Economic, social development and revenue generation are a few of the motivations behind city and municipal government broadband access deployments for city employees, residents, employers, and visitors. Municipal wireless networks have grown 134 percent and will double as municipalities are expected to invest nearly $700 million over the next two years to build wireless networks while current industry statistics indicate that the growth in wireless networks is accelerating. At the top of the list is the ability to improve a cities competitiveness enabling new social and business opportunities, worker productivity, IT and related communications cost savings, as well as public safety including police, fire and emergency services.

Municipalities are finding that it makes sense to be the service provider for their residents and businesses, unable to attract a service provider to a given area or due to disagreements in pricing, franchise fees or other concern, the city builds, owns and manages the infrastructure, determines who will have free and paid access. The city may offer services themselves as the service provider, or wholesale parts of the network to another entity, however, this depends on the personnel and financial resources of the city. Typically the city will own and manage the infrastructure, charging fees to any broadband service provider that wants to offer service in a particular area. Interestingly enough, some municipalities, even when they have highly desirable markets to offer the local carrier, are now taking control of their own communications services to ensure that all constituents have equal access to vital information services.

The focus on municipal networks stems from goals and mandates to provide:

- New communications and services including competitive, low-cost, dedicated and opportunistic Internet access
- Provide response-critical data access to first responders, reduce crime and secure critical infrastructure
- Improve communication efficiency and responsiveness of public workers
- Instant ad-hoc network setup for emergencies and events, monitor automobile traffic flow, location based dispatch, vehicle video security
- New economic opportunities and make the city a destination of choice for businesses, residents and visitors
- Services addressing the digital divide
The following table of contents should assist you in the navigation of this document. While this version is focused on the needs of specific municipalities, this is considered a “living” document and will be updated with new information our customers worldwide provide input and as the need arises.

INDEX

1. Corporate Overview

2. Introduction

3. Empowering Municipalities

4. Three Approaches to Wireless

5. Mesh Network Evolution

6. Municipal Questions
   a. RF Interference
   b. Health Concerns
   c. Towering Issues

7. Delivering Wireless Mesh Networks

8. Applications over Mesh Networks

9. Comparing Technologies

10. Dynamic Mesh Architecture

11. Security and Wireless Networks

12. Business Models for Consideration

13. Strix Systems Solution
1. Corporate Overview

Strix Systems is the worldwide leader in wireless mesh networking. Strix Access/One® products are the industry’s only modular and most scalable mesh platform, delivering the largest capacity, highest throughput and lowest latency. This new generation of product was specifically designed to support high quality voice, video, and data in both fixed and mobile applications in large-scale deployments. Sold globally to service providers and municipalities in conjunction with its partner ecosystem, Strix Access/One solutions have been deployed in hundreds of networks worldwide, outdoor and indoor, in metro, public safety, government, homeland security, medical, energy, industrial, transportation, hospitality, education, enterprise, and residential markets.

Strix Systems’ market leadership is derived from the strength of its products and by Strix commitment to enable the success of its municipal and service provider partners. According to market research firm Heavy Reading, Strix Systems held the number one market share of wireless mesh network radio shipments during 2005, with over 16,000 radios shipped. The company’s growth continues in 2006 with a projected four-fold increase in shipments.

Strix 3rd generation multi-radio mesh networks are being deployed globally in a number of countries and in a variety of applications. Notable examples of Strix deployments include: 187 square miles of contiguous municipal networks in Tempe, Chandler and Gilbert, AZ; citywide deployment in Chittagong, Bangladesh, a city of 3.5 million people, where initial deployments will serve an estimated 200,000 voice subscribers; rail system video surveillance in Mumbai (Bombay), India; Beijing Public Security Bureau supporting mobile command vehicles, public Internet access and 2008 Olympic venues, Beijing, China; and high speed internet access in Kenya’s 4 largest cities. Strix is working with partners to provide high speed Internet access on trains in a number of projects in the US and overseas and recently announced, Strix Systems was selected by NTT West to deployment of wireless mesh services to 100 cities and over 50 million people in Japan.

The Company

Strix Systems is headquartered in Calabasas, CA, with offices in North America, EMEA and Asia Pacific.

Founded in 2000, the company is led by an experienced management team headed by Bruce Brown, CEO: previously CEO Efficient Networks (acquired by Siemens in 2001), CEO Vertel and President ADC Fibermux. Investors include Palomar Ventures, El Dorado Ventures, UV Partners, and Crosslink Capital. With a capitalization of $60M, Strix is projecting a fourfold increase in revenues in 2006 and continued substantial growth beyond.

Mission

Not just an equipment provider: Strix Systems goal is to make our municipal and service provider partners successful.

Strix 3rd generation carrier-class wireless mesh platform has been designed from the service provider perspective: to support multi-service business models, to make deployments easy and to make them cost efficient. This best-of-breed wireless mesh platform is coupled with the industry’s finest tier 1 professional services and an ecosystem of SI and application partners to comprise Strix top to bottom approach. The Strix management team has pioneered the municipal WiFi market and is ready to assist municipalities and service providers in the full range of planning, footprint acquisition, design, and deployment undertakings.
Strix is a company that municipalities and service providers can depend on.

“Tempe was the first city to roll out its wireless mesh network, and Strix played a strategic role in enabling that to happen,” said David Heck, Deputy CIO of the City of Tempe. “Strix engineering talent and dedication meant that the city was able to bring up its network quickly and expand it beyond Tempe.” “Planning and deploying wireless mesh networks in four large cities is a massive undertaking,” said Dr. Kai Wulff, Managing Director of Kenya Data Networks. “Strix support capabilities, plus its ability to help us determine a deployment roadmap as we expand throughout Kenya, were thus major factors in our decision to work with the company.”

Enabling Successful Deployments and Business Models

The Strix Systems platform advantage

Successful municipal networks must be capable of supporting multiple services in a rapidly evolving market; maximizing revenue, minimizing cost, and incorporating new technologies over a 5 to 10 year time horizon. The ability to support the rapid growth in voice services and multimedia video streaming in addition to enterprise-class data applications is essential. Furthermore, field upgradeability to accommodate subscriber density fluctuations, radical changes in service mix (e.g., cellular convergence) and new technology is critical to the success of the network.

Strix Access/One platform is designed to meet all these needs. The platform is based on the Strix DMA™ (Dynamic Mesh Architecture) and patented design: a layer 2 switching architecture with multiple radios available for subscriber access and 2 radios dedicated to backhaul. This 3rd generation architecture, unique in the industry, provides the robust high quality transport to carry voice, data and video traffic for up to an unparalleled 10 hops with minimal latency and little reduction in throughput. By contrast, first and second generation single and dual radio platforms are incapable of carrying traffic for more than a few hops without significant reduction in throughput and high latency. The Strix architecture has been incorporated into the product family of carrier class outdoor products, enterprise products and CPE.

Strix Access/One is the industry’s most cost effective wireless mesh platform delivering up to 3x more radios per square mile at a lower overall cost (TCO) than any other system.

The platform is deployed in mesh sectors of up to 100 nodes (up to 600 radios) covering 4 or more square miles from a single Internet backhaul location. This materially reduces site acquisition time, cost and complexity, substantially reduces time to market and results in the industry’s lowest TCO. No other platform can match this capability.

The industry’s only modular (chassis-based) system: delivering the largest capacity, highest throughput and lowest latency to support voice, data and video applications.

Strix OWS is field upgradeable to 6 radios in a compact chassis with a variety of antenna options. Up to four radios can be dedicated to subscriber access: thus enabling a substantial increase in in-building penetration (with sector antennas) and supporting a 3x increase in subscriber density. In addition, the introduction of new technology (WiMAX, 4.9GHz) is easily accomplished, without a fork-lift upgrade.
The Strix platform has been tested in large scale deployments such as Tempe, AZ (40 square miles, 800 nodes, over 3000 radios) and by independent test labs (Iometrics). These tests conclusively show Strix as the industry’s best performing wireless mesh network platform; maintaining a throughput of 35 Mb/s over multiple hops, supporting substantial VoIP call volumes with excellent quality ratings (MOS=5) in the presence of high-bandwidth data. In addition, mobility handoff is below the 50 millisecond delay stipulated by telecom operators, thus enabling full mobility as well as high speed rail deployments exceeding 200 mph.

The platform is designed for zero-configuration and scaling for country-wide deployments. Easily managed, Strix graphical and command-line interfaces (CLI) enable quick visual management and detailed statistics to provide complete network awareness. Strix products provide hardware-accelerated automatic AES encryption between wireless nodes and WiFi Protected Access 2 (WPA2) security for client access.

**Technology leadership**

Strix Systems delivers the industry’s highest performance: based on Strix DMA™.

**Meeting the need for real-time applications and scalability**

“We chose the Strix solution because we saw the high throughput and low latency the system offers across large networks,” said Dave Heck, Deputy CIO for the City of Tempe. “After evaluating the Strix Access/One OWS installation proposed for Tempe, it was clear that this system could scale while maintaining the levels of throughput needed, keeping latency low enough to support real-time applications.”

**Future Convergence**

With the introduction of WiFi phones and dual-mode Cellular/WiFi phones, the increased use of video surveillance and other video and interactive multimedia content, convergence is just around the corner. Strix Systems is uniquely qualified to address the converged services opportunity with its robust high performance architecture that enables true multi-service broadband access with 100% reach-ability and 100% mobility without boundaries.

Successful worldwide deployments prove Strix technology leadership and top to bottom approach. Strix is committed to enabling the success of its municipal and service provider partners.

Strix Systems, your partner in success!
2. Introduction

WiFi has captured the attention of the mainstream consumer and is now recognized as a viable, effective and complete solution for municipal, city and even country-wide networks. Businesses across all vertical markets have recognized the tremendous operational benefits enabling their employees with wireless laptop and hand-held access to data, voice over IP (VoIP), instant messenger, online collaboration, video and more. Now business and residential users alike are accustomed to the ability to travel anywhere and get connected at any time. With the increased market momentum and successful deployments announced on a regular basis, wireless is and will continue to extend to even larger coverage areas. Moreover, global-scale wireless networks define the future of “next generation networks”.

The advent of wireless “mesh” network technologies, the economics, mobility and reach-ability enable new opportunities to close the gap on the digital divide while enabling improved productivity and new revenue streams.

Mobility – Today’s wireless communications enables increased mobility allowing you to stay connected to the data, applications, and tools to meet critical company and customer requirements. While wireless/cellular technologies have failed to provide the bandwidth, throughput, robustness and feature-fullness that broadband wireless mesh can offer. Wireless mesh networks enable workforce mobility for timely access to critical business resources which means increased productivity, improved decision-making, and accelerated customer responsiveness.

Reach-ability – Wired networks are inherently limited by the economics of reach-ability. Today’s wireless mesh networks extend the reach of network applications, whether for voice, video or data, technical innovations have introduced multi-radio wireless mesh network architectures that deliver on a broad-scale. For hot-zones, city-wide or entire countries, today’s generation of wireless mesh networking enables reach-ability without limits.

Digital Divide – A significant line is drawn between those that have future growth opportunities and those that do not. It’s called the digital divide. It has an immediate and profound effect our U.S. economy and our ranking as a nation of technology innovation shaping the world. From a 2002 Workforce study, “The Digital Divide is not just about access to technology,” says Robert Caret, President, San Jose State University, and a Joint Venture: Silicon Valley Network board member. “It’s about access to education and careers.” While all ethnic groups and genders are increasing their Internet access and use, the gaps continue to widen.

