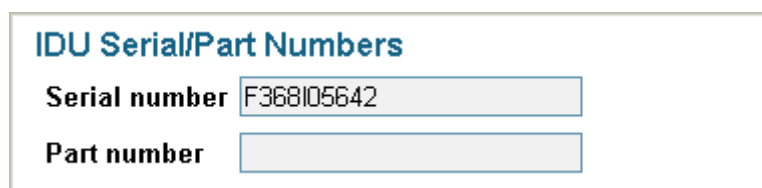
- 1 Select **Configuration > General > Unit Parameters**. The Unit Parameters page opens.



Unit Parameters	
System name	
Slot label	
IP address	192.168.1.27
System description	IP-10 agent
Contact person	
System location	
System up time	6 days, 6 hours, 22 minutes, 59 seconds
Voltage input (Volt)	47
Measurement system	Metric ▼
IDU temperature	49°C
RFU temperature	42°C

- 2 Verify that the three left characters of the license key match the three right characters of the IDU Serial Number, displayed near the bottom of the Unit Parameters page.

Note: You may have to scroll down the Unit Parameters page to display the IDU Serial Number.



IDU Serial/Part Numbers	
Serial number	F368105642
Part number	

- 3 Select **Configuration > General > Licensing**. The Licensing page opens.

Licensing - Slot 1 (Active)

Current License

License type

License code

Demo License

Demo admin

Demo timer

License Features

ACM license	Not allowed
Switch application license	Single pipe
Capacity	10
Network resiliency license	Allowed
TDM-only capacity license	Not allowed
TDM-only capacity value	0
Synchronization Unit License	Allowed
Enhanced Traffic Manger License	Allowed
Asymmetrical scripts license	Allowed
Enhanced compression license	Allowed
Per usage license	Not allowed

- 4 Enter the license key in the **License code** field.
- 5 Click **Apply**.
- 6 Perform a cold reset of the IDU. The new license will take be activated only after a cold reset.
- 7 Select **Configuration > General > Licensing**. The Licensing page opens.
- 8 Verify that the license parameters were updated.

Notes:

If the license key itself is not legal (e.g., a typing mistake or an invalid serial number), a License Violation alarm is raised specific to the problem with the license. In the event of a License Violation alarm, radio port capacity is automatically limited to ~3Mbps, allowing only management channels to the remote end. In order to clear the alarm, you must configure the system to comply with the loaded license, then issue a cold-reset. When the system returns online, it checks the legality of the configuration against the license limits. If no violation is detected, no alarm is raised, and the radio is fully operational.

You may use the Demo license for 60 days for full capacity and a full feature-set.

Configuring XPIC on page 36 are followed correctly.

11.6.1 XPIC Commissioning Tests

11.6.1.1 Individual Link Verification

Before operating in XPIC configuration, each of the links (V and H) should be commissioned individually in order to verify its proper operation.

- 1 Power up only IDU V at both ends and verify its frequency channel and Tx power configuration.
- 2 Verify that the RSL is no more than +/-2 dB from the expected level.
- 3 Run Ethernet packet loss test on the link for at least 15 minutes to ensure error-free operation.
- 4 Power up only IDU H at both ends and verify its frequency channel and Tx power configuration.
- 5 Verify that the RSL is no more than +/-2 dB from the expected level.
- 6 Run Ethernet packet loss test on the link for at least 15 minutes to ensure error-free operation.

11.6.1.2 XPIC Configuration Verification

- 1 Configure the IDU MRMC with an XPIC script.
- 2 Verify that the RSL at all four RFUs is no more than +/-2 dB from the expected level.
- 3 Verify that no alarms exist.
- 4 Run Ethernet packet loss test on each IDU for at least 1 hour to ensure error-free operation.

Note: In a 2+2 configuration, repeat each step above for each of the four coupled RFU combinations.

11.6.1.3 XPIC Recovery Verification

In order to verify XPIC operation, simulate the faults described below.

- 1 Disconnect the IDU-RFU cable for each of the IDUs (one at a time), and verify that the other link is operating.
- 2 Power down each of the IDUs, and verify that the other link is operating.
- 3 Swap the V and H cables and check that the relevant alarm is generated.
- 4 Mute and then un-mute one RFU at a time and verify that the other link is operating.

Note: In a 2+2 configuration, repeat each step above for each of the four coupled RFUs connected to the two standby IDUs.

11.7 FibeAir IP-10 Commissioning Log

The Commissioning Log is an integral part of the commissioning procedure and should be filled in for each installed link.

The Commissioning Log gathers all relevant information regarding the installed link and contains a checklist of all recommended commissioning tests.

Maintaining the Commissioning Log is important for tracking your installations, and to provide essential data for Ceragon Networks.

Upon completing the Commissioning Log, send the log to Ceragon support center at support@ceragon.com.

FIBEAIR IP-10 LINK COMMISSIONING LOG		
1. GENERAL INFORMATION		
Customer:		
Radio model:		
Configuration:		
Radio link code:		
Site 1 name & add:		
Site 2 name & add:		
2. INDOOR UNIT	Site 1	Site 2
IDU model:		
IDU p/n:		
IDU s/n:		
IDU SW:		
Main channel		
FW Mux:		
FW Modem:		
Modem Script:		

FIBEAIR IP-10 LINK COMMISSIONING LOG (continued)		
3. RFU	Site 1	Site 2
RFU model:		
RFU p/n:		
RFU Main s/n:		
SW RFU:		
Tx frequency (MHz):		
Rx frequency (MHz):		
Link ID:		
Tx power (dBm):		
ATPC on/off:		
ATPC ref level:		
RFU Polarization:		
4. ANTENNA	Site 1	Site 2
Antenna model:		
Antenna size:		
Manufacturer:		
Mounting type:		
Mounting losses:		
5. LINK PARAMETERS	Site 1	Site 2
Link distance:		
Rain zone:		
Expected RSL (dBm):		
Expected Diversity RSL (dBm):		
RSL Main (dBm):		
RSL Diversity (dBm):		
Deviation from exp?		
RSL ≤2 dB?		
XPI level >25dB		

FIBEAIR IP-10 LINK COMMISSIONING LOG (continued)		
6. COMMISSIONING TESTS	Site 1	Site 2
Front panel LEDs:	All green	All green
Line loopback:	Pass	Pass
IF loopback:	Pass	Pass
RFU loopback:	Pass	Pass
Fast Ethernet test:	Pass	Pass
Gigabit Ethernet test:	Pass	Pass
Wayside E1 test:	Pass	Pass
Wayside Eth test:	Pass	Pass
Switching test:	Pass	Pass
7. MANAGEMENT CONFIGURATION	Site 1	Site 2
Eth Main IP address:		
Default router:		
In-band enabled?		
Gateway/NE:		
In-band channel 1:		
In-band channel 2:		
Ring IP address:		
Ring IP mask:		
Network ID:		
8. REMARKS/NOTES		

FIBEAIR IP-10 LINK COMMISSIONING LOG (continued)	
9. INSTALLATION INFORMATION	
Installed by:	Name:
	Company:
	Date:
	Signature:
Commissioned by:	Name:
	Company:
	Date:
	Signature:

12. Appendix A: Line Interfaces

This section provides a description of the FibeAir main channel, wayside channel, and order wire channel interfaces.

The interfaces are located on the FibeAir IDU front panel.

The following interface terms should be noted:

- For connectors or signals labeled TX, the signals are sent from FibeAir.
- For connectors or signals labeled RX, the signals are sent to FibeAir.

12.1 Main Channel Interfaces

Main channel interfaces include the following:

Gigabit Ethernet (Optical)



1000Base-SX (Multi Mode)	
Wavelength:	850 nm
Receptacle:	MSA compliant, SFP (Small Form Factor Pluggable Ports)
Connector:	LC
Max Segment Length:	220 m (1351 ft), 500 m (1650 ft)
Cable Type:	For Max Segment = 220 m: 62.5 µm MMF
	For Max Segment= 500 m: 50 µm MMF
1000Base-LX (Single Mode)	
Wavelength:	1350 nm
Receptacle:	MSA compliant, SFP (Small Form Factor Pluggable Ports)
Connector:	LC
Max Segment Length:	550 m (1805 ft), 5000 m (16404 ft)
Cable Type:	For Max Segment = 550 m: 62.5 µm MMF, 50 µm MMF
	For Max Segment = 5000 m: 10 µm SMF

Gigabit Ethernet / Fast Ethernet (Electrical)

100/1000BaseT (Twisted Pair Cable)	
Connector:	RJ-45
Max Segment Length:	Up to 100 m (328 ft) per IEEE802.3
Cable Type:	Compatible with shielded and unshielded twisted pair category 5 cables.
Supports MDI (Medium Dependent Interface)	

Optional 16xE1/DS1

Connector	MDR 69-pin
Used with:	Twisted pair
Interface Type	E1/DS1
Number of ports	16 per unit (optional)
Timing mode:	Retimed
Framing	Unframed (full transparency)
Coding	E1: HDB3
	T1: AMI/B8ZS
Range:	5 m
Line Impedance	120 Ω /100 Ω balanced. Optional module for 75 Ω unbalanced
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, ANSI T1.105, T1.102-1993, T1.231, Bellcore GR-253-core, TR-NWT-000499

12.2 Wayside Channel Interface

The wayside channel is used as an auxiliary audio or data channel.

10/100BaseT (Ethernet)



Connector:	Shielded RJ-45
Used with:	UTP Cat 5
Protocols supported:	Ethernet (10/100BaseT), half or full duplex
Timing mode:	Retimed
Range:	100 m
Impedance:	100 Ω

12.3 Protection Channel Interface

Protection



Connector:	Shielded RJ-45
Used with:	UTP Cat 5
Protocols supported:	Ethernet (10/100BaseT), half or full duplex
Timing mode:	Retimed
Range:	100 m
Impedance:	100 Ω

12.4 Management Channel Interface

Out-of-Band Management



Connector:	Shielded RJ-45
Used with:	UTP Cat 5
Protocols supported:	Ethernet (10/100BaseT), half or full duplex
Timing mode:	Retimed
Range:	100 m
Impedance:	100 Ω

12.5 Order Wire Channel Interface



The Order Wire is used for audio transmission for testing or maintenance purposes.

The specifications for this channel are as follows:

Termination Type:	Headset stereo plug, 2.5 mm
Frequency band (KHz)	0.3-3.4
Input impedance (ohms)	~2000
Output impedance (ohms)	32

12.6 User Channel Interface



The user channel is a CVSD audio channel that delivers 64 Kbps, via an RJ-45 connector.

The interface can be used for one of the following:

- Asynchronous RS-232
- Asynchronous V-11
- Co and Contra Directional

13. Appendix B: Connector Pin-Outs

This appendix provides pin-outs for FibeAir IDU connectors, including the following:

- External Alarms Connector
- Protection/Wayside/Management Connector
- Power Connector
- 16 x E1/DS1 Connector
- Ethernet 10/100/1000 Connector
- Ethernet 10/100 Connector
- User Channel Connector
- Craft Terminal

13.1 External Alarms Connector Pin-Out

The External Alarms connector is a D-type 9-pin connector.

Note: For a 1+1 configuration, the pins are as listed in the table below. For 1+0, pins 7 and 9 are interchanged.

Pin	Signal	I/O	Color	Description
1	EXT_IN5	Input	Black	External input alarm #5
2	EXT_IN4	Input	Brown	External input alarm #4
3	EXT_IN3	Input	Red	External input alarm #3
4	EXT_IN2	Input	Orange	External input alarm #2
5	EXT_IN1	Input	Yellow	External input alarm #1
6	GND	GND	Green	GND
7	RELAY_1_NO	Output	Blue	Relay #1, normally open pin
8	RELAY_1_C	Output	Purple	Relay #1, common pin
9	RELAY_1_NC	Output	Grey	Relay #1, normally closed pin

13.2 Protection/Wayside/Management Connector Pin-Out

The Protection/Wayside/Management connector is an RJ-45, 8-pin, female type connector.

RJ-45 Male Connector Pin	Signal
1	Twisted Pair, Out - Tx
2	
3	Twisted Pair, In - Rx
6	
4	Not Connected
5	
7	Not Connected
8	

13.3 Power Connector Pin-Out

The power connector pin-out is as follows:

Left Pin (#1)	Right Pin (#2)
-48V (return current)	0V

Note that right/left refers to viewing the panel from the front.

13.4 16 x E1/DS1 Connector

The 16 x E1/DS1 connector is a SCSI 68-pin connector.

