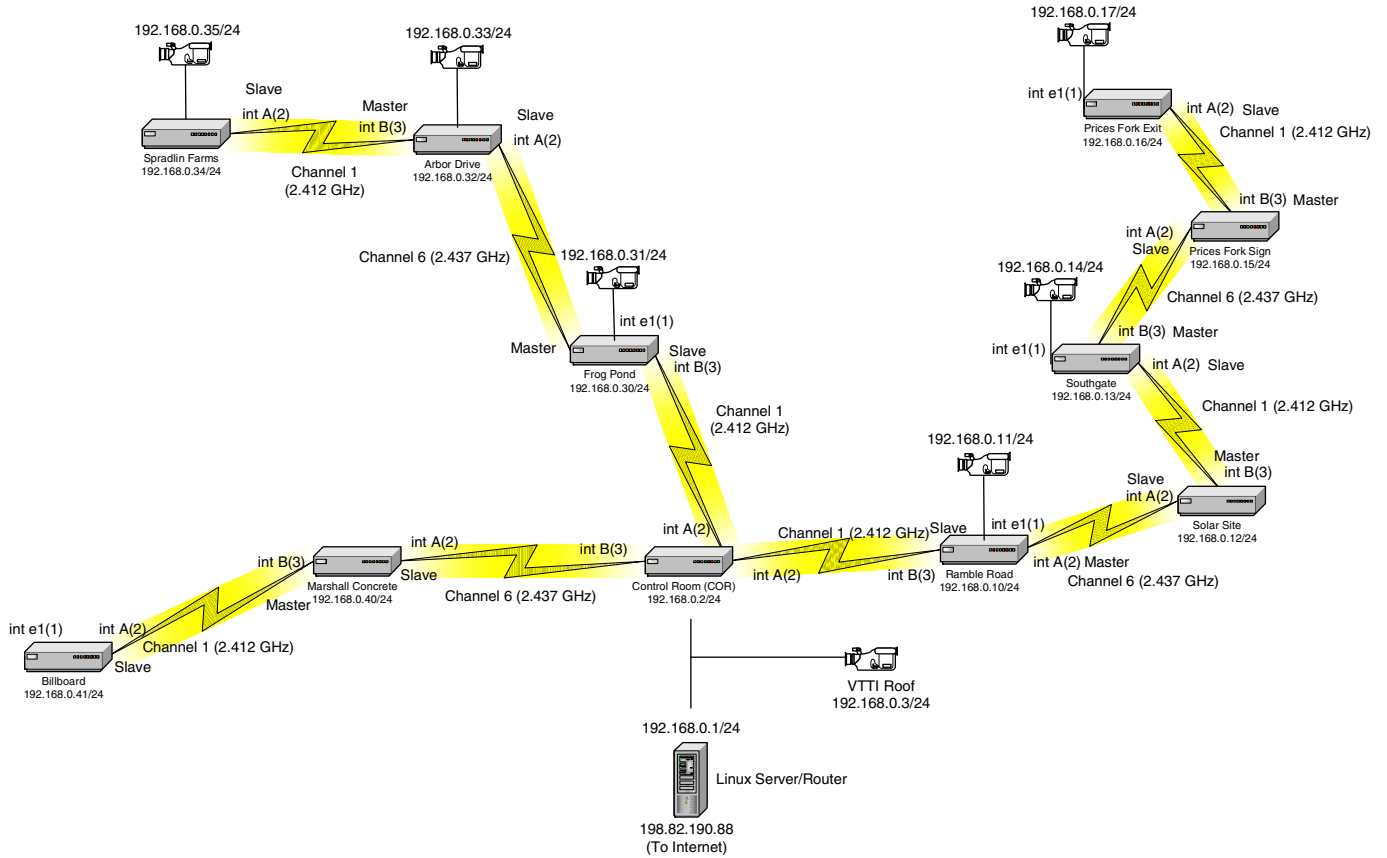


# Serial Wireless LANs Along DOT ROW



Submitted by:

Ashwin Amanna  
Assistant Director

Dr. Aaron Schroeder  
Director  
Center for Technology Deployment  
Virginia Tech Transportation Institute

## ABSTRACT

This paper presents the use of Commercial off-the-shelf (COTS) wireless Internet technology to meet the security, mobility and safety needs of departments of transportation (DOTs). COTS wireless is an economical, scalable alternative to traditional fiber optics and telephony communications solutions. A virtual Ethernet network is created along a highway right-of-way (ROW) by installing wireless point-to-point links in a serial fashion that can extend upwards of 30 miles per section from a base node. This local area network (LAN) becomes a seamless extension of the DOT's communications for field devices such as cameras, RWIS, traffic sensors, and field personnel. This paper discusses cost comparisons to traditional communications, specific types of wireless technologies, their capabilities, architectures, and security issues based upon Virginia Tech's real-world deployments and test-bed installations. Digital video applications along wireless networks are specifically addressed. The paper concludes with a discussion of the near-term future of wireless technologies.