Economics – wireless mesh networks minimize the expense of leased facilities removes the number of wired backhaul lines while providing increased coverage and greater capacity versus any other technology. Wireless mesh takes full advantage of existing network resources, reducing costs where they would otherwise increase over time due to an increased number of users coming on-line without adequate revenues to cover the cost of backhaul access. Wireless mesh networks deliver service at a fraction of the cost of any other solution which provides coverage to municipal, suburban and rural areas while it enables incremental deployment and profitability.
3. Empowering Municipalities with Wireless Mesh Networks

Wireless “Mesh” takes the capabilities of enterprise-class WiFi with security and QoS (Quality of Service) and makes the network accessible throughout large-scale areas, extending business, residential, public safety, government and other applications well beyond traditional boundaries. Instead of utilizing point-to-point and point-to-multipoint wireless devices for limited connectivity to specific locations, wireless mesh networks are sophisticated self-configuring, self-optimizing and self-healing making it possible to deploy extremely large-scale, intelligent, high speed networks with predictable performance. Such capabilities enable high densities of users and sophisticated applications such as fully automated aircraft taxiing control and baggage handling as well as the transport of high-bandwidth video surveillance and alarm controls, which, due to wireless mesh networks, all become a reality. More importantly, predictable performance and scalability also means that services such as mobile roaming can be supported. Today, trains capable of reaching speeds over 150 miles per hour deliver high-speed internet access to business travelers while in transit. Mobile roaming also enables police, fire and emergency medical personnel with the ability to access critical information transmit medical monitoring data, gain access to video surveillance from any location, and share investigation details at the scene of a crime. WiFi is no longer restricted to any boundaries and enables fast, secure, communications and is capable of covering vast distances and all sorts of terrain.

In contrast to wireless mesh networks, traditional technology choices impose serious limitations impeding their effectiveness. Cable modems and DSL can provide high speed broadband services to specific communities, but there are no provisions for mobility or the less fortunate who can not afford these services. Additionally, municipalities need city-wide network access for their own purposes which would be cost prohibitive if acquired through a carrier. Cellular data offerings remain bandwidth limited although carriers have promised higher speed services in the future. Existing issues remain with quality; coverage and capacity which have lead some to examine alternative forms of communications for emergency and catastrophic situations. It’s therefore
questionable whether or not the future for carrier wireless services, given their existing strategic technologies, are capable of supporting the required emerging and critical applications.

Today, wireless mesh networks enable citizens and businesses the low-cost mobile broadband solution access they desire. It enables greater productivity, improving the efficiency of municipal workers and enabling seamless communications for first responders and emergency services during crisis situations. Low cost, widely available broadband Internet access creates new opportunities for municipalities by improving communications, responsiveness and the quality of services delivered by local government to their constituents. Police, fire, emergency response, e-government, and public works are some of the areas where improved communications and efficiencies are needed. Widely available network access and services provided by local government enables greater opportunity for economic development and helps close the gap on the digital divide.

Nationwide, municipal police, fire and EMS departments have been among the first to adopt metropolis WiFi mesh networks. High-speed, in-field data access dramatically improves police officer effectiveness and efficiency by getting critical information in their hands on the street. Once the networks are installed, many municipalities find new uses, ranging from building inspection and automatic meter-reading, to collaboration for large-scale public events and public safety command-center operations.

- Public WiFi Access: Municipal-wide wireless mesh networks bridge the digital divide and drives economic development
- Public Safety: Wireless mesh networks provide reliable and resilient remote access for first responders (police, fire, EMS)
- Municipal Applications: Wireless mesh networks enable remote worker connectivity, automated meter reading and unattended wireless sensor communications for water, gas and electricity.
- Fixed and Ad-hoc wireless: Wireless mesh networks are flexible and enable point-to-point, point-to-multipoint, completely mobile and ad-hoc network communications where needed without limitations.

4. Three Approaches to Wireless

As deployments of standard and hardened single radio access points for hot spots and hot-zones signaled the start of the wireless mesh networks revolution, the previous implementations were primarily focused on basic connectivity due to performance limitations of those architectures. Scaling a large wireless network with this technology was not possible and as a result there was little acceptance of wireless in places other than homes, hot spots and businesses. So as the technology has matured, there have been three generations of access point technology and three generations of wireless mesh networking technology.

The first approach was a centralized network model—an unintelligent network with independent access points (APs) wired to the same LAN. This first generation of access point technology
established a grass-roots movement which impacted the entire industry. Those devices, limited in
functionality, capacity, coverage and penetration, have been well suited for the home and small
business, however requiring the user be in close proximity to the devices.

The second approach was a centralized model—implemented by the majority of wired switch
vendors because it was the only option to bring wireless groups of people from the wired network to
their existing wired switches. The trend with this model was to strip the intelligence from the AP and
put it all on the switch; however, this approach introduces many undesirable effects (for example, a
single-point-of-failure, bandwidth bottlenecks, and a lack of scalability and flexibility). Furthermore, a
new switch must be purchased whenever APs are added and the port limitation of the existing
WLAN switch is exceeded. With both of these WiFi approaches, there’s one consistent fact—they
are not really wireless, just “less” wired. Ethernet to the AP is required. This approach is still used
today. These networks will be replaced or augmented by wireless mesh networks. Additionally, the
second generation of product has a one-to-one relationship to the wired network it attaches to.
These access points have been useful for enterprise applications where wired infrastructure exists.
Every access point connects to the network and then provides wireless access to an area in or
outside a building.

The third approach - an intelligent distributed mesh network—Introdued by Strix Systems, provides
distributed intelligence within each access point, or node. Capable of automatically establishing
secured connectivity between small to large numbers of multi-radio mesh nodes, Strix Access/One
is a self-configuring, self-healing and self-optimizing system that minimizes the effort required to
build even the largest mesh network. The “Mesh” is the dynamic relationship between multiple
nodes that have multiple paths to a given destination. In contrast to other solutions which require a
centralized “intelligent” gateway, each node makes decisions with regard to other associated nodes.
The nodes form a web, or blanket, of connectivity over large areas – such as cities. Active paths
are the primary connections which transport user and backhaul traffic. Passive paths are available
to immediately take over should there be any interference or condition which brings down a path or
node. The solutions provides the ultimate resilience for wireless broadband networks and with the
ability to provide sustained high throughput and low latency, mesh networks are capable of
reducing the ongoing costs of these networks. Designed properly, mesh networks are high
performance, reliable and redundant, and can be extended to include thousands of devices. This
type of network can be installed quickly and doesn’t require elaborate planning and site mapping to
achieve reliable communications. Simply moving a network node or dropping another node into
place can fix a weak signal or dead zone immediately.

5. Wireless Mesh Evolution

During this evolution from WiFi to wireless “Mesh”, several manufactures attempted to utilizes
single radio architectures and then use IP routing for managing network links. IP routing served two
purposes, to attempt to segment user traffic and reduce broadcast domains, while additionally
attempting to manage the sophisticated requirements of a wireless mesh network. This has met
with disaster as seen in many implementations which, to date, are still incomplete, but it’s important
to understand the limitations of the wireless mesh network approaches, which we refer to as
“generations”, specifically as it relates to the throughput and latency of a wireless mesh network.
1st Generation Wireless Mesh – *The single radio approach* – one radio switches between access and backhaul: The 1st generation mesh is considered the most basic of mesh networks and is the weakest approach to wireless mesh. Based on single radios, this limits client access and backhaul to a single radio with one channel. This immediately reduces performance by 50% per hop as a single-radio mesh architecture, one radio must constantly switch from performing backhaul ingress to backhaul egress to client access, thus introducing significant latency. This increasing latency directly impacts throughput so that a 54Mbps backhaul becomes 24Mbps at the next hop and then 12Mbps at the next hop. While these are theoretical throughput rates simple math shows that only limited throughput is available to each wireless client in this single-radio approach. For example, if you have 5 APs with only 20 wireless clients connected to each, with all APs and clients sharing the same 802.11b channel (5 Mbps), that equates to 50-100 Kbps per user-same as a dial-up connection. And since all wireless clients and APs must operate on the same channel, network contention and RF interference results in unpredictable latency.

In a single-radio configuration there are several additional issues that occur: 1) increased collisions which impact performance of all user connections to a node and wireless users connection can reduce the entire performance of the if their connection is slower than the backhaul. 2) A wireless user can not transmit when a node in the vicinity is sending traffic to other nodes or other users, and 3) IP as a form of creating and maintaining a mesh network impacts the network in terms of the performance as latency is increased and throughput is impacted by IP link state changes and routing tables. While vendors may indicate that the impact is no more than 5 or 10%, the impact is greater than simply a percentage of bandwidth.

2nd Generation Wireless Mesh – *The dual-radio approach* - sharing the backhaul: With the dual radio approach, one radio is dedicated to wireless client support while the other radio is dedicated to wireless backhaul - with the backhaul channel shared for both ingress and egress traffic. Since a dual-radio approach provides a separate radio for client access and a separate radio for backhaul, this relieves some of the client side congestion, however because there is only one backhaul radio, it must switch back and forth between ingress and egress transport. The backhaul mesh connection is shared which provides some, although limited, improvement to the backhaul bottleneck and latency continues to increase from node to node, similar to the single radio architecture.

<table>
<thead>
<tr>
<th></th>
<th>1st Gen WMN</th>
<th>2nd Gen WMN</th>
<th>3rd Gen WMN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Density</td>
<td>1 Radio</td>
<td>2 Radios</td>
<td>3 or more Radios</td>
</tr>
<tr>
<td>Modularity</td>
<td>Fixed Config.</td>
<td>Fixed Config.</td>
<td>Chassis-based</td>
</tr>
<tr>
<td>Scalability</td>
<td>Very Limited</td>
<td>Limited</td>
<td>High</td>
</tr>
<tr>
<td>Latency over Hops</td>
<td>High</td>
<td>Medium High</td>
<td>Low</td>
</tr>
<tr>
<td>Throughput over Hops</td>
<td>Very Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Real Time Applications Support</td>
<td>Limited</td>
<td>Limited</td>
<td>High</td>
</tr>
</tbody>
</table>
3rd Generation Wireless Mesh – *The multi-radio wireless mesh* - unparalleled scalability and performance: In contrast to 2nd generation access points, mesh enables “full duplex” performance by providing dedicated radios for client access and dedicated radios for ingress backhaul and egress backhaul. Each radio is free to handle the requirements of the wireless user. This basic design principle establishes near-zero throughput loss per hop with minimal latency.

Typically at least three radios are used per network node, including one radio for wireless client traffic, a second radio for ingress of 802.11a wireless backhaul traffic, and a third radio for egress of 802.11a backhaul traffic. This approach to wireless mesh networking offers significantly higher performance than either the single or dual radio approaches. It allows for dedicated mesh backhaul links that can transmit and receive simultaneously because each link is on a separate channel.

Because the three functions of client ingress, backhaul egress, and backhaul ingress are handled by dedicated radios high throughput is maintained across 10 hops, and, as important, latency per hop is kept to 4 to 5 milliseconds, totaling only less than 48 milliseconds across 10 hops is well within the range for high quality voice. Each connection within the node supports quality of service and supports multiple SSIDs/VLANs, therefore voice traffic receives the proper prioritization from the wireless handset, across the mesh, to the wired termination point.