Pin #	Signal	Label on the Twisted Pair	Type
1	OUT - TIP1	Ch1 Tx	TWISTED PAIR
35	OUT - RING1		
2	OUT - TIP2	Ch2 Tx	TWISTED PAIR
36	OUT - RING2		
3	OUT - TIP3	Ch3 Tx	TWISTED PAIR
37	OUT - RING3		
4	OUT - TIP4	Ch4 Tx	TWISTED PAIR
38	OUT - RING4		
5	OUT - TIP5	Ch5 Tx	TWISTED PAIR
39	OUT - RING5		
6	OUT - TIP6	Ch6 Tx	TWISTED PAIR
40	OUT - RING6		
7	OUT - TIP7	Ch7 Tx	TWISTED PAIR
41	OUT - RING7		
8	OUT - TIP8	Ch8 Tx	TWISTED PAIR
42	OUT - RING8		
9	OUT - TIP9	Ch9 Tx	TWISTED PAIR
43	OUT - RING9		
10	OUT - TIP10	Ch10 Tx	TWISTED PAIR
44	OUT - RING10		
11	OUT - TIP11	Ch11 Tx	TWISTED PAIR
45	OUT - RING11		
12	OUT - TIP12	Ch12 Tx	TWISTED PAIR
46	OUT - RING12		

16 x E1/DS1 Connector (Continued)

Pin #	Signal	Label on the Twisted Pair	Type
13	OUT - TIP13	Ch13 Tx	TWISTED PAIR
47	OUT - RING13		
14	OUT - TIP14	Ch14 Tx	TWISTED PAIR
48	OUT - RING14		
15	OUT - TIP15	Ch15 Tx	TWISTED PAIR
49	OUT - RING15		
16	OUT - TIP16	Ch16 Tx	TWISTED PAIR
50	OUT - RING16		
19	IN - TIP1	Ch1 Rx	TWISTED PAIR
53	IN - RING1		
20	IN - TIP2	Ch2 Rx	TWISTED PAIR
54	IN - RING2		
21	IN - TIP3	Ch3 Rx	TWISTED PAIR
55	IN - RING3		
22	IN - TIP4	Ch4 Rx	TWISTED PAIR
56	IN - RING4		
23	IN - TIP5	Ch5 Rx	TWISTED PAIR
57	IN - RING5		
24	IN - TIP6	Ch6 Rx	TWISTED PAIR
58	IN - RING6		
25	IN - TIP7	Ch7 Rx	TWISTED PAIR
59	IN - RING7		
26	IN - TIP8	Ch8 Rx	TWISTED PAIR
60	IN - RING8		
27	IN - TIP9	Ch9 Rx	TWISTED PAIR
61	IN - RING9		
28	IN - TIP10	Ch10 Rx	TWISTED PAIR
62	IN - RING10		
29	IN - TIP11	Ch11 Rx	TWISTED PAIR
63	IN - RING11		

16 x E1/DS1 Connector (Continued)

Pin #	Signal	Label on the Twisted Pair	Type
30	IN - TIP12	Ch12 Rx	TWISTED PAIR
64	IN - RING12		
31	IN - TIP13	Ch13 Rx	TWISTED PAIR
65	IN - RING13		
32	IN - TIP14	Ch14 Rx	TWISTED PAIR
66	IN - RING14		
33	IN - TIP15	Ch15 Rx	TWISTED PAIR
67	IN - RING15		
34	IN - TIP16	Ch16 Rx	TWISTED PAIR
68	IN - RING16		
17	SHELL	-	SHIELD
18	SHELL	-	SHIELD
51	SHELL	-	SHIELD
52	SHELL	-	SHIELD

13.5 Ethernet 10/100/1000 Connector Pin-Out

The Ethernet 10/100/1000 connector is an RJ-45, 8-pin, female type connector.

RJ-45 Female Connector Pin	Signal
1	Twisted Pair (Tx & Rx)
2	
3	Twisted Pair (Tx & Rx)
6	
4	Twisted Pair (Tx & Rx)
5	
7	Twisted Pair (Tx & Rx)
8	

13.6 Ethernet 10/100 Connector Pin-Out

The Ethernet 10/100 connector is an RJ-45, 8-pin, female type connector.

RJ-45 Female Connector Pin	Signal
1	Twisted Pair, Out - Tx
2	
3	Twisted Pair, In - Rx
6	
4	Not Connected
5	
7	Not Connected
8	

13.7 User Channel Connector Pin-Out

The user channel connector is an RJ-45 connector.

Pin	Asynchronous RS-232	Asynchronous V11	I/O
1	NC	UC_TXD_P	Out
2	NC	UC_TXD_N	Out
3	NC	NC	NC
4	GND Signal Ground	GND Signal Ground	COM
5	UC_RS232_TXD Transmitted Data	NC	Out
6	UC_RS232_RXD Received Data	NC	In
7	NC	UC_RXD_P	In
8	NC	UC_RXD_N	In

13.8 Craft Terminal Connector Pin-Out

The craft terminal connector is a 9-pin RS-232 connector.

Pin #	Acronym	Full Name	Direction	Meaning
3	TxD	Transmit Data	—»	Transmits bytes out of PC
2	RxD	Receive Data	«—	Receives bytes into PC
7	RTS	Request To Send	—»	RTS/CTS flow control
8	CTS	Clear To Send	«—	RTS/CTS flow control
6	DSR	Data Set Ready	«—	I'm ready to communicate
4	DTR	Data Terminal Ready	—»	I'm ready to communicate
1	DCD	Data Carrier Detect	«—	Modem connected to another
9	RI	Ring Indicator	«—	Telephone line ringing
5	SG	Signal Ground	-	-

14. Appendix C: Fan Tray Replacement

If it is necessary to replace the fan tray in the IDU, replace it as follows:

- 1 Remove the current fan tray by releasing the safety screw and removing the tray.
- 2 Insert the new fan tray entirely in its place and tighten the safety screw.

Installation Guide



FibeAir[®] IP-20G FibeAir[®] IP-20G Assured

Doc ID: DOC-00041192 Rev E.08

June 2018

© Copyright 2018 by Ceragon Networks Ltd. All rights reserved.

Notice

This document contains information that is proprietary to Ceragon Networks Ltd. No part of this publication may be reproduced, modified, or distributed without prior written authorization of Ceragon Networks Ltd. This document is provided as is, without warranty of any kind.

Trademarks

Ceragon Networks®, FibeAir® and CeraView® are trademarks of Ceragon Networks Ltd., registered in the United States and other countries.

Ceragon® is a trademark of Ceragon Networks Ltd., registered in various countries.

CeraMap™, PolyView™, EncryptAir™, ConfigAir™, CeraMon™, EtherAir™, CeraBuild™, CeraWeb™, and QuickAir™, are trademarks of Ceragon Networks Ltd.

Other names mentioned in this publication are owned by their respective holders.

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

1. FibeAir IP-20G Hardware Overview.....	11
1.1 Ethernet Traffic Interfaces	12
1.2 Ethernet Management Interfaces.....	13
1.2.1 Management Interface Cable Options.....	13
1.3 TDM Interfaces (E1/DS1 1x16) (Optional).....	13
1.4 Radio Interfaces	14
1.5 Power Interfaces.....	14
1.6 Synchronization Interface	14
1.7 Terminal Interface.....	14
1.8 External Alarms	15
1.9 FibeAir IP-20 Assured Platform	16
2. Preparing for Installation.....	17
2.1 Transportation/Storage	17
2.2 Inspection	17
2.3 Unpacking Equipment at the Site	18
3. Installing the IP-20G IDU	19
3.1 Kits required to perform the installation	19
3.2 Tools.....	19
3.3 Installing the IP-20G IDU in the Rack (19")	20
3.4 Grounding the IP-20G	21
3.5 Replacing an IP-20G IDU or SM-Card	22
4. Connecting the Power Cable.....	24
4.1 Power Supply Notes.....	26
5. Cabling Requirements for Unit Redundancy.....	27
5.1 Cabling for Ethernet Interfaces	27
5.2 Cabling for E1/DS1 Interfaces	27
5.3 Cabling for T3 Synchronization	27
5.4 Inter-IDU Protection Connectivity and Management	28
6. Performing Initial Configuration	29
6.1 Establishing a Connection	29
6.1.1 Connecting to the Unit with a Serial Connection.....	29
6.1.2 Connecting to the Unit with a LAN Connection	30
6.2 Logging On	31
6.3 Changing Your Password.....	32



- 6.4 Configuration33
- 6.5 Applying a Pre-Defined Configuration File34
- 7. Specifications..... 36**
 - 7.1 Environmental Specifications for IDU36
 - 7.2 Environmental Specifications for RFU.....36
 - 7.3 Mechanical Specifications.....37
 - 7.4 Power Consumption Specifications38
- 8. Acceptance & Commissioning Procedures..... 39**
 - 8.1 Site Acceptance Procedure40
 - 8.2 Site Acceptance Checklist Notes44
 - 8.3 Radio Link Commissioning Procedure46
 - 8.3.1 Scope.....46
 - 8.3.2 Commissioning Test46
 - 8.4 IP-20 Commissioning Log47

List of Figures

Figure 1: IP-20G Front Panel and Interfaces	11
Figure 2: Management Interface Pin Connections	13
Figure 3: IDU (Full Configuration)	19
Figure 4: Power Supply Grounding	24
Figure 5: Correct Wiring of Power Connector	25
Figure 6: Connecting the Power Cable	25
Figure 7: IP-20G with Unit Redundancy – Protection and Management Connection	28
Figure 8: Terminal Interface	29
Figure 9: Management Interface	30
Figure 10: Login Window	31
Figure 11: Change User Password Page	32
Figure 12: Quick Configuration – From File Page	34
Figure 13: Quick Configuration – From File Page – Configuration File Loaded	35



List of Tables

Table 1: 2 x FE Splitter Cable Marketing Model13

Table 2: Y-Cable for Electrical Splitter Mode FE Traffic Interface Protection27

Table 3: Y-Cable for E1/DS1 Protection.....27

Table 4: Splitter Cable for Protection and Management28

Table 5: IDU Mechanical Specifications37

Table 6: RFU-C Mechanical Specifications.....37

Safety Precautions & Declared Material

General Equipment Precautions



Use of controls, adjustments, or performing procedures other than those specified herein, may result in hazardous radiation exposure.



When working with a FibeAir IDU, note the following risk of electric shock and energy hazard: Disconnecting one power supply disconnects only one power supply module. To isolate the unit completely, disconnect all power supplies.



Machine noise information order - 3. GPSGV, the highest sound pressure level amounts to 70 dB (A) or less, in accordance with ISO EN 7779.

Static electricity may cause body harm, as well as harm to electronic components inside the device.

To prevent damage, before touching components inside the device, all electrostatic must be discharged from both personnel and tools.

High Frequency Electromagnetic Fields!

Exposure to strong high frequency electromagnetic fields may cause thermal damage to personnel. The eye (cornea and lens) is easily exposed.

Any unnecessary exposure is undesirable and should be avoided.



In radio-relay communication installations, ordinary setup for normal operation, the general RF radiation level will be well below the safety limit.

In the antennas and directly in front of them the RF intensity normally will exceed the danger level, within limited portions of space.

Dangerous radiation may be found in the neighborhood of open waveguide flanges or horns where the power is radiated into space.

To avoid dangerous radiation the following precautions must be taken:

- **During work within and close to the front of the antenna; make sure that transmitters will remain turned off.**
- **Before opening coaxial - or waveguide connectors carrying RF power, turn off transmitters.**
- **Consider any incidentally open RF connector as carrying power, until otherwise proved. Do not look into coaxial connectors at closer than reading distance (1 foot). Do not look into an open waveguide unless you are absolutely sure that the power is turned off.**

ESD



This equipment contains components which are sensitive to "ESD" (Electro Static Discharge). Therefore, ESD protection measures must be observed when touching the IDU.

Anyone responsible for the installation or maintenance of the FibeAir IDU must use an ESD Wrist Strap.

Additional precautions include personnel grounding, grounding of work bench, grounding of tools and instruments as well as transport and storage in special antistatic bags and boxes.



Laser

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

The optical interface must only be serviced by qualified personnel, who are aware of the hazards involved to repair laser products.

When handling laser products the following precautions must be taken:

- **Never look directly into an open connector or optical cable.**
- **Before disconnecting an optical cable from the optical transmitter, the power should be switched off. If this is not possible, the cable must be disconnected from the transmitter before it is disconnected from the receiver.**
- **When the cable is reconnected it must be connected to the receiver before it is connected to the transmitter.**



Grounding: This equipment is designed to permit connection between the earthed conductor of the DC supply circuit and the earthing conductor at the equipment.

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Restricted Access Area: DC powered equipment should only be installed in a Restricted Access Area.

Installation Codes: The equipment must be installed according to country national electrical codes. For North America, equipment must be installed in accordance to the US National Electrical Code, Articles 110-16, 110-17 and 110-18, and the Canadian Electrical Code, Section 12.

Overcurrent Protection: A readily accessible listed branch circuit overcurrent protective device, rated 15 A, must be incorporated in the building wiring.

Grounded Supply System: The equipment shall be connected to a properly grounded supply system. All equipment in the immediate vicinity shall be grounded the same way, and shall not be grounded elsewhere.

Local Supply System: The DC supply system is to be local, i.e. within the same premises as the equipment.

Disconnect Device: A disconnect device is not allowed in the grounded circuit between the DC supply source and the frame/grounded circuit connection.

RoHS Compliance Declaration

Electronic Information Products Declaration of Hazardous/Toxic Substances

Component	Hazardous Substance					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr VI)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB/Circuit Modules	Comply	Comply	Comply	Comply	Comply	Comply
Mechanical Parts	Comply	Comply	Comply	Comply	Comply	Comply
Cables	Comply	Comply	Comply	Comply	Comply	Comply

About This Guide

This guide describes the FibeAir IP-20G installation procedures. This guide also provides initial configuration instructions for once the hardware installation is complete.