### **The needs of the DOT**

Departments of Transportations (DOTs) are under increasing pressure to maintain control over their widespread infrastructure. The desire to provide secure and accurate information to travelers is pushing the existing DOT communications infrastructure to the limit. In an ideal world, fiber optics would be available along every interstate right-of-way (ROW) and along every major arterial. Dedicated home-run fibers would be available for traffic monitoring cameras and the myriad of other DOT field devices, such as weather sensors (RWIS), acoustic sensors, variable message signs (VMS), license plate readers (LPR), and HAR. The quantity of field devices that DOTs desire can number into the thousands along ever major stretch of interstate and major arterial.

The reality, however, is far from ideal. In the early days of ITS, hundreds of millions of dollars were spent on dedicated camera fiber optic systems; however, those days are long gone. The cost for fiber optic installation is more than DOTs are willing to spend, and the long time frame for bringing a system online is longer than they want to wait. Recently, several DOTs have attempted to develop public/private partnerships to deploy large-scale fiber optic networks using DOT ROW. These attempts have often failed due to lack of interest from the financially ailing telecom industry. Traditional telephony solutions, such as DSL, ISDN, phone modems, and T1s, are viable alternatives; however, the bandwidth can be limiting, each individual installation incurs a monthly bill, and these options may not be available in highly rural areas.

### **The wireless alternative**

Recent advances in wireless technologies have made this communications medium a viable, economical, and scalable alternative for DOTs. The infrastructure requirements are a fraction of fiber optic installation, with minimal disruption to existing infrastructure. With appropriate infrastructure in place, a wireless network can go online within hours, as opposed to the months of construction required for a fiber optic network. Wireless links can be used as temporary installations until a fiber optic network becomes available or can be made permanent for long-term use. From a scalability issue, adding another wireless link over a small distance is much more reasonable than extending a fiber optic network. Furthermore, the use of open standard wireless IP devices ensures that the owners do not cubbyhole themselves into one type of proprietary technology and costly services contracts from one vendor.

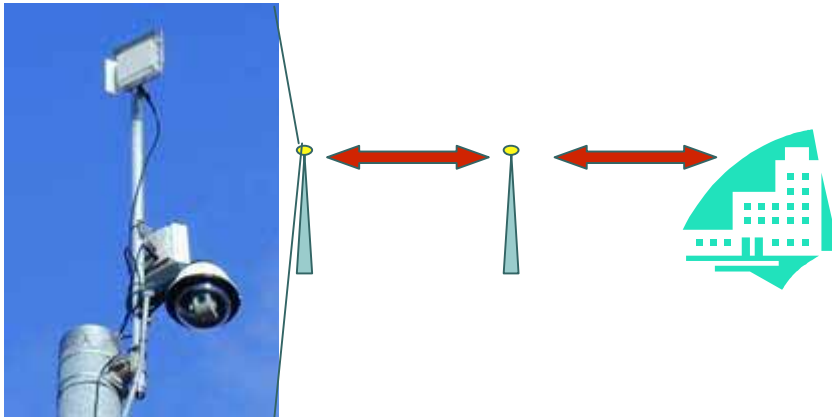
The wireless network becomes the property of the DOT; therefore, the recurring monthly costs associated with individual ISDN and phone lines are minimized. The bandwidth capabilities of wireless can support streaming video, which is the most bandwidth-intensive application. If the network can handle video, then it can certainly handle the low data rates associated with other field devices, such as RWIS and traffic counters. Overall, wireless systems provide a good value based on the cost per installation versus the available bandwidth they provide.

Table 1 provides a general comparison between fiber optics, wireless, and traditional telephony solutions.

