

A large, stylized yellow arrow pointing towards the top-left corner of the page.

# Technology Overview

Wireless  
Outdoor  
Router  
Protocol  
(WORP)

A large, stylized blue arrow pointing towards the bottom-right corner of the page, starting from the right side and extending to the bottom edge.



## What is WORP?

WORP is a fast and efficient protocol, designed to optimize the performance of multi-play outdoor wireless Point-to-Point (PtP) and Point-to-Multipoint (PtMP) links using packet radio technology, including the use of cutting edge Multiple-Input-Multiple-Output (MIMO) technology.

The use of standard 'COTS' radios enables Proxim to offer a low cost, feature-rich, mission critical solution that is ideal for surveillance, physical security, and last-mile access.

WORP overcomes the performance degradation, which standards-based wireless technologies are susceptible to when used for outdoor long-range connectivity, caused by the effect known as the "Hidden-Node" problem.

## What is the "Hidden-Node" Problem?

All wireless CSMA/CA radios assume that all Subscribers have carrier sensing (detection of signal). This means that all the radios in a system can "hear" each other's radios signals and not start a transmission while others are transmitting.

This is easily achieved for an in-building installation but is not feasible in outdoor point-to-multipoint environments where directional antennas are used and all Subscriber Units (SUs) can hear the Base Station Unit (BSU) but the SUs often cannot hear each other. In a busy network the result is that a SU starts a transmission while another SU is already transmitting and both messages interfere and get corrupted.

The Request-to-Send/Clear-to-Send mechanism (RTS/CTS), an attempted solution to this issue, is a concept that has been included in other wireless protocol standards and although it mitigates the worst effects somewhat, it does not solve the Hidden-Node problem. In a network with only light non mission-critical or real-time traffic and only a handful of radios will usually work. However, when there is a need to scale the network beyond that, any RTS that is sent from a SU to the BSU will likely corrupt any data that another SU was already sending. Again this results in unnecessary packet loss and multiple re-transmissions, causing the network performance to drop almost as dramatically as without the RTS/CTS mechanism. In addition this mechanism adds quite some overhead by increasing the number of frames by two for every data transmission, so the maximum throughput drops significantly when enabling this mechanism.

## The Solution: WORP

The WORP smart polling algorithm ensures that collisions cannot occur by only allowing one SU to transmit at any time, without increasing overhead (the number of frames). In fact it reduces the overhead by sending acknowledgements embedded in the next data frame, so it can reduce the number of frames by up to 50%, which increases the performance of the network.

WORP contains many other industry-standard communication protocol enhancements from IP (Internet Protocol) features that give WORP its competitive edge while at the same time making it feature-rich and reliable.

## What are the Benefits of WORP in an Outdoor Environment?

### More Net Bandwidth

By solving the Hidden-Node problem, WORP increases the overall net bandwidth of the multipoint system. The net bandwidth using WORP is higher than any other protocol solution used in an outdoor environment. WORP is a more efficient protocol that protects the system from packet collisions and transmits the data in an optimal way, which increases the overall performance.

### More Concurrent Subscribers

An outdoor point-to-multipoint solution may connect from 5 to 10 SUs, but in heavy traffic deployments performance starts to suffer from collisions with as little as only two SUs. A solution using WORP, on the other hand, can connect over 100 SUs without adverse effects on usable bandwidth, allowing more concurrent SUs to be active in a wireless multipoint environment.

### Smart Scheduling

WORP uses smart scheduling for the polling of SUs to avoid wasting bandwidth on SUs that have no traffic to be sent. The BSU dynamically decides how frequent a SU should be polled based on the current traffic to and from each SU and the priority settings for that traffic. This scheduling is adapted dynamically to the actual traffic. The scheduling is further optimized by following the bandwidth limits as configured for each SU.

## Bandwidth Control

WORP allows the operator to control network bandwidth, protecting the network from excessive use of the bandwidth by any one SU. Additionally it allows service providers to differentiate their service offerings.

### Asymmetric Bandwidth Control

Asymmetric bandwidth gives the network manager the ability to set different maximum bandwidth rates for a variety of device and customer groups. This allows service providers to further differentiate their service offerings and maximize revenues.

## Quality-of-Service (QoS)

WORP takes care that the most important data arrives with priority by differentiating between priorities of traffic as defined in the profiles for QoS similar to the 802.16 WiMAX QoS standard definition.

WORP allows the service providers to prioritize the traffic, allocating bandwidth based on type of the traffic. The QoS is comprised of the following elements:

- Packet Identification Rules (PIRs), which classify the traffic
- Service Flow Classes (SFCs), which define priority, bandwidth, latency and jitter for the traffic
- Quality-of-Service Classes (QoSC's), which define which of these SFCs will be used for which traffic, classified by set of PIRs

There is also a table which defines which QoSC will be assigned to which particular SU during registration.