Municipalities have several concerns with regard to wireless communications:

1) Interference with existing municipal communications, carrier’s, businesses and residences
2) The health ramifications of wireless networking communications
3) Tower density effects real-estate values – what about WiFi?
4) Business models – what’s the best model?
5) Comparing technologies
6. Municipal Questions

**Impact of RF Interference**

RF interference involves the presence of unwanted, interfering RF signals that disrupt normal system operations. While the details or wireless protocols and the process is more complicated, as a basis for understanding the impact of RF interference in wireless LANs, imagine 802.11 access points connecting wirelessly. Each 802.11 station only transmits packets when there is no other station transmitting. If another station happens to be sending a packet, the other stations will wait until the medium is free. An interfering RF signal of sufficient amplitude and frequency can appear as a "rogue" 802.11 station transmitting a packet. This causes legitimate 802.11 stations to wait until the interfering signal goes away however, the interfering signal may start abruptly while a legitimate 802.11 station is in the process of transmitting a packet. If this occurs, the destination will receive the packet with errors and not reply to the source station with an acknowledgement. In return, the source station will attempt retransmitting the packet, adding overhead on the network.

802.11 wireless devices will continue operation in the presence of RF interference by automatically switching to a lower data rates; this slows performance, but enables connectivity to the network. The worst case, which is fairly uncommon, is that the 802.11 stations will hold off until the interfering signal goes completely away. And in most cases this is a matter of seconds or minutes. The source of most common interferences include: microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless in the same general area.

**Health Concerns**

Concern over the potential health effects of wireless signals has been around since the early 1990s, with most of the attention focused on cell phones. The FCC adopted limits for safe exposure to radio frequency (RF) energy. Radiofrequency radiation (RFR) is the propagation of electromagnetic energy through space. It has two basic properties: frequency and intensity. The effects of RFR are measured is by absorption in human tissue. The unit for this measurement is called the specific absorption rate (SAR) and is expressed in watts per kilogram (W/kg). The biological effects of WiFi are typically connected to studies on cell phone technology. Cell phones and WiFi operate on different levels of power intensity, but the standard for SAR is the same. While some research has been conducted on the biological effects of WiFi on human tissue, more research has is available on the effects of cell phone use. The FCC requires cell phone manufacturers to ensure that their phones comply with these objective limits for safe exposure. Any cell phone at or below these SAR levels (that is, any phone legally sold in the U.S.) is a "safe" phone, as measured by these standards. The FCC limit for public exposure from cellular telephones is an SAR level of 1.6 watts per kilogram (1.6 W/kg), or between 0.6 watts and 3 watts. Robert Bradley, director of consumer and clinical radiation protection at Canada's federal health department indicates "If you look at the body of science, we're confident that there is no demonstrable health effect or effects from wireless technology.". A study was performed in 2005 at the Foundation for Research on Information Technologies in Society in Zürich, Switzerland. This study conclusively showed that by operating at a distance of 20 cm, WiFi equipment is well below the U.S. standards for W/kg. Dr. John Moulder, a professor of radiation oncology at the Medical College of Wisconsin, who has researched and reviewed the biological effects of RFR, indicated that WiFi posses no health risks. Moulder and others point out that WiFi equipment emits less intense radiation than cell phones. Whereas most cell phones have a peak power output of 2 W, most WiFi routers have a peak power output of less than 100mW which is typical of indoor access points, and 400mW for outdoor units, but unlike cell phones and their base stations, WiFi devices do not communicate continuously. Dr. Kenneth Foster, a professor of bioengineering at the University of Pennsylvania, recently completed a study...
of WiFi, taking over 350 measurements at 55 sites across four countries. According to his research, not only does WiFi equipment emit less radiation under load, it does so in much smaller bursts. “When the networks were not being used, the duty cycle was 0.01 percent or so. That means that it is radiating power for 0.01 percent of the time.” While WiFi and microwaves use the same 2.4 GHz frequency, a microwave oven sends much more intense emissions than a WiFi device or cell phone. However, “Studies have shown that environmental levels of [radiofrequency] energy routinely encountered by the general public are far below levels necessary to produce significant heating and increased body temperature,” stated a 1999 FCC paper entitled “Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields.” Dr. Linda Erdreich, who has studied the biological effects of RFR for many years, and is now a senior managing scientist at Exponent, a scientific consulting firm, agrees with this assessment “We know that there is an adverse effect [associated with RFR] and it starts with heating tissue, but all of these things are well below the standard,” she says. Outside the United States, similar conclusions have been made by related entities in Canada, Europe and Australia. The Australian Radiation Protection and Nuclear Safety Agency and the Canadian Spectrum Management and Telecommunications use the same United States SAR value of 0.08 W/kg in an uncontrolled environment. Despite this internationally compiled body of factual evidence regarding the health effects of WiFi, there remain a few concerned citizens who are not convinced. Dr. Erdreich says “I think that the reason why there are differences of opinions is because people are looking at single studies and not at the whole picture.”

A **“Towering” Issue for Municipalities**

Tremendous growth in cellular demand has increased the demand for telecommunications towers and that number will increase as municipalities grow.

Municipalities and the wireless telecommunications companies struggle to find a happy medium between the need for towers and the desire most cities have to limit the number of towers. As higher bandwidth is required to support the continued increase in demand for cell phone service coverage, the number of cell towers will increase as well. Especially in those areas that are highly populated, have a large number of roadways, variable terrain and tall buildings, the growth in cellular towers is increasing to meet that demand. However, many cities feel as though they are at the mercy of the telecommunication companies on these issues. The municipal council and municipal engineers simply do not know the questions to ask to determine if the tower is needed. In addition, cities are often using their standard building ordinances as the guidelines to review these applications.

Advancements in technology are only part of the reason why more towers are needed. As first generation cellular services were upgraded to second generation (2G) the need for towers increased in order to deliver the more, although modest, bandwidth. Since the introduction of 2.5, 3G and EVDO the number of subscribers has increased now that multi-use phones, PDA’s and Smartphones have become available, this ultimately means more towers are needed.

The issue of aesthetics becomes a critical one in exclusive neighborhoods or historical areas, but, will be a problem anywhere as tower deployments continue. The towers themselves are considered unsightly and generally effect property values. This argument is often called the “Not-In-My-Backyard” issue. While towers are generally no more than 200 feet, ordinances for height and setback from property lines are negotiated at a local level and consume government and citizens
resources. The municipality can otherwise address this issue by purchasing expensive “stealth” towers, but this again isn’t an effective method to control the installment of towers and in many cases the location of the towers would not naturally fit-in to the landscape of the environment.

There are other issues that go unresolved by simply adding a tower that looks like a large tree. As mentioned previously, the health effects from towers emissions must be considered.

Based on Section 704 of the Telecommunications Act of 1996, health effects related to cellular and PCS services are not an issue cities can address directly. Wireless carriers are required to meet all FCC guidelines for emissions and safety and the only regulatory part the municipality can play in this is to verify that the companies are in fact meeting FCC guidelines. Another issue, while not a major concern in most circumstances, is the fear of falling towers. This issue is often raised as another flag by complaining citizens. However, realistically, modern telecom towers rarely fall, even in high winds, direct tornado hits, and earthquakes. Additionally wireless companies are required to submit design information to the Federal Aviation Administration (FAA) to verify the tower design will not interfere with any airports or air traffic areas.

In heavy contrast to the use and issues related to the installation and pervasiveness of cellular tower deployments, wireless mesh network deployments have little emissions and can be deployed practically anywhere. 802.11 wireless network technologies use the similar frequency to home wireless phones that we utilize every day. At 2.4 GHz, 4.9 GHz and 5.8 GHz, the radios that support these frequencies can be installed on top of buildings, street signals and many other locations that are already utilized for municipal purposes which thereby reduces the cost of deployments and any concerns for health risks.

7. Delivering Municipal Wireless Mesh Networks

The ability to provide high throughput equates directly to the number of voice and data users on the network and regardless of the number of hops. The mesh backbone must be able to support the traffic load from the mesh nodes. Inadequate ability to maintain high consistent bandwidth across multiple hops will result in fewer users being supported. The common solution by some vendors is to add more equipment after the initial plan is in place. Then additionally add a greater number of wired termination points within the network. These are critical concerns related to the successful delivery of a wireless mesh network:

- **Low latency across multiple hops**
  
  High throughput is not enough. To avoid jitter, each hop must minimize the packet latency. The holding time of a packet at any node in the mesh must be minimized (ideally to a negligible 5 milliseconds per hop). As such, a single packet should be forwarded even before all of the packets in a particular data stream are received from a previous node. Movement of data across the mesh must be asynchronous as oppose to synchronous, where some type of highly synchronized inter-node packet routing protocol is required.

- **End-to-end QoS**
  
  *Packet prioritization of voice*—High throughput and low latency in and of themselves are not enough when the network is loaded. To deal with contentions and spontaneity of load demand, voice streams must be prioritized across the entire mesh backbone and terminated with end-to-end traffic prioritization. It is no longer adequate to provide a class of service just between the wireless handset and the device-serving AP radio like in the case of wired APs. Mesh introduces the requirement of QoS across the entire backbone to avoid contention that may occur at each hop in the mesh. This class of service needs to be automatic, driven by the infrastructure, and is best
handled via separate VLANs/SSIDs dedicated to voice. While some expect that WiMAX (802.16d/e) will provide a better answer to voice over wireless, WiMAX still faces many challenges which are, to a large degree, already overcome with WiFi. WiMAX is: 1) still a long ways from being deployed in a non-proprietary format, 2) facing many chipset issues which will not be resolved in the short-term, 3) end-user devices will not support WiMAX until its fully stabilized and non-proprietary and 4) can not be counted on as a ubiquitous solution for city-wide and country-wide deployments.

**Scalability & Capacity**

Point-to-point and point-to-multipoint systems are static configurations designed in a star topology and have no provisions for scalability or capacity. Multi-radio mesh networks, on the other hand, support connectivity from multiple directions simultaneously, without a decrease in performance as traffic is switched from one radio to another. As a result of preserving performance, the system redefines previous expectations of wireless communications, enables a large number and wide range of applications, and is highly adaptable and scalable.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Reliability</th>
<th>Adaptability</th>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point-to-point</td>
<td>High</td>
<td>Low</td>
<td>None (2 endpoints)</td>
</tr>
<tr>
<td>Point-to-multipoint</td>
<td>Low</td>
<td>Low</td>
<td>Moderate (7-30 endpoints)</td>
</tr>
<tr>
<td>Mesh Networks</td>
<td>High</td>
<td>High</td>
<td>Maximum (1000's of endpoints)</td>
</tr>
</tbody>
</table>

Single, dual and common multi-radio systems impose a “transport tax” which reduces performance by ½ for every wireless node connected back to a wired site. This transport tax degrades performance by ½, ¼, 1/8 and 1/16 by the time you get to the fourth node. Therefore, regardless of the number of users claimed, single, dual and most multi-radio products can not support any, but the smallest number of users. Initially, claiming possibly 64 users, the reality follows - 32 becomes 16, 16 becomes 8, 4, etc… until no bandwidth remains. On the other hand, Strix multi-radio mesh products will not only preserve performance over long distances, but also more than adequately support hundreds of users per node. Additionally, this provides a predictable infrastructure for real-time voice, video and data access.

**Resilience & Reliability**

In a typical point-to-point wireless network, reliability between one node and another might be only 70% or less. To provide reliability equivalent to that of wired networks, mesh networks

Strix Systems, Inc., www.strixsystems.com, info@strixsystems.com 1.877.STRIXSYS
All trademarks, logos and service marks are the property of Strix Systems.
Copyright © 2000-2007 Strix Systems, Inc. All rights reserved.
automatically and dynamically adapt to the network infrastructure and the environment. Each node is enabled with distributed localized node intelligence, network topology-independent fast re-routing, and instant roaming hand-off, near-zero throughput loss, multi-hop traffic distribution and near-zero latency for long-range multi-hop deployments.

