White Paper

Proxim AN SRA COMPANY

Technology Overview

Wireless Outdoor Router Protocol (WORP®)

Wireless Everywhere – Connecting the Internet of Things

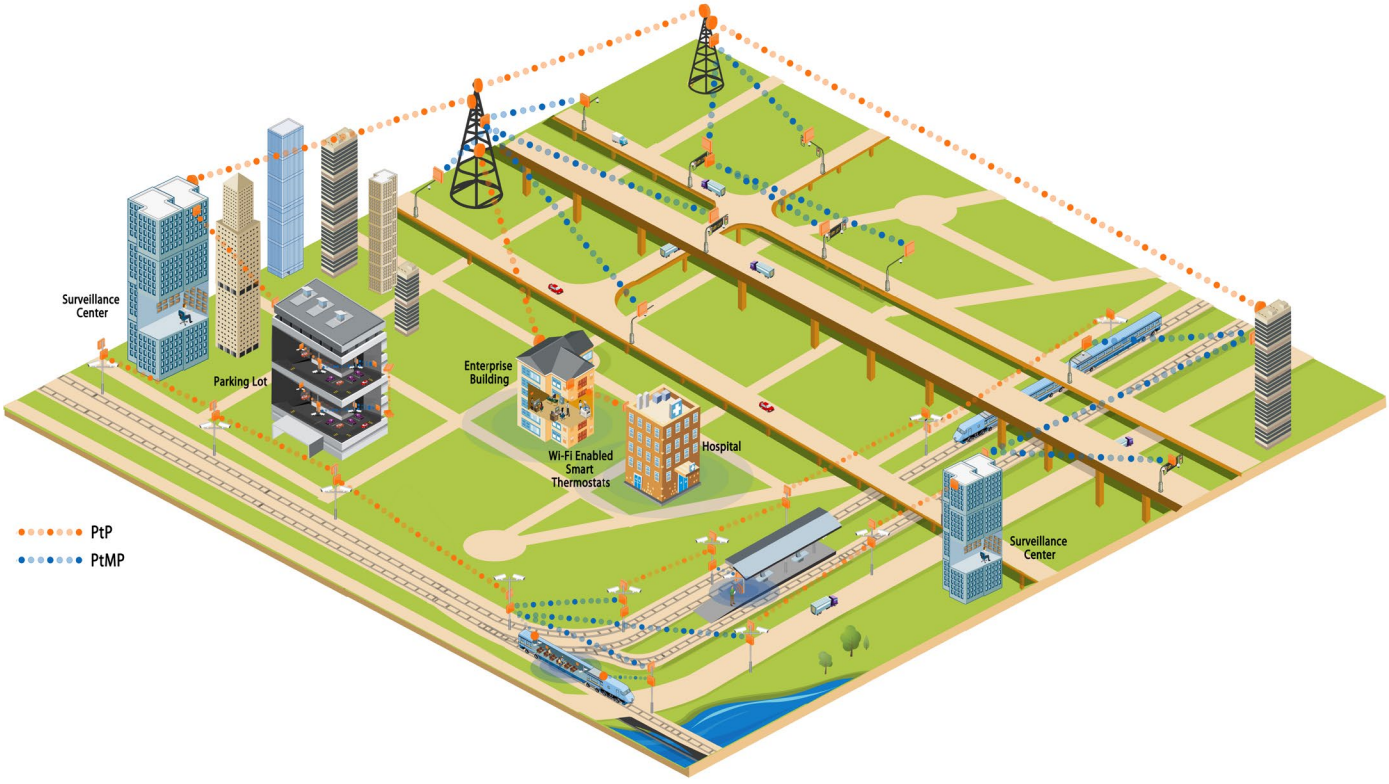
proxim wireless

Introduction

Over the past 20 years wireless has become an integral part of everyday life. The number and types of wireless networks and applications has also blossomed, moving far beyond original point to point microwave links or large tower cellular networks. Today wireless exists in a mind numbing array of standards from Wireless USB, ZigBee™, and WiFi to GSM, 3G, WiMAX and LTE. In between lay dozens of additional applications and protocols.