What You Should Know

An IP-20G system consists of an IP-20G indoor unit (IDU) and one or more radio frequency units (RFUs). This manual provides instructions for the installation of the IP-20G IDU only. Some features described in this manual may not be available in the current release. Consult the Release Notes for the functionality supported in the specific release you are using.

Target Audience

This guide is intended for use by personnel of all levels certified by Ceragon personnel such as system engineers, technicians, or supervisors.

Related Documents

- IP-20G Technical Description
- User Guide for FibeAir IP-20G and IP-20GX
- IP-20 Series MIB Reference
- FibeAir RFU-C Installation Guide, DOC-00017708
- FibeAir RFU-A Installation Guide, DOC- 00029790
- FibeAir RFU-HP Installation Guide, DOC-00015514
- Ceragon Activation Key Management System, DOC-00019183

1. FibeAir IP-20G Hardware Overview

FibeAir IP-20G is a compact unit that fits in a single rack unit, with a passive cooling system that eliminates the need for fans. An IP-20G system consists of an IP-20G indoor unit (IDU) and one or two radio frequency units (RFUs). A coaxial cable connects the IDU to each RFU, transmits traffic and management data between the IDU and the RFU, and provides DC -48V power to the RFU.

An IP-20G IDU contains six Ethernet interfaces, one or two radio interfaces depending on the hardware configuration, and optionally a 16 x E1/DS1 interface.

The IDU also includes two FE management interfaces, a DB9 dry contact external alarms interface, an RJ-45 synchronization interface, and an RJ-45 terminal console interface for connection to a local craft terminal.

IP-20G receives an external supply of -48V, with an optional second power interface for power redundancy.

The following hardware assembly options are available for the IP-20G IDU:

- One or two radio interfaces
- One or two power interfaces
- With or without 16 x E1/DS1 interfaces

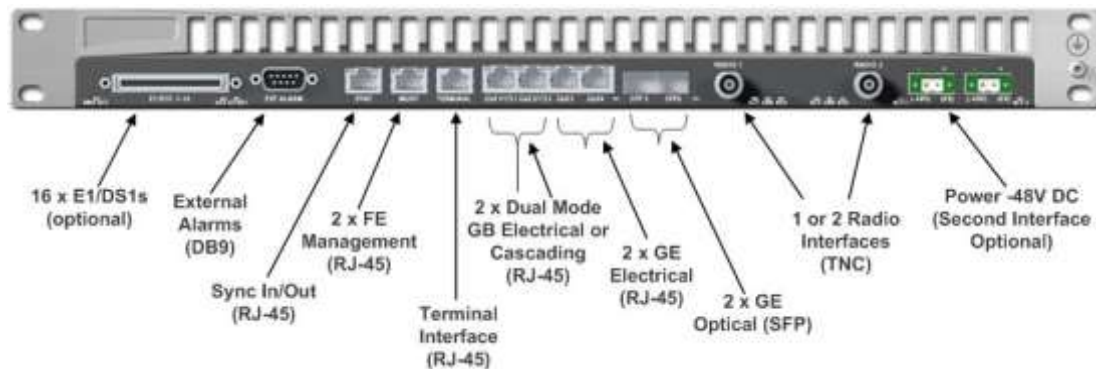


Figure 1: IP-20G Front Panel and Interfaces

1.1 Ethernet Traffic Interfaces

The front panel of the FibeAir IP-20G contains four electrical and two optical GE Ethernet traffic interfaces:

- 2 x GE dual mode electrical or cascading interfaces (RJ-45) – GbE1/CS1, GbE2/CS2
- 2 x GE electrical interfaces (RJ-45) –GbE3, GbE4
- 2 x GE optical interfaces (SFP) – SFP5, SFP6

Important Note: When using electrical ports GbE 1 through GbE 4 to connect between the IP-20G IDU and an outdoor unit such as IP-20C or IP-20S, in areas in which severe lightning conditions are likely to occur, it is required to use lightning protection.

1.2 Ethernet Management Interfaces

FibeAir IP-10G contains two FE management interfaces, which connect to a single RJ-45 physical connector on the front panel (MGMT).

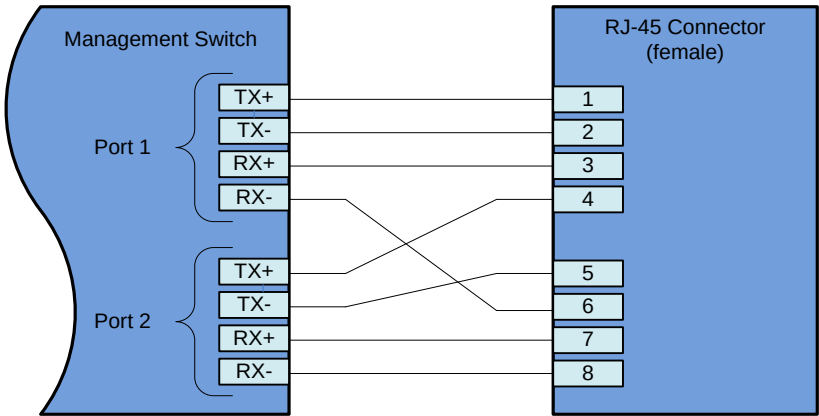


Figure 2: Management Interface Pin Connections

1.2.1 Management Interface Cable Options

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.

Table 1: 2 x FE Splitter Cable Marketing Model

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

1.3 TDM Interfaces (E1/DS1 1x16) (Optional)

Optionally, FibeAir IP-20G can be ordered with an MDR69 connector in which 16 E1/DS1 interfaces are available (ports 1 through 16).

1.4 Radio Interfaces

FibeAir IP-20G includes one or two radio interfaces, depending on the hardware assembly option that was selected. Each radio interface uses a TNC connector type. Each radio interface is connected to an RFU via coaxial cable. This connection is used for traffic between the RFU and the IDU. It is also used to provide -48V DC power from the IDU to the RFU, as well as for management and configuration of the RFU.

The radio interfaces are labeled Radio 1 and, if there is a second radio interface, Radio 2.

1.5 Power Interfaces

FibeAir IP-20G receives an external supply of -48V current via one or two power interfaces (the second power interface is optional for power redundancy). The IP-20G monitors the power supply for under-voltage and includes reverse polarity protection, so that if the positive (+) and negative (-) inputs are mixed up, the system remains shutdown.

The allowed power input range for the IP-20G is -40V to -60V. An under voltage alarm is triggered if the power goes below the allowed range, and an over voltage alarm is triggered if the power goes above the allowed range.

1.6 Synchronization Interface

FibeAir IP-20G includes an RJ-45 synchronization interface for T3 clock input and T4 clock output. The interface is labeled SYNC.

1.7 Terminal Interface

FibeAir IP-20G 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.

1.8 External Alarms

IP-20G 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.

1.9 FibeAir IP-20 Assured Platform

Ceragon's FibeAir® IP-20 Assured platform enhances network reliability and security, ensuring that mission-critical networks maintain availability, and protecting the confidentiality and integrity of their users' data.

The FibeAir IP-20 Assured platform is compliant with FIPS 140-2, including:

- Compliance with FIPS 140-2 specifications for cryptography module.
- FIPS 140-2 Level 2 physical security.
- AES-256 encryption (FIPS 197) over radio links.

The FibeAir IP-20 Assured platform also provides:

- Secured communication and protocols for management interface.
- Centralized user authentication management via RADIUS.
- Advanced identity management and password policy enforcement.
- Security events log.
- Secure product architecture and development.

The following products are included in the FibeAir IP-20 Assured platform:

- FibeAir IP-20G Assured
- FibeAir IP-20GX Assured
- FibeAir IP-20A Assured
- FibeAir IP-20N Assured
- FibeAir IP-20LH Assured
- FibeAir IP-20C Assured
- FibeAir IP-20S Assured

Note:	FibeAir IP-20 Assured is supported with certain versions of CeraOS. To determine whether a specific CeraOS version supports FibeAir IP-20 Assured, check the Release Notes for the CeraOS version.
--------------	--

2. Preparing for Installation

This section provides instructions for transporting, inspecting, and unpacking the equipment for an IP-20G system prior to installation.

2.1 Transportation/Storage

The equipment cases are prepared for shipment by air, truck, railway and sea, suitable for handling by forklift trucks and slings. The cargo must be kept dry during transport and storage.

For sea-transport, deck-side shipment is not permitted. Carrier-owned cargo containers should be used.

It is recommended that the equipment is transported to the installation site in its original packing cases.

If any intermediate storing is required, all cases must be stored under dry and cool conditions and out of direct sunlight.

2.2 Inspection

Check the packing lists and ensure that correct parts numbers quantities of goods have arrived.

Inspect for any damage on the cases and equipment. Report any damage or discrepancy to a Ceragon representative, by e-mail or fax.

2.3 Unpacking Equipment at the Site

The equipment is packed in sealed plastic bags and moisture absorbing bags are inserted. Any separate sensitive product, i.e. printed boards, are packed in anti-static handling bags. The equipment is further packed in special designed cases.

Marking is done according to standard practice unless otherwise specified by customers.

- Customers address
- Contract No
- Site name (if known)
- Case No

Dimensions and weight of each case are specified in the packing specification issued for the respective shipment.



Caution!

It is essential that whenever unpacking or disassembling the equipment and handling printed circuit boards, special precautions should be taken to avoid ESD (Electrostatic Static Discharge). Generally, units with static discharge protection should not be unpacked until the installation takes place.

Ensure you are properly grounded at a controlled ESD point before and during unpacking and handling of any sensitive component.

To avoid malfunctioning or personnel injuries, equipment or accessories/kits/plugin unit installation, requires qualified and trained personnel.

Changes or modifications not expressly approved by Ceragon Networks could void the user's authority to operate the equipment

Where special cables, shields, adapters and grounding kits are supplied or described in this manual, these items must be used, to comply with the relevant regulations.

3. Installing the IP-20G IDU

This section provides instructions for installing a FibeAir IP-20G IDU.

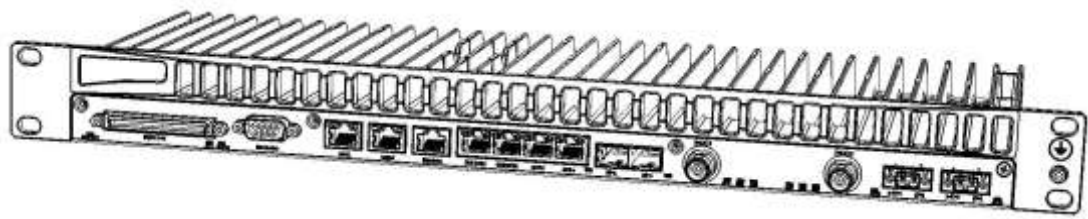


Figure 3: IDU (Full Configuration)

3.1 Kits required to perform the installation

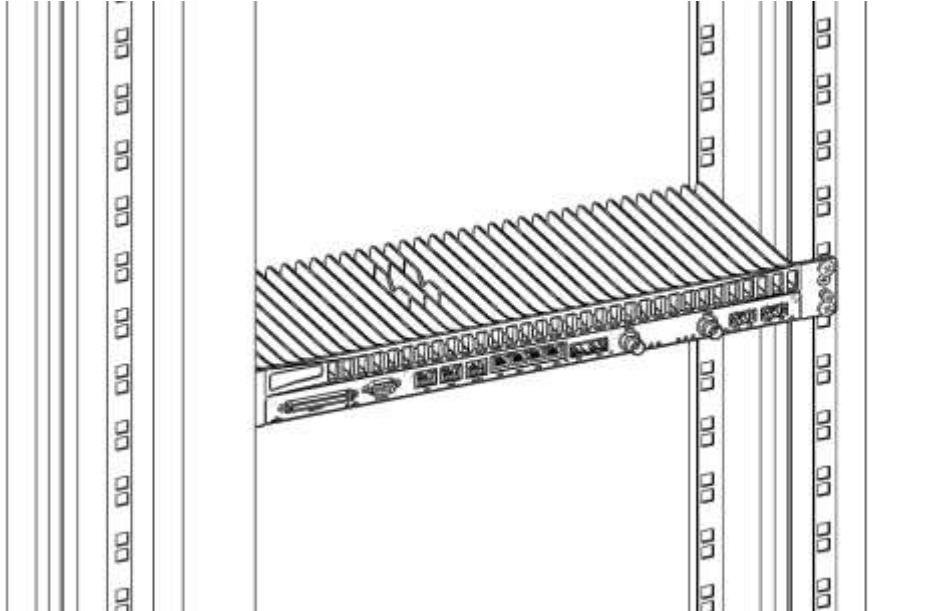
Description	Quantity
IP-20G chassis	1
19" rack / sub-rack	1
SM-Card Cover	1

3.2 Tools

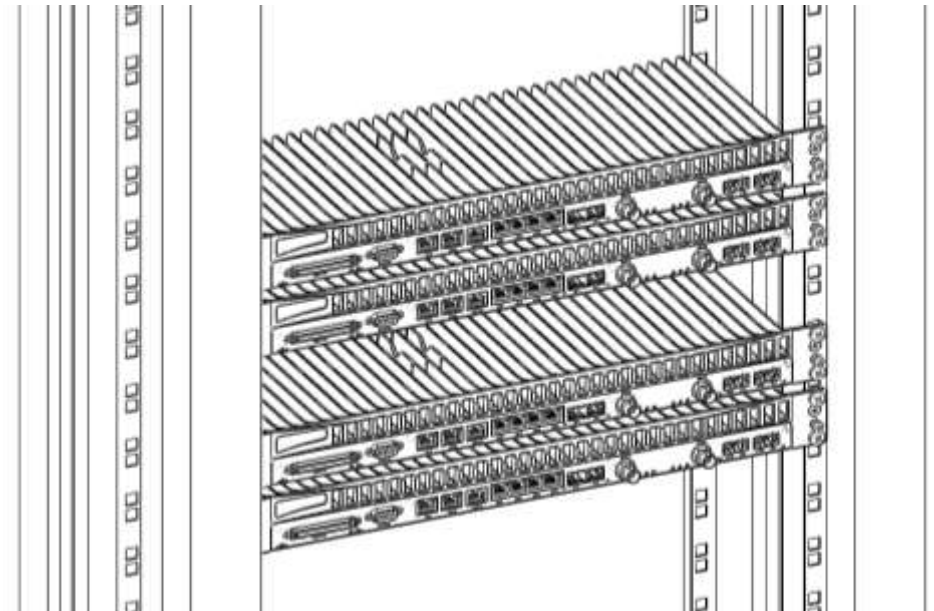
- Philips screwdriver
- Flat screwdriver

3.3 Installing the IP-20G IDU in the Rack (19")

- 1 Insert and hold the IP-20G IDU in the rack, as shown in the following figures. Use four screws (not supplied with the installation kit) to fasten the IDU to the rack.