Each node automatically locates all other network nodes, selecting the best path based on real-time backhaul path and RF analysis using roundtrip delay (RTD), signal-to-noise ratio (SNR) and other criteria. The nodes continue to scan, evaluate and optimize for the best and alternate paths to each node and each wired node. If the criterion of the best path drops below the set threshold, or the path is blocked, the system continues the self-healing process to acquire the next best path – all with milliseconds. The nodes continuously performs self-tuning, optimizing each path for best performance and congestive redirection, even for mobile nodes moving at high speeds such as trains.

Unlike IP routing solutions that require networks to re-converge in order to route around trouble, each node is capable to make these decisions locally without the overhead of cumbersome routing algorithms. This ensures the fastest transitions and zero-downtime. The resulting mesh network is highly scalable, reliable, and enables instant roaming handoff.

In a traditional point-to-point and point-to-multipoint network, a node, either newly installed or changing RF signal states, might not be readily capable of communicating back to its central node. It might be too far away, or there might be a physical barrier in between, or the node might be in a dead spot caused by multi-path interference. Alternatively, a mesh network immediately establishes connectivity through the mesh, using alternate paths as needed as soon as nodes are turned on.

8. Applications for Mesh Networks

Multi-radio wireless mesh networks offer the broadest number of applications due to the associated benefits of high performance, low latency, resiliency and scalability. Applications such as video surveillance for public safety, WiFi voice for the enterprise and the public at large, meter reading, alarm triggers, remote control etc. can all take advantage of wireless mesh networks. As Industry becomes more aware of this technology, more applications will evolve.
Public Safety. The need to gain access to information, images, and video in order to make critical decisions related to is imperative. In municipalities law enforcement officers can improve safety and efficiency by connecting to headquarters and accessing drivers license photos, booking photos, restraining orders and other suspect information while SWAT teams moving to a hostage situation or firefighters racing to a blaze can consult building blueprints, hazardous materials databases, video surveillance or collaborate with teams and provide alternative modes of communication when cellular service or GSM doesn’t work. Public safety and first responder personnel make critical decisions on a daily basis that affect the safety of themselves, the citizens they protect and those they work with. Current systems are proprietary and limited communications within their own agencies and departments. The requirement for a compatible high performance safety communications system is more important today than ever before. With city-wide WiFi wireless networks, the ability to provide time-critical information such criminal records, driver’s license photos, passport information, mug shots, building blueprints and surveillance videos, has never before been possible. Now with the advent of outdoor, mobile and indoor Access/One components, response times and real-time collaboration throughout the chain of command and with other agencies is possible and will increase agency productivity. Today’s WiFi is secure but homogeneous, unlike proprietary public safety systems, WiFi networks remove the barriers between agencies and departments that must work together in time-critical situations. Field personnel can use any wireless device, including in-vehicle computers, laptops, personal digital assistants (PDAs), scanners, or phones, to retrieve or transmit all information sources available routinely to office personnel.

Public Works. Government departments need to utilize mobile technologies in order to improve communications and increase the efficiencies work in the field. Mobile connectivity to city workers allows building and health inspectors, social workers, animal control, public works employees and city officials to respond instantly to traffic or city maintenance situations, building-code and safety, and other occurrences where immediate access to existing or updated data can be crucial. Reports can be filed in the field, photos can be transferred, and laptop or hand-held analysis information can be collaborated from the field to specialists.

Digital Divide. Strix Systems and its partners are bridging the education gap. Closing the Digital Divide enables people to help themselves, improving rural health and education, empowering individuals, providing jobs, or address more complicated inter-related issues of poverty. Whether a
U.S. city or an international region, the digital divide is not just about education. It's a problem, tackled one step at a time that will open doors to new personal growth and business opportunities.

**Public Services.** Municipalities can provide free or low-cost wireless Internet access to the masses while municipal services are boost local businesses by encouraging people to linger, and spend money in downtown areas. This may be residents of the community or travelers from abroad. Cities are using wireless networking to re-vitalize their image as smart and progressive, a place where people want to live, play, learn, work and where businesses can flourish. Some cities commonly offer these services at no charge, using surplus capacity from paying business and government subscribers.

**Surveillance.** Government agencies use wireless video surveillance solutions for monitoring high-crime areas, courtrooms, and security checkpoints in public buildings and to prevent vandalism. Industrial enterprise and small businesses have also embraced video surveillance where with staggering results - car crime reduced by 80%, robbery decreasing by 68%, violence down by 30% and criminal damage decreasing by almost 60% while multiple studied of surveillance on municipalities show that installing surveillance systems has resulted in a 20 to 30 percent reduction in street crimes. Surveillance cameras not only reduce crime, but fear as well, improving the community and the quality of life.

**Meters and Sensors.** Meters and sensors enable accurate real-time interaction and control during critical and non-critical situations. Whether it's for the purpose of remotely shutting a door to a public facilities, accurately measuring and reporting flood statistics, detecting, reporting and taking control of a gas leak occurrence, monitoring and controlling safe/unsafe conditions, or remotely notifying and automatically switching pumps at public water storage, switches at an electric facilities or turning on a city-wide emergency warning systems. Wireless networking enables real-time information, signaling and switching for early detection and prevention resulting in saved money and saved lives.

**Transportation & Traffic Management.** Local governments currently implement traffic-light controllers, highway message boards and surveillance cameras using wired connections. The need to expand traffic management services increases, yet the ability to provide wired connectivity, or Fiber, is limiting and practically impossible in many situations. As municipalities deploy wireless mesh networks, the once expensive wired connectivity can be reduced to only specific areas where it already exists, while all other areas can utilize secured, ubiquitous high-speed access to enable traffic/transit monitoring and engage wireless video surveillance. Streaming live video can be sent from a particular physical location or from a remote vehicle, such as an ambulance or command station, while in transit during medical or public safety emergencies. Real-time communications with signals, road signs, electronic gates and other devices can be turned on or controlled as needed along the way. While for a public railway system Internet access is provided along the tracks for hundreds of miles. The possibilities are endless.

**Intelligent Vehicle Systems.** Current developments include the definition of Dedicated Short-Range Communications (DSRC) enabling vehicles to communicate with one another and external objects such as stop signs, intersections, signals, railroad crossings, etc, and initiate procedures to avoid crashes. Many auto manufactures will be integrating WiFi and initially intend to use WiFi to enhance existing GPS mapping with current road speed and traffic condition details, map updates etc.

**Federal Government.** Wireless mesh networks are increasingly used for tactical and strategic operations by defense and intelligence communities to provide greater situational visibility resulting in more information available about the physical environment. Deployed in significant military operations, field telemetry, mobile/vehicle applications, harbors/ports, and emergency temporary networks, Wireless Mesh network infrastructure enables troops to monitoring buildings and other structures that obscure line of sight and potentially conceal threats. As the demand for timely, life-saving information increases and new multimedia applications are developed to exploit minute details, wireless mesh networks can give military personnel immediate, relevant data from key facilities, borders, and sensitive infrastructure. Strix Access/One Wireless Mesh provides defense and intelligence communities with advanced technologies to address these challenges.

**Distributed Industrial Enterprise.** Often carry the burden of expensive wired network and telecommunications infrastructure, this can be offset by the deployment of high-speed self-configuring and self-tuning wireless mesh networks for static and mobile broadband communications. Whether drilling for oil, monitoring power and gas flows or creating a temporary network for an outdoor event,
network communications to support real-time voice, video and data can be quickly and easily added, both indoor and out, to provide a completely resilient and secured network for private and public communications.

**Hot-Zones.** Well beyond the traditional definition of a collection of hot-spots, today’s hot-zones provide total coverage for large areas and can allow roaming within a zone or from one zone to another. This model may be implemented by a city government or commercial entity and provide such benefits as security patrol for large distributed areas, parking, airports, public parks and outdoor venues such as stadiums. Support for real-time applications over a wireless infrastructure is a strategic and critical advantage. All applications can be supporting including, but not limited to: voice, video/multimedia streaming, video surveillance, ticket scanning and customer relations management, shipment and baggage tracking and handling as well as many other innovative applications such as automated remote aircraft parking assistance or data record transmission from vehicles in motion. Hot-zones are also implemented by service providers to offer internet access and business-to-business services where mobility is key and other carrier services are impractical to deploy.

**Service Provider Network Extension.** Service providers and cable operators can cost effectively and scalably deploy wireless mesh networks delivering voice, video and data to underserved and strategically important populations - across large urban areas, rural counties, and entire regions. In areas where high-speed Internet doesn’t exist, service providers now have the ability to extend their wired networks, with the same performance and resilience, wirelessly to provide total coverage. Additionally, it's strategically important to gain access into competitive territories. Wireless mesh networks enable the reach-ability making it possible to provide services to entire populations previously too difficult, too costly, or impossible to serve.

9. **Compare and contrasting architectures and technologies**

**Point-to-point, Multi-point and Wireless Mesh**

In point-to-point networks, each link requires a dedicated connection; in point-to-multipoint set-ups, the multipoint transceiver winds up being the bandwidth bottleneck and the point of worst failure. A mesh can distribute bandwidth and risk, while reducing the cost of deployment and expansion.

**Point-to-point**

Point-to-Point technology can be used to implement high speed backhaul links and is generally the choice where high bandwidth and low latency are concerns. Implemented as single links or daisy-chained, these solutions are typically performed by single-radio products which reduces bandwidth.

**Point-to-Multipoint**

Multi-point solutions are commonly referred to as "hub & spoke". Each link can be hardened with redundancy for higher availability as needed. In a carrier deployment, this configuration is generally targeted at lower speed applications, i.e. < 10 Mb/s per end-site. These solutions also typically have high latency and jitter and lack a redundancy solution preventing voice and video services from being offered.

**Wireless Mesh**

A wireless mesh network is the wireless co-operative communication infrastructure between a number of individual wireless nodes. Depending on the architecture each node is/should be capable of self-configuration, self-optimization and self-healing. The networking infrastructure for wireless mesh is decentralized and does not/should not require a gateway to control, via IP or other protocol, the localized situation for each node. Each node builds multiple connections to surrounding nodes and simultaneously determines primary and secondary paths based on details from each adjacent
node. Devices that do not adhere to these dynamics should be classified as point-to-point or point-to-multipoint.

**Single, dual and multi-radio architectures**

**Single & Dual Radio Solutions**

When comparing design architectures of a single radio, dual radio or multi-radio system, there remains one fundamental problem that plagues a single-radio technology based wireless network - the traffic collisions that take place on a single channel supporting all the nodes and users of that entire network. This is the main characteristic of a one radio mesh. On a single-radio mesh everything is in one channel; Access and backhaul. This includes incoming and outgoing user connections and traffic as well as the traffic from each other surrounding wireless node. Consider that only one individual device can communicate at a time due to the fact that a single radio must stop and listen to one user and device at a time. Users can negatively impact other users if they connect at a data rate that is lower than the backhaul data rate. One example is that a user devices will have more attenuation from a node because they are behind a wall, or are a using a PDA. They will sync at lower speeds, in many cases at 1Mbps. Also, while a user is sending or receiving a packet to a node, if the link rate is 1Mbps the entire node then operates at 1Mbps. A wireless user can not transmit when a node in the vicinity is sending traffic to other nodes or other users. This is applicable not only to the users associated to that particular node but, to all users that can see (detect signals from) that node, even if they are already associated with other nodes, all of those wireless users must wait. To make matters worse, especially when higher power radio nodes with omni directional antennas are used to cover larger areas, a greater number of users will be waiting while just one node is transmitting.