**Table 1: Comparison of Communication Alternatives**

<u>Option</u>	<u>Major Benefits</u>	<u>Major Drawbacks</u>
Fiber Optics	<ul style="list-style-type: none"> <li>• Fast Data Transfer up to Hundreds of Mbps</li> <li>• Redundant and robust architectures</li> </ul>	<ul style="list-style-type: none"> <li>• Expensive installation</li> <li>• Major disruption to existing traffic during installation</li> <li>• Permanent</li> <li>• Requires maintenance contract</li> <li>• May not be viable for rural areas</li> </ul>
Traditional Telephony	<ul style="list-style-type: none"> <li>• Variable Data Transfer 56k to T1, T3 speeds</li> <li>• Repairs covered by provider</li> </ul>	<ul style="list-style-type: none"> <li>• Permanent</li> <li>• Reoccurring costs</li> <li>• Contract for 1 year</li> </ul>
Wireless Internet	<ul style="list-style-type: none"> <li>• Broadband Data Transfer 11Mb to Hundreds of Mb (aggregate)</li> <li>• Scalable</li> <li>• Fast installation</li> <li>• Limited dig-in costs</li> <li>• Reconfigurable</li> <li>• Open standards</li> <li>• Technology improves every 3-5 years</li> <li>• DOT owns ROW</li> </ul>	<ul style="list-style-type: none"> <li>• Most require Line-of Sight</li> <li>• Terrain / road geometry may pose issues</li> <li>• Most COTS equipment not environmentally hardened</li> <li>• Susceptible to interference in unlicensed spectrums</li> <li>• Weather fade depending on spectrum</li> </ul>

The wireless network becomes just an extension of the DOT’s current fiber optic, Ethernet and telephone network. The medium used to communicate to devices becomes transparent to the user, and the application of wireless is no different than fiber or telephone.



**Figure 1 Typical application of Wireless**

### A cost comparison

To compare the costs of wireless to fiber optics and traditional telephone solutions, a mock scenario was developed. The scenario involved placing two cameras, two VMS, and one traffic speed/count sensor along an interstate ROW and collecting the data back at a DOT District Headquarters. The district office was located several miles from the interstate, and the overall length covered between devices was over 8 miles. Three options were analyzed: 1) constructing a new fiber optic network from the DOT District HQ to each field device; 2) installing individual telephony subscription services to each device; 3) installing a wireless network extending from the DOT District HQ to each device.

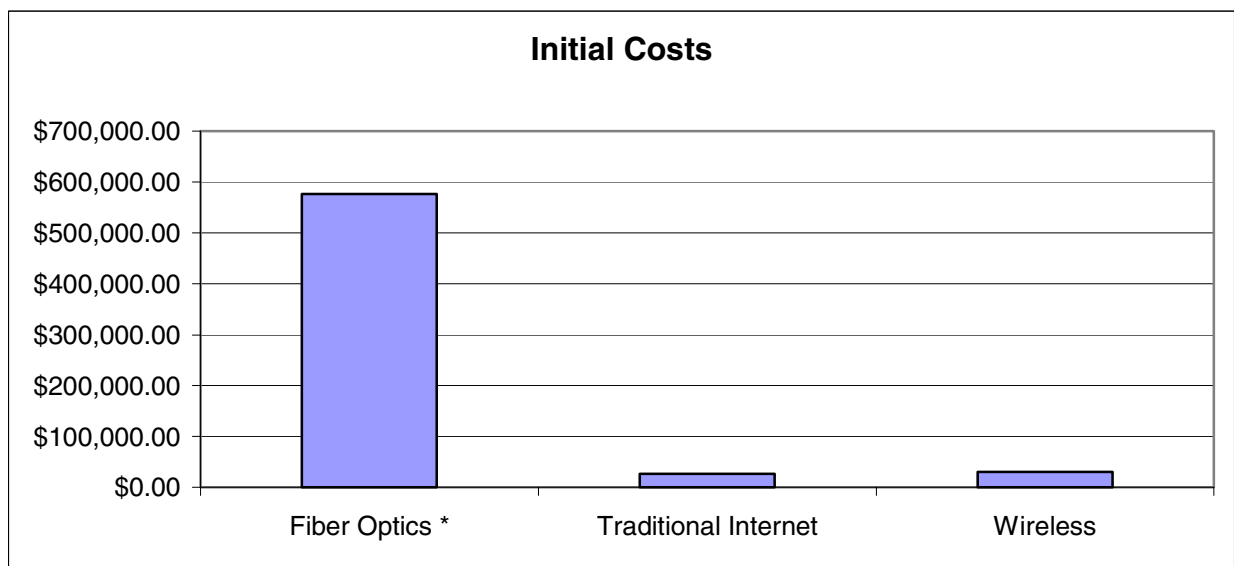
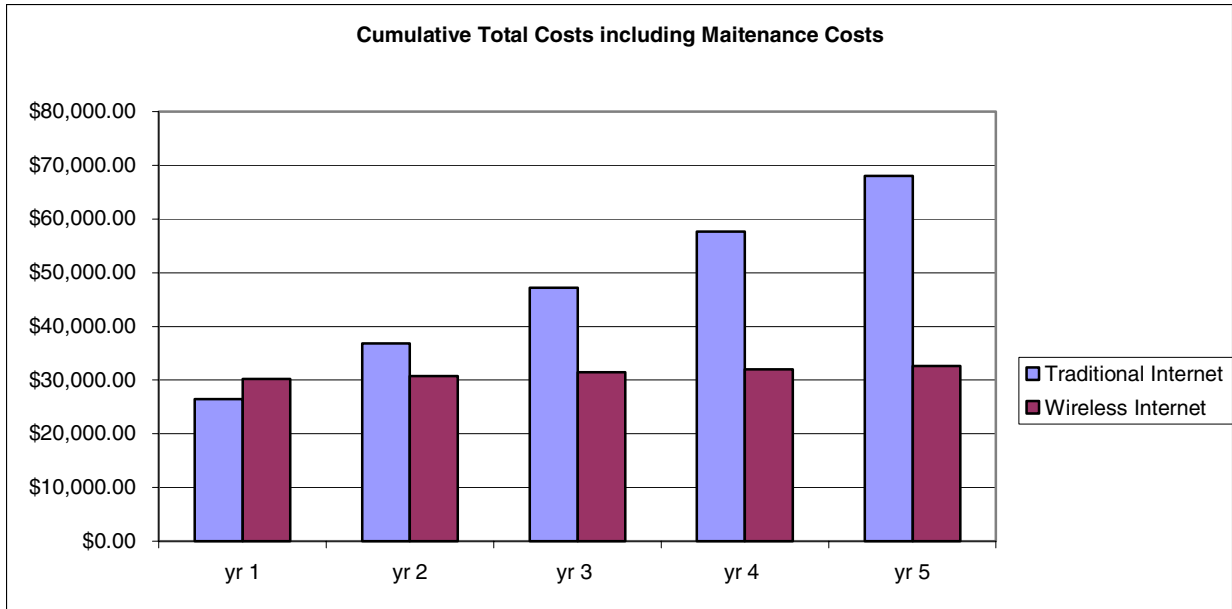