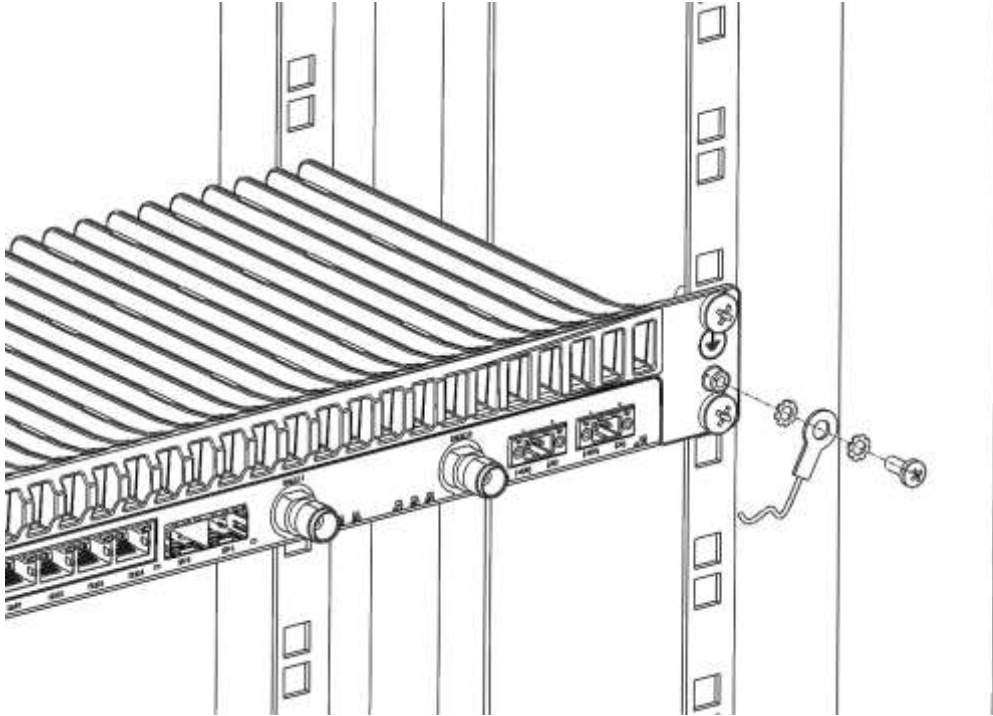
If you are installing multiple IP-20G units in a single rack, make sure to leave a space of 1RU after every two IP-20G units, as shown in the figure below. This restriction also applies to IP-20G units installed in proximity with third party units.



3.4 Grounding the IP-20G

Connect a grounding wire first to the single-point stud shown in the figure below, and then to the rack, using a single screw and two washers. Verify that the grounding resistance is 0-2 ohms.

Note: The grounding wire must be 16 AWG or thicker.



3.5 Replacing an IP-20G IDU or SM-Card

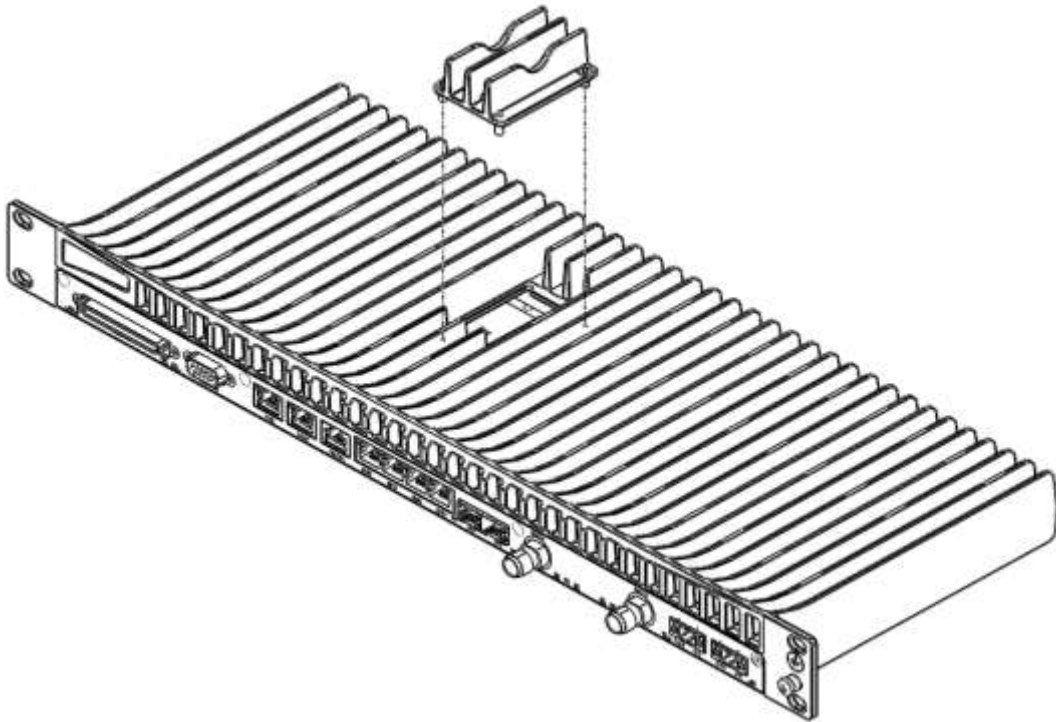
If you should need to replace the IP-20G IDU, you must first remove the SM-Card Cover so that you can insert it into the new IDU.

The SM-Card holds the configuration and software for the IDU. The SM-Card is embedded in the SM-Card Cover, so re-using the existing SM-Card Cover is necessary to ensure that the unit's software and configuration is maintained.

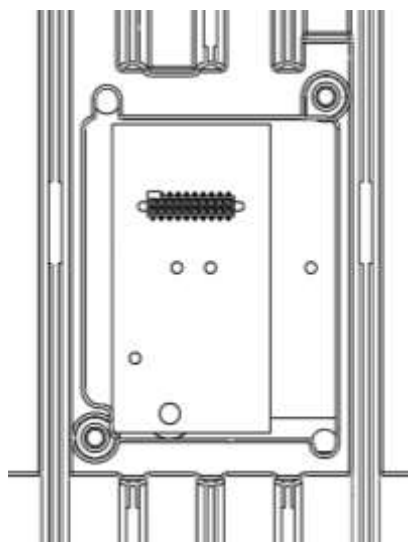
In some cases, you may need to replace the SM-Card itself in order to upgrade the unit's configuration.

To remove the SM-Card Cover:

- 1 Switch the unit power off.
- 2 Loosen the screws of the SM-Card Cover and remove it from the IDU.



- 3 In the new IDU or, if you are upgrading the SM-Card, the old IDU, make sure that there is no foreign matter blocking the sockets in the opening where the SM-Card is installed.



- 4 Gently place the SM-Card Cover in its place and tighten the screws, using a Phillips screwdriver.

4. Connecting the Power Cable

Important!

Before connecting the power supply to the IP-20G unit, you must verify that the positive pole in the external power supply is grounded! Power supply grounding should be in according with the following figure:

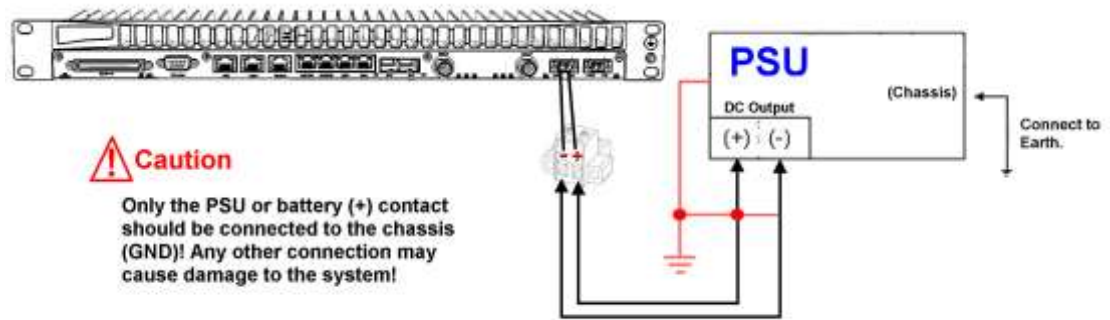


Figure 4: Power Supply Grounding

FibeAir IP-20G utilizes a single-feed power interface. Optionally, IP-20G can be ordered with a second power interface for power redundancy. A power cable connector is included with the IP-20G unit.

The following power cables are available for use with an IP-20G unit:

Ceragon Part Number	Marketing Model	Marketing Description
WA-0567-0	CBL-PWR-OE-OE-16A-2.2m	Power cable Open-end/Open-end, 16A, 2.2m
WA-0568-0	CBL-PWR-OE-OE-16A-5m	Power cable Open-end/Open-end, 16A, 5m

To connect a power cable to the IP-20G:

- 1 Expose the wires of the power cable.
- 2 Loosen the top two screws on the connector.
- 3 Verify that the wiring is according to the correct polarity.

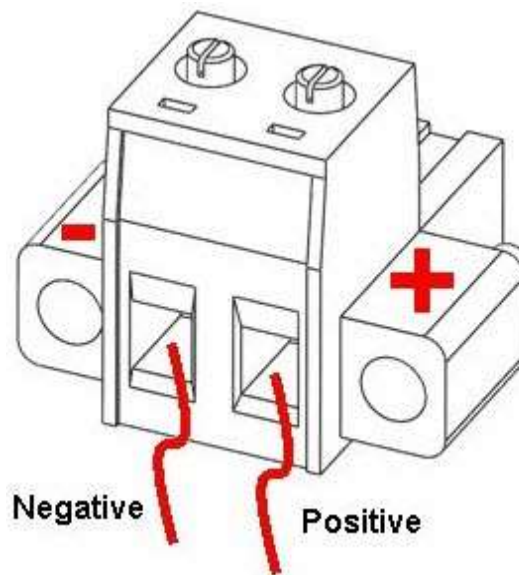


Figure 5: Correct Wiring of Power Connector

- 4 Insert the wires into the connector.
- 5 Secure the wires in the connector with the screws.
- 6 Plug the connector into the IP-20G power interface and tighten the two screws on the sides of the connector to secure the connector.

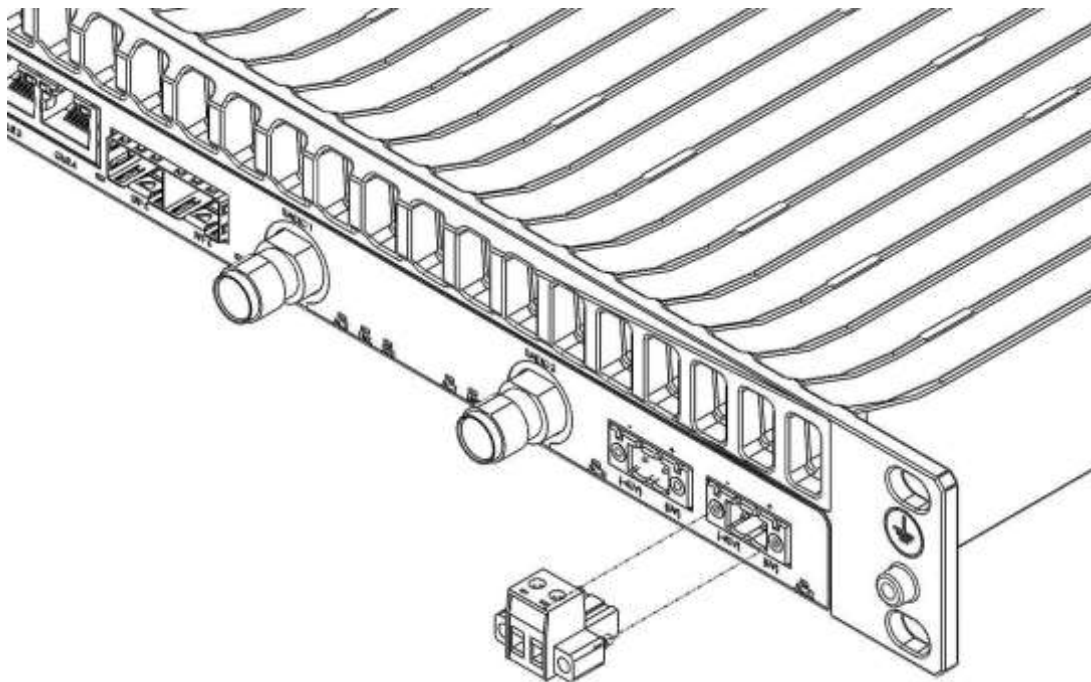


Figure 6: Connecting the Power Cable

4.1 Power Supply Notes

When selecting a power source, the following must be considered:

- Voltage range: -40 VDC to -60 VDC.
- Recommended: Availability of a UPS (Uninterrupted Power Source), battery backup, and emergency power generator.
- The power source must be grounded.
- The unit has more than one supply connection - Remove all power from the unit for servicing.