## Reliable Data Transfer with Selective Retransmission

WORP guarantees reliable data transmission for all traffic except broadcast/multicast which cannot be acknowledged and retransmitted by its nature.

The reliable data transmission is achieved by means of acknowledgement and selective retransmission of data that was lost during transmission. To avoid throughput slowdown, where subsequent data should wait for retransmission of one piece of data, a windowing mechanism is used where transmission continues as long as subsequent data fits in the window while in the mean time retrans-

mits are scheduled and any acknowledged data is removed from the window. At the receiver side all data that fits in the window is stored and sent to the bridge for transmission on Ethernet in the same order as that it was received in the transmitter, within the same priority class, as different priorities will be sent in order of their priority.

In case data cannot be reliably transmitted within the window or within the specified QoS timeout, it will be discarded to avoid a collection of old and no longer relevant data to choke a link during and after a disturbance of the link, so that fresh data can be sent as soon as the link throughput improves again.

### Lower Overhead

Overhead of a WORP link is minimized by the use of Super-Packeting, Fragmentation and Bursting.

### Link Quality Optimization

The signal quality of both sides of the link is available at each end, so an optimal decision can be taken to improve the link, not just based on local but also on remote signal conditions. In order to support link quality optimization, WORP transports fields that contain the signal quality report from each side to the peer side.

### MIMO, Guard Interval, Data Streams and Antenna Selection

WORP now supports cutting edge MIMO (Multiple-Input-Multiple-Output), multiple Guard Intervals, Data Streams and antenna selection.

### Dynamic Data Rate Selection (DDRS)

The DDRS feature is WORP's ability to dynamically adjust data rate at which the wireless traffic is sent. This feature is especially important in point-to-multipoint networks, when different SUs can sustain different data rates because of the different distance from the BSU, or other environmental realities. With DDRS, WORP dynamically optimizes the wireless data rate to each of the SUs independently from other SUs in the network, keeping the overall net throughput at highest possible level for each device. This feature optimizes throughput even for the links which have different RF conditions on the BSU and on SU, by optimizing downlink and uplink data rates independently from each other.

### Roaming and Handoff

With roaming, WORP supports mobility of the SUs, together with all the network nodes connected to the SU. The network topology change incurred by roaming event is handled automatically by additional Proxim's proprietary protocol running on the network backbone making sure that all relevant information about the new topology is updated in time, keeping the traffic through roaming SU virtually uninterrupted.

### Security

128-bit and 256-bit AES encryption – the first to get FIPS 140-2 level 2 certification on a stand-alone radio. Every WORP frame is encrypted; there is no data leakage in broadcast or management frames as there is nothing going over the air without being encrypted to the specified encryption method.

Mutual Authentication avoids man-in-the-middle attacks. Intra-Cell blocking avoids data from one SU being visible to another remote station.

There are plenty more features related to data transfer management and link quality that are not directly affecting WORP but which are supported in WORP radios:

- VLAN
- Filtering and Access control
- Radius
- Bridging, Routing and NAT
- Secure remote management and quality monitoring
- Dynamic Frequency Selection (DFS), preferred channel, blacklisting and ACS
- Satellite Density and Cell Size
- Spectrum Analyser
- Antenna alignment

## WORP Functionality

### Broadcasts & Registration

In a WORP based system, the BSU acts as the traffic controller. For SU to recognize the system, the BSU transmits broadcasts. These broadcasts occur frequently, at least every 150ms or faster as configured.

The BSU only broadcasts to SUs that have the same encryption key, network name and BSU name.

A station that wants to join can do so as soon as it sees the BSU's broadcast. When the set maximum number of SUs has registered to the BSU, the broadcasts will stop until a SU deregisters.

Registration and mutual authentication is based on MD-5 using a shared secret. Bandwidth negotiation for a specific SU occurs between the SU and BSU to perform bandwidth management. For every registered SU one bridge port number is allocated, up to a 250 maximum.

### Polling Satellites, Request for Service and Dynamic Scheduling

The BSU will poll each SU regularly, minimally every 4 seconds (sleep mode). When a SU has new data, it will request to be polled immediately if it was not polled since the last broadcast as soon as it sees the BSU broadcast.

The BSU schedules the SUs for polling dynamically based on the amount of data waiting to be sent to each SU to optimize the use of the available bandwidth.

### Windowing, Retransmit and Timeout

Data is sent between SU and BSU with an incrementing sequence number, and every frame is acknowledged. New data is sent immediately even if the "window" of sequence numbers is not yet filled. Bottom of the window is the last acknowledged sequence number.

Retransmission only occurs when several frames have been sent for which no acknowledgment has been received. Retransmission is done selectively on the missing frames only.