**Multi-Radio solutions**

An effective Multi-radio design is one which supports more than 3 radios. This design typically provides superior coverage, the highest possible throughput, decreased latency, increased scalability and greater capacity as well as carrier-grade resilience and reliability compared to any single and dual-radio architecture.

**Technologies**

**WiFi vs. DSL and Cable**

WiFi outperforms DSL and cable by comparison. While speed ranges can be similar depending on the service offered by a wireless service, such as 1, 2, 4, 6, 11, 24, 54 and 108Mbits/second, wireless offers automatic link performance negotiation which provides the optimal speed depending on range and reliability. Theoretically DSL can provide a theoretical connection speed up to 8Mbits/second, although speeds of 1.544Mbits/sec for download and 512Kbits/sec for upload are common using Asymmetric Digital Subscriber Line (ADSL). SDSL, the symmetric version, commonly referred to as a T1 replacement technology, supports up to 1.544Mbit per second in both directions while VDSL, the “V” standing for Very high bit-rate, can provide 55Mbits/sec but is costly to deploy and performance drops off significantly after 1000 feet from the Telco. Cable, on the other hand typically offers between 1 Mbps and 6 Mbps bandwidth for downloads, and bandwidth between 128 Kbps and 768 Kbps for uploads, however the most common complaint from users is that Cable networks slow down more often than DSL networks during peak usage times.

The key to choosing the technology, however, comes down to the business model and whether broad, unrestricted and mobile access for potential subscribers is important. In every case, the cost to deploy a WiFi solution is more cost effective and will deliver the same, if not higher, performance, in addition to enabling the ability to use the wireless network for new voice, video a data services
such as for public safety, wireless meter reading, video surveillance and medical emergency communications.

**WiFi vs. fiber-to-the-home**

Fiber is very scalable, yet only reaches a small number of users. In essence, some would say “fiber does everything and goes nowhere”. The high cost of construction and installation stand in the way of the prevalence of fiber networks. The cheapest alternative, copper, which includes DSL, has the opposite advantage of being available practically anywhere; however, it has the drawback of not being scalable. In essence, it goes everywhere but does nothing. Fiber can provide far greater bandwidth, up to 80 times faster than the 256kbp/s offered by San Francisco’s new wireless network, but the disadvantages are obvious: 100 times more expensive and therefore harder to sell, in addition to various regulatory challenges and lobbying from incumbents.

From a consumer perspective the cost of fiber to the home typically runs from $1000 to $1500. For a city the size of Palo Alto, California, for example, the total cost of installation for FTTH would be approximately $40 million. However, many residents chose not to pay for these upgrades as other forms of access already exist. Wireless mesh network access, at a fraction of the cost paid on a monthly basis is far easier to sell and enables options for a range of services including mobility.

**WiFi vs. 3G**

2/2.5G voice services are installed worldwide typically in a footprint of one tower per square mile. In the last 5 years those voice-only networks have been upgraded to support broadband access up to 2 Mbps in most deployments, however, today’s common end-user experience with 3G overlays is in the hundreds of kilobits per second for download and even slower for uploads. Latency is also typically measured in the number of seconds as opposed to milliseconds. From an end-user perspective applications including Microsoft Outlook, email attachments, VPN’s, Smart-phone and PDA applications are unusable. Besides that, 3G technology is only included in cellular phones and mobile devices while Smartphones and PDAs include, and are being equipped with, WiFi as a standard technology.
802.11a and 802.11g offer up to 108Mbits/second connectivity options.

While a tremendous investment, 3G certainly falls short of its stated performance considering the carriers low-density cellular network is incapable of delivering adequate RF signal power thereby increasing penetration and coverage. Additionally while power may increase signal to the end-user, the end-user device is not capable of sending to a cell tower that may exist 1 mile in the distance. Part of the issue is related to the physical attributes of path loss. In other words, the signal from the tower to the end-user mobile phone, for example, is limited by transmission power and interference between adjacent cells to those devices and beyond basic connectivity, greater speeds requires greater RF power. The cost and complexity of existing 3G base stations in addition to the high equipment capital cost, site preparation and required backhaul for each cell with high-speed carrier connections makes increased 3G cell densities and costs problematic. From an end-user perspective, mobile application connectivity and performance is spotty and inconsistent.

Facts about cellular: Cellular coverage takes place by means of dividing the city into small cells. This provides for frequency reuse across a city, so that millions of people can use cell phones simultaneously. In a typical analog cell-phone system in the United States, the cell-phone carrier receives about 800 frequencies to use across the city. Each cell is composed of a base station, tower and building contacting the radio equipment. Typical coverage areas produced from these sites are 10 square miles (26 square kilometers).

- Cell Transmit power: Today's cellular voice systems operate at a maximum of roughly 200-400 Watts EIRP transmitted from the base station, and between 0.6 and 3 watts from the handset. At the top of the tower, each antenna transmits at 60 watts. As each carrier provides services to a given area, additional antennas are required. Therefore the more antennas, the greater the power transmitted. In urban areas cells may operate at lower power to reduce cell size and maximize capacity. In the case where cell size is reduced for expanded capacity, increasing the power would simply cause unwanted interference between cells.
- **Channel Bandwidth:** One licensed channel is typically allocated to all data users within a cell. Allocation of additional channels by the operator would only add capacity for more users, not increase end-user speeds since the radios are not designed to use more than one channel per user. Even if radios could hypothetically be redesigned to exploit more channels by taking away channels allocated to voice services (each operator has a limited number), such a channel-hungry design would consume expensive licensed channels and take away from aggregate user capacity while only increasing speeds proportional to the number of channels consumed at best.

- **Cell Density:** The only practical way to increase received signal level is by increasing the density of cell sites within the coverage region. This works to reduce the average loss through the environment that the signal incurs before reaching the handset (or base station), hence ensuring an overall increase in received signal strength and aggregate capacity. However, increased cell density in a 3G and EVDO deployment requires additional expensive base station equipment, sites and backhaul to the Internet for each cell.

**WiFi vs. WiMAX**

Comparing WiMAX to WiFi is equivalent to comparing apples to oranges. Initially it’s easy to see why the comparison would exist, as most people think WiMAX is merely a more robust version of WiFi. Indeed they are both wireless broadband technologies, but they differ in the technical execution and ultimately their business case is very different. In addition to the technical differences that exist, the marketplace difference is that equipment is more or less non-existent for WiMAX and certainly not geared towards a residential environment with very high pricing to be expected. It has taken over 2 years to develop WiMAX technology so far. Two flavors exist: one flavor is called 802.16d. Its purpose is to provide the “backhaul” of Internet access traffic to and from business and residential users. The other flavor is called 802.16e, which duplicates the functions that WiFi already offers. While 802.16e will not be available for quite some time, 802.16d will be used within the next two years to provide higher speed interconnections between wireless nodes and high-bandwidth Internet connections. Whether the technology is utilized in a municipal deployment is yet to be seen and the existing benefits and cost efficiencies of WiFi coupled with high-speed backhaul solutions overshadow the need for WiMAX in the short and long-term.
Routing-based Mesh Networks

Ad-hoc routing instead of a true “Mesh” architecture

There are two fundamental methods to perform mesh networks, one is utilizing layer 2 and a combination of high performance features to enable high-throughput mesh networks in support of voice, video and data. The other method is to use layer 3 IP routing. While there are approximately 70 different methods of routing for wireless mesh networks, wireless products supporting layer-3 routing protocols, there are several that are considered viable: Ad-hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR), a routing Topology Broadcast based on Reverse-Path Forwarding (TBRPF) protocol and proprietary schemes.

Utilizing IP as a way to manage a wireless mesh network creates unnecessary overhead. The benefit of utilizing an IP routing algorithm to build a mesh network could be to utilize the IP network for multi-path routing. While complex, a multi-path routing algorithm, unfortunately, especially in a large network with single radio nodes, IP routing methods have proven difficult to scale due to the fact that in a single radio system, both client and network backhaul create an immediate bottleneck - only one path can be transmitting or receiving at a time. In a wired network, a multi-path routing algorithm will provide a “preferred path” and “back-up path” or provide a true simultaneous path (multi-path) capability; only the preferred path part of an IP routing multi-path algorithm will work in a single radio environment.

As with any IP routing algorithm, significant changes take place when a link goes down or a new path appears. In a wireless configuration, connectivity and the strength or quality of a connection will vary, and therefore the IP routing algorithm must re-route and stabilize quickly, sending all adjacent nodes the relevant information about its routing path neighbor(s). In a wireless network, there is performance degradation due to such advertisements, and maintenance of this information can be significant and there are claims that overhead related to maintenance of a “Predictive” IP algorithm is no more than 5% of the total network capacity, however this is only part of the problem.
Theoretically an IP routing protocol should provide a performance benefit as a network becomes more populated, stabilizes and packets may be optimized on a per-path basis, however, in a wireless “mesh” network, preferred and secondary paths change more quickly and due to the nature of wireless CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) technology inherent in every wireless networking product, multiple paths must be built and stabilized immediately and issues such as collisions or link-state changes causing links to go down and up again cause IP routing algorithms to bounce back and forth perpetuating an indeterminate decision process. A stable wireless network is required in order to keep the routing management traffic to a minimum. If that can be accomplished, then a multi-path IP routing method does provide some benefit. In the real world however, wireless connections will go down and up, and computer-to-server communications will be disconnected while the routing-over-wireless topology converges. Worst case examples are seen in some large-scale single-radio networks utilizing proprietary “Predictive” routing mesh algorithms.

Some examples of interruptions include, but are not limited to: computer-to-server communications split over two connections to the same destination. Should this connectivity be disrupted, the impact can be significant, taking twice the time to resynchronize the network and causing retransmissions of millions of packets for data, voice and video. A “Predictive” IP routing algorithm must re-route and stabilize instantaneously and the fact is – that just doesn’t happen.

The real question is whether a layer 3 routing protocol is needed to perform these re-routing functions if a layer 2 wireless mesh network devices can perform the same functions, without proprietary IP routing algorithms and do it faster! Often times it’s a religious debate and it shouldn’t be, because the facts are clear. Layer 3 routing technologies are not currently capable of effectively supporting large-scale wireless mesh network deployments.

As Bob Moskowitz, a senior technical director at TruSecure Corporation and active in the IETF and IEEE 802.11, has stated: “…you really can’t build a mesh network on IP routing unless the mesh is relatively stable (only a few link changes per hour), with measurable traffic outage. But those IP routing protocols take too long to stabilize, especially in mesh networks that are themselves inherently unstable.

One final statement with regarding to single-radio devices – the physics of a single radio device when used in a multi-hop configuration is such that any traffic traversing through that device will lose half its performance as it moves on to the next node. No IP routing architecture or algorithm can assist or improve such a devices performance. The only method to sustain performance from one node to the next is via an optimized hardware design which implements a mesh algorithm at the physical layer across a modular multi-radio design. This has proven to provide the highest performance, lowest latency and reduced total cost of ownership.
10. Dynamic Mesh Architecture

The dynamic mesh architecture is the evolution of high-performance switching and localized node intelligence resulting in maximum consistent throughput from radio to radio with minimal latency. Wireless mesh nodes build the network automatically by scanning for adjacent devices, blocking rogues (not part of network) in the process. The nodes establish simultaneous communications channels to the adjacent nodes over encrypted tunnels and optimize those connections within milliseconds. Each node continues to scan, determine optimal paths and make changes as necessary without any additional management overhead to a centralized gateway which would degrade performance. As wireless mesh networks are deployed and their size and complexity continues to grow, mesh networks with multiple hops can become increasingly vulnerable to problems including bandwidth degradation, radio interference and network latency. In real life cases under these circumstances it’s not unusual to see throughput as low as 256k, 128k or even 56k per user. Today’s dynamic mesh architecture provides the highest consistent throughput and low latency enabling optimal high performance paths anywhere on the network. Additionally, services such as user authentication, portal services etc. can be distributed anywhere throughout the network without performance penalty.