Important!

Make sure to use a circuit breaker to protect the circuit from damage by short or overload. In a building installation, the circuit breaker shall be readily accessible and incorporated external to the equipment. The maximum rating of the overcurrent protection shall be 10 Amp, while the maximum current rating is 5 Amp.

5. Cabling Requirements for Unit Redundancy

5.1 Cabling for Ethernet Interfaces

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

Table 2: 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,

No special cabling is required for other Ethernet protection modes.

5.2 Cabling for E1/DS1 Interfaces

If the E1/DS1 interfaces are being used, a Y-cable is used to connect the active and standby E1/DS1 interfaces. The following table shows the Part Number and Marketing Model of the Y-cable required for E1/DS1 protection.

Table 3: Y-Cable for E1/DS1 Protection

Part Number	Marketing Model	Description
wa-0391-0	IP-10 16E1 protection Y-cable, MDR68	CABLE,2xSCSI68 LEFT ANGL SCSI68,0.6M,120 OHM,ADAP

5.3 Cabling for T3 Synchronization

If T3 synchronization input is being used, a Y cable is used to connect to the active and standby Sync interfaces.

5.4 Inter-IDU Protection Connectivity and Management

IP-20G 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-20G units, to ensure that management is not lost in the event of switchover. A special cable is required to enable this connectivity.

Table 4: 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-20G 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.

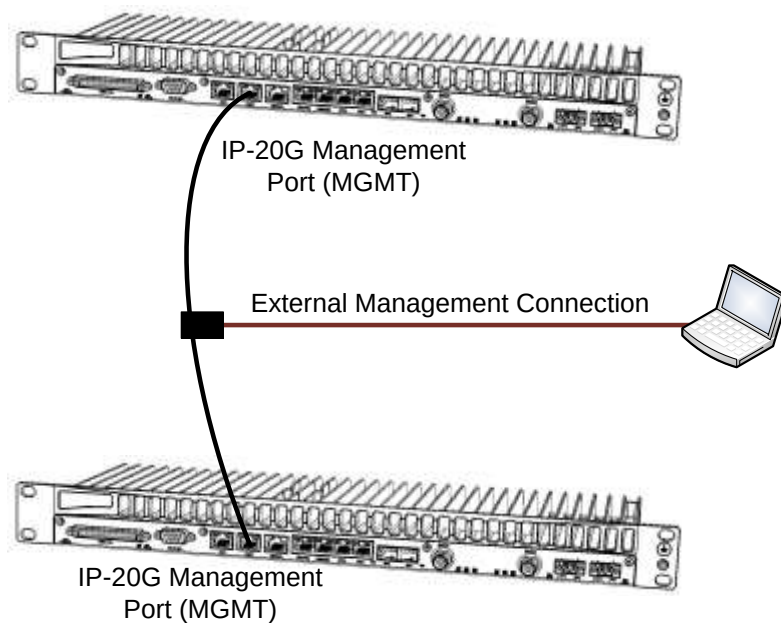


Figure 7: IP-20G with Unit Redundancy – Protection and Management Connection

The local management connection uses IP-20G management interface 1. The inter-unit protection connection uses IP-20G management interface 2.

6. Performing Initial Configuration

This section describes how to establish a management connection with the IP-20G unit and lists the configuration steps that should be performed in order to enable basic radio connectivity. For detailed configuration instructions, refer to the User Guide for Chassis-Based Systems: FibeAir IP-20N, IP-20A, IP-20LH, and Evolution IP-20LH.

6.1 Establishing a Connection

You can connect to the IP-20G unit using a TP cable with a LAN connection or using a Serial RS-232 cable.

6.1.1 Connecting to the Unit with a Serial Connection

- 1 Connect an RS-232 cable with an RJ-45 interface from your laptop or PC to the Terminal Interface on the IP-20G front panel.

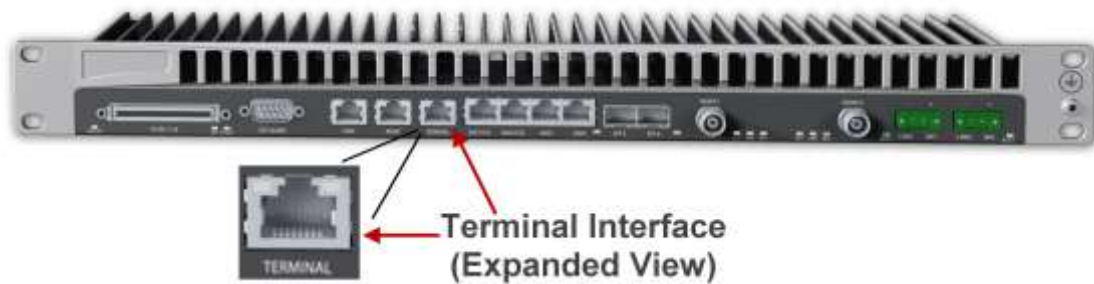


Figure 8: Terminal Interface

- 2 Configure the following settings for the COM port you are using on your PC or laptop:
 - Bits per Second – 115,200
 - Data Bits – 8
 - Parity – None
 - Stop Bits – 1
 - Flow Control - None

6.1.2 Connecting to the Unit with a LAN Connection

FibeAir IP-20G contains two FE management interfaces, which connect to a single RJ-45 physical connector on the front panel (MGMT). For details on which type of cable to use to utilize either one or both management interfaces, refer to *Management Interface Cable Options* on page 13.

Connect the cable to Management interface (MGMT) on the IP-20G front panel, and to the LAN port on the PC.



Figure 9: Management Interface

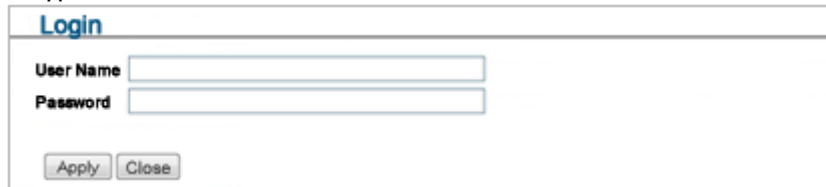
To establish a connection between the PC and the IP-20G unit, it is necessary to have an IP address on the PC within the same subnet as the unit. The default IP address of the IP-20G unit is 192.168.1.1. Set the PC address to e.g. 192.168.1.10 and subnet mask to 255.255.255.0. Note the initial settings before changing.

Note: The chassis IP address, as well as password, should be changed before the system is set in operation. For more information on these procedures, see User Guide for Chassis-Based Systems: FibeAir IP-20N, IP-20A, IP-20LH, and Evolution IP-20LH.

- 1 Select Control Panel> All Control Panel Items >Network and Sharing Center.
- 2 Click Change adapter settings.
- 3 Select Local Area Connection> Properties> Internet Protocol Version 4 (TCP/IP).
 - IP address: 192.168.1.10
 - Subnet mask 255.255.255.0
 - No default gateway
- 4 Press **OK** to apply the settings.

6.2 Logging On

- 1 Open an Internet browser (Internet Explorer or Mozilla Firefox).
- 2 Type in the default IP address "**192.168.1.1**" in the Address Bar.



A screenshot of a web browser's login window. The window has a title bar with the word "Login" in blue. Inside the window, there are two text input fields. The first is labeled "User Name" and the second is labeled "Password". Below these fields are two buttons: "Apply" and "Close".

Figure 10: Login Window

- 3 Enter the following values:
 - User Name: admin
 - Password: admin
- 4 Click **Apply**.

6.3 Changing Your Password

It is recommended to change your default Admin password as soon as you have logged into the system.

To change your password:

- 1 Select **Platform > Security > Access Control > Change Password**. The Change User Password page opens.

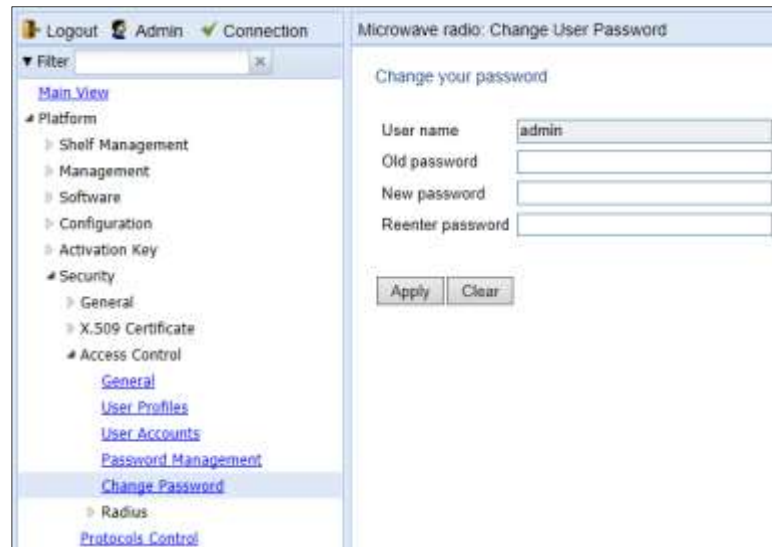


Figure 11: Change User Password Page

- 2 In the **Old password** field, enter the current password. For example, upon initial login, enter the default password (**admin**).
- 3 In the **New password** field, enter a new password. If **Enforce Password Strength** is activated, the password must meet the following criteria:
 - Password length must be at least eight characters.
 - Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters. For purposes of meeting this requirement, upper case letters at the beginning of the password and digits at the end of the password are not counted.
 - The last five passwords you used cannot be reused.
- 4 Click **Apply**.

In addition to the Admin password, there is an additional password protected user account, “root user”, which is configured in the system. The root user password and instructions for changing this password are available from Ceragon Customer Support. It is strongly recommended to change this password.

6.4 Configuration

Before connection over the radio hop is established, it is of high importance that the elements are assigned a dedicated IP address, according to an IP plan for the total network.

Note: If connection over the hop is established with identical IP addresses, an IP address conflict will occur, and remote connection to the element on the other side of the hop may be lost.

By default all elements have the same IP settings:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Note: After the new IP address is set, the contact with the element will be lost. In order to reconnect, the PC must have an IP address within the same subnet as the element.

In addition to setting the IP addresses, the following configuration steps should be performed in order to establish basic connectivity. For a detailed description of these procedures, refer to the User Guide for Chassis-Based Systems: FibeAir IP-20N, IP-20A, IP-20LH, and Evolution IP-20LH.

- Enable the Radio Interfaces
- Set the Radio Frequencies
- Configure the License
- Unmute the Radio

6.5 Applying a Pre-Defined Configuration File

IP-20 units can be configured from the Web EMS in a single step by applying a pre-defined configuration file. A pre-defined configuration file can be prepared for multiple IP-20 units, with the relevant configuration details specified and differentiated per-unit.

The pre-defined configuration file is generated by Ceragon Global Services and provided as a service.

The pre-defined configuration file must be compatible with the CeraOS version the IP-20 device is running. Configuration files created for CeraOS 9.2 cannot be used with CeraOS 9.2.5 or higher. Configuration files must also be compatible with the type of IP-20 device. For example, a configuration file created for IP-20GX cannot be applied to an IP-20G device.

For further information on the creation of pre-defined configurations, consult your Ceragon representative.

To apply a pre-defined configuration file:

- 1 Select **Quick Configuration > From File**. The Quick Configuration – From File page opens.