Timeout and discard happens when data is too long in TX queue: (more than 1.5 sec with a max buffer size of 512 frames) and when data is too long in retransmit queue (16 entries) with timeout dependent on the radio data rate and the number of Subscriber Units registered.

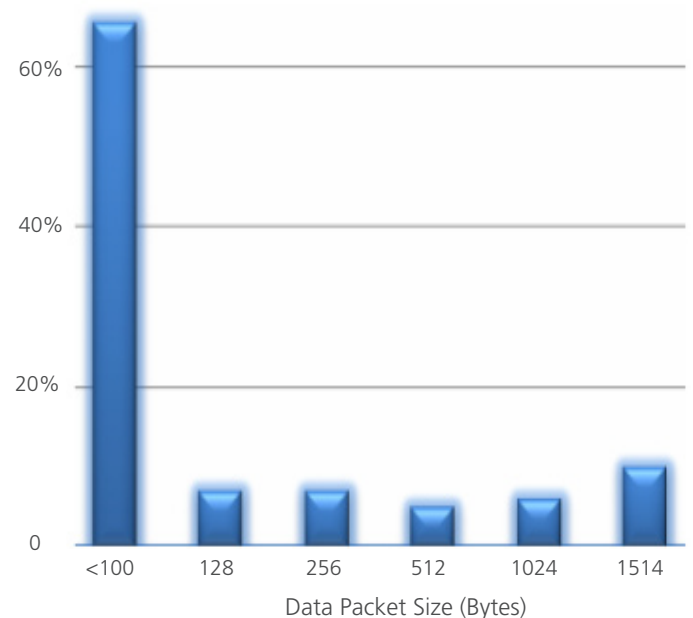
### Throughput, Super-Packeting and Fragmentation

In a network environment, maximum performance will be achieved when the frames have data-packet sizes are of 2304 bytes. Ethernet packets have maximum 1514 bytes. Generally 60% of IP messages are short (<100 bytes). These short frames impact the effective throughput.

WORP uses super-packeting and fragmentation to improve the effective throughput of the system by minimizing the overhead.

With super-packeting, WORP puts multiple packets into one frame. Fragmentation splits packets over two frames.

Graph shows the short frames impacting the effective throughput



### Encryption

All WORP communication is sent in data frames, so every piece of information is always sent following the configured encryption type.

## Bandwidth Control

The network service provider can limit (throttle) the bandwidth that each customer is allowed to use. This is accomplished in the Subscriber Units. Bandwidth control can be configured per SU-BSU link. It is asymmetric, upstream and downstream can be configured independently, so the service providers can provide various service offerings to their customers.

Bandwidth control is a security mechanism for the ISP. It guarantees fair sharing of the available bandwidth over the active systems, so one single SU cannot completely consume all the bandwidth in the system.

Bandwidth control is able to set the Maximum Information Rate (MIR) but not the Committed Information Rate (CIR). Bandwidth control can be configured in 2 ways: static in each interface on the SU and BSU or centrally via a Radius Server.

## WORP Security

WORP offers a variety of security features for securing data in the network. First, the protocol is not publicized or standardized, which makes it less vulnerable for hackers than any standards based system. Secondly, WORP requires the SU to register on the BSU to do a mutual authentication with identification via a MD-5 secret string. Both know that their peer belongs to the network (avoiding both rogue SU and BSU). Additionally WORP uses 128-bit or 256-bit encryption using WEP+ with weak key avoidance to encrypt the data being sent. Fourth, Access Control (authentication) occurs locally and via Radius server.

Finally, all remote management methods are password-protected. Different passwords can be set for SNMP read, SNMP read/write, Telnet and HTTP.

## About Proxim

Proxim Wireless Corporation (OTCQX: PRXM) (PINKSHEETS: PRXM) is a leading provider of end-to-end broadband wireless systems that deliver the quadruple play of voice, video, data and mobility to all organizations today. Our systems enable a variety of wireless applications including Point-to-Point Wireless Backhaul, Security and Surveillance, VoIP, Last Mile access, and Enterprise LAN Connectivity. We have shipped more than 1.8 million wireless devices to more than 235,000 customers in over 65 countries worldwide. Proxim is ISO 9001:2000 certified. Information about Proxim can be found at [www.proxim.com](http://www.proxim.com). For investor relations information, e-mail [ir@proxim.com](mailto:ir@proxim.com) or call **+1 413-584-1425**.

Proxim and Tsunami are registered trademarks of Proxim Wireless Corporation in the US Patent and Trademark Office. All other products or services are the property of their registered owners.

Proxim\_WP\_WORP



**Proxim Wireless Corporation**  
1561 Buckeye Drive, Milpitas  
CA 95035, USA