Traditional first, second generation and some third generation wireless mesh solutions cannot scale to the size of the wireless networks to which they are currently tasked. As stated by industry expert Esme Vos…

“Municipal wireless networks come under such a spotlight that less than promised performance won’t slip by, said Esme Vos, founder of Muniwireless.org. "You’d better expect people to call you on it,"

The inherent multi-hop dilemma (referring to the throughput degradation) makes these types of mesh networks questionable candidates for large-scale network deployments. Even for deployments that begin as simple “hot-zones” such as airports, this requires a new breed of wireless mesh network to provide the consistent and predictable performance and reliability across the network regardless of the number of hops it employs.
Independent lab testing indicates that with a single or dual radio product, a staggering 80% loss will occur over only 5 hops in noise-free test conditions. To be effective, utilizing the dynamic mesh architecture with multiple radios will deliver the highest throughput, lowest latency, and end-to-end quality of service not only between the wireless handset and access points, but also across the mesh links to the wired termination point.

11. Security and Wireless Networks

Municipal wireless networks are designed for accessibility yet require maximum security. They announce themselves broadly so that mobile devices have an opportunity to connect easily. Unfortunately, once the wrong person, or hacker, gets on to an unsecured and unmonitored public access network, the entire network and assets are at risk. Security experts talk to specific attacks such as denial of service (DoS), passive and active eaves-dropping, man-in-the-middle, poisoned caches, session hijacking, replay and traffic analysis, the solution lies in protecting the information used to launch these attacks. The payoff is assured confidentiality, elimination of unauthorized access to corporate secrets, and protection against liability lawsuits for unlawful network use by outsiders.

Securing a wireless network involves authenticating potential users, authorizing access to only specific information, and encrypting data to prevent eavesdropping. Wireless devices send their “certificates” to the server via authenticated network nodes, which enable full access between the device and the wireless network only when authentication is completed. Dynamic keys then keep the session private by protecting the data, as well as source and destination addresses, the packet size, and number of packets. By using the strongest available authentication and encryption standards, the wireless system should be standards-compliant and compatible with a wide range of client devices and commonly deployed security servers. Sophisticated wireless systems utilize high performance hardware encryption. These systems are typically capable of automatically encrypting network management and control data while Virtual Local Area Networks (VLANs) are available at each node on the backhaul and wired connection to assure that secured and fully authenticated users have high performance access to the appropriate wired LAN resources while management functions are restricted to approved users. More capable secure wireless mesh devices are also capable of encrypting not only the network management and control data, but the entire transport path. In addition, “client-side” privacy protects against client-to-client attacks and enforces communication to a controlling authentication gateway. Rogue access point detection is also critical. As these access points are detected, the mesh network assists in preventing even benign users from unauthorized access. Finally, user security should be maintained as individual users roam across the network.

Fewer than half the installed wireless equipment, let alone wireless mesh network systems, have security properly configured and running. So the first step is to close the door.

Future Technologies

Meeting the current and future needs for large-scale coverage and truly mobile computing and
communications across the globe, WiFi Mesh will continue to dominate as large-scale deployments continue. The future of wireless networks includes WiFi, 3G, WiMAX, encryption and other technologies to build the most robust, pervasive and secure networks. Each technology has its place, such that WiMAX will be utilized for WiFi backhaul and 3G provides access in areas not currently covered by WiFi mesh. Together they will provide global connectivity. The driving force behind future technologies is the cost effectively delivery of technologies to deliver converged networks. Converged networks enable the ability to deploy new applications that take advantage of the combine voice, video, data infrastructure. The unique advantages of a converged infrastructure stems from the fact that devices on the converged network can access voice services as well as traditional data services simultaneously. The integration of messaging and video services will take advantage of the infrastructure in place, but additional unique applications will emerge such that WiFi and other technologies are not only integrated within computers in fire trucks and police cars, but that transportation systems will utilize city-wide and country-wide wireless mesh for its performance and resilience to enable new innovations for transportation safety, hands-free navigation and information services, video and more. The future technology which enables the delivery of this information is available today in the form of wireless mesh networks. That being said, radio technologies will improve to better take advantage the environment to gain increase penetration and signal distribution while keeping within unlicensed spectrum power specifications in addition to provide performance increases and greater user densities and various aesthetic design considerations.

12. Business Models

Several business models have been used to bring wireless mesh networks to entire municipalities. Government ideally seeks to reduce risks and costs while providing an infrastructure that maximizes the benefits across a large spectrum of users. The effectiveness of such a network and potential efficiencies gained are key considerations, while government should work with commercial entities to share the costs and risks of the municipal networks. A sustainable partnership provides the government as an ISP’s anchor tenant, lowering build out costs and customer acquisition opportunities, while the government gains a new way to improve business operations, offer city amenities, and improve public safety.

Building, operating, and maintaining a city-wide, or larger, network to support a large number of users is complex. Although city and county authorities have departments of information technology, traditionally they do not have the same resources as a commercial service provider, and depending on the technology used, may not have the specific expertise to take on this role. This is why a practical business model enabling the long-term viability of the commercial entities and the network must be initiated. Anything less will likely fail.

Several models have been considered:

- Public Ownership & Management: City finances, owns, and operates the network.
- Public Ownership/Private Management: City finances and owns the network, and a private company operates the network.
- Privately Owned: While this falls into the category of today’s carriers, this model defines that a private company owns and operates the network, wherein the contractor finances the cost of design, construction, and operation of the network and subsequently owns and operates the network without using any city assets for deployment of necessary network infrastructure.
• A Public/Private Partnership: A private contractor finances the cost of design, construction, and operation of the network and subsequently owns selected components of the network and operates the entire network. The contractor leverages the city’s installed and expanded fiber network, which the city owns and makes available to the private company as well as other available city assets for deployment of necessary network infrastructure. The city acts as the anchor tenant on the network and has a role in governance.

Public/Private Partnership Approach

Typically, after considerable review, the most efficient, cost effective and sustainable networks, with considerations to capital budget constraints, existing bond obligations, exposure to risk, potential regulatory/legal impediments, and the complexity of network start up and ongoing operations management, is the Public/Private partnership business model with provisions for the use of city infrastructure (publicly-owned building rooftops, towers, street lights and other “hanging assets”) for the deployment of the system.

Using the public/private partnership model, with practical access to intellectual property, finances and infrastructure to deploy and operate such an open system, this allows the development and operation of a city-wide broadband network. This network will immediately address local government’s public safety issues and growing demand within the communities for economical, universal access to high speed broadband services. At the same time, the commercial partner has gained the city as the anchor tenant and greatly reduced operating costs arranged with the city on equipment, hanging assets and reduced fee arrangements.

Additionally the public/private partnership allows the wholesaling of the network to other providers and retail services to residents, businesses and visitors.

<table>
<thead>
<tr>
<th>Business Model Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Ownership</td>
</tr>
<tr>
<td>Existing Network Infrastructure</td>
</tr>
<tr>
<td>Construction Costs</td>
</tr>
<tr>
<td>Wireless Equipment Ownership</td>
</tr>
<tr>
<td>System Operation &amp; Maintenance</td>
</tr>
<tr>
<td>Customer Service</td>
</tr>
<tr>
<td>Technology Replacement Cost</td>
</tr>
<tr>
<td>Marketing &amp; Sales</td>
</tr>
<tr>
<td>Digital Inclusion Initiatives</td>
</tr>
</tbody>
</table>

An example of municipal/city responsibilities:

1.1. The municipality will own and finance network as the anchor tenant
   1.1.1 Provide required network and CPE financing
   1.1.2 Provide facilities for authentication server, core switches, and core routers
1.1.3 Provide authentication hardware and software
1.1.4 Provide core network (routers and switches)

1.2. Provide partner the access to mounting assets
   1.2.1 Provide access to Xcel Energy mounting assets
   1.2.2 Cover pole attachment fees.
   1.2.3 Provide access to SLP mounting assets
   1.2.4 Help facilitate access to non-Xcel Energy and non-SLP mounting assets

1.3. Maintain ownership of the subscribers
   1.3.1 Provide community brand image
   1.3.2 Monitor subscriber satisfaction
   1.3.3 Maintain subscriber "hot-line"
   1.3.4 Monitor feedback regarding management partner performance
   1.3.5 Maintain ownership of domain names

1.4. Set policies and procedures
   1.4.1 Set operating policy and customer service guidelines
   1.4.2 Approve partner’s service offerings and prices
   1.4.3 Approve all marketing and promotion activities on a timely basis
   1.4.4 Set policy for potential advertising and sponsorship revenues
   1.4.5 Set policy for revenue sharing of advertising profits

1.5. Provide specified support to Management Partner
   1.5.1 Provide liaison staff support – business manager or other as appropriate
   1.5.2 Support marketing efforts via existing communication mechanisms
   1.5.3 Monitor financial performance, including reports as required by city
   1.5.4 Manage lines of responsibility between city and partners
   1.5.5 Provide main and redundant internet connections
   1.5.6 Provide backhaul connections for bandwidth injection points
   1.5.7 Sponsor educational workshops
   1.5.8 Provide e-government portal for sign-up, registration and authentication

An example of partner/ISP responsibilities:

Partner Responsibilities – the following would necessitate the approval of the municipality.

2.1. Provide subscriber/customer contact information
   2.1.1 Maintain customer satisfaction
   2.1.2 Manage customer expectations
   2.1.3 Provide a working group or forum for customer feedback
   2.1.4 Fund and manage sales and marketing efforts
   2.1.5 Perform monthly billing to customers
   2.1.6 Provide 24x7 help desk services
   2.1.7 Provide multi-tiered support for all major computer hardware and software
   2.1.8 Provide full-time “sign-up” staffing from e-government web page
   2.1.9 Conduct and schedule professional customer installations

2.2. Perform network operations
   2.2.1 Operate and maintain wireless network and related wired connections and services
   2.2.2 Provide required wireless network software/firmware upgrades
   2.2.3 Maintain the core network including gateways, routers and switches
   2.2.4 Monitor and maintain main and backup Internet connections
   2.2.5 Perform daily wireless and wired network analysis
2.2.6 Make recommendations and improvements as necessary

2.3. Operate the ISP
   2.3.1. Maintain and manage authentication (process)
   2.3.2. Provide email services, including servers
   2.3.3. Provide all services including servers required to operate the partner, except for authentication server which is managed by city.
   2.3.4. Provide operational statistics

The public/private partnership model provides the following benefits:

- The city maintains full ownership of the existing, valuable, network infrastructure.
- Depending on the final agreement the city will/may have no financial risk. The capital investment and issues related to construction, start up, systems operations and maintenance, and rapidly evolving wireless technology refresh/replacement will be the responsibility of the private partner.
- The city does not need to be involved in the requisition, configuration, deployment and support of the technology and will focus its efforts solely on the management and analysis of the business requirements, procurement and contract management of Broadband Wireless Network services.
- The city will utilize its influence to leverage its contractual commitments from the commercial partner including a comprehensive community benefits agreement with seed funding, and digital inclusion applications and content solution support from the provider.
- Allows ubiquitous network coverage to every point in the city at availability levels and technical standards designed to meet public safety requirements and guaranteed by the provider.
- The city does not need to provide expertise or resources into marketing, sales, revenue generation, customer service and technical support required to sustain this business.
- The city charges the commercial partner for access to city assets.

