firetide®
Reliable connectivity anywhere™

WHITE PAPER

Deploying Wireless Access for Municipalities

September 2008

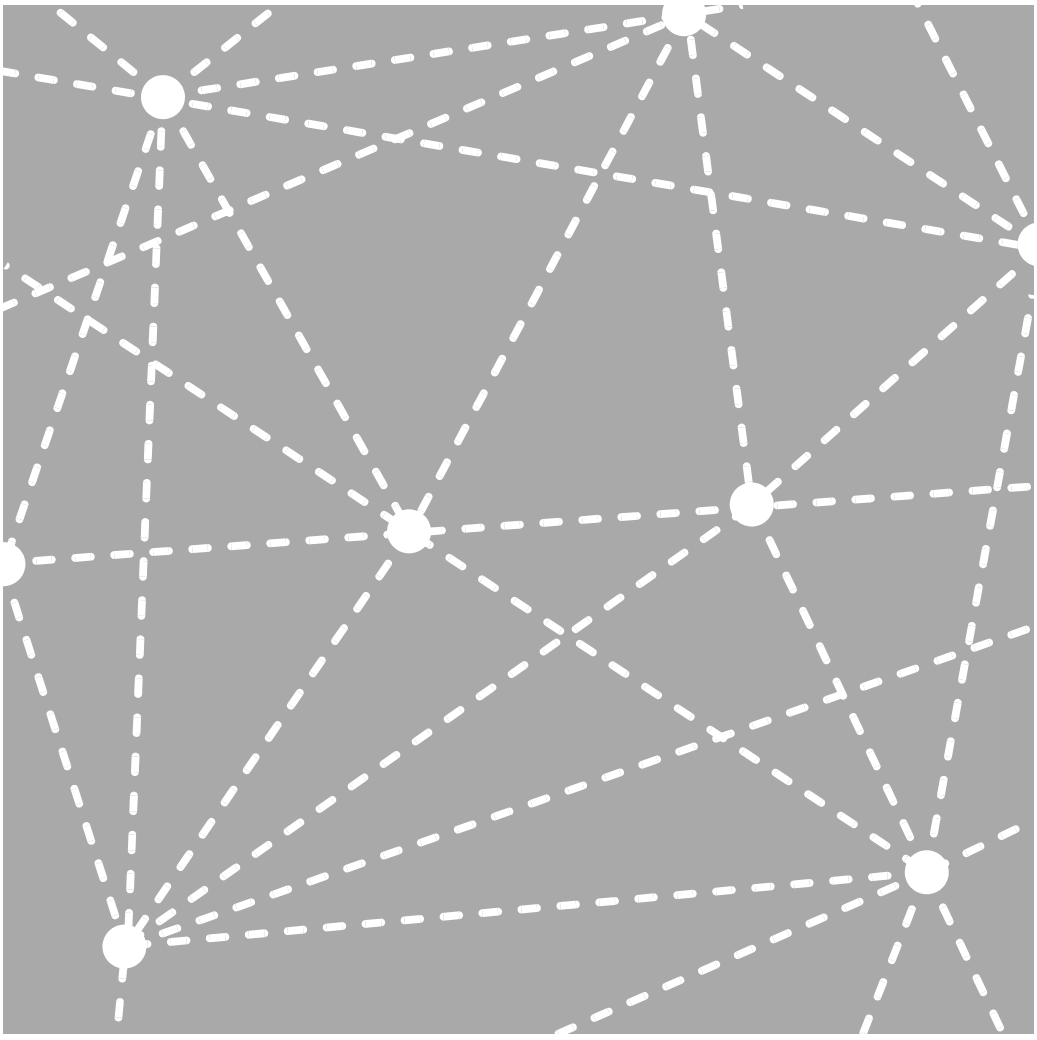


Table of Contents

Executive Overview

This document describes the Firetide system and its application in municipal wireless access deployments. It explains backhaul design as well as edge design. The emphasis is on outdoor WiFi access. Issues of sharing infrastructure between general-purpose access and public safety access are addressed.

Municipal Wireless Deployment Technology

A municipal wireless deployment requires Wi-Fi access points, of course, but it requires more than this if it is to be successful. A complete deployment needs an effective backhaul system that can support the access point density required, and it needs service delivery methods that can manage customers and network demand in a way that meets all service commitments.

Because the backhaul is a critical component on which all other service delivery depends, it's best to begin an analysis by looking at how backhaul techniques can connect to the primary Internet point of presence (POP).

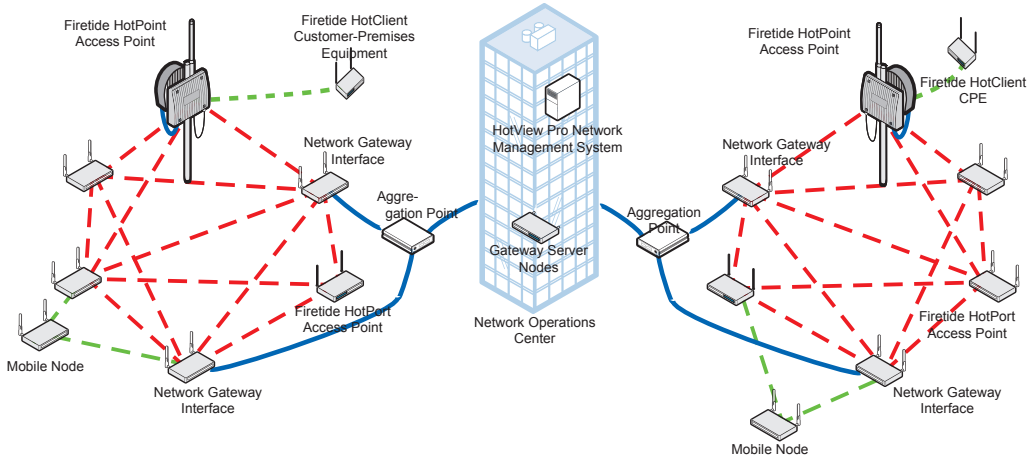
Building Out

Every municipal deployment has a point of presence where the municipal network is connected to the public Internet backbone. The POP contains routers, servers, and other equipment. It may be located within municipal property, or it may be in a 'carrier hotel', under the management of an ISP or carrier.