When we look at last mile access, connections covering from the edge of the WAN or Internet to the individual or device, leaving aside point to point implementations, these networks can be broken down into two main categories:

- Wireless for People (WFP) – Direct communications between a person via a personal device (phone, tablet, PC, camera, music device) and the internet or other networks.
- Wireless for Things (WFT) – Connecting not only machines (video cameras, remote monitoring devices, ITS systems, macro Base Stations or small cells via backhaul) but buildings, power grids, homes, Intelligent Transportation Systems (ITS).



Many of the Wireless for Things deployments are also used extensively in Enterprise applications. Private networks within a domain such as a multi site company, health care/hospital complex, military and banking are examples.

Each of these applications, Wireless for People or Wireless for Things, have distinct requirements and capabilities designed into them at the Physical Layer (PHY), Media Access Control (MAC) and even network level to meet the unique criteria necessary for the application.

WFP is well served by 3G/4G mobile broadband technologies such as UMTS, WiMAX or LTE in the Metropolitan Area Network (MAN) and in the Local Area Network (LAN) by WiFi. These technologies have strong standards, large ecosystems and well un-

derstood requirements – coverage, capacity, ease of use, and mobility or portability. In addition today and going forward there is a great deal of work being done to blend the WFP protocols together such that a person or device can access any available network dynamically. In the end, the user is just simply connected.

In contrast, WFT generally have no standards, devices are fragmented based on specific applications, and WFT has very different requirements when compared to WFP– efficiency, latency, security, and flat networks. When choosing a solution for this segment, a deep understanding of the PHY and even more importantly the MAC will reveal stark differences between systems and vendors. Differences that manifest themselves at the application layer with pixilated, jerky video or the number of users the available capacity can support. Table 1 summarizes the differences in requirements between Wireless for People and Wireless for Things.

	Coverage	Mobility	Throughput	Efficiency	Latency	Core complexity
Wireless for People	100%	Required	5 to 10Mbps	50%	30ms to 100'smsec	High- $$$
Wireless for Things	Targeted	Some applications	100's of Mbps	85% and up	10ms guaranteed	Low -$

Table 1 - Wireless Application Requirements and Performance

Proxim, a leader in advanced outdoor wireless systems, has developed over the course of the past eleven years a protocol specifically aimed at the universe of WFT, optimizing and improving over that time to deliver the most efficient, most robust and field tested protocol available in WFT - Wireless Outdoor Router Protocol (WORP®).

Wireless for People

It is clear the intent and hence requirements for WFP networks are substantially different from those driving WFT systems. The top line requirements for WFP systems are:

- Connectivity
- Mobility or Portability
- Performance – throughput

WFP can be further broken down into MAN and LAN segments. MAN is addressed by mobile broadband technologies such as UMTS, CDMA2000, WiMAX and LTE. The LAN is now dominated almost exclusively by 802.11 or WiFi. However as is shown below, with some rare exceptions (e.g., meter reading, RFID tags, etc…) each of these fails when applied to WFTs, whose applications and requirements were never considered during development.

Mobile Broadband

Mobile Broadband delivers on all three key requirements on a wide area basis, and the coverage is global. WiFi while providing the 3 features above also adds open and easy access, and deployment by anyone anywhere by virtue of it's operation in license exempt frequency bands and the de-centralized access control.

However each of these fails when applied to the WFT world. Mobile Broadband systems have several flaws in this application. WFT needs high efficiencies, low and consistent latencies, and simple flat core network architectures. In contrast Mobile Broadband systems suffer:

- Low Efficiencies – There is a tremendous amount of signaling needed to support hundreds of users per cell with seamless mobility, and do it at speeds up to 300km/hr. This coupled with legacy signaling embedded for voice, applied to data and new applications results in IP packet throughput for these systems at ~50%.
- High and Variable Latencies – When carrying IP data, 3G networks have latencies ranging in the hundreds of msecs, and even LTE struggles to control jitter with latencies on data payloads being variable and ranging from 30 to 40ms all the way up to 100ms and more. Performance that is ill suited for example in carrying video streaming traffic cost effectively.
- Complex, Hierarchal Architecture –UMTS/LTE networks require substantial core elements before the first "Thing" can be connected. While necessary to support true mobile broadband efficiently, these complex cores add no value to the universe of WFT instead increasing the cost for the Radio Access Network core.

WiFi

WiFi when applied to the WFT universe also suffers from several serious challenges such as poor efficiency little latency control and the network crippling hidden node effect.

