

BPR-W Wireless Proxy Router

Product Datasheet · BPR-W10 / BPR-W60
ALN-DS-BPR-W-EN · v1.1 · 2026-10-26 · English translation for review

Product overview

BPR-W integrates multiple sub-routers, wireless access and proxy configuration in one device. Each sub-router has its own router MAC address, DHCP, NAT and proxy settings, and broadcasts a corresponding SSID. Devices connected to that Wi-Fi network use its configured proxy egress, allowing networks to be assigned by phone, store or business group.

BPR-W10 provides 10 sub-routers and SSIDs; BPR-W60 provides 60. The two models differ only in sub-router and SSID capacity; other product specifications are the same.

Core capabilities and application value

Capability	Function and value
Centralized network deployment	Configure multiple wireless networks and their egress in one place, reducing separate-router wiring and maintenance.
ALBulk batch management	Import proxies, configure SSIDs and update router MAC addresses in batches; import and export supported lists.
Individual node maintenance	Edit, test and save a selected proxy without reimporting the entire list.
Disconnect on proxy failure	The affected Wi-Fi network loses external access rather than falling back to the local broadband connection.
Address leak protection	Product documentation lists IP, DNS and WebRTC address leak protection alongside egress management.
Router-side identity updates	Replace brand-router MAC addresses in batches, optionally together with proxies, to update MAC/egress combinations.
Internal management and resources	Use internal port mapping to manage downstream devices and access rules to reach upstream NAS or servers.
Multi-unit wireless deployment	Set channel, channel width and transmit power per unit, considering coverage and interference.

Typical business uses

Phone farms, centralized phone deployments, cross-border e-commerce groups, social media operations, regional advertising tests and offices requiring grouped egress and centralized device management. Proxy locations and routes depend on the resources configured by the customer.

01 / Models and Technical Specifications

Model capacity

Item	BPR-W10	BPR-W60
Sub-routers	10	60
Broadcast SSIDs	10	60
Proxy configuration capacity	One egress per group; 10 groups	One egress per group; 60 groups
Sub-router settings	Independent router MAC, DHCP, NAT and proxy	Same
Selection basis	10 business network groups	60 business network groups

Capacity interpretation

Proxy capacity is the number of network groups with separately configurable egress, not a guarantee of distinct public IP addresses. Distinct IPs depend on the proxy resources. SSID count is not a validated concurrent-client capacity.

Common hardware and interfaces

Item	Specification
WAN	1 × Gigabit Ethernet
LAN	1 × Gigabit Ethernet
Wireless band	5 GHz
Wireless standard / rate	802.11ac; nominal maximum 1300 Mbps
Product dimensions	W182 × H182 × L80 mm
Package dimensions	L250 × W234 × H138 mm
Package contents (existing manual)	1 router, 1 power adapter, 2 antennas
Management	ALBulk; existing instructions use the Windows configuration tool
Proxy protocols	SOCKS5, HTTP

Technical notes

1300 Mbps is a nominal wireless link rate, not Internet speed or proxy throughput. Sub-routers share radio, wired and upstream resources; actual rates depend on RF conditions, bandwidth, proxies and load.

The confirmed domestic-market enclosure differs in appearance while hardware configuration and parameters carry over. Dimensions retain the current specification values; applicability to the particular sales enclosure should be checked against the unit.

Unconfirmed quantitative specifications

Supply voltage/current, system power consumption, net weight, operating/storage temperature and humidity, certifications, CPU/RAM/storage, proxy throughput, concurrent connections, maximum clients and latency do not yet have a complete set of confirmed values and are not guaranteed metrics in this edition.

02 / Proxy Configuration and Egress Protection

Proxy management specifications

Function	Configuration and behavior
Batch import	Use Import Proxy on the Proxy page to load a TXT proxy list and assign nodes to sub-routers.
Authentication	SOCKS5 and HTTP nodes support authenticated and unauthenticated formats.
Individual replacement	Select a node, use Modify or Edit Proxy, then Set Proxy to apply; no full-list reimport is required.
Node test	Ping checks node connectivity; it does not replace application availability or throughput testing.
Per-node DNS	Select or enter DNS for the selected node, then save with Set DNS.
Batch DNS	Apply to all applies the DNS setting to all nodes.
Export	Export nodes as TXT, edit them and reimport in the required format.
Provider API	Enter a supported provider's API details in Proxy API for node updates; provider compatibility and update intervals remain to be documented.

Behavior when a proxy fails

If a Wi-Fi group's proxy fails, external access for that group stops without bypassing the proxy through the local broadband egress. An operator can edit the affected node, apply it and test connectivity without reconfiguring other groups' proxy lists.