Figure 2 Initial costs for mock scenario

As can be expected, the initial costs of fiber optic installation were significantly higher than the telephony and wireless options. The other two options initially were priced very close together. The next step involved analyzing the telephony and wireless solutions over time.

The telephony option included installation of two 256k Internet connections at the cameras and 56k dial-up Internet accounts for the VMS and traffic sensor. The wireless solution involved installation of serial wireless network utilizing COTS 802.11b equipment. The difference in initial installation/startup costs between the two options was relatively small; however, over time, the recurring monthly subscription costs associated with the telephony options began to accrue.



**Figure 3 Wireless compared to Telephony over time**

Based upon the above comparisons, wireless should be considered a viable alternative to traditional communications mediums that are required to meet the needs for field devices. Wireless need not be considered a solitary end-all solution, rather it should be considered another available option to be used in conjunction with existing communications infrastructure.

### **Why COTS?**

Traditionally, the transportation industry has shied away from off-the-shelf products in favor of proprietary design-build solutions. While this approach has its merits, it often results in a DOT being “on the hook” to one vendor and one specific technology. This can lead to expensive service contracts and a lack of desire to change or upgrade technologies even though a better, cheaper solution usually becomes available over time. COTS products are driven by a market much larger and more dynamic than the transportation arena. This marketplace breeds a phenomenon that is to the buyer’s advantage: capabilities increase while, at the same time, costs come down. In addition, COTS products tend to follow a standard, making interoperability and use of different vendors easy. In many situations, improved products roll out on three to five-year timelines. Radios that we purchased for \$2,000 three years ago have been replaced with products that are three times as fast for half the cost.

### **Types of Wireless**

Wireless technologies available today range from recently declassified military systems to commonplace analog cellular. The FCC regulates all wireless spectrums and has created several unlicensed bands that allow devices to operate without a formal license.

This research effort focuses on COTS products operating in the unlicensed bands. In addition, it focuses on products that either operate on the IP standard or that, at least, seamlessly “pass through” IP traffic.

