Municipalities Adopt Successful Business Models for Outdoor Wireless Networks

Choosing the right outdoor wireless solution gives cities the flexibility to pick the business model that best meets their needs.

Outdoor wireless networks offer compelling benefits to cities of all types: extending services to citizens, encouraging tourism, and helping field-based workers to be more productive and more responsive. There are several successful business models for cities to choose from when implementing an outdoor wireless network, including a wholesale business model, a managed-services model, and a hybrid approach. Having the right network foundation and combination of partners gives cities the flexibility to choose the business model that works best for them.

SUMMARY

Outdoor wireless networks help cities deliver new and improved services to citizens on a larger scale and with greater efficiency. They can help cities achieve a wide variety of goals, from improving public safety to fostering economic development. As city officials contemplate investing in outdoor wireless networks, they often have questions about planning, deployment, ownership, and management of the network.

Putting together the right team of partners is an essential step. For an outdoor wireless network, the core team should include the application vendor, systems integrator, field installation partner, service provider, and network vendor.

There are several successful business models for owning and managing an outdoor wireless network, including managed-services and wholesale models and a hybrid approach that combines elements of both. One model may be more appropriate than another based on the city's budget, IT resources, or other considerations.

Over the long term, the choice of wireless technology and network foundation will also be important factors in success. For example, the wireless technology that cities are choosing overwhelmingly is Wi-Fi. Wi-Fi offers significant advantages such as low cost, ubiquity, and the flexibility of using the same devices for the indoor wireless LAN (WLAN) and outdoor coverage.

There are several requirements for the network infrastructure. For example, cities want to be sure that they have a foundation that provides the flexibility and scalability to expand coverage and support new services over time. They want to be sure that the network is highly secure to help ensure privacy of information; the network must also be highly reliable to help ensure the

continuous availability of services and information. In addition, the network must be easy to manage, which includes the ability to manage indoor and outdoor wired and wireless networks as one unified network. Ease of management also includes the ability to intelligently segment and track traffic, in order to connect users to specific applications and enable cities or service providers to bill for services and usage.

CHALLENGE

Municipal governments, like large-enterprise organizations, are taking advantage of Internet connectivity to operate more efficiently and improve service delivery. Unlike private corporations, however, municipalities not only conduct their business inside buildings, such as city hall or municipal warehouses, but also outdoors, providing services such as:

- Building and fire code inspections
- City parks and recreational facility upkeep
- Code enforcement
- City maintenance
- Traffic monitoring, community policing, and other public-safety duties

Indeed, cities around the world are deploying outdoor wireless networks to answer a wide range of municipal mandates, including:

- Delivering new and improved services to constituents while containing budgets and headcounts
- Narrowing the “digital divide” by giving all citizens equal access to education, health, and technology resources over the Internet
- Fostering economic development by providing the infrastructure and services to attract businesses, tourism, and residents
- Improving public safety by giving law enforcement and emergency response teams real-time access to information, including video surveillance, over the wireless network

For instance, the City of Everett, Washington, is extending network-based police tools to officers in the field with mobile network access. “We’ll be able to put our officers back in contact with the public, giving us additional eyes and ears in the community,” says Boyd Bryant, police sergeant and public information officer for the City of Everett Police Department, and supervisor of the department’s technology projects. “And with the ability to access driver’s license photos, booking photos, outstanding warrants, and the future potential of remote fingerprint scanning services, officers will be much better equipped to identify and apprehend criminals.”

Clearly, city officials who are considering wireless-based services are watching municipal wireless projects with great interest. For many, it is not a question of whether these networks will be in their future but when and how. Specifically, officials want answers to questions such as these:

- What is the best business model to use? Should I work with a service provider or manage the wireless network myself?
- Which technology should I use—Wi-Fi, WiMax, or cellular? Will that choice affect what services I can offer over the network?
- Who will I need to work with to successfully plan and implement an outdoor wireless network?
- How will deploying, owning, and managing the network impact my existing IT operations?