From this point, service can be delivered over high-speed data lines to some locations, but few cities have a sufficient density of high-speed data lines to support a fully wired backhaul. Thus, most deployments use wireless technology to reach out from one, or a handful, of wired aggregation points to provide overall coverage.

Thus, wireless mesh is acting as the primary Ethernet distribution and backbone infrastructure for the network. Whether there is a single connection to the wired Internet, or multiple connections to the Internet, the mesh is the key foundation for all service delivery.

Figure 1. Typical Municipal Network



Backhaul Coverage

How much coverage is required? This depends on the range of applications planned for the system. Possible municipal applications can include:

- Ethernet-equivalent data access for police, fire, and public safety applications.
- 802.11 WiFi access for police, fire, and public safety applications.
- Video surveillance cameras.
- Free public Wi-Fi access.
- Metered public Wi-Fi access.
- Ethernet-equivalent Internet Service Provision for residential and SOHO users.

Each of these services requires a coverage pattern and a bandwidth requirement. These will determine the build-out strategy you follow.

From each wired aggregation point, you will extend wireless links to each chosen Wi-Fi access point location. This leads to the first design decision: point-to-point wireless or mesh wireless?

Point-to-Point vs Mesh

A number of vendors offer radio equipment designed to transmit data at high speeds, often over fairly long distances. This equipment can be quite useful, but most municipal deployments don't need the long distance. They do need multipoint coverage, however. Firetide HotPort mesh nodes are an excellent choice for such deployments.

User Access

User access is proved in one of three basic ways, depending on the class of user.

- Ordinary Wi-Fi users connect via 802.11 access points, which are in turn connected to the Firetide mesh nodes. The access point connects to the mesh node as an ordinary Ethernet device. Firetide supports both co-located nodes and access points, and more importantly, separately-mounted ones. It's often the case that the optimum node placement location is not quite the same as the optimum access point location.
- Public-safety and other restricted-use clients connect to specialized access points configured to meet their requirements. There are several options, described in more detail in the section on access points.
- Some users require a wired Ethernet connection. This can be delivered using wireless transceivers located at the user site. This is covered in detail in a later section.

Each class of user has definable access rules and bandwidth limits. In addition, strong security mechanisms insure privacy across classes of users.

Firetide HotPort Mesh Nodes for Backhaul

Firetide HotPort Mesh Nodes are designed expressly to provide Ethernet-equivalent backhaul infrastructure for municipalities and enterprises. They offer several key advantages for this application:

- HotPort nodes are fully Ethernet compatible, and therefore interface smoothly with other networking equipment.
- A HotPort mesh is functionally equivalent to an Ethernet switch, and so it does not interfere with existing Internet routing techniques.
- The HotPort is 'tri-band'; that is, it supports 2.4 GHz, 5 GHz, and the US Public Safety Band at 4.9 GHz. The nodes are universal, so equipment does not become obsolete if you change bands or re-deploy elsewhere.
- Firetide provides sophisticated multi-level encryption and security features, so that data is safe, and the mesh cannot be eaves-dropped or hacked.
- As a managed Ethernet switch, each HotPort mesh has programmable Quality of Service (QoS) and full VLAN support.
- Dual-radio nodes support full duplex, two-way operation.

A well-engineered Firetide mesh backhaul solution is fully capable of supported any or all of the applications common to municipal deployments. Because the nodes form a mesh, there is redundancy. Edge nodes have multiple paths back to the wireline aggregation point, thus loss of a single node does not compromise overall service.

Figure 2. HotPort Outdoor Node Mounted on Pole

Wireless Mesh Build-Out

Build-out begins by working out from the wireline aggregation point (or points). An RF site survey is performed, so that the optimum RF channel and node placements can be determined, and antennas are purchased as required. Nodes are built out from the aggregation point in a mesh or grid pattern. This helps to insure redundant coverage.

Typically, the mesh is built out 'live', that is, as each node is deployed, network management personnel see it appear in the management software system. Thus, any minor problem can be addressed quickly and easily while the installation crew is on site.

Siting the Mesh Nodes

Mesh node sites are determined by several factors:

- Desired location of access points.
- Desired location of surveillance cameras (if applicable)
- RF coverage and range of the node itself.

In a municipal environment, it's often best to locate the mesh nodes relatively high above the ground, to provide clearance over buildings and trees. A short Ethernet cable connection supports other equipment that may be located closer to the ground.

The dual radio capability of Firetide nodes gives more flexibility in placement, because the two radios can operate on different bands. Since each radio has its own antenna, each antenna can be optimized for that particular RF link.

Growing the Mesh

The modular capability of Firetide's equipment lets you follow a 'pay as you go' strategy. Initially, individual islands of connectivity are provided around the wired aggregation points. Services are fully deployed in these islands, thus generating revenue.

Islands are then expanded, based on demand. New islands can also be created.

Eventually, as the islands grow, the meshes provide 100% backhaul coverage over the entire municipal area. If bandwidth continues to grow, meshes can be overlaid to provide additional capacity, or additional wired exit points can be added to existing meshes.

Mesh Security

HotPort nodes provide security with a defense-in-depth strategy. This begins with over-the-air encryption. All radio traffic, including operation overhead as well as payload, is encrypted. Second, all traffic across the mesh (entry to exit) can be encrypted a second time, this protecting even while it is inside a node.

In some cases you might connect two meshes with a wired link running over a potentially-accessible wire. Firetide uses a separate, securely-encrypted tunnels for this.

Node security is accomplished with signed certificates. This blocks any attempt to add an unauthorized node to a mesh or perform a 'man in the middle' attack.

It's also possible to limit access by restricting it to pre-defined Ethernet MAC addresses.

Deploying Access Points

Access point deployment is driven by one over-riding variable: most laptops and other 802.11 client devices have low-power radios, typically 50 milliwatts (mW), versus the 400 mW found in most base stations. Thus, an access point's coverage is determined by its ability to hear clients, not the other way around.

This means that access points must be deployed more densely that backhaul nodes. It also means that planners should consider whether universal 802.11 Wi-Fi access coverage is a worthwhile goal, or whether coverage only in key areas is sufficient to meet the municipality's needs. Note that there are other ways to provide Internet access besides Wi-Fi, and these may be more appropriate for some classes of users.

How much coverage can an access point provide? There are a large number of variables, but generally speaking a typical Wi-Fi connection has a range of 150 to 300 feet.