**Table 2: Frequency Bands of Unlicensed Spectrum**

BAND	Frequency	Application
ISM BAND	902-928 MHz	Fixed wireless cordless phones, other transmitters
802.11b/g	2.4-2.4835 GHz	Fixed wireless, WLANs, microwave ovens, cordless phones
802.11a	5.725-5.850	Fixed wireless systems, WLANs
U-NII BAND	5.15-5.35 GHz	WLANs
	5.725 – 5.825 GHz	WLANs

802.11b, 802.11a, and U-NII products can be used to create wireless local area networks (WLANs). A major criteria used to assess a WLAN is the amount of bandwidth available on the network. In simple terms, bandwidth can be considered the size of water pipe available: the larger the pipe, the more data that can be sent. Note that the advertised aggregate throughput does not take into account the various overhead required for IP and is not indicative of real world payload throughput. Analysis of the true throughput will be addressed later.

**Table 3: Aggregate Throughput of COTS products**

Device	Advertised Aggregate Throughput
802.11b	11 Mb/s
802.11g	54 Mb/s
802.11a	54 Mb/s
Proxim QB 20 (U-NII band)	18 Mb/s

Originally, the 802.11 products were designed for client – Access Point applications such as office and campus environments. They have been adapted for long distance point-to-point backbone applications. Recently, 802.11a products specifically designed for point-to-point applications have been released. As one transmits longer distances, the time delays associated with the distance originally caused issues with the control protocol. Similarly, 802.11g products designed for local area use have started to be designed with external antenna adapters.

The distance that a radio can transmit over one “hop” is related to the signal power inherent in the radio, the amplification of an external antenna, the tower height at which it is mounted, and the level of clear line-of-sight available. The FCC places limitations on the amount of output power after antenna amplification in order to minimize conflicts between users.

The table below summarizes the distances capable with 802.11b products. Note that the available throughput begins to degrade at the farther distances. Product literature for 802.11a products lists distances of up to 30 miles.

**Table 4: Distance Chart for 802.11b radios**

<b>Antennas</b>	24dBi	14dBi	12dBi	10dBi	7dBi
<b>24dBi</b>					
(1Mb/s)	16.3mi	11.8mi	10.7mi	9.7mi	8.8mi
(2Mb/s)	15.2mi	10.5mi	9.6mi	8.8mi	7.5mi
(5.5Mb/s)	13.5mi	8.9mi	8.1mi	7.5mi	6.3mi
(11Mb/s)	12.0mi	8.0mi	7.0mi	6.3mi	5.4mi
<b>14dBi</b>					
(1Mb/s)	11.8mi	7.5mi	6.8mi	5.9mi	5.0mi
(2Mb/s)	10.5mi	6.3mi	5.8mi	5.0mi	4.1mi
(5.5Mb/s)	8.9mi	5.4mi	4.7mi	4.1mi	3.4mi
(11Mb/s)	8.0mi	4.4mi	3.8mi	4.4mi	2.5mi

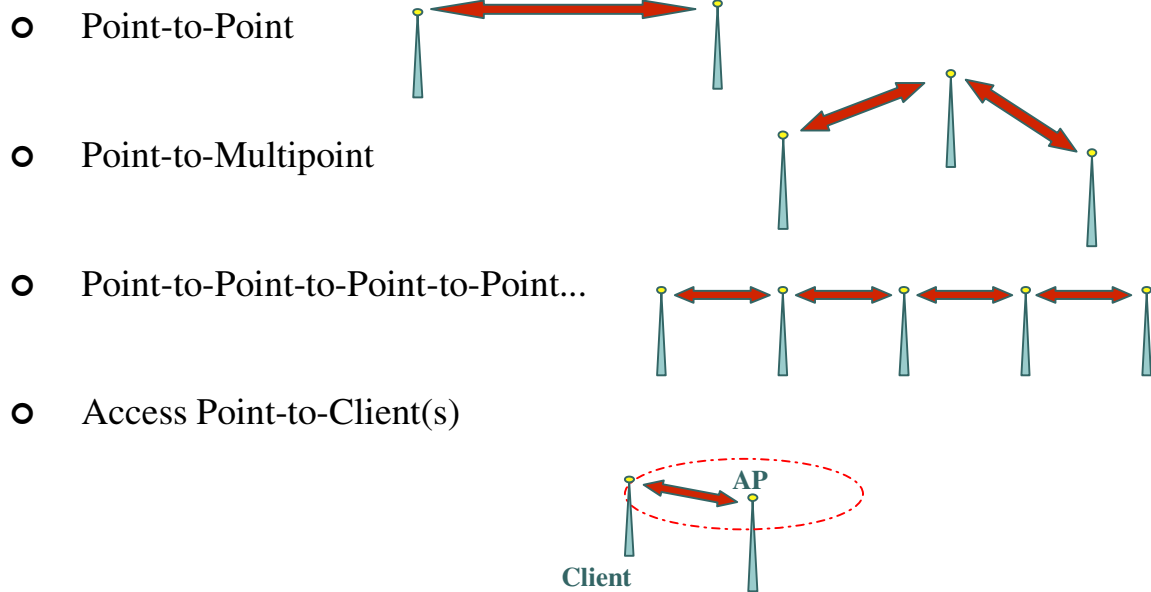
A limitation on long distances with 802.11b products is the requirement of clear line-of-sight (LOS). Signals can be transmitted through trees with limited success; however, in wet conditions, the signal will degrade significantly due to reflection from water on foliage. One advantage for the DOTs is that outside of owning a mountain top or having access to cell towers, the best line-of-sight through a region is the existing interstate infrastructure. Since the DOT owns the ROW along an interstate, it can use it to create wireless LANs easily. To minimize the chance of interference from competing systems, using highly directional antennas to focus as much power along the ROW corridor is suggested.