- Efficiency – WiFi suffers from low efficiency and even poorer scalability. Maximum IP packet throughput in an 802.11a 54Mbps network with a single user is ~25 to 30Mbps. With as few as 5 total users on the network aggregate throughput is reduced to even less. When considering an 802.11N solution in a 2x2 MIMO, 40MHz channel configuration with a raw over the air data rate of 300Mbps the results are similar. In this case the maximum IP throughput equals 173Mbps (out of 300Mbps raw) for a single client and as little as 72Mbps aggregate for 8 clients. Table 2 summarizes these results.

802.11 Mode	Raw Over the Air Data Rate	Single Client Effective IP Throughput/Efficiency	8 Client Effective IP Throughput/Efficiency
802.11a	54Mbps	25Mbps/46%	12Mbps/22%
802.11n	300Mbps	173Mbps/58%	72Mbps/24%

Table 2 - 802.11 Efficiencies

- Latencies – WiFi has never been designed to address real time traffic in anything but a best effort, throw more Mbps at the problem approach. Hence there is minimal control of latencies and certainly no jitter control in a WiFi network. As the networks become more loaded latency increases and throughput decreases rapidly. For WiFi deployed in a Mesh topology, latency control is extremely difficult as the path through the mesh network to the internet connection or other devices changes dynamically.
- Hidden Node – WiFi networks rely on de-centralized control of access to the medium – Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). For this approach to work each client must be able to "hear" all the other clients in the network. In a typical WiFi scenario this is not an issue as individuals and their devices are using omni or 360 degree antennas.

For WFT, the locations of the client devices or Subscriber Units can be on the side of a building, or in the opposite direction 2 miles from the other clients, or deployed in several other scenarios which end up breaking this requirement of all clients being able to hear each other. The result has clients constantly trying to access the network when they think it's clear, only to interfere with other hidden client transmissions. This can result in very poor performance and in some cases a completely congested, useless network. Numerous studies exist which investigate the hidden node impact on a WiFi network and the attendant reduction in throughput.