Indoor vs Outdoor

Signals in the 2.4 GHz and 5 GHz bands do not penetrate solid structures well, so it can be difficult to get signals from outdoor APs to indoor users, and vice versa. Firetide offers a solution to this problem, covered in a later chapter.

For municipal wireless planners, it's best to deploy access point coverage in outdoor public areas first. There are two reasons: these are typically where laptop-equipped users will be, and it's relatively straightforward to deploy.

Density

Access points are often deployed in clusters of two to four APs. This offers several benefits:

- Directional antennas can be used to increase the coverage area.
- Access points can be placed on different channels to increase capacity.
- An access point can be dedicated to the Public Safety band (4.9 GHz in the US) for those applications which require it.

Clustering also keeps deployment costs under control, because it allows multiple APs to share a single backhaul node.

Split Mesh Node / Access Point Deployments

An advantage of the Firetide architecture is the split mesh node / access point features. While the access point can be co-located with the mesh node, it's often advantageous to mount the two modules separately. The HotPort node is place high, for good coverage. Typically this will be a rooftop or pole. The access point is then placed closer to the ground, where the users are. The two modules are connected with a short Ethernet wire.

Tri-Band Operation and Public Safety

While the majority of today's Wi-Fi clients are 802.11b/g and use the 2.4 GHz spectrum, there are distinct advantages to supporting all three bands. Foremost is support for the US Public Safety band, at 4.9 GHz. This band is largely interference-free, due to its restricted use; whereas the 2.4 GHz band is crowded both with 802.11 users and items such as microwave ovens.

Deploying a public-safety system as part of an overall municipal deployment reduces costs by increasing the total number of users supporting the infrastructure. Quality of service for first-responders can be assured by correct provision of VLANs, bandwidth allocations, and QoS settings. It's even possible, during severe emergencies, to disable general public access and preserve full system capacity for emergency personnel.

The 802.11a band, at 5 GHz, is also lightly used. While not as popular in consumer products, client cards are available, and it is a viable choice for service deployment where possible.

Security and Access

A multi-service, multi-access network requires sophisticated access and security controls. Even free service needs access controls, to prevent hostile users from sending spam or conducting attacks on other systems.

Security begins with encryption. The gold standard for Wi-Fi security is WPA2 with 802.1X authentication. This provides extremely strong encryption; more importantly, it makes it difficult to crack keys by avoiding pre-shared ones. Rotating keys mean that even a cracked key isn't useful.

Public Access

It's often desirable to allow easy public access, either as a free service or a paid service. This can be done with passwords, but it's usually easier to direct the user to a login page, where the user can enter account information and then be granted access to the Internet. Such browser-redirect services are nearly universal in modern wireless deployments.

A related feature is the so-called Walled Garden. This feature provides a range of web sites and web pages that users may visit, but prevents them from leaving without additional authorization.

Dealing with Hack Attempts

A common method of hacking networks is to set up a so-called rogue access point. This can be a real AP, or a PC masquerading as an AP. In either case, it represents a serious potential security hole, both because it can allow unauthorized users onto the Internet, and because it can be used to capture passwords and other sensitive information.

Firetide access points detect and report any and all sources of apparent AP activity in their area. Thus they are able to spot rogue APs and alert system administrators of their presence.

Quality of Service

In the few years that 802.11 has existed, user expectations have evolved from simply wanting any kind of access to demanding high-speed, low-latency connections that can support VoIP, video, and large file downloads. Modern 802.11 wireless networks must support QoS. Firetide's AP family supports QoS.

Mobile Users

Many users of modern wireless nets are mobile. Not simply likely to move from one coffee shop to another, but to be active users of wireless while moving, on foot or in a vehicle. In particular, emergency-service personnel need reliable wireless access even while moving rapidly in police cars, fire trucks, or ambulances.

Standard 802.11 systems don't support this. Typically, moving form one AP to another requires manual reconnection. It is possible to manage the process in a way that smoothly hands off the user from one AP to another in a way that makes any service interruption virtually invisible. Firetide offers this via its Mobility Controller platform.

Firetide HotPoint Access Points

Firetide has developed a family of 802.11a/b/g access points that meet all of the requirements of modern multi-service municipal deployments. In particular, they offer:

- Full support for 802.11a/b/g service.
- Full support for public-safety frequencies.
- Sophisticated security and access-control features.
- Rogue access-point detection.
- Walled-garden and browser-redirect capabilities.
- Support for QoS, including 802.11e
- Support for mobile clients, even across multiple meshes in a city-wide configuration.

HotPoint APs are available in indoor and outdoor configurations. Functionality is the same in both units.

Figure 3. Model 4501 Indoor HotPoint AP

AP Placement

While it might seem more convenient to package the AP and the backhaul node in the same enclosure, this is less useful than it appears. Firetide has chosen to package the two units separately because it is usually the case that the AP wants to be close to the ground, where users are, while the backhaul node wants to be at higher elevation, where its range can be optimized.

Subways and other underground or heavily-obstructed sites present a unique opportunity for this split architecture. By separating the HotPort backhaul node and the HotPoint AP, it's easy to provide 802.11 Wi-Fi in underground subway stations and similar locations. The backhaul node can be placed above ground, to insure good signal strength, and a run of Ethernet cable is used to connect to an underground access point. The AP can be powered over this line as well. Lines can be run through airshafts, conduit, or whatever is convenient.

Multiple APs

This document has discussed the multiple roles APs can play in providing access for different classes of users. This is a powerful capability, but if it had to be implemented with multiple physical access points it would not be cost-effective. The next section describes Firetide's solution to this challenge, using virtualization technology.

Virtualization and its Role in the Network

The IT industry is going through a transition as virtualization technology rewrites the rules on efficient service delivery. While much of the focus has been on virtualization for servers, the technology is extremely useful in other parts of the IT infrastructure as well.

Virtualization is not a new technology. It was first reduced to practice by IBM in the 1970s, and remains the standard for most mainframes today. Virtualization took off in the data center when modern server-class microprocessors from Intel and AMD added a few key hardware 'hooks' to simplify the implementation. These hooks eliminated almost all of the overhead associated with virtualization, allowing virtualized system to deliver near-100% capacity.

Virtualization is not new to networking, either. Virtual LANs were developed almost immediately after Ethernet became widespread in the 1980s in order to isolate traffic.