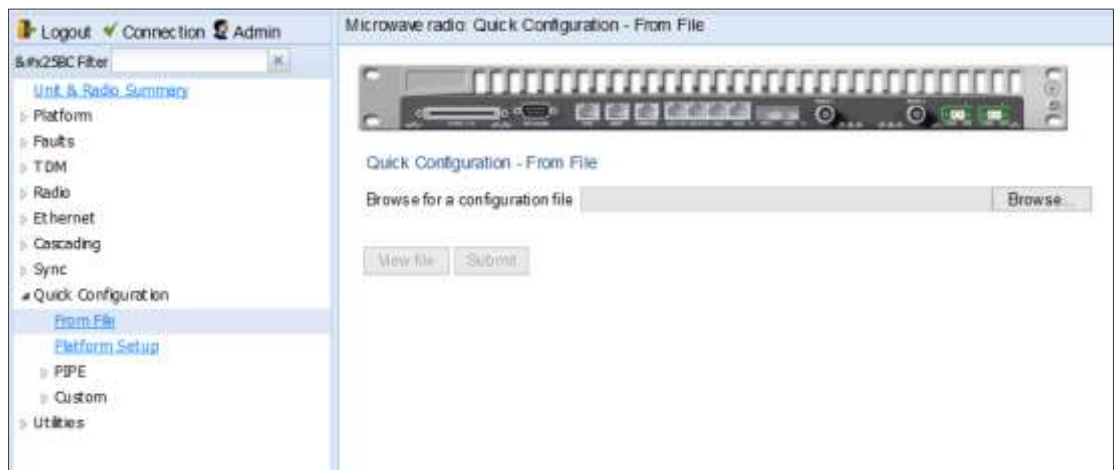


Figure 12: Quick Configuration – From File Page

- 2 Click **Browse**, and select the configuration file for your unit.



Figure 13: Quick Configuration – From File Page – Configuration File Loaded

- 3 In the **Device List** field, select the IP-20 unit you are configuring.
- 4 Optionally, click **View file** to display the configuration file (read-only).
- 5 To initiate the configuration, click **Submit**. Progress is updated in the Quick Configuration – From File page.

When the configuration is complete, the unit reboots.

If the configuration file includes changing from ETSI to ANSI mode, the unit reboots at that point in the configuration. After the reboot, you must return to the Quick Configuration – From File page and re-initiate the configuration.

Note: If the pre-defined configuration file included a new IP address for the unit, make sure to configure an IP address on the PC or laptop you are using to perform the configuration within the same subnet as the IP-20 unit's new IP address.

7. Specifications

7.1 Environmental Specifications for IDU

- Operating: ETSI EN 300 019-1-3 Class 3.2
- Temperature:
 - **-5°C (23°F) to 55°C (131°F)** – Temperature range for continuous operating temperature with high reliability.
 - **-25°C (-13°F) to 65°C (149°F)** – Temperature range for exceptional temperatures, tested successfully, with limited margins.

Note: Cold startup requires at least **-5°C (23°F)**

- Humidity: 5%RH to 95%RH

7.2 Environmental Specifications for RFU

- Operating: ETSI EN 300 019-1-4 Class 4.1
- Temperature:
 - **-33°C (-27°F) to +55°C (131°F)** – Temperature range for continuous operating temperature with high reliability:
 - **-45°C (-49°F) to +60°C (140°F)** – Temperature range for exceptional temperatures; tested successfully, with limited margins:
- Humidity: 5%RH to 100%RH

7.3 Mechanical Specifications

Table 5: IDU Mechanical Specifications

IDU Dimensions	Height: 44 mm/1.73" (1RU) Width: 426 mm/16.77" Depth: 180 mm/7.08" Weight: 2.5 kg/5.5 lbs.
IDU-RFU Connection	Coaxial cable RG-223 (300 ft), Belden 9914/RG-8 (1000 ft) or equivalent, TNC connectors to the IDU, N-type connectors (male) to the RFU.

Table 6: RFU-C Mechanical Specifications

RFU-C Dimensions	Height: 200 mm/7.87" Width: 200 mm/7.87" Depth: 85 mm/3.35" Weight: 4kg/9 lbs.
RFU-C Standard Mounting OD Pole	50 mm-120 mm/2"-4.5" (subject to vendor and antenna size)

7.4 Power Consumption Specifications

The following table shows the maximum power consumption for IP-20G IDU and supported RFUs. The++ maximum power consumption for the entire system is the sum of the IDU and the RFUs connecting to it.

Configuration		Power (W)	Comments
IDU Eth-only with single RFU		23.5W	
Addition for second RFU		2.9W	
Addition for 16 E1s		11W	
RFU-C	6-26 GHz	1+0: 22	RFU only.
		1+1: 39	
	28-38 GHz	1+0: 26	RFU only.
		1+1: 43	

8. Acceptance & Commissioning Procedures

This chapter provides Ceragon's recommended Acceptance and Commissioning Procedure for IP-20. Acceptance and commissioning should be performed after initial setup is complete.

The purpose of this procedure is to verify correct installation and operation of the installed link and the interoperability with customer end equipment.

Ceragon's Acceptance and Commissioning procedure includes the following stages:

- Site Acceptance Procedure
- Commissioning of radio link

The Site Acceptance Procedure is a checklist that summarizes the installation requirements of the site at which the products were installed.

The commissioning tests cover the required configuration information that should be recorded, and the tests that should be performed on the radio link.

8.1 Site Acceptance Procedure

The purpose of the following procedures is to verify that all installation requirements were noted and checked. Following this procedure will ensure proper, long-lasting, and safe operation of the product.

The checklist below summarizes the installation requirements of the site.

SITE ACCEPTANCE CHECKLIST	
1. SITE INFORMATION	
Customer:	
Radio model:	
Site name:	
Site code:	
Radio link code:	
Site address:	
2. ANTENNA MOUNTING	
Antenna mount type:	
Mount is of sufficient height to clear local obstructions	OK
Mount is safely positioned to not cause a safety hazard	OK
Mount is secure and perpendicular	OK
Mount is grounded as per site specifications	OK
All steelwork is Galvanized or Stainless Steel as appropriate	OK
3. ANTENNA	
Antenna type (model and size):	
Antenna is securely fixed to mount	OK
Antenna is grounded as per site specifications	OK
Antenna sway braces are installed correctly (where applicable)	OK
Antenna Radome is securely fitted (where applicable)	OK
Water drain plugs are fitted and removed, as appropriate	OK
Antenna sealing O-Ring is properly fitted and not damaged	OK
Antenna/Launch unit polarization is as per link requirements	OK

SITE ACCEPTANCE CHECKLIST (continued)	
4. RADIO FREQUENCY UNIT (RFU)	
Type of RFU mount:	(Direct or Remote mount)
RFU is securely mounted to the antenna or pole	OK
RFU is grounded as per installation instructions	OK
RFU's polarization is as per link requirements	OK
RFU is installed properly and has no physical damage	OK
<i>For Remote-Mount Only:</i>	
Remote mount kit is securely mounted to the pole	OK
Flexible waveguide has no physical damage and connectors are sealed	OK
All flexible waveguide bolts are secured using washers and lock-washers, as appropriate	OK
Flexible waveguide is secured to the pole	OK
6. COAX CABLE	
Overall cable length:	
Cable type:	
N-Type connectors assembled properly on the cable	OK
Cable connected securely to RFU and IDU	OK
Cable connector is weather-proofed (sealed) at the RFU	OK
At the RFU, cable has a service/drip loop to prevent moisture from entering the connector	OK
Cable is secured using suitable restraints to fixed points at regular intervals (0.5 m recommended)	OK
Cable has no sharp bends, kinks, or crushed areas. All bends are per manufacturer specifications	OK
Grounding/lightning protection is as per site specifications	OK
Lightning protection type and model:	
Cable point-of-entry to building/shelter is weather-proof	OK
Cable ends are properly labeled	OK

SITE ACCEPTANCE CHECKLIST (continued)	
7. FLEXIBLE WAVEGUIDE	
Overall flexible WG length:	
Flexible WG type:	
Flexible WG is connected securely to RFU and Antenna	OK
Flexible WG connector is weather-proofed (sealed) at the RFU	OK
At the RFU, the flexible WG has a service/drip loop to prevent moisture from entering the connector	OK
Flexible WG is secured using suitable restraints to fixed points at regular intervals (0.5 m recommended)	OK
Flexible WG has no sharp bends, kinks, or crushed areas. All bends are per manufacturer specifications	OK
Flexible WG point-of-entry to building/shelter is weather-proof	OK
Flexible WG ends are properly labeled	OK
8. INDOOR UNIT	
IDU is securely mounted to the rack	OK
IDU is located in a properly ventilated environment	OK
IDU fans are functional and air flow to the fans is not disrupted	OK
IDU and rack are grounded as per site specifications	OK
Traffic cables and connections are properly terminated as per manufacturer/cable instructions	OK
All cabling is secured, tidy, and visibly labeled	OK
9. DC POWER SUPPLY - Two Inputs	
Measured DC voltage input to the IDU:	(-40.5 to -60 VDC)
Power-Supply maximum current:	(at least 3 Ampere per carrier)
Power-Supply is properly grounded	OK
DC power backup type:	
IDU DC connector is secure and the DC input leads are correctly terminated (no bare wires are visible)	OK
IDU DC connector (+) and (GND) leads are shorted and GND is grounded	OK
10. RACK INSTALLATION	
Rack is mounted to the shelter floor with four screws	OK
Rack is mounted to the shelter wall with two screws	OK

SITE ACCEPTANCE CHECKLIST (continued)	
11. REMARKS/NOTES	
12. GENERAL INFORMATION	
Site accepted by:	Name:
	Title:
	Company:
	Signature:
	Date:
Site approved by:	Name:
	Title:
	Company:
	Signature:
	Date:

8.2 Site Acceptance Checklist Notes

The following notes provide important additional information about the Site Acceptance Checklist.

1 Antenna Mounting

- Mounting pole is of sufficient height to clear local obstructions, such as parapets, window cleaning gantries, and lift housings.
- Mounting Pole is of sufficient height, and is safely positioned, so as not to cause a safety hazard. No person should be able to walk in front of, or look directly into the path of the microwave radio beam. Where possible, the pole should be away from the edge of the building.
- Mounting pole is secure and perpendicular. A pole that is not perpendicular may cause problems during antenna alignment.
- Mounting pole is grounded as per site specifications. All operators and site owners have specific requirements regarding the grounding of installations. As a minimum, typical requirements are such that any metal structure must be connected to the existing lightning protection ground of the building. Where it extends beyond the 45 degree cone of protection of existing lightning conductors, additional lightning protectors should be installed.
- All steelwork is Galvanized or Stainless Steel, as appropriate to prevent corrosion.

2 Antenna

- Antenna is grounded as per site specifications. See the third point in the Antenna Mounting section above.
- Antenna sway braces are fitted and installed correctly, where applicable. Typically, for an antenna of 1.2 m or larger, an extra sway brace is fitted to the mounting frame of the antenna. This sway brace should not be mounted to the same pole as the antenna, but should be installed directly back to the tower or an alternative point.
- Antenna Water Drain Plugs are fitted and removed, where appropriate. Some antennas have moisture drain plugs installed at various points around the antenna. The purpose of these plugs is to allow any moisture that forms on the inside of the antenna or radome to drip out and prevent a pool within the antenna. Only the plugs at the bottom of the antenna, after installation, should be removed. All other plugs should be left in position.

3 RFU (Outdoor Unit)

- The RFU is grounded as per installation instructions. See the third point in the Antenna Mounting section above.
- The RFU polarization is as per link requirements and matches the polarization of the antenna.

4 Indoor Unit

- The main traffic connections are correctly terminated and crimped as per cable and connector manufacturer instructions. All fiber optic patch leads should be routed carefully and efficiently, using conduits to prevent damage to the cables.
- All other user terminations are secure and correctly terminated.
- All labeling is complete as per site requirements. Labeling is specific to each customer. At a site with only one installation, labeling may be unnecessary. However, at sites with multiple installations, correct and adequate labeling is essential for future maintenance operations.

Typical labeling requirements include:

Antenna labels - for link identity and bearing

RFU labels - for link identity, frequency, and polarization

Coax cable labels - for link identity, close to the RFU, IDU, and either end of any joint

IDU labels - for link identity

8.3 Radio Link Commissioning Procedure

8.3.1 Scope

This section describes the recommended commissioning tests for IP-20 radio link in a 1+0 configuration.

The purpose of the commissioning tests is to verify correct and proper operation of the product.

8.3.2 Commissioning Test

The following tests should be performed on each installed link.

8.3.2.1 Link Verification

- Received Signal Level (RSL) is up to +/- 4 dB from the expected (calculated) level at both ends of the link.
- Radio Bit Error Rate (BER) is 10E-11 or lower.
- If working with ATPC, ATPC is operating as expected (RSL = reference level).

8.3.2.2 Ethernet Line Interfaces Test

- Connect Ethernet Packet Analyzer to the GbE port. Use physical loop at remote end (or connect second analyzer). Run Packet Loss test for at least one hour (load rate as per Ceragon's specifications for the chosen MRMC).
- Connect Ethernet Packet Analyzer to the FE port. Use physical loop at remote end (or connect second analyzer). Run Packet Loss test for at least one hour (load rate as per Ceragon's specifications for the chosen MRMC).

Interoperability Verification

- Connect customer end equipment to the line interfaces, and verify correct operation.
- Further interoperability tests should be performed in accordance with the specific requirements of the connected end equipment.

8.3.2.3 Management Verification

- Launch the HTTP management and verify that you can manage the link and that you are able to perform changes to the link configuration (frequency channel, Tx power, system name, time & date, etc.)
- Verify that correct parameters are reported when performing the above.
- Verify that there are no active alarms on the link.
- If the management station is located at a remote site (Network Operation Center), verify that the management station can manage the link and receive traps.