Other models attempted with little or no success to date:

**Advertising-based**

All references indicate that advertiser-based models are not viable. Those who introduced the advertising-only models in the beginning did not survive or changed their practice. The CPM (cost per thousand views) rate for ads combined with the number of users required to reach any significant revenue is hardly attainable through the use of a login page and you need a customer-base initially before anyone will pay for advertising, but the advertisers are the ones who would effectively be paying for the network. The cost of acquiring a site, equipment, employees is high, no matter if it’s licensed spectrum or not, and this doesn’t account for the general business expense of operating under codes, complying with local/federal laws etc.

*Randy Hughes, a telecom manager with Longmont Power & Communications indicates that… “A business based on pure advertisement is a high-risk venture and, in my opinion, unproven,” said of the city’s decision to opt for a fee-based service.*

**Free Network with Sponsor-based Professional users**

Access is free, internet is free. The network is organized as a community, non-profit project. Keep operating cost at a minimum. Use (only) volunteers who work for free. Let professional...
users and sponsors pay for the hardware investment costs they need, from their budgets. Build an all-wireless local infrastructure. Professional users are the schools, libraries, elderly homes, local businesses, and city government. Local site-to-site connectivity can be provided by across the municipals wireless mesh network using dedicated radio connections, VLANs or VPNs. Non standard configurations require additional equipment and installation services provided by the Professional user. Free internet is available through sponsoring and sharing of existing surplus bandwidth.

Municipalities and Franchise Arrangements

Municipalities, in some cases, are concerned about existing franchise arrangements with telecom and cable providers. New opportunities for consolidating services will displace the multiple subscriptions consumers have such as cable or satellite TV, "land-line" and/or cell phone service, and broadband and/or wireless Internet service for our home computers etc. This convergence of telecom technologies poses fiscal, local control and other challenges to municipal governments.

As telecom services converge, the traditional methods of categorizing services for regulatory and taxing purposes no longer make sense. In the modern digital world, all telecom services are simply bits and bytes flowing over lines and through the air and it’s becoming increasingly difficult to determine whether a particular service is cable, telephone, Internet or some other service. Two key areas of current concern are a cities ability to continue to enter into franchise agreements with service providers and to charge utility user's taxes (UUTs). With governmental regulatory frameworks out of date, cable, telephone and Internet services now use utilize much of the same infrastructure or similar delivery methods while the government systems make no significant distinctions between cable and telephone services, yet renewable franchise agreements exist for video/cable providers and not Telecom providers.

There are several viewpoints to be taken from this discussion: First, for the cable provider these agreements require franchise fees for using public rights-of-way, but they also provide the means by which municipalities are able to mandate specific service levels; guarantee access to and funding for public, educational and governmental access television; and secure cable providers’ support for these efforts.

A cities ability to enter into franchise agreements with cable providers which include these protections and revenues is currently in question as a result of the pressure to change existing approaches to regulating telecom services.

Two key areas of concern for cities include the future ability to enter into franchise agreements with service providers and to charge utility user's taxes (UUTs).

- The legislation enacting and governing the Federal Excise Tax (FET), which involves knowing where a telephone call originated and/or terminated; or
- The place of the customer’s primary use.

With the convergence of technologies, it's not always easy to identify the customer's primary place of use. Additionally, the method used for FETs is becoming irrelevant as a basis for taxation and is threatened with extinction through legislative or regulatory actions. As a result, the definitions used in current UUT ordinances are rapidly becoming useless and no longer apply to the technology delivering the services. Further, the federal government has made it clear that it intends to repeal the FET in the next few years. Utility user taxes (UUTs) originally applied to traditional utilities such as gas, electricity, land-line telephone, cable television and, in some cities and counties, water. Telephone UUT has expanded over the last few years to include cellular providers and most telecommunications UUT ordinances. With the FETs being out of date and irrelevant as a basis for taxation, and as the UUT ordinances are rapidly becoming useless and no longer apply to the
technology delivering the services, changes must be made in the next few years to account for the discrepancies.

Another concern for local governments is how regulatory changes will impact their ability to collect 9-1-1 access fees. The 9-1-1 access fee has been adopted by California cities to recover the substantial costs of providing 9-1-1 emergency dispatch services. Fees are collected by the service providers and remitted to the local jurisdiction for the purpose of maintaining and improving access to and reaction from local emergency response and dispatch systems.

Telecommunication providers are lobbying for the elimination of 9-1-1 fees as well as UUTs. These fees help offset costs for 9-1-1 development and interconnectivity statewide. Regulators such as the California Public Utilities Commission are struggling with whether or not to regulate all of these services and, if so, how and to what extent.

Various sectors of the telecom industry have differing, sometimes contradictory, perspectives - determined largely by their current infrastructure investments and how they can best use those to leverage market advantage. The cable industry, for example, asserts that the local franchising system works, and telephone companies that want to provide Internet and video service should also be subject to local franchising requirements. In contrast, the telephone companies say that their main concern is speed to market, and within this context argue that local taxes are too onerous to collect, pay and account for, and that local franchise agreements are too complex, take too much time to negotiate, and need to be standardized. At the same time, their federal legislative proposals indicate a strong desire to avoid most public interest obligations in order to cut costs.

In the California Legislature the discussion increasingly focuses on the notion that, whatever methods are adopted at the local, state or federal level to collect fees or taxes, there must be a level playing field, ensuring equal access to customers, including use of the public rights-of-way.

As part of this centralized franchise, one option under review - thought beneficial by the industry - is to apply and collect franchise fees at the state level, thereby completely removing franchise agreements from local control, "standardizing" the rate and centralizing the point of collection. A variation on this approach, recently adopted in Texas, is a state franchise that allows franchise fees to be collected at the local level.

Local government has several concerns with centralizing franchises in general, including:

- Possibly losing control over the "time, place and manner" of accessing and using the right-of-way, currently provided by law;
- Probably losing some or all local franchise fees and the centralized government collection and allocation of those fees;
- Losing leverage to mandate and control local community programming and access, and to require support for PEG (Public, Educational and Government (PEG) Channels) access facilities and equipment;
- Controlling and leveraging service "roll out" to support local goals and programs, such as economic development or redevelopment;
- Ensuring equitable service delivery within their communities; and
- Losing the authority to enforce consumer protection regulations and to require institutional networks.

One of the many options being looked at in the California Legislature is a statewide franchise "template" or agreement. However as with most complicated subjects, the devil is in the details. Any change to the franchising system for the telecom industry has the potential to also effect changes in all other utility franchise agreements and access to rights-of-way. In the mean-time any new agreements should be heavily scrutinized as it may be a long time before any changes in the system take place.

Strix Systems is the industry's technology and market leader delivering the highest performance broadband multi-radio wireless mesh network products for large-scale city and country-wide deployments. Strix Access/One® solutions are deployed in hundreds of networks worldwide, providing capacity for over one million users, outdoor and indoor, for metropolitan areas, public safety, government, energy, transportation, hospitality, education, enterprise, residential and carrier access markets.

**Market leadership**

Strix Systems is the industry’s market leader. According to market research firm Heavy Reading, Strix Systems held the number one market share of wireless mesh network radio shipments during 2005, with over 16,000 radios shipped and over 16,000 in the first half of 2006. Strix Systems has emerged as a market-leader primarily due to the strength of Strix Systems’ products and technology. Many first-generation wireless mesh vendors have struggled to successfully deploy high-performance mesh networks while Strix Systems developed a solution that meets market requirements for performance, quality of service and the flexibility needed for every application.

**Technology leadership**

Strix Systems delivers the industry's highest performance. Strix Access/One, based on Strix Dynamic Mesh Architecture™, provides the highest quality wireless transport delivering 100% reach-ability and mobility for tomorrow’s voice, video and data applications. As proof, Iometrix, an independent testing firm, performed as series innovative tests measuring backhaul performance for data and voice under various conditions of stress, maximum client capacity, In-motion roaming delays, and re-convergence times in the event of mesh node or link failure and voice quality in the presence of data. These tests conclusively reveal Strix Systems Access/One as the highest performing wireless mesh network products on the market disproving the commonly held belief that throughput will taper off when wireless hop counts increase. Strix Systems maintained a maximum consistent throughput of 35 Mbit/s which remained constant over one, two, three, and four hops while simultaneously handling the largest number of high quality voice over IP (VoIP) calls and performing high-speed mobility hand-off. Remarkably, Strix Systems continued to maintain excellent connectivity where others would simply fail.

Strix takes advantage of standards-based technologies including 802.11a, 802.11b, 802.11g, 802.11j and 802.16 (WiMAX ) and the products employ RF-independence with communications in the 2.4Ghz, 4.9Ghz and 5Ghz frequency ranges. Strix Access/One products encompass industry-leading innovations enabling "always available" high performance, high density connectivity from any location in any geography enabling data, voice and video.

Building and maintaining a wireless mesh network is a dynamic process. The architecture is itself a distributed network intelligence which utilizes fast, sophisticated algorithms running on high performance hardware, controlled by a significantly intelligent, fast, and efficient software design. Identifying that no existing technologies exist on the market to enable 100% mobility and reach-ability for a broad-range of data, voice and video, Strix Systems developed Strix DMA™ - Dynamic Mesh Architecture as the infrastructure for large-scale wireless mesh network deployments.
Strix Dynamic Mesh Architecture

The Company developed the Strix Dynamic Mesh Architecture™ (Strix DMA™) enabling the highest throughput, lowest latency, greatest scalability, 100% mobility and reach-ability for a broad-range of data, voice and video applications.

The Strix DMA™ comprises two elements: HPMA™ and SMFR™. The Company’s High Performance Modular Architecture (HPMA™) hardware engages any radio with any technology in any configuration through integrated hardware design. HPMA™ dynamically adapts to network infrastructure and the environment, extremely scalable, HPMA engages multiple radios and provides enhanced transmission power and receiver sensitivity. Strix HPMA also improves upon standards-based 802.11a, 802.11b, 802.11g, 802.11j and 802.16 (WiMAX) technologies that operate in the 2.4Ghz, 4.9Ghz and 5.8Ghz frequency, doubling throughout and delivering 100Mbps non-blocking performance across radios.

Strix Scalable Mesh Fast Re-route™ (SMFR™) is the industry’s most scalable wireless mesh network technology enabling distributed localized node intelligence, network topology-independent fast re-routing, instant roaming, near-zero throughput loss, and near-zero latency over multiple hops. SMFR™ offers the fastest roaming handoff, and largest capacity achieved by distributed node intelligence, dynamic zero-latency path selection, and maximum multi-hop traffic distribution.