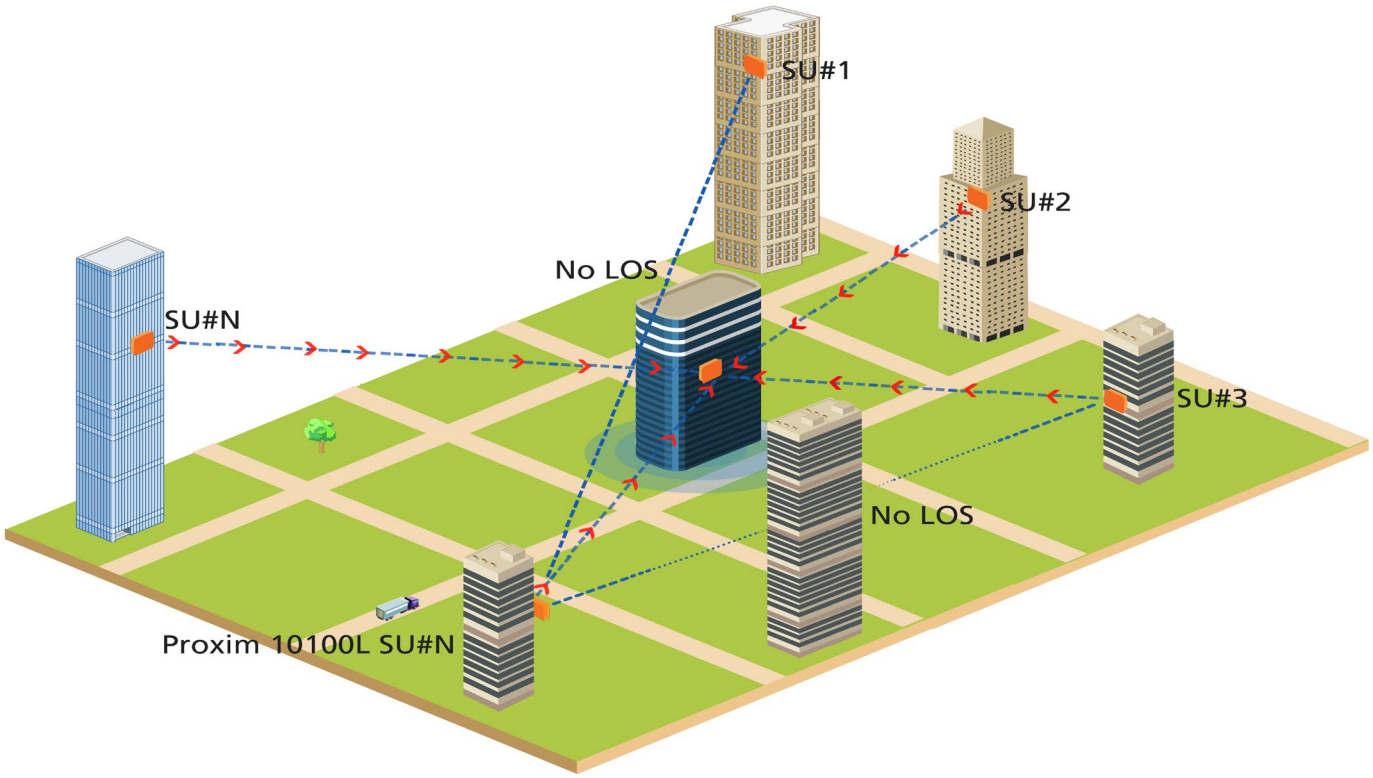


Figure 1 Hidden Node

Wireless for Things – Wireless Outdoor Router protocol (WORP®)

It is clear from the above descriptions that Mobile Broadband and WiFi technologies have serious issues when applied to WFT. What is needed is a robust, field proven protocol that has been designed from the ground up to address the unique and difficult requirements presented in the application space of WFT. Proxim with over 10 years and hundreds of thousands of engineer hours invested has such a protocol – WORP®.

- Efficiency – WORP® is 85% efficient on average. For a standard 20MHz channel with a raw capacity of 78Mbps (16QAM 3/4, 2x2 MIMO) WORP® delivers 72Mbps of actual use able data for an efficiency of 92%. Even more importantly, WORP® throughput performance scales. Whether it is one client device or SU or 50, WORP® ensures the aggregate capacity is never less than 80% of the available raw physical data rate. This is achieved with via several methods including fragmentation and super packing. This can be compared to the efficiency of the 802.11 MAC noted previously.

- Latencies – WORP® can enforce QoS in terms of latencies, and in some cases more importantly jitter, on an SU by SU basis as opposed to the same QoS for all SUs connected to the BSU. When supporting video traffic, throughput is required but small jitter is also of critical importance. Tests with 802.11 for a network with moderate use will see latencies in the 20-75msec range. If the network is loaded in terms of traffic or number of clients this can rise to the hundreds of msecs. In contrast WORP® maintains latencies under 5msec for a small number of Subscriber Units, up to 40-50msecs for a network with as many as 40 Subscriber Units.

- Hidden Node – Unlike WiFi, WORP® is a centralized radio resource management MAC protocol. The approach to bandwidth allocation and admission control via a polling mechanism is similar to WIMAX but without the high overhead. This means the BS is in control of all devices accessing the wireless medium. Not only is this one of the core reasons for WORP®'s efficiencies and QoS support, but it also ensures the hidden node problem is not an issue. As a result WORP® networks are

among the most efficient, precisely controlled and managed wireless networks. WORP®'s centralized management at the Base Station controls all nodes.