8.4 IP-20 Commissioning Log

The Commissioning Log is an integral part of the commissioning procedure and should be filled in for each installed link.

The Commissioning Log gathers all relevant information regarding the installed link and contains a checklist of all recommended commissioning tests.

Maintaining the Commissioning Log is important for tracking your installations, and to provide essential data for Ceragon Networks.

Upon completing the Commissioning Log, send the log to Ceragon support center at support@ceragon.com.

IP-20 LINK COMMISSIONING LOG		
1. GENERAL INFORMATION		
Customer:		
Radio model:		
Configuration:		
Radio link code:		
Site 1 name & add:		
Site 2 name & add:		
2. RFU	Site 1	Site 2
RFU model:		
RFU p/n:		
RFU s/n:		
RFU SW:		
IDU model:		
IDU p/n:		
IDU s/n:		
IDU SW:		
Tx frequency (MHz):		
Rx frequency (MHz):		
Link ID:		
Tx power (dBm):		
ATPC on/off:		
ATPC ref level:		
RFU Polarization:		

3. ANTENNA AND RFU MOUNT	Site 1	Site 2
Antenna vendor and model:		
Antenna size:		
Mounting type:		
Mounting losses:		
4. LINK PARAMETERS	Site 1	Site 2
Link distance:		
Rain zone:		
Expected RSL (dBm):		
Expected Diversity RSL (dBm):		
RSL Main (dBm):		
RSL Diversity (dBm):		
Deviation from exp?		
RSL ≤ 4 dB?		
5. COMMISSIONING TESTS	Site 1	Site 2
Line loopback:	Pass	Pass
RFU loopback:	Pass	Pass
Radio BER:	Pass	Pass
FE test:	Pass	Pass
GbE test:	Pass	Pass
6. MANAGEMENT CONFIGURATION	Site 1	Site 2
Eth IP Address:		
Eth IP mask:		
Default router:		
In-band VLAN		
7. REMARKS/NOTES		



8. INSTALLATION INFORMATION	
Installed by:	Name:
	Company:
	Date:
	Signature:
Commissioned by:	Name:
	Company:
	Date:
	Signature:



República Federativa do Brasil
Agência Nacional de Telecomunicações

Certificado de Homologação

(Intransferível)

Nº **03157-14-01398**

Validade: Indeterminada

Emissão: 29/12/2020

Requerente:

CNPJ: 00.538.268/0001-81

CERAGON AMERICA LATINA LTDA

Fabricante:

CERAGON NETWORKS LTD.

24 RAOUL WALLENBERG ST.

Nº

ISRAEL

Este documento homologa, nos termos da regulamentação de telecomunicações vigente, o Certificado de Conformidade nº TÜV 14.1335, emitido pelo **TÜV Rheinland Brasil**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação de telecomunicações.

Tipo - Categoria:

Modem para Transceptor Digital - II

Modelo - Nome Comercial (s):

IP20G M1 1DC - (IP20G M1 1DC) /IP20G M1 2DC - (IP20G M1 2DC) /IP20G M2 1DC - (IP20G M2 1DC) /IP20G M2 2DC - (IP20G M2 2DC)

Características técnicas básicas:

Designação de Emissões	Tipo de Modulação	Capacidade de Transmissão (kbit/s)
14M0D1W	QPSK (4QAM)	20,39
14M0D1W	8QAM	30,20
14M0D1W	16QAM	41,00
14M0D1W	32QAM	53,90
14M0D1W	64QAM	65,98
14M0D1W	128QAM	79,44
14M0D1W	256QAM	87,00
14M0D1W	512QAM	99,87
14M0D1W	1024QAM	111,98
14M0D1W	2048QAM	116,46
20M0D1W	QPSK (4QAM)	20,39
20M0D1W	8QAM	30,20
20M0D1W	16QAM	41,00
20M0D1W	32QAM	53,87
20M0D1W	64QAM	65,98
20M0D1W	128QAM	79,44
20M0D1W	256QAM	87,00
20M0D1W	512QAM	99,87
20M0D1W	1024QAM	111,98
20M0D1W	2048QAM	116,46
27M5D1W	QPSK (4QAM)	40,98
27M5D1W	8QAM	64,76
27M5D1W	16QAM	82,64
27M5D1W	32QAM	108,38
27M5D1W	64QAM	133,33
27M5D1W	128QAM	160,14
27M5D1W	256QAM	182,24
27M5D1W	512QAM	200,97
27M5D1W	1024QAM	226,72
27M5D1W	2048QAM	243,12
28M0D1W	QPSK (4QAM)	40,98
28M0D1W	8QAM	60,76
28M0D1W	16QAM	82,64

Designação de Emissões	Tipo de Modulação	Capacidade de Transmissão (kbit/s)
28M0D1W	32QAM	108,38
28M0D1W	64QAM	133,33
28M0D1W	128QAM	160,14
28M0D1W	256QAM	182,24
28M0D1W	512QAM	200,97
28M0D1W	1024QAM	226,72
28M0D1W	2048QAM	243,12
29M7D1W	QPSK (4QAM)	40,98
29M7D1W	8QAM	60,77
29M7D1W	16QAM	82,64
29M7D1W	32QAM	108,38
29M7D1W	64QAM	133,33
29M7D1W	128QAM	162,50
29M7D1W	256QAM	182,24
29M7D1W	512QAM	200,97
29M7D1W	1024QAM	226,72
29M7D1W	2048QAM	243,12
30M0D1W	QPSK (4QAM)	40,98
30M0D1W	8QAM	60,77
30M0D1W	16QAM	82,64
30M0D1W	32QAM	108,38
30M0D1W	64QAM	133,33
30M0D1W	128QAM	160,14
30M0D1W	256QAM	182,24
30M0D1W	512QAM	200,97
30M0D1W	1024QAM	226,82
30M0D1W	2048QAM	243,12
40M0D1W	QPSK (4QAM)	58,22
40M0D1W	8QAM	86,31
40M0D1W	16QAM	117,12
40M0D1W	32QAM	153,98
40M0D1W	64QAM	188,84
40M0D1W	128QAM	228,19
40M0D1W	256QAM	255,50
40M0D1W	512QAM	268,51
40M0D1W	1024QAM	323,20
40M0D1W	2048QAM	349,34
55M0D1W	QPSK (4QAM)	82,86
55M0D1W	8QAM	122,84
55M0D1W	16QAM	166,70
55M0D1W	32QAM	219,08
55M0D1W	64QAM	268,77
55M0D1W	128QAM	324,63
55M0D1W	256QAM	367,10
55M0D1W	512QAM	402,86
55M0D1W	1024QAM	464,86
55M0D1W	2048QAM	503,90
56M0D1W	QPSK (4QAM)	82,86
56M0D1W	8QAM	122,84
56M0D1W	16QAM	166,70
56M0D1W	32QAM	219,08
56M0D1W	64QAM	268,77
56M0D1W	128QAM	324,63
56M0D1W	256QAM	367,10
56M0D1W	512QAM	402,86
56M0D1W	1024QAM	464,86
56M0D1W	2048QAM	503,90

Observação: a modulação "4QAM" que aparece entre parênteses na tabela acima é equivalente à modulação "QPSK" e assim foi usada esta última denominação neste relatório para manter a mesma nomenclatura do certificado anterior.

O produto Ceragon modelo IP20G possui as seguintes interfaces:

Dezesseis interfaces E1 cada uma com impedância de 75 ohms e acessíveis através de um conector multipinos;

Quatro interfaces Gigabit Ethernet com conector RJ-45;

Duas interfaces ópticas Gigabit Ethernet com módulos ópticos SFP;

Uma interface serial COM com conector RJ-45;

Uma interface com conector RJ-45 para recepção de sinais de sincronismo externo;

Uma interface com conector RJ-45 para gerenciamento de rede.

Uma ou duas interfaces com conectores TNC para conexão de cabo coaxial para

transmissão/recepção de sinais de frequência intermediária (FI).

O produto Ceragon modelo FibeAir IP20G recebe alimentação 48 Vcc e possui as seguintes variantes:

- Variante M1-DC: possui uma fonte de alimentação e uma interface de FI (um conector TNC);
- Variante M1-2DC: possui uma fonte de alimentação e duas interfaces de FI (dois conectores TNC, um para cada interface);
- Variante M2-1DC: possui duas fontes de alimentação operando em redundância e uma interface de FI (um conector TNC);
- Variante M2-2DC: possui duas fontes de alimentação operando em redundância e duas interfaces de FI (dois conectores TNC, um para cada interface).

Ensaio de SAR não aplicável: o equipamento não é terminal portátil

Observações

Na sua utilização o produto deve estar ajustado na(s) potência(s) e frequência(s) autorizadas pelo órgão técnico competente da Agência Nacional de Telecomunicações – Anatel.

Este certificado substitui o de mesmo número emitido em 07/02/2019

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos da regulamentação de telecomunicações, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SCH – Sistema de Gestão de Certificação e Homologação, disponível no portal da Anatel. (www.anatel.gov.br).

Secundino da Costa Lemos
Gerente de Certificação e Numeração - substituto

Cisco 1905 Series Integrated Services Routers

Product Names: CISCO 1905/K9 and CISCO 1905-SEC/K9

Cisco® 1900 Series Integrated Services Routers (ISRs) build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich-media collaboration to the branch office while maximizing operational cost savings. The Cisco Integrated Services Routers Generation 2 (ISR G2) platforms are future-enabled with multicore CPUs, Gigabit Ethernet Switching with enhanced Power over Ethernet (PoE), and new energy monitoring and control capabilities that enhance overall system performance. Additionally, a new Cisco IOS® Software Universal image enables you to decouple the deployment of hardware and software, providing a stable technology foundation that can quickly adapt to evolving network requirements. Overall, the Cisco 1900 Series offers exceptional total cost of ownership (TCO) savings and network agility through the intelligent integration of market-leading security, unified communications, wireless, and application services.

Product Overview

The Cisco 1905 builds on the best-in-class offering of the Cisco 1841 Integrated Services Routers. All Cisco 1900 Series ISRs offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and advanced security services. In addition, the Cisco 1905 Integrated Services Router has an integrated serial interface module and an enhanced high-speed WAN interface card (EWHIC) slot that supports a choice of LAN, 3G or ISDN modules (Figure 1).

Figure 1. Cisco 1905 Integrated Services Router



Key Business Benefits

The Cisco ISR G2 routers provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs. Table 1 lists the business benefits of the Cisco 1905 Series Integrated Services Routers.

Table 1. Key Features and Benefits of the Cisco 1905 Integrated Services Router

Benefits	Description
Service integration	The Cisco 1905 offers increased levels of services integration with data, security, wireless, and mobility services enabling greater efficiencies and cost savings.
Services on demand	A single Cisco IOS Software Universal image is installed on each Cisco ISR G2. The Universal image contains all of the Cisco IOS Software technology sets that can be activated with a software license, allowing your business to quickly deploy advanced features without downloading a new Cisco IOS Software image. Additionally, larger default memory is included to support the new capabilities.
High performance with integrated services	The Cisco 1905 enables deployment in high-speed WAN environments with concurrent services enabled up to 10 Mbps.

Benefits	Description
Network agility	- Designed to address customer business requirements, the Cisco 1900 Series with the modular architecture offers a performance range of modular interfaces and services as your network needs grow. - Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy efficiency	- The Cisco 1900 Series architecture provides energy-savings features that include the following: - Intelligent power management allowing you to control power to the modules based on the time of day. Cisco EnergyWise™ technology will be supported in the future. - Services integration and modularity on a single platform performing multiple functions optimizes raw-materials consumption and energy usage. - Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the TCO, including materials and energy use. - High-efficiency power supplies are provided with each platform.
Investment protection	- The Cisco 1900 Series maximizes investment protection: - Reuse of a broad array of existing modules supported on the original ISRs provides a lower TCO. - A rich set of Cisco IOS Software features is carried forward from the original ISRs and delivered in the universal image. - This router gives you the flexibility to grow as your business needs evolve.

Architecture and Modularity

The Cisco 1905 is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support expanding customer requirements, increased bandwidth, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 1905.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular platform	- The Cisco 1905 ISR is a modular platform with an integrated serial interface and an additional high-speed WAN interface card (HWIC) slot to provide connectivity and services for varied branch-office network requirements. - It offers a choice of LAN, Serial, 3G, or ISDN modules to accommodate field upgrades to future technologies without requiring replacement of the platform.
Processors	The Cisco 1905 is powered by high-performance multicore processors that support growing demands of branch-office networks by supporting high-throughput WAN requirements.
Embedded IP Security/Secure Sockets Layer (IPsec/SSL) VPN hardware acceleration	- Embedded hardware encryption acceleration is enhanced to provide higher scalability, which, combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (both IPsec and SSL acceleration). - The onboard encryption hardware (co-processor) outperforms the advanced integration modules (AIMs) of previous generations.
Integrated Gigabit Ethernet ports	All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN-routed ports.
Serial port	The Cisco 1905 has an integrated serial port (HWIC-1T) for serial WAN connectivity.
Innovative universal-serial-bus (USB)-based console access	- A new, innovative, mini-Type B USB console port supports management connectivity when traditional serial ports are not available. - The traditional console and auxiliary ports are also available. You can use either the USB-based console or the RJ-45-based console port to configure the router.
Optional external PoE power supply for distribution of power	An optional upgrade to the power supply provides inline power, 802.3af-compliant PoE, and Cisco Standard Inline Power to optional integrated switch modules.