<table>
<thead>
<tr>
<th>Up to 6 radios per node</th>
<th>Multi-use network support with QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual radios serve unique purposes in a node – ingress or egress in the mesh backbone</td>
<td>Strix DMA implements Quality of Service supporting mixed-use networks where varying security schemes are implemented based on user type and different levels of priority can be assigned to the various network traffic.</td>
</tr>
<tr>
<td>Benefit: better performance across the entire network with the ability to support more users per node and fewer nodes per square mile</td>
<td>Benefit: Networks can serve multiple purposes, eliminating the expense of deploying multiple networks with the appropriate types of traffic receiving priority, and the integrity of the data remaining secure.</td>
</tr>
<tr>
<td><strong>Multiple Channels in the mesh</strong></td>
<td><strong>High multi-hop capabilities</strong></td>
</tr>
<tr>
<td>The mesh backbones can be built on separate channels amongst nodes to address interference issues.</td>
<td>Ability to multi-hop traffic throughout the network without degrading performance.</td>
</tr>
<tr>
<td>Benefit: Overall network performance is not impacted by interference in any part of the wireless network.</td>
<td>Benefit: minimizes the cost of ongoing network operations, and reduces the complexity of network planning and design associated with too many wired drops in the network.</td>
</tr>
<tr>
<td><strong>Multiple RF support</strong></td>
<td><strong>Voice, video and data support</strong></td>
</tr>
<tr>
<td>All 802.11 technologies can be supported from Strix O/WS nodes.</td>
<td>Low latency with high performance mesh backbones that can support multiple types of traffic.</td>
</tr>
<tr>
<td>Benefit: Different spectrums can be used for the mesh backbones and for the clients, minimizing interference issues and maximizing the network's performance.</td>
<td>Benefit: Real-time voice and video applications can be run on the mesh, increasing the overall usefulness of the network.</td>
</tr>
</tbody>
</table>
Strix SMFR automatically locates all other network nodes, selecting the best path based on real-time backhaul path analysis using roundtrip delay (RTD), signal-to-noise ratio (SNR) and other criteria. Strix nodes continue to scan and evaluate the best and alternate paths to each wired node, if the criteria of the best path drops below the set threshold or the path is blocked the system continues the self-healing process to acquire the next best path – all with milliseconds. SMFR™ continuously performs self-tuning, optimizing each path for best performance and congestive redirection, even for mobile OWS nodes moving at 200MPH.

SMFR™ optimizes path selection regardless of network topology or size. Unlike slow IP routing solutions that require networks to re-converge in order to route around trouble, SMFR™ makes these decisions locally at the node without the overhead of cumbersome routing algorithms. This ensures the fastest transitions and zero-downtime. The resulting mesh network is highly scalable, reliable, and enables instant roaming handoff.

**Key features and benefits**

*Independent lab tests reveal unmatched performance and capacity*

Independent testing by Iometrix revealed Strix Systems to have unmatched performance over multiple hops while additionally handling the largest number of high quality voice calls. The tests conducted under the guidance of a test plan developed by Iometrix and the continuing standards work by the Institute of Electrical and Electronics Engineers Inc. (IEEE) 802.11 Task Group for Tests. The tests were performed utilizing RF-shielded equipment from Azimuth Systems Inc.
The first edition of the plan specified a series of rigorous tests to determine:

- Backhaul performance for data and voice under various conditions of stress
- Maximum client capacity
- In-motion roaming delays
- Re-convergence times in the event of mesh node failure
- Voice quality in the presence of data

The results from testing of the Strix Access/One equipment disprove the commonly held belief that throughput will taper off when hop counts increase. Maximum throughput was sustained, remained constant over one, two, three, and four hops. The tests also proved that the products provide sub-second mobility hand-off delay and that Strix nodes can backhaul the industry’s highest number of high quality voice (VoIP) calls; regardless of the number of hops.

- Access/One® products’ single-node capacity rates at the industry standard five stars.
- Access/One® equipment supported 36 excellent-quality calls over four hops (five stars). This slid to 23 calls when voice data had to compete with data occupying half of the bandwidth.
- Access/One® products’ mobility handoff delay gets under the 50 millisecond delay requirement of telecommunications operators.
- Access/One® products’ failover roaming delay of one second is at the highest level in the wired Ethernet environment

Strix Systems’ multi-radio, multi-RF, and multi-channel architecture lowers capital expenditures (CapEx), operational expenditures (OpEx). The Company’s future-proof technology is scalable up to the maximum number of radios depending on the type and size of deployment. This is the most cost effective method to deploy wireless mesh networks as most networks require more than two radios. In contrast to competing solutions which employ fewer radios, it costs less per megabit, and in man-power, to purchase and deploy ~one~ six-radio node compared with three two-radio nodes. Multi-radio, multi-RF nodes cost less per radio, are cheaper to install per radio, and more cost effective by allowing for greater distances between nodes and fewer backhauls per network.

**Strix End-to-End Solution**

**Access/One® Networks**

Strix Access/One family of products provides the broadest coverage in the industry reduces the number of nodes required per square mile and accelerates deployment therefore lowers CapEx and operational expenditures (OpEx) which amounts to lower cost of ownership. Unrivaled value is delivered via the highest capacity in the industry—a maximum of 768 users per node as well as over 100 Mbps throughput per node resulting in 3-6 times the norm. Enable minimal throughput loss and minimal latency for over 10 hops means real-time application support with a minimum number of wired connections required for a given area and significantly lower CapEx and OpEx. Provide future-proof modularity lets the OWS 2400 scale to up to six radios as needed and migrate smoothly to WiMAX without a forklift upgrade and the lowest cost per radio in the industry results in significantly lower capital expenditures (CapEx).
Strix Systems award-winning Access/One® Products

Access/One® Network Products

Our Access/One® family of products provide the broadest coverage in the industry, reduce the number of nodes required per square mile, accelerate network deployment, and lower capital expenditures and operational expenditures. Strix’s Access/One® family of products is a fully integrated and coherent wireless network system that delivers intelligence, scalability, security and high performance.

Access/One® Network OWS

Strix’s Access/One® Network Outdoor Wireless System (OWS) 2400 and 3600 are the industry's only modular, multi-radio, multi-RF, and multi-channel products for outdoor deployments. These products enable exceptional range, coverage and penetration for large-scale city/metropolitan and country-wide networks.

Access/One® Network OWS enables the deployment of 802.11 and 802.16 networks across large urban areas, rural counties and entire regions. Ideal for government agencies, public utilities, high-speed transportation systems and mobile users who want uninterrupted service on a citywide basis, the OWS delivers any mix of backhaul and client access services in a single form-factor to simplify planning and installation. This reduces deployment costs while delivering the industry's highest performance wireless mesh networking system. The OWS can also support any radio in any combination of 802.11 a/b/g/j, 802.16 (WiMAX), 2.4GHz, 4.9GHz and 5.8GHz. Each radio is dedicated for specific functions in the outdoor network within a single node. Supporting up to six radios means enables maximum flexibility to deliver multi-radio mesh backbones, and multi-RF client connectivity for various real time applications.

Access/One® Network IWS

Our Access/One® Network Indoor Wireless System (IWS) is the industry’s first fully modular wireless mesh system for mission critical data, voice, video, public wireless Internet access and fast-roaming mobility. The IWS is designed for ease of deployment, easy to manage, scalability, resilient and reliable. The IWS provides high density access allowing the industry’s largest number of users connected through the system at any time and delivers innovative and intelligent management functionality. Each node is intelligent and independent capable of self configure, self discovery, self tuning and self healing. The IWS can be used by large enterprises, distributed corporation, state, local and federal government agencies, public transportation and more.

Access/One® Network EWS

The EWS-100 is the Company’s Customer Premise Equipment (CPE) device for low-cost residential and business connectivity. The EWS provides dual radio access, simplifying connectivity between Strix outdoor wireless mesh networks and the end-users indoor Local Area Network (LAN). The EWS-100 provides double the wireless transmission power for 802.11g and 802.11a. This provides increased...
connection range and allows customers a user-friendly plug-n-play experience. The unit provides an Ethernet connection for multiple PC’s and devices such as multimedia gateways also provides remote management functions for Strix partners to manage all aspects of the users connection into the outdoor wireless network. A significant achievement is the ability of the EWS and Strix outdoor wireless mesh networks to provide 100% mobility during the transition from the inside home or office to the outside network.

Manager/One®

While Access/One OWS, IWS and EWS are self-managing, the same management is further enhanced via Strix Manager/One® software interface, giving the network management personnel complete configuration, monitoring, statistics, fine-tuning and customer assistance control over the wireless mesh network’s operation.

Strix Manager/One provides enhanced control over the network and configuration can be as simple as a single push of a button, whether for a single unit installation, a city or country-wide deployment. Each network device can be managed as a group or individually via a secured connection and an assortment of graphical and statistical displays provide the detail needed to isolate potential trouble spots. Segment View provides a window into each Ethernet connection segment within the network, with a choice of views (list or icon). Simply choose the view you prefer with a click of the mouse. GPS Positioning provides exact geographic mapping of Strix network elements. Once the mesh network is formed, the network creates and inventory control used for secured encrypted bi-directional authentication of Strix network devices list which is distributed to all Strix devices participating in the network and any devices that are not part of the inventory list cannot participate in network topology building, exchanging configuration information, or managing Strix devices. Secure Remote Management and an industry compatible and Strix enhanced proprietary MIB (Management Information Base) make management simple. SNMP management consoles such as HP OpenView and other industry-leading systems can be used to manage the network remotely and securely. Network Management traffic on the Ethernet between the network server and module is automatically encrypted to prevent “listening” on the LAN/WAN.

Conclusion

Today municipalities are taking it among themselves to be the carrier of network communication services to their communities. While the need to provide these services has increased so has the inability for large carriers to provide these services. Utilizing a business model that includes the public municipality as a primary tenant and a private entity to deliver the services, a municipality today can provide a city-wide wireless network infrastructure to meet their growing needs. Municipalities may have concerns with regard to the continuation of telecom franchise agreements, yet when in these arrangements municipalities have little, if any, control over such issues as antenna location, density and the delivery of and time-frame of services offered, not to mention additional complexities making these franchises increasingly more difficult and costly to manage. WiFi presents an opportunity for municipal government to take control of the services delivered to their municipalities.
Three or more years ago most people’s perception of WiFi was based on their use of a low-end wireless bridge or router in the home. That same bridge/router then found its way into public hotspots including coffee shops and airports. Today with the improvements in WiFi technology, and through much innovation, that same WiFi technology is no longer limited to small 100 meter areas, but can now provide miles of coverage. While traditional approaches to wireless would provide point-to-point and point-to-multipoint connectivity, there was still no way to provide ubiquitous wireless connectivity throughout a large scale area and provide the redundancies with the resilience and qualities of service required for a city-wide network. It was the introduction of the 3rd approach and 3rd generation of wireless products that would make large-scale wireless a reality. The evolution, or some would say “revolution”, of wireless mesh networks enables a broad range of new municipal services to be delivered, dramatically improving existing communications between departments and agencies while enabling city-wide access to response-critical resources.

With over 300 municipal wireless mesh network RFPs in progress, municipalities have truly realized the opportunities that wireless mesh networks provide, but as community awareness and involvement increases so do their concerns. Having gained significant media attention, cell phones have been heavily scrutinized, and equally tested, with no confirmation of danger. While cell phones are each equipped with power ranging up to 3 watts - which we hold to our head, there is cause for some concern and there have been unofficial warnings with regard to their high use and use by children. However, studies have also shown that a WiFi device in the home, having 1/15th the power of a cell phone doesn’t pose any risk, besides the fact that a WiFi device is not placed in proximity to a persons head. In a large-scale wireless deployment, power for a WiFi device serving hundreds of people may have power ranging to 500 mW - still 1/10th that of a single cell phone. It’s more likely that personal microwaves in our kitchens, having 10 times the power of a cell phone, no matter how infrequently they are used, will cause negative biological effects in humans.

Today’s Wireless Mesh Networks break down the boundaries of existing communications systems and define the future of “next generation networks”. By utilizing an intelligent distributed “Mesh” network where distributed intelligence resides within each access point, the highest performance and in-field future-proof modularity makes it possible to take advantage of new technology such as 4.9GHz for public safety, 802.11n, WiMAX and newer technologies as they come available.

Strix Systems answers the hard questions and provides the products and services that make a single investment with the lowest total cost of ownership possible.

Strix Systems, Inc., www.strixsystems.com, info@strixsystems.com 1.877.STRIXSYS
All trademarks, logos and service marks are the property of Strix Systems.
Copyright © 2000-2007 Strix Systems, Inc. All rights reserved.