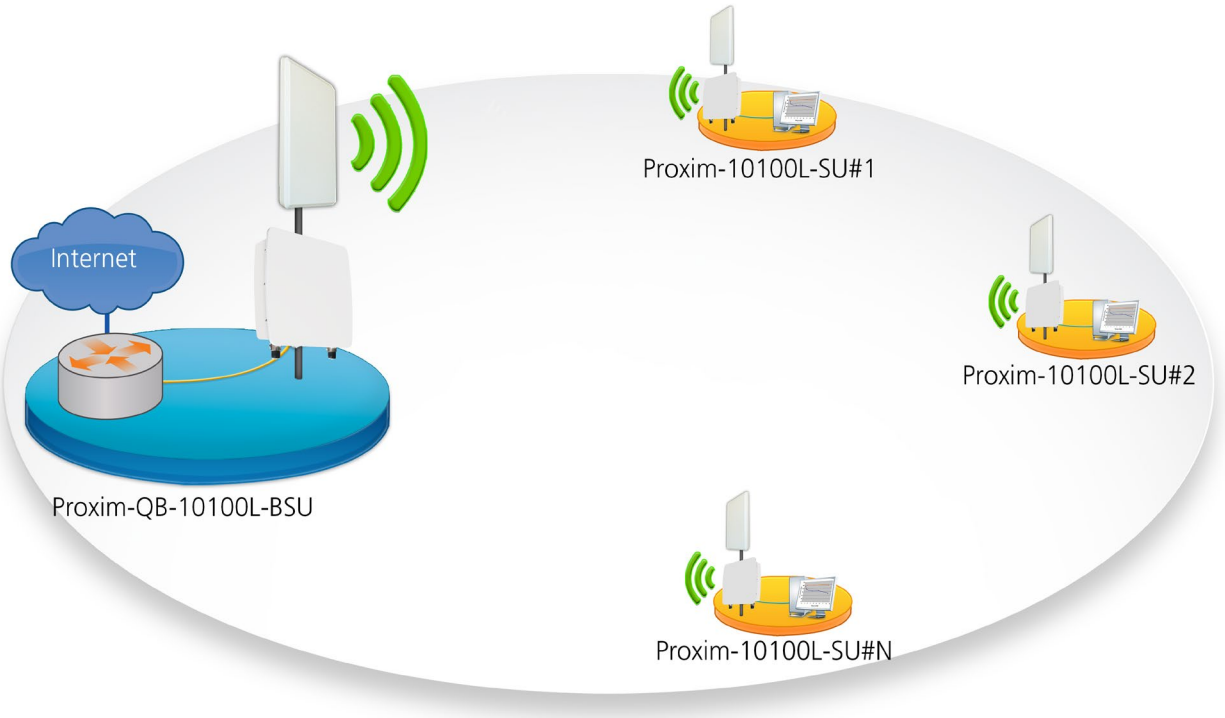


Figure 2 - Proxim Infrastructure

- Flat Core – Unlike UMTS or LTE deployment of a Proxim wireless network with WORP® requires no expensive core elements. The BSU connects to an aggregation router or a switch for an Internet connection and that's it. This results in backbone infrastructure for a Proxim network costing ~$200 to $1000.

In contrast an Evolved Packet Core (EPC) needed for even the smallest of LTE RAN networks deployed is considerably more complex driving not just CAPEX but over the long runhigher OPEX. Figure 3 below shows the key EPC elements – the Mobility Management Entity (MME), Serving Gateway (SGW), PDN Gateway (PGW), Home Subscriber Server (HSS), and Policy and Charging Rules Function (PCRF) server.

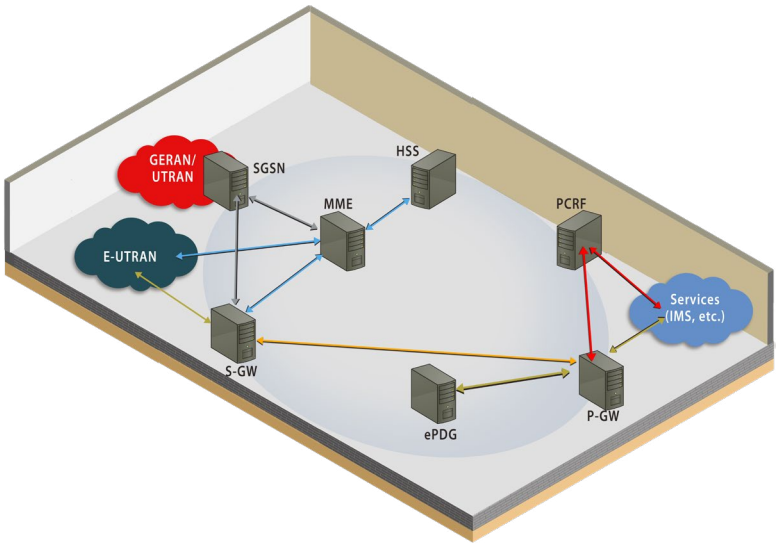


Figure 3 - EPC Infrastructure

Ten Years of Development

MAC protocols in wireless networks are inherently complex. Creation, development, testing, deployment and fine tuning can take years. Indeed the 802.11/WiFi MAC is now 20 years old and is still being updated. UMTS and even more so LTE spent between 5 to 10 years in the lab before being robust enough for commercial deployment.