Firetide's Innovation

Firetide has combined the virtual-LAN concept, already widely used in both wired and wireless LAN deployments, with the virtual server concept developed for server rooms, to create the HotPoint family of fully-virtualized access point solutions. The HotPoint AP system supports up to 16 instances of an access point on each hardware system, and fully supports the mapping of these virtual access points (VAPs) to VLANs. This lets network designers deploy multiple access points systems for multiple applications without the expense of multiple instances of hardware.

The VAP Concept

Each VAP is a unique wireless entity. It has an ESSID, the name seen by users. It has unique settings for security, DHCP, NAT, and other typical access point functions. Thus it is easy to create and dedicate a VAP to a particular class of users (e.g. guest) or clients (e.g. barcode scanners).

Benefits

Today's wireless environment must support a wide range of applications; far beyond simple email and web access. Both enterprise and municipal deployments require multiple different types of wireless infrastructure. Increasingly, enterprises need to provide multiple levels of access for web and email, so that both employees and guests are accommodated. In addition, wireless VoIP phones benefit from a dedicated wireless network. Many older wireless devices, such as handheld barcode scanners, do not support some of the more sophisticated security environments, such as 802.1X, and are best segregated on a dedicated network. Thus, it's common to see requirements for half a dozen separate wireless LANs, and some enterprises may need ten or more.

Municipal deployments often have even more categories of users, as public-safety personnel are added to the mix. In addition, many municipal wireless deployments function as general-purpose ISPs to residences and small businesses, and so have need of multiple wireless infrastructures.

VAP + VLAN

With the Firetide HotPoint Virtual AP (VAP) solution, you can create an instance of a virtual AP for each class of user, or use, that you have. The VAP is given security settings, IP address settings, and other parameters typical of a wireless access point.

Next, the VAP is assigned to a VLAN. This VLAN is then routed through whatever levels of security and authentication your enterprise requires. Different classes of users are kept separate and secure.

VAPs plus VLANs let you route and isolate wireless traffic as required to meed all of your organization's security needs.

Managing Bandwidth

Piling multiple classes of users into virtual machines would be of little value if performance suffered. Firetide's virtualization technology lets you assign bandwidth limits to each virtual AP. This insures that high-priority users, such as VoIP clients, get the bandwidth and latency they need.

Keeping Wireless Management Easy

Hundreds of physical access points combined with dozens of virtual APs on each box could be a management nightmare. Firetide has addressed with issue with a unified management tool, HotView Pro, that provides simultaneous visibility into the virtual AP world, the physical access point world, and the backhaul system.

Views - The Concept

Users of wireless services see an SSID - the name of the service that pops up on the user's computer screen. Behind this there can be multiple collections of hardware and service offerings.

IT managers, on the other hand, see hardware, IP addresses, security settings, and related information. It is largely an independent view from that seen by users.

Firetide's management platform, HotView Pro, addresses these different views by providing Groups. Specifically, **AP Groups** are a management entity, and allow IT managers to control large numbers of hardware platforms simultaneously. You can define as many AP Groups as required, and management access privileges can be different for each group.

VAP Groups are collections of VAPs. A VAP Group defines the settings users see for that virtual access instance. You can then choose to instantiate a given VAP Group on individual hardware platforms. It isn't necessary to have every VAP exist on every platform.

Firetide further simplifies management by separating the management IP address space from the user IP address space. Thus, all management can be done over a separate, private, subnet (which can be on its own VLAN, if desired). This enhances security - users cannot get to the management subnet.

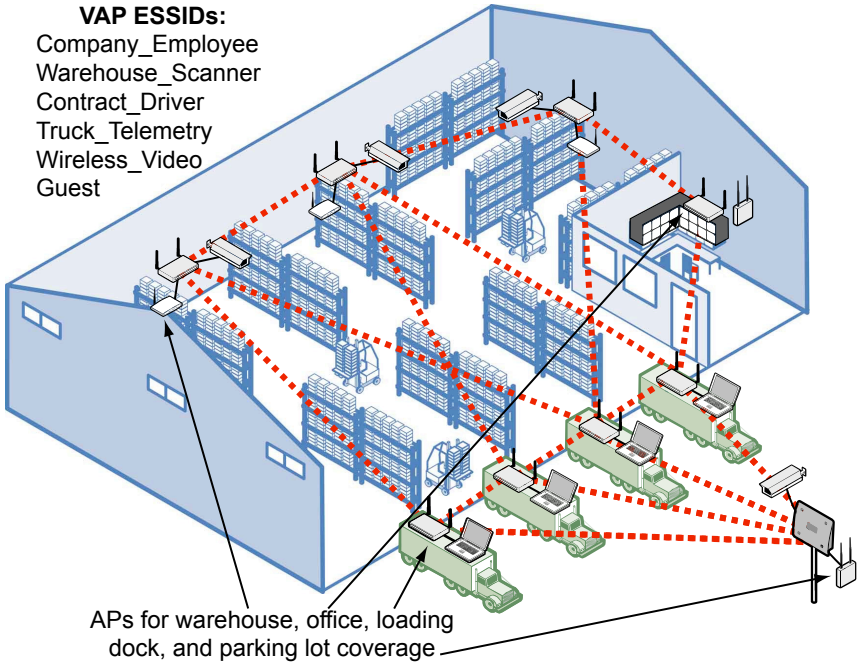
Table 1 list some of the key settings available within each grouping.

Table 1. AP Group and VAP Group Settings

AP	AP Group	VAP	VAP Group
Management IP Address Radio Settings Firewall Settings	Management Login/Password	DHCP Settings DNS Settings NAT Settings	ESSID Security Method/Key MAC Address Control VLAN User Datarate Control

Figure 4 shows a typical application scenario, with multiple VAPs distributed across a collection of physical access points.

Figure 4. Typical AP-VAP Deployment



The same physical collection of nodes is able to offer secure employee wireless access and separate secure access for warehouse barcode scanners. (Low-end devices such as scanners often do not support the most recent security technologies, and so should be kept on their own, separately-secured network). Trusted contract truck drivers have a secure mesh that is still isolated from company data. Guest have a non-secure network. Wireless video cameras are supported on their own bandwidth-controlled mesh.