Modularity Features and Benefits

The Cisco 1905 provides enhanced modular capabilities (refer to Table 3) that offer you investment protection. A sub-set of modules available on previous generations of Cisco routers, such as the Cisco 1841 ISR, are supported on the Cisco 1905. Additionally, you can easily interchange modules used on the Cisco 1905 with other Cisco routers to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

Table 3. Modularity Features and Benefits

Feature	Benefits
Cisco Enhanced High-Speed WAN Interface Card (EHWIC) 	• The EHWIC slot replaces the HWIC slot and can natively support HWICs and WAN interface cards (WICs). • One integrated EHWIC slot is available on the Cisco 1905 for flexible configurations supporting a choice of LAN, Serial, 3G, or ISDN modules.
USB 2.0 ports	• One high-speed USB 2.0 port is supported. The USB port enables another mechanism for secure token capabilities and storage.

Cisco IOS Software

The Cisco 1905 Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, Cisco IOS Software Releases 15M and T support a comprehensive portfolio of Cisco technologies, including new functions and features delivered in Releases 12.4 and 12.4T, and new innovations that span multiple technology areas, including security, high availability, IP Routing and Multicast, quality of service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all functions is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Three major technology licenses are available on the Cisco 1905 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at <http://www.cisco.com/go/sa>.

- IP Base: This technology package is available as default
- Data
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

For additional information and details about Cisco IOS Software licensing and packaging on Cisco 1905 Series Integrated Services Routers, please visit <http://www.cisco.com/go/sa>.

Key Branch-Office Services

The industry-leading Cisco Integrated Services Routers offer unprecedented levels of services integration. Designed to meet the requirements of the branch office, these platforms provide a complete solution with security, mobility, and data services. Businesses enjoy the benefit by deploying a single device that meets all their needs and saves on capital expenditures (CapEx) and operating expenses (OpEx).

Integrated Network Security for Data and Mobility

Security is essential to protect a business' intellectual property while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources. As part of the architectural framework of the SAFE Blueprint from Cisco that allows organizations to identify, prevent, and adapt to network security threats - the Cisco 1900 Series Integrated Services Routers facilitate secure business transactions and collaboration.

The Cisco IOS Software Security technology package license for the Cisco 1900 Series offers a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks in one solution set. The Cisco 1905 offers native hardware-based encryption acceleration in its co-processor to provide greater IPsec throughput with less overhead for the router processor when compared with software-based encryption solutions. Cisco Integrated Services Routers offer a comprehensive and adaptable security solution for branch-office routers that include features such as:

- Secure connectivity: Achieve secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN.
- Integrated threat control: Respond to sophisticated network attacks and threats using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering and Flexible Packet Matching (FPM).
- Identity management: Intelligently protect endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI).

Detailed information about the security features and solutions supported on the Cisco 1900 Series routers is available at <http://www.cisco.com/go/routersecurity>.

Mobility Services

Wireless WAN

Cisco 3G wireless WAN (WWAN) modules combine traditional enterprise router functions such as remote management, advanced IP services such as voice over IP (VoIP), and security, with mobility capabilities of 3G WAN access. Using high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, Frame Relay, and ISDN. Cisco 3G solutions support 3G standards High-Speed Packet Access (HSPA) and Evolution Data Only/Evolution Data Optimized (EVDO), offering you a true multipath WAN backup and the ability to rapidly deploy primary WAN connectivity. For more information about 3G solutions on Cisco Integrated Services Routers, please visit <http://www.cisco.com/go/3g>.

Integrated LAN Switching

The Cisco 1905 Integrated Services Router will support the EHWIC LAN modules when they become available in the future. The Cisco 1905 supports the existing singlewide Cisco EtherSwitch® HWIC, which greatly expands the capabilities of the router by integrating industry-leading Layer 2 switching.

Managing Your Integrated Services Routers

Network management applications are instrumental in lowering operating expenses (OpEx) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end-to-end network. “Day-one device support” provides immediate manageability support for the ISR, enabling quick and easy deployment, monitoring, and troubleshooting from Cisco and third-party applications.

Organizations rely on Cisco, third-party, and in-house-developed network management applications to achieve their OpEx and productivity goals. Underpinning those applications are the embedded management features available in every ISR. The new ISRs continue a tradition of broad and deep manageability features within the devices. Features such as Cisco IOS IP Service-Level Agreements (IP SLAs), Cisco IOS Embedded Event Manager (EEM), and NetFlow allow you to know what is going on in your network at all times. These features along with Simple Network Management Protocol (SNMP) and syslog support enable your organization’s management applications.

Refer to Tables 4 through 6 for details about Cisco IOS software feature and protocol support, Cisco IOS software management capabilities, and Cisco Network Management applications for Cisco 1905 Integrated Services Routers.

Table 4. Cisco 1905 with Cisco IOS Software Feature and Protocol Support

Feature	Description
Protocols	IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPsec, generic routing encapsulation (GRE), Bidirectional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast, MPLS, Layer 2 Tunneling Protocol Version 3 (L2TPv3), 802.1ag, 802.3ah, and Layer 2 and Layer 3 VPN.
Encapsulations	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Application Recognition (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS Software, refer to the Feature Navigator tool at: <http://www.cisco.com/go/fn>.

Table 5 highlights several ISR management capabilities that are available within Cisco IOS Software.

Table 5. Cisco IOS Software Management Capabilities

Feature	Description of Feature Supported by Cisco Integrated Services Routers
WSMA	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML-based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
EEM	Cisco IOS EEM is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
IPSLA	Cisco IOS IP SLAs enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video, in an IP network.
SNMP, RMON, syslog, NetFlow, and TR-069	Cisco 1900 Series ISRs also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.

Cisco Network Management Applications

The applications listed in Table 6 are standalone products that you can purchase or download to manage your Cisco network devices. The applications are built for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Solutions

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	• Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers. This tool simplifies routing, firewall, IPS, VPN, unified communications, and WAN and LAN configuration through GUI-based easy-to-use wizards.
Networkwide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	• CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco integrated Services Routers, using new instrumentation such as Cisco IOS EEM. • In addition to supporting basic platform services of the ISR, CiscoWorks also provides added-value support for the Cisco Services-Ready Engine, (SRE) enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.
Networkwide staging, configuration, and compliance	CiscoWorks NCM	• CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	• Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Configuration and provisioning	Cisco Unified Provisioning Manager	• Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	• Easily manage Cisco IOS Software activation and license management for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager.
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	• Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

Summary and Conclusion

As businesses strive to lower the TCO in running their networks and increase their overall employee productivity with more centralized and collaborative network applications, more intelligent branch-office solutions are required. The Cisco 1905 offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 1905 is designed to consolidate the functions of separate devices into a single, compact system that can be remotely managed.

Product Specifications

Table 7. Product Specifications of Cisco 1905 Integrated Services Router

	Cisco 1905 Integrated Services Router
Services and Slot Density	
Embedded hardware-based cryptography acceleration (IPsec + SSL)	Yes
RJ-45 onboard LAN 10/100/1000 ports	2
Serial port	Slot 0 (integrated HWIC-1T)
EHWIC slot	1
Memory (DDR2 DRAM): Default/maximum	256 MB/512 MB (license upgradable)
USB Flash memory: Default/maximum	256 MB/256 MB (internal)
External USB flash-memory slots (Type A)	1
USB console port (mini-Type B) (up to 115.2 kbps)	1
Serial console port (up to 115.2 kbps)	1
Serial auxiliary port (up to 115.2 kbps)	1
Integrated power supply	AC
Power-supply options	PoE (external)
Redundant power-supply support	No
Power Specifications	
AC input voltage	100-240V ~
AC input frequency	47-63 Hz
AC input current range AC power supply (maximum) (amps)	1.5-0.6
AC input surge current	<50A
Typical power (no modules)	25W
Maximum power capacity with AC power supply	60W
Maximum power capacity with PoE power supply (platform only)	70W
Maximum PoE device power capacity with PoE power supply	80W
Physical Specifications	
Dimensions (H x W x D)	1.75 x 13.5 x 11.5 in. (4.45 x 34.29 x 29.21 cm)
Rack height	1 rack unit (1RU)
Rack-mount 19 in. (48.3 cm) EIA	Optional
Wall-mount (refer to installation guide for approved orientation)	Yes
Weight: With AC power supply (no modules)	8 lb (3.175 kg)
Weight: With PoE power supply (no modules)	12.8 lb
Maximum weight: Fully configured	14 lb
Airflow	Back to side
Environmental Specifications	
Operating Condition	
Temperature: 5906 ft (1800m) maximum altitude	32-104°F (0-40°C)
Temperature: 9843 ft (3000m) maximum altitude	32-77°F (0-25°C)
Altitude	10000 ft (3000m)
Humidity	10 to 85 percent relative humidity (RH)
Acoustic: Sound pressure (typical/maximum)	32.9/58.3 dBA
Acoustic: Sound power (typical/maximum)	41.9/67.2 dBA

Cisco 1905 Integrated Services Router	
Transportation and Storage Condition	
Temperature	(-40 to 158°F (-40 to 70°C))
Humidity	5 to 95 percent RH
Altitude	15000 ft (4570m)
Regulatory Compliance	
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 IEEE 802.3 RTTE Directive

Supported Modules

The Cisco 1905 supports a wide range of modules that span industry-leading breadth of services at the branch office. Please refer to Table 8 for the list of modules supported on the Cisco 1905.

Ordering Information

Table 8 gives ordering information for the Cisco 1905 Router. For information about how to order the Cisco 1900 Series, please visit the Cisco 1900 Series Ordering Guide. To place an order, visit the [Cisco Ordering Home Page](#). For additional product numbers, including the Cisco 1900 Series bundle offerings, please check the [Cisco 1900 Series Integrated Services Router Price List](#) or contact your local Cisco account representative.

Table 8. Cisco 1905 Series Basic Ordering Information

Product Number	Product Description
Cisco1905/K9	Cisco 1905 with 2 GE, 1 HWIC-1T, CAB-SS-V35MT, 1 EHWIC slot, 256MB USB Flash (internal), 256MB DRAM, IP Base
Cisco1905-SEC/K9	Cisco 1905 with 2 GE, 1 HWIC-1T, CAB-SS-V35MT, 1 EHWIC slot, 256MB USB Flash (internal), 256MB DRAM, SEC Lic
Software License	
SL-19-IPB-K9(=)	IP Base License (Paper) for Cisco 1900
SL-19-DATA-K9(=)	Data License (Paper) for Cisco 1900
SL-19-SEC-K9(=)	Security License (Paper) for Cisco 1900
Feature License	
FL-SSLVPN10-K9(=)	Cisco SSLVPN Feature license PAK (Paper) - 10 users

Product Number	Product Description
FL-SSLVPN25-K9(=)	Cisco SSLVPN Feature license PAK (Paper) - 25 users
Memory License	
FL-1900-256U512MB*	Cisco 1905 Memory License 256MB to 512MB DRAM Upgrade
Modules (Slot 1)	
HWIC-3G-HSPA	3G HWIC (Non-US) HSPA/UMTS 850/1900/2100MHz 4-band EDGE/GPRS
HWIC-4ESW	Four port 10/100 Ethernet switch interface card
WIC-1B-S/T-V3	1-Port ISDN WAN Interface Card (dial and leased line)
HWIC-1T	1-Port Serial WAN Interface Card
HWIC-1B-U	1-Port ISDN BRI U High-Speed WAN Interface Card
HWIC-4B-S/T	4-port ISDN BRI High-Speed WAN Interface Card
EHWIC-3G-HSPA-U	3.5G EHWIC (Non-US) HSPA/UMTS 850/900/1900/2100MHz with SMS/GPS
EHWIC-3G-HSPA+7	(Non-US) 3.7G HSPA+ Release 7 EHWIC w/ SMS/GPS
EHWIC-4ESG	4-port single-wide Gb Ethernet switch EHWIC

* 512MB is required for SEC and Data Technology Package License with IOS Software Version 15.3(1)T and onwards.

To download the Cisco 1905 with Cisco IOS Software, go to [Download Software](#), click "Router Software", and go to "Cisco ISR 1905 Integrated Services Router."

ISR Migration Options

Cisco 1900 Series Routers are included in the standard Cisco Technology Migration Program (TMP). Refer to <http://www.cisco.com/go/TMP> and contact your local Cisco account representative for program details.

Warranty Information

The Cisco 1900 Series Integrated Services Routers have a 1-year limited liability warranty.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you reduce the cost and complexity of branch-office deployments. We have the depth and breadth of experience across technologies to architect a blueprint for a branch-office solution to meet your company's needs. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help maintain operational health, strengthen software application functions, solve performance problems, and lower expenses. Optimization services are designed to continually improve performance and help your team succeed with new technologies. For more information, please visit <http://www.cisco.com/go/services>.

Cisco SMARTnet® technical support for the Cisco 1900 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- Access to the industry's largest dedicated technical support staff 24 hours a day

For More Information

For more information about the Cisco 1900 Series, visit <http://www.cisco.com/go/1900> or contact your local Cisco account representative.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)