SOLUTION

For a city considering an outdoor wireless deployment, there are many interdependent factors to consider. The first factor is the range of possible business models for the project. The business models the city chooses are, in turn, dependent on understanding the roles of the different partners in such a project, choosing the right wireless technology, and building the right network foundation to support the city's project goals. Let's take a look at each of these sets of issues in turn.

Choosing the Appropriate Business Model

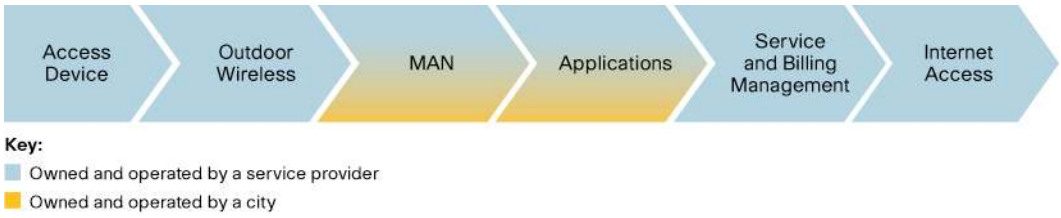
There are multiple business models to choose from when implementing an outdoor wireless network. Three of the most popular are the managed-services model, the wholesale model, and the hybrid model.

Managed-Services Model

In a managed business model (sometimes referred to as a public-private partnership), the network is owned and managed by a service provider. The service provider may sell advertisements and charge fees to citizens for connectivity. Government agencies may connect to the network for free or for a low monthly fee. The local government can also generate revenue by leasing buildings and light poles to the service provider for mounting the wireless equipment.

One of the chief values of this business model is that the city shifts the project from a capital equipment investment to an operational cost, which helps keep budgets under control and taxpayers satisfied. Figure 1 illustrates the managed-services model.

Figure 1. Managed-Services Model



As Figure 1 shows, when a city (shown in orange in the figure) uses a managed-services model, it can maintain some level of control of the metropolitan-area network (MAN) and applications, while outsourcing responsibility (and costs) for access devices, the outdoor wireless network, service and billing management, and Internet access to the service provider or systems integrator.

Wholesale Model

In a wholesale business model, the network is owned by the city. In this model, the city government often uses most of the network for internal operations, and may share some excess bandwidth with citizens to connect to the Internet using guest access privileges (often provided free of charge).

One of the chief values of this model is that it gives the municipality complete freedom to change applications. It also gives the city the option to allow business and residential customers to work with more than one service provider.

Note that in the wholesale model, the city needs to ensure that its IT department has the skills to operate the outdoor wireless network. Figure 2 shows the wholesale model.

Figure 2. Wholesale Model

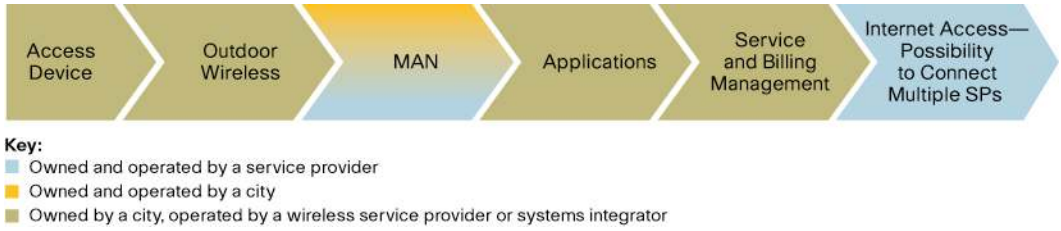
As Figure 2 shows, using a wholesale model, a municipality maintains control of the complete network (perhaps sharing some control of the MAN with a service provider), from the access devices to service and billing, except for Internet access. With this model, the city has the option of connecting to multiple service providers for Internet access.

Hybrid Model

The hybrid model combines the attributes of the managed-services and wholesale business models. In this option, the city owns the network but outsources operation and maintenance tasks, as well as the application development, to a systems integrator or a wireless Internet service provider (WISP).