Each of these (WiFi, UMTS, LTE) not only spent years being developed and deployed, but there was a huge ecosystem of engineers and money supporting and working on the problem.

When working in the world of WFT, there is no standard and as such each company serving this space has been forced to develop their own. Many simply use the WiFi MAC in this application and suffer the consequences noted above – poor efficiency, high variable latency and the hidden node. This is not surprising; it takes huge expenditures and time to develop a robust, efficient protocol that meets the WFT requirements.

Only Proxim offers to the market WORP®, a protocol designed from the ground up for WFT. Over the years Proxim has not only solidified a very robust MAC, but has added improvements over time that make WORP® stand apart:

- ARQ – Automatic re-transmission request delivers improved reliability and robustness to the RF link. ARQ compensates for the use of TCP in a wireless domain. When TCP detects a lost packet, it assumes congestion (it was designed for a wired network), backs off accessing the network medium, and implements a slow start algorithm for the next network access attempt. A small amount of interference, 2-5%, can result in up to a 40% throughput reductions. By automatically detecting corrupted or lost packets at the PHY layer, ARQ in WORP® ensures every packet delivered up the OSI stack to the TCP protocol is valid and TCP never implements the back-off and slow start algorithms.
- DDRS – Dynamic Data Rate optimizes each link between the BSU and SU for maximum capacity based on signal conditions. This is done in real time on a packet by packet, SU by SU basis. Each RF link will have the optimal modulation and error correction based on signal quality metrics.
- QoS/CoS – WORP® has implemented QoS with a goal not just to limit bandwidth or Maximum Information Rate (MIR) but to ensure latency and jitter requirements of a given application can be met. WORP® can enforce latencies as low as 1 – 2 msecs, ranging up to a maximum of approximately 15msecs based on frame size and 50 msecs for a densely populated network. Moreover QoS/CoS can be enforced on a link by link basis with a base station's coverage zone and deliver up to 32 different classes of services depending upon the need. VoIP, Real-Time HD video streams and non-real time traffic can all be mixed within the same BSU's coverage zone.
- Security – Not just AES256 but FIPS 140-2. For those applications where top level security is needed, support of FIPS is a must. WORP® is currently being used in several DoD applications where security is not a feature but a must have.
- Roaming and Mobility – For those applications such as video backhaul from a train, the ability to hand traffic from one BSU to another is required. WORP® supports this ability, which is similar to mobility, but without sacrificing the efficiency that is so central to it's core value.

As impressive as WORP® is today, Proxim continues to improve and evolve the protocol with new capabilities such as application optimization for backhaul and video surveillance. With ten years, thousands of man hours and tens of millions of dollars in investment, WORP® stands head and shoulders above WFP systems as well as competing protocols when addressing WFT.

Summary

The World of Wireless tends to focus on delivering connectivity to people. While this certainly is incredibly important, it completely ignores the needs and applications when connecting "things" over wireless. When choosing what system to deploy for

video backhaul, small cell backhaul, enterprise Internet Access or dozens of similar applications in the wireless world of things, the choices are clear:

Use a Mobile Broadband technology with it's high cost and poor performance, or implement an 802.11 solution with again poor performance and even more challenging the hidden node problem.

Or you can choose to deploy a protocol conceived, designed and delivered to meet the needs of the World of Things – WORP®. No other proprietary protocol on the market has been deployed as long, and had the number of engineer hours poured into it (over 200,000) making it by far the best and most robust solution for WFT. When choosing your outdoor wireless solution, remember what your key requirements are and choose the best solution for your networks – WORP®.

About Proxim

Proxim Wireless Corporation (OTC Markets: PRXM) provides Wi-Fi®, Point-to-Point and Point-to-Multipoint 4G wireless network technologies for wireless internet, video surveillance and backhaul applications. Our ORiNOCO® and Tsunami® product lines are sold to service providers, governments and enterprises with over 2 million devices shipped to over 250,000 customers in over 90 countries worldwide. Proxim is ISO 9001-2008 certified. For more information, visit www.proxim.com. For Investor Relations please contact us at InvestorRelations@proxim.com.

Proxim_WP_WORP®

Proxim AN SRA COMPANY
www.proxim.com
Proxim Wireless Corporation
47633 Westinghouse Drive,
Fremont, CA 94539, USA