Backhaul

Firetide's virtualized access-point solution has been designed to work with either wired backhaul, wireless backhaul, or a mix of both. HotView Pro, the management tool, gives you control over Firetide's wireless backhaul system.

By using HotView Pro along with HotPort nodes and HotPoint access points, you gain a complete management system. It offers full control, but also lets you limit types of access for different classes of administrators.

Leveraging Virtualization to Deliver Next-Generation Services

Existing application demands in the enterprise are more than enough reason to move to a virtualized access-point deployment architecture, but Firetide's VAP technology is the key enabler for a new application category: that of delivering Internet service to homes and small business in the metropolitan environment.

Firetide's unique advantages in this application are discussed in the next section.

Broadband Internet Service Delivery via Wireless

For many consumers and small businesses, choices for Internet access are limited. At best, a given location might have a choice of either cable-based service or DSL. Competition is low and costs are high. Satellite-based access does not support VoIP or VPNs well. Cellular data, even with advanced 3G technologies, is not reliable enough and may not be cost-effective, depending on the carrier.

Recently there have been several well-publicized efforts to deploy wireless Internet access across a municipal area. Some of these efforts have met with limited success. In part this has been because of the use of equipment designed primarily for short-range indoor applications, namely, traditional 802.11b/g access points. While basic 802.11 wireless protocols are more than adequate for delivery of Internet service wirelessly, the system must be designed for this function.

The Challenges of Municipal Wireless

The challenges of municipal wireless can be summarized in two words: buildings and trees. This is not meant to over-simplify. Rather, it summarizes a real-world characteristic of modern wireless systems: the microwave frequencies at which they operate are affected by buildings and trees. Trees absorb signals at 2.4 and 5 GHz. Buildings absorb or reflect signals, depending on construction material.

This problem is compounded by the fact that most wireless client hardware - e.g., your laptop - is equipped with a 50 mW transmitter, rather than the 400 mW transmitters common in base station. Thus, it's often the case that the user can hear to base station, but the base station cannot hear the user.

While every city is different, the net result of these real-world conditions is that the radio links must be short, in other words, numerous access points are required in order to 'blanket' a community with a signal strong enough to reach typical consumer wireless equipment.

Possible Solutions

One much-discussed future solution is WiMAX, also known as 802.16. This technology allows a central base station to provide connectivity to hundreds or even thousands of subscribers over a range of many kilometers.

The technology has been successfully demonstrated and there have been trial deployments. However, WiMAX faces some of the same technical challenges as 802.11, and some challenges unique to WiMAX. Because WiMAX operates in the microwave range, it is susceptible to the same RF conditions as 802.11. In fact, some of the most successful deployments have been in rural farm areas - lots of flat land and no trees.

WiMAX is also a shared-medium technology - all users must contend for bandwidth with the base station. Thus real-world performance varies with usage. Again, some of the most successful WiMAX deployments have been in rural areas where the total subscriber base is small.

WiMAX has a role to play in Internet delivery, but it is not well suited for denser municipal deployments. What, then, would be the ideal solution for municipal access?

Deployment Density

Access nodes must be deployed throughout the coverage area, to avoid problems with trees and buildings. While adequate transmitter power is a requirement, most transmission problems caused by trees and buildings cannot be solved by increasing power levels. Government regulations restrict maximum levels, and in cases where reflections are a problem (e.g. buildings) more power simply yields more powerful reflections.

Only by placing access nodes relatively close to subscribers can adequate performance be assured and permitted power levels

RF Power Levels

RF power levels must be sufficient, in both directions, to insure reliable and fast service. Wireless is a two-way service, but most laptops and many home wireless access points use low power transmitters (50 mW is common in laptops) and low-gain antennas. A high-power access point may be able to transmit to a laptop, but it cannot hear the laptop's weak reply.

Capital and Operation Costs

The cost per node and cost per subscriber must be low. Traditional enterprise-class access points have many advantages but they are no cost-effective when deployed on a per-subscriber basis.

Overall administration costs must be contained, and in particular it must be simple and easy to add subscribers and define their service levels. A unified management system that administers service level agreements, IP addresses, service access, and billing system interface is required.

Service Level

Cost-effective deployment requires both the ability to guarantee adequate service levels for customers who choose to pay for premium service, and to limit the bandwidth usage of non-premium customers in order to preserve overall system capacity and profit margins.

Firetide has developed a system which meets all of these requirements. It is described in detail in the next section.

The Firetide Internet Access Solution

Firetide's Internet access solution is built around a customer-premised platform engineered specifically for municipal Internet access applications. The Firetide HotClient 2100 and 2200 CPE (Customer Premises Equipment) platform offers high transmit power and high-gain antennas in a system designed to sell at consumer price points. Setup is trivially simple; in most cases it is only a matter of plugging the unit in.

More importantly, the system is engineered to support policy management, including full and flexible bandwidth management. All administration is done centrally by the Internet Service Provider (ISP).

Figure 5. Firetide HotClient CPE

The HotClient CPE works in conjunction with a neighborhood access point. Typically this is a Firetide Model 4601 HotPoint Outdoor Access Point. One AP is sufficient to service dozens of subscribers in a neighborhood.

The Key Advantage

The most critical advantage of Firetide HotClient CPE is that it has been explicitly designed to meet the requirements of Internet access delivery in municipal environments. The unit transmits at 400 mW, so it can easily reach the neighborhood access point, even through walls. It features quality high-gain omnidirectional antennas, and can be equipped with higher gain directional antennas where required.

Another advantage of the Firetide solution is that it delivers Ethernet, not just wireless. While 802.11 wireless is a convenient access solution for many application, many homes and businesses have wired-Ethernet equipment. The Firetide HotClient has a 100bT Ethernet port; it can be connected to hubs, switches, routers, firewalls, or even a local 802.11 access point. Furthermore, it can be connected to all such devices. It is truly a DSL-equivalent (or better) Internet access delivery platform; it just used a wireless delivery method.

Bandwidth Management

Paired with Firetide 4501 and 4601 HotPoint APs, the system provides full bandwidth control and policy management. Using the HotView Pro Network Management System (NMS), the ISP can specify upstream and downstream data rates for each client. In addition, bandwidth can be defined as guaranteed or best-effort. Best-effort bandwidth can be further enhanced by limiting the amount of over-subscription. For example, a channel with a 10 Mbps capacity can be specified with a 50% oversubscription rate. This will allow up to 15 Mbps of demand to use the channel, but not more. Thus, the risk of service degradation under peak load conditions is eliminated.