One of the chief values of this model is that it gives the municipality a measure of control but at the same time allows the city's IT department to use the expertise and resources of the systems integrator or WISP to make system changes as needed. Figure 3 illustrates the hybrid model.

Figure 3. Hybrid Model



As Figure 3 shows, using a hybrid model, a municipality owns the network but outsources most of the day-to-day operations to a systems integrator or WISP.

In order to select the appropriate business model, the city must first determine the appropriate:

- Vendors
- Outdoor wireless technology
- Network foundation

Choosing the Right Partners for a Successful Project

In an outdoor wireless deployment, a core team of vendors should support the city's IT department. The roles in this partnership include the following:

- **Application vendor:** The application vendor is generally a software developer who has developed a specialized application for municipalities, such as field-based video surveillance, ticketing, meter reading, permit processing, and licensing.
- **Field installation partner:** The field installation partner is specially trained and certified by the network equipment provider to configure, deploy, and test an outdoor wireless network.

- **Systems integrator:** The systems integrator integrates the application vendor's software with other city systems, and works with the service provider on specifying the management, operation, and maintenance procedures for the complete solution.
- **Service provider:** The service provider plays a crucial role in an outdoor wireless deployment, providing Internet access, managing customer premises equipment (CPE) for small and medium-sized business or residential customers (as the need arises), as well as handling the billing, security, maintenance, and service for the network (depending on the business model).

  The service provider is also the vendor that can aggregate multiple access technologies into one cohesive network, such as Wi-Fi outdoor wireless and cellular networks for "always on" applications.
- **Network vendor:** The network vendor should provide an end-to-end solution, including wired and wireless coverage, to allow users to roam between networks without disruption. The network vendor should also offer the network capabilities that the city requires, such as service and access management, traffic segmentation, security, and billing support. And the vendor should propose or provide network design consultancy services.

It is also possible that some of these vendors may be able to perform multiple roles in an engagement. For example, a service provider might provide field installation and/or systems integration, in addition to ongoing network support.

Choosing the Wireless Technology That Provides the Best Performance and Cost-Effectiveness

There are several technologies that cities may consider for their outdoor wireless infrastructure, including Wi-Fi, WiMAX, and cellular. Each has its respective strengths. However, for access, Wi-Fi is unquestionably the technology of choice for cities today. There are numerous reasons for the popularity of Wi-Fi, including:

- Wi-Fi operates in an unlicensed spectrum and therefore is free of charge.
- Wi-Fi has reached ubiquity in the mobile computing space and is spreading to the consumer market. This means that cities don't have to buy special-purpose endpoint devices for their wireless applications, but can use a broad range of affordable, off-the-shelf devices, including laptops, dual-mode GSM/Wi-Fi handsets, digital cameras, and PDAs. According to the Wi-Fi Alliance, over 2600 products have been certified to date.[1]
- Wi-Fi enables the city to use the same devices for the indoor WLAN and outdoor coverage, enabling users to move transparently from one space to another without changing devices, losing connectivity, reregistering, and so on.

[1] For more information, visit http://certifications.wi-fi.org/wbcs_certified_products.php

Choosing the Network Foundation That Provides the Greatest Flexibility

Choosing the right network infrastructure gives cities the flexibility they need to select the right business model, and continue to adapt and grow over time. To decide on the right business model, cities need to define their goals and priorities for the wireless network and then consider what network capabilities are most important in meeting these priorities. For example, the city may want to:

- Implement and support traffic and service management, network aggregation, and connection to one or several service providers.
- Intelligently segment traffic and apply quality of service (QoS) to prioritize different types of traffic over the network.
- Track network usage by application and users in order to support billing of specific user groups.
- Reduce the total cost of ownership (TCO) of the network, including acquisition, operations, and incremental growth costs.