Failure criteria, detection intervals, recovery timing and applicable firmware still require test records. Independent node editing is not a guarantee that saving settings causes zero interruption to other traffic.

IP / DNS / WebRTC leak protection

Existing documentation lists all three types of address leak protection. Disconnect-on-failure, DNS protection and WebRTC protection are separate verification items; one does not establish the implementation of the others. Acceptance should record firmware, client OS, browser, DNS settings and results.

Router-side network identity

ALBulk includes a database of over 100 million brand-router MAC addresses for generation and batch replacement. A group can change from MAC A + proxy A to MAC B + proxy B. This changes router-side characteristics, not phone identifiers or application fingerprints, and does not guarantee accounts will avoid linkage or platform risk controls.

03 / Wireless and Internal Network Management

Wireless AP specifications

Function	Capability
SSIDs	Batch naming and individual editing, within W10 / W60 capacity.
MAC addresses	Generate brand-router SSID/MAC combinations, refresh in batches and apply to the device.
List management	Import/export SSID and MAC lists as TXT.
Password	Change the Wi-Fi password across networks.
Wireless on/off	Enable or disable all Wi-Fi networks.
Hidden SSID	Hide wireless network names.
Channel and width	Set channel and channel width; choices depend on hardware, firmware and regional settings.
Transmit power	Adjustable; the supported power range remains to be confirmed.
Client isolation	The manual lists isolation between clients on the same Wi-Fi network.

Dense multi-unit deployments

Configure each BPR-W's channel, channel width and transmit power through ALBulk. Plan neighboring channels, adjust power for coverage overlap and load, and verify quality at actual client locations. Channel adjustment does not imply arbitrary band switching or automatic multi-unit RF optimization.

Internal port mapping

A management PC can reach a device under a selected sub-router, for example using RDP. Select Sub-Router, enter the terminal's LAN IP, LAN Port and mapped port, then add and apply the rule.

Internal management traffic stays on the local path, bypasses the business proxy and requires no additional public IP. This is internal access, not an implied public remote-access or traversal service.

Upstream and downstream access rules

Access rules control whether sub-router clients can reach the management-side network. Enable the required access and mappings for NAS or server resources. Existing documentation identifies these rules as a V3.3 update; verify installed software and firmware at delivery.

Sub-routers have separate network configurations but share physical hardware. They are not described as fully physically isolated; reachability depends on client isolation, access rules and port mapping.

04 / Topology and Deployment Selection

CloudLink connectivity

Customers may use an existing VPS or obtain a cloud server from providers such as Alibaba Cloud or Tencent Cloud, configure it as a dedicated proxy through CloudLink and assign it to sub-routers. Cloud resources are customer-provided, not automatically included with the hardware.

The existing procedure uses a static-IP server running Ubuntu 22.04. In Cloud Link, enter a name, Host, SSH port and login details, then Bind. Select Sub Router and the bound Host, then Modify and Set Proxy to apply.

Open the ports required by the actual configuration: SSH defaults to TCP 22; documented proxy ports are 23585, 26516 and 32411 over TCP/UDP. Compatibility with other OS versions and environments remains to be confirmed.

Typical topology

Upstream router / ONT -> WAN [BPR-W]
SSID 01 -> sub-router 01 -> proxy egress 01
SSID 02 -> sub-router 02 -> proxy egress 02
SSID 10 / 60 -> corresponding sub-router and egress
Management PC -> LAN / management Wi-Fi -> configuration

This diagram shows logical assignments. Clients use the sub-router/proxy of their SSID. NAS/server access and downstream control require access rules, mappings and site wiring.

Scenarios and application value

Scenario	Configuration focus	Value
Phone farm / store groups	Assign SSID, MAC and proxy by phone or group	Clear grouping and targeted node maintenance.
Regional ad tests	Assign target-region proxies to groups	Test by region; location depends on proxy resources.
Dense phone deployments	Plan channels, width, power and upstream capacity	Reduce interference and organize deployment areas.
Device and data management	Internal mappings and NAS access rules	Retain needed internal management paths.

Model and component selection

Select W10 or W60 by required business network groups, not an inferred client limit. Evaluate wireless coverage, proxy quality, upstream bandwidth and management needs when scaling.

Deployment checks

Install antennas and connect WAN -> connect the management PC -> configure SSID/MAC -> import proxies or bind CloudLink -> save and test nodes -> verify egress and failure protection -> configure internal access -> test wireless quality under site load.

Website: www.alnets.net **Email:** sale@alnets.net