Backhaul

To complete the path for Internet service delivery, the HotPoint APs must be connected to the backbone. City-wide traffic can be connected to the Internet using any of several schemes, or a combination thereof.

Conventional wired backhaul can be used. With this technique, copper or fiber connections are made to the wired side of the HotPoint APs. Since many municipalities have fiber deployment, either from the incumbent local phone company or from competitive local carriers, this can be used whenever APs can be sited at locations convenient to the fiber grid.

For other AP locations, wireless backhaul must be used. This is accomplished by deploying Firetide HotPort mesh nodes. An array of HotPort nodes forms an Ethernet switch that extends over a large area. HotPoint APs are then connected to it. Other Ethernet equipment (such as cameras) can be connected as well.

The Firetide Wireless mesh solution offers a key advantage over wired backhaul: it can be used to support other services as well. Many municipalities deploy a Firetide mesh to provide support for emergency services such as police and fire. A Firetide mesh is also an excellent backhaul system for video cameras, increasingly popular for surveillance and public safety applications.

Firetide's management platform, HotView Pro, can manage HotPoint APs which are connected directly to wired backhaul, as well as HotPoints which are backhauled via HotPort mesh nodes.

Evaluating Firetide's Access Solution

Earlier, we defined four requirements for a successful municipal Internet access solution: the need for deployment density; adequate RF power, initial deployment cost and operational cost, and service level management. How does Firetide's solution measure up to these requirements?

Deployment Density

Firetide offers an affordably deployment solution because the only component which must be widely deployed is a simple, low-cost system box. Because it has a powerful radio, neighborhood access points can be deployed sparsely; far more sparsely than would be possible with conventional 802.11 clients, such as those found in laptops. Thus, the Firetide system architecture meets the density deployment guidelines.

RF Power

The high power level of the HotClient CPE means it can reach through buildings and deliver the range necessary to reach distant access points. Both the HotClient and the HotPoint AP use 400 mW radios, assuring a clear signal in both directions. (Radio power can be reduced when required.)

Service Level Management

Firetide HotView Pro offers a complete unified system for defining, managing, and enforcing Service Level Agreements. It can work with an ISP's existing RADIUS authentication server if desired. It can also interface to a billing system.

Furthermore, this management system supports all of the components of the Firetide Wireless architecture. This makes management and support easier to learn and easier to do.

Capital Cost and Operational Cost

The sparse deployment capability of the Firetide system means capital costs are kept under control. Furthermore, since the Internet access service can piggyback onto Firetide's municipal wireless Ethernet technology, cost savings are possible. How does this work?

Understanding Bandwidth Management in the Firetide System

Firetide has engineering its wireless architecture to offer sophisticated security and bandwidth management across the system. When Firetide HotPort mesh nodes are used in conjunction with Firetide HotPoint access points and Firetide HotClient CPE systems, you can engineer the bandwidth and security you need for all applications, including:

- Video Surveillance
- Mobile Internet Access for Police & Fire
- Fixed Internet Access of Police & Fire
- General-purpose 802.11 Access Point Support
- HotPoint CPE-based Internet Access Delivery

How does this work?

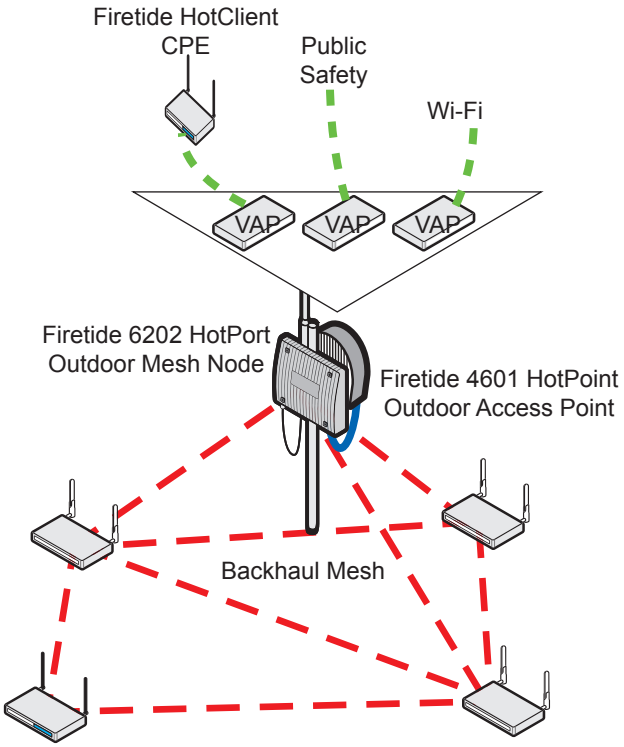
The Firetide Mesh, created by a set of Firetide HotPort nodes, is a full-featured Ethernet switch with management and VLAN capabilities. In a typical metropolitan deployment, a separate VLAN is created within the Firetide wireless mesh switch, and IP surveillance cameras are connected to it. This isolates and prioritizes this high-priority traffic.

A second VLAN is used to support the HotPoint AP - HotClient CPE Internet access delivery system. This VLAN is typically assigned a lower priority.

Each HotPoint AP supports a virtualization model - it can actually behave as if it were up to 16 separate access points. In many cases, system designers will designate one virtual AP in support of the CPE deployment, and another virtual AP to support police, fire, and safety. Each virtual AP can be assigned its own VLAN, traffic priority, and traffic shaping.