The following are some of the important capabilities that cities should look for in selecting a network foundation:

- **End-to-end solution:** The network foundation encompasses indoor wired and wireless spaces, outdoor wireless coverage, and the network backbone, and provides a service delivery platform for such functions as identifying end users and the applications and resources that they are allowed to access.
- **Standards-based:** The network supports security standards, such as IEEE 802.11i, Wi-Fi Protected Access (WPA), and WPA2, and both licensed and unlicensed frequencies, including 802.11a/b/g.
- **Easy to deploy:** Wireless access points configure themselves for optimum performance, eliminating the need for personnel to manually configure each device.
- **Highly reliable:** The solution is “self-healing” because it automatically selects an alternate path through network if a link fails and also automatically avoids congested areas.
- **Unified, easy management:** There are many requirements for management, including the ability to provide management of the indoor and outdoor wired and wireless networks as one unified network, allowing mobile users to roam without reauthenticating as they travel from indoor to outdoor areas and without any computer or PDA configuration change. The network should also provide the ability and intelligence to segment and manage traffic, assign different priorities to traffic based on applications or users, manage subscriber service access control, and support billing, traffic analysis, data mining, and more.
- **Scalable:** The network enables cities to build and expand outdoor wireless coverage incrementally, from a small footprint (such as hot zones and hotspots) to pervasive coverage (a network mesh), without reconfiguring the installed base. Scalability of a mesh network is a function of the number of channels available, which is why the network should use different channels for access and backhaul. Scalability is also dependent on the ability to use directional antennas to get the best spectrum usage (this is the same capacity optimization used in cellular networks).

- **Secure:** The network incorporates integrated security technologies to maintain the confidentiality of private information, to protect against the spread of viruses by denying access to infected computers, and to provide different levels of access to municipal constituents. In addition to supporting the latest industry standards for security, such as 802.11i, WPA, and WPA2, the network should protect against imitation access points.

Business Model Case Studies

The following are examples of two municipalities that have implemented outdoor wireless networks and the different business models that they chose:

- **City and project:** With a population of nearly 13,000, Lebanon, Oregon, mirrors hundreds of other small-town environments where offering affordable high-speed Internet access has been a challenge. In Lebanon, the Wi-Fi mesh solution covers 60 percent of the town, but the focus is on rolling out new city services on top of the mesh network. The city plans to test the mesh network with police cars and public works vehicles equipped with mobile terminals. This way, officers and city workers can wirelessly connect to their existing IT infrastructure and take advantage applications, IP communications, and streaming video. “With mobile tools and field reporting using wireless, this will be a big step in the evolution of efficiency,” said Tom Oliver, information service manager for the city of Lebanon.
- **Business model:** In this example of a wholesale model, the city of Lebanon owns and operates the network and relies on PEAK Internet, a local ISP, for installation and Internet connectivity.
- **City and project:** HarborLink Network, LLC, is a wireless LAN solution provider in the heart of downtown Dayton, Ohio. City of Dayton officials have big ideas about the types of services their metro wireless network can support in the future. They envision a day when a citywide wireless network will support remote reading of water meters, real-time video streaming to police cruisers, wireless links between emergency vehicles and hospitals for processing blood tests remotely, and even parking meter enforcement.

  William Hill, director of information and technology services for the city of Dayton, says its wireless mesh network pilot is a precursor to deployment of a comprehensive citywide network that will cover “every public space, every street and every sidewalk within the city limits.”
- **Business model:** In this example of a managed-services model, HarborLink manages the wireless network for Dayton, providing the entire spectrum of wireless services and applications that might be used in a municipality. The wireless LAN solution provider can offer front-end Internet access service, which is based on advertising, completely free to the public. They can also add additional services, such as a VLAN for law enforcement.

Conclusion

Hundreds of cities and towns are deploying outdoor wireless networks or have plans to do so. While all cities share a common responsibility to serve and safeguard their citizens, there is tremendous diversity in how and why cities invest in outdoor wireless networks. The right network infrastructure and combination of partners will provide cities with the flexibility they need to choose the right business model to wire their cities for growth and prosperity.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-325079-00 11/06