This architecture is shown in the following figure:

Figure 6. CPE Multiservice Architecture



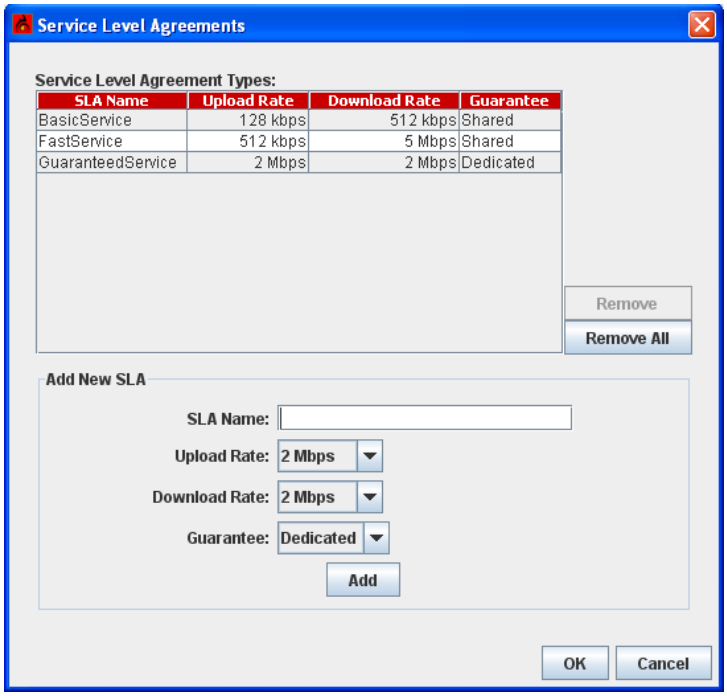
With a Firetide wireless mesh as the backbone (and backhaul), multiple services can be provided for different applications and to different classes of users. Whether it's video surveillance traffic, VoIP traffic, public safety applications, mobile nodes, or Internet access, the Firetide architecture has been designed to deliver the bandwidth, security, and level of service needed.

Understanding Service Level Agreements

A key advantage of the Firetide system is its flexible ability to define and enforce Service Level Agreements (SLAs). Service Providers can offer guaranteed or best-effort service, and can set maximum data rates per subscriber. SLA parameters include upstream and downstream bandwidth limits, and a choice of shared or dedicated access. You can define as many SLAs as you want, and then assign users to them.

In addition to controlling bandwidth and access priority with SLAs, a Policy Manager lets you define the behaviors to be taken when bandwidth is exceeded or other defined events occur.

Figure 7. Sample SLA Definitions



You can change the SLA configuration of a HotClient at any time, and you can also override a its SLA setting and give it custom settings.

Initial Configuration

When HotClient CPEs are used with Firetide HotPoint APs, configuration is automatic, based on a centralized Radius Server. A Radius implementation is included with Firetide HotView Pro, or you can use an existing Radius server.

Firetide's Automatic Configuration mode means that neither your installers nor your clients need to perform any configuration or setup operations. The HotClient will automatically authenticate via the Radius security server, and then acquire its configuration from HotView Pro.

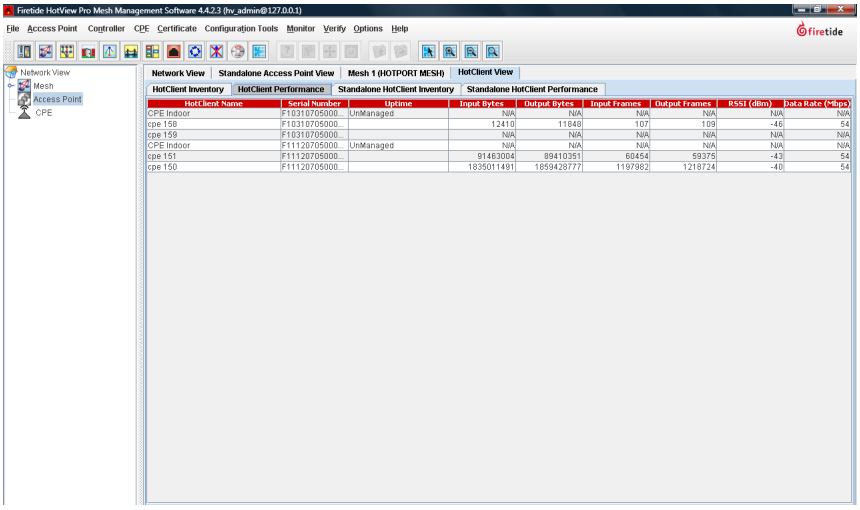
In this mode, each HotClient is made known to the system by entering its serial number into HotView Pro prior to deployment. The HotClient, when installed, will power up, find the Firetide AP, and automatically configure itself.

Thus, you can define service levels and define users, then send HotPoint CPEs to customers for self-install in most cases, and the HotPoint will come up automatically.

Performance and Monitoring

Internet-access customers will not stay with an ISP who cannot deliver the promised service quality. Thus the ISP must be able to monitor the performance of every customer. The Firetide HotView Pro Network Management System provides this, as shown in Figure 8:

Figure 8. HotClient Performance Monitor



By monitoring this data, potential problems can be identified quickly. Because HotView Pro is integrated, system engineers can quickly view access point and backhaul node performance, and correct any problems before they affect service delivery.

The System View

This White Paper has examined municipal wireless access deployments from a layered perspective. It has looked at aggregation points, wireless backhaul via HotPort nodes, wireless access via HotPoint access points, and Internet service delivery via HotClient customer-premises nodes. It's worthwhile examining access deployments from a vertical perspective as well

The Firetide system architecture meets all of the needs of practical, real-world municipal wireless deployment. It is capital-cost effective and it is capable of delivering multiple service levels to multiple classes of users.

This infrastructure can support police, fire, public safety, and other applications. Cities interested in public-access wireless, as well as Internet service providers interested in reaching new customers in new ways, should carefully evaluate Firetide's system to determine if it meets their needs.

Vertical Integration Benefits

By deploying a vertically-integrated system, municipalities gain several advantages. Foremost is cost-effectiveness. The system can be built on a pay-as-you go basis, building out gradually. The second advantage is multi-application and multi-service support. By sharing services and classes of users across the infrastructure, costs are shared more widely.

The ability to deliver revenue-generating DSL-equivalent access to homes and small businesses is another contributor to the overall cost-effectiveness. Reliable DSL-equivalent service generates a higher and more predictable revenue stream than simple Wi-Fi access.

Vertical integration also enhances security and performance. By providing a consistent security model across all components and employing a defense-in-depth strategy, the Firetide system is able to keep all information secure. Performance is assured by monitoring usage and enforcing policy rules across the system, in addition to providing VLAN support and QoS.

Last but not least, the ability to manage the entire system with a single unified management platforms saves time and effort and makes fault isolation and correction much easier.

Vertical Applications

Video Surveillance

Video surveillance is often cited by municipalities as the key reason for a wireless mesh deployment. Video cameras in public places reduce crime and increase the feeling of safety on the part of the general public. It also improves police efficiency by allowing more officers to spend more time investigating crimes.

Firetide's mesh technology has been designed to meet the needs of video surveillance, and has been proven in hundreds of video-surveillance deployments. But most importantly for municipal deployments, Firetide's architecture supports effective prioritization of traffic, so that adequate bandwidth is available for cameras as well as other applications.

Internet Service Delivery

Most cities have areas where high-speed Internet access is not readily available. Wireless delivery works well in these situations, if the system is correctly designed for it. In particular, the radios must be powerful enough to deliver signals through walls. Just as important, there must be a model to manage overall bandwidth demand, so that subscribers are assured of reasonable access speeds.

Firetide has developed a system around a low-cost wireless node that can be placed on the customer premises. This features enough radio power to provide a strong signal, and is backed up by a bandwidth-policy management system that lets ISPs guarantee different classes of service at different price-points.

Public WiFi Access

Many cities want to offer residents basic Wi-Fi access, either free or for a nominal fee. Firetide's architecture, because of its Virtual Access Point (VAP) capability, makes it easy (and inexpensive) to add one or more Wi-Fi access points for public access, using Firetide equipment already installed.

Police, Fire, and Public Safety

Police radios have worked well for police departments for many years, but increasing data and video demands mean that many police, fire, and public safety departments need radio equipment that can deliver data to personnel in the field. This lets patrol officers view video surveillance, lets fire departments see inside burning buildings, and reduces paperwork and lost manpower by filing more reports and other data automatically.

Mobility

Mobility is a vertical application across any municipal mesh. This may not seem obvious at first glance, but managing IP addresses, frequency assignments, security, and other settings across multiple meshes is a global design, not a mesh-local one.

Firetide supports high-speed mobility for 802.11 Wi-Fi users and also high-speed mobility for Firetide mesh users. This is done using the Firetide Mobility Controller, an application that manages all global settings associated with mobile clients. For further information on the Mobility Controller, refer to the HotView Pro Reference Guide.

Management

Regardless of the range of vertical applications in use, Firetide provides a complete management tool for its system. HotView Pro manages and monitors the Firetide Mesh, Firetide APs, and the Firetide CPE system. It can also manage third-party access points. HotView Pro is 24/7 and provides complete performance and error-logging capability. It can interface to external authentication systems such as Radius, and external databases for error-logging. In addition, it is fully SNMP-compliant.

Summary

Firetide's wireless system architecture meets the technical and application needs of municipal deployments. Just as importantly, it meets the cost constraints. Because it can be deployed on a pay-as-you-go basis, it can fit into a budget without requiring large up-front expenditures. Because it's multi-service and multi-application, it lets the cost be shared across multiple groups of users, and provides the service level guarantees to make it possible to bill for Internet service, thus generating real-world cash flow as well as supporting municipal services.

Glossary

These terms are useful to an understanding of wireless mesh technology in general and Firetide products in particular.

- **802.11** - a family of protocols developed under IEEE guidelines for sending Ethernet packets over radio links. 802.11a, 802.11b, and 802.11g are currently the most widely used.
- **Bandwidth damping** - a speed-limiting effect which can occur in half-duplex networks.
- **dB**, or **decibel** - the commonly-used measure of power in RF systems.
- **Ethernet Direct** - a wired connection within one mesh. An **Ethernet direct** connection is visible to the mesh routing algorithm, which considers its capacity and speed when routing packets within a mesh. Thus, **Ethernet Direct** links increase the capacity of the mesh in which they are contained.
- **Fresnel Zone** - the area surrounding an RF signal that must remain largely free of interfering objects.
- F**ull-duplex** - some radio systems support simultaneous transmission and reception.
- **Gateway Group** - a collection of nodes configured to offer multiple egress points from the mesh. When a **Gateway Group** is used, it is usually also the **Head Node**, but this is not required.
- **Half-duplex** - many radio systems can either transmit or receive, but cannot do both at the same time. Thus in a group of nodes all within radio range of each other, at any given time only one node can be transmitting.
- **Head Node** - the node on the mesh which is logically closest to the NMS. Typically this is the node which is plugged into the enterprise backbone, and from there to the NMS system.
- **Integrated AP** - A Firetide HotPoint Access Point that is connected to a Firetide mesh node.
- **Interoperability** - in the Firetide context, use of HotPort Series 6000 nodes and older HotPort Series 3000 nodes in the same mesh.
- **Link** - a connection between two nodes within a single mesh. Also known as a path. Links are generally wireless RF connections, but can be wired connections in some cases. (See **Ethernet Direct**.) The key point is that the connection is between two nodes within the same mesh; that is, within the same mesh-routing domain.
- **Mesh Bridge** - a wired connection between two distinct meshes. The meshes can be near each other, or even physically overlapping if they are logically isolated. They can also be arbitrarily far apart. Because a **Mesh Bridge** connection is between two meshes, it is not part of any mesh-routing algorithm.
- **Mobile node** - a Firetide mesh node installed in a vehicle or any other place where it moves relative to the other nodes.
- **Multipath** - the condition where a radio receiver receives two versions of the same signal, because one signal took a more direct path and the other signal a reflected path.
- **Network Management System** (NMS) - another name for HotView or HotView Pro, the system

for configuring and monitoring network behavior. Note that the NMS is NOT required for network operation; only for initial configuration.

- **Node** - one of the elements of a mesh. It has one or more radios, and a CPU which implements the packet-switching algorithm. Nodes also offer wired-Ethernet ports as entry points to the wireless mesh.
- **QoS/Class of Service** - mechanism used to insure that time-critical traffic (e.g. VoIP) gets delivered promptly.
- **Roaming** - the ability to support 802.11 clients as they move from access point to access point.
- **Standalone AP** - A Firetide HotPoint Access Point that is connected directly to the wired enterprise LAN.
- **Third-party AP** - an AP not made by Firetide. Firetide supports third-party APs, as well as other Ethernet-compatible devices.
- **VLAN** - a dedicated virtual Ethernet switch. Ethernet devices assigned to one VLAN are isolated from devices assigned to another VLAN. This is often used to provide security, and in combination with QoS, to provide traffic prioritization.

Firetide, Inc
16795 Lark Avenue, Suite 200
Los Gatos CA 95032 USA
+1 408 399 7771 phone
+1 408 399 7756 fax
info@firetide.com
www.firetide.com