The curvature of the earth also poses limitations on how far a signal can be transmitted at a given height. At a typical telephone pole height of 35 feet, a signal can be transmitted (given clear LOS) up to 5 miles.

Some new 802.11a products are quoting non-line-of sight (NLOS) capability, but the researchers involved in this effort have not verified this capability at this time. There are some proprietary wireless products available today that are capable of NLOS; however, their costs are significantly more than the COTS products that are being looked at for this study.

### **Suggested Architectures**

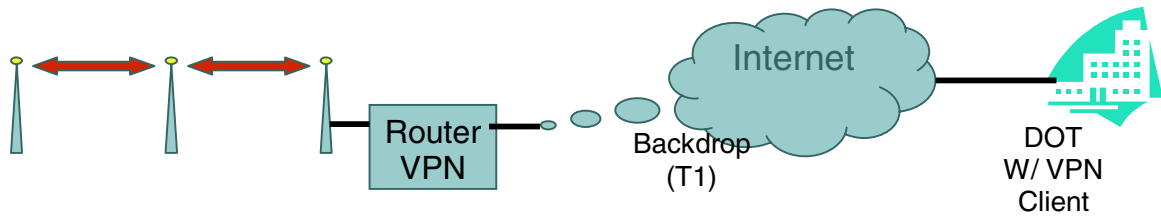
The design of a WLAN will depend on several factors, including desired capabilities, terrain, and available infrastructure. In general, they can be constructed in the following architectures: single point-to-point, point-to-multipoint, serial point-to-point, and client-Access Point (point-to-multipoint).



**Figure 4 Wireless Architectures**

Note that there is a distinction between the Access Point (AP)-client architecture and the other architectures. The first three are considered backbone architectures and operate on a different “level” than the client-AP. In general, the client-AP architecture is not recommended because it adds more security issues. In addition, the majority of this discussion will focus on static locations. However, a mobile application of client-AP architecture that has shown seamless connectivity at highway speeds has been deployed and tested. This will be discussed later.

Point-to-multipoint architectures are the most robust because each link is independent of the other link. In serial point-to-point, each previous link is dependent on subsequent links. However, for most linear highway environments, a serial application is the only option. The number of “hops” that a serial network can go depends on the technology used and the requirements placed on the network. One drawback of a serial daisy-chained wireless network, is that the available bandwidth begins to degrade over successive hops. This will be discussed in greater detail later. The serial LANs can be installed as a completely self-contained network terminating at a DOT office, or they can be set up to interface with the Internet through a T1 or better connection. With this type of design, the remote network and associated field devices can be accessed from anywhere on the Internet.



A typical scenario on a highway ROW would involve telephone pole height towers placed approximately 1-3 miles apart, depending on the terrain and highway topography. With 802.11b technology, an 8-hop system still has over 500kb of bandwidth available at the furthest node, which is adequate to support a jpeg still or MPEG4 streaming video. A base node or Internet connection should be placed in the middle, with wireless nodes extending in two directions away from it. With an 802.11b system, this segment could span 16 to 24 miles of highway ROW.

Newer technologies, such as 802.11a point-to-point systems start out with a higher aggregate throughput than 802.11b and, therefore, could extend well past 8 hops and still have enough bandwidth to support MPEG 4 streaming video.

The video or traffic data could then be disseminated to the agencies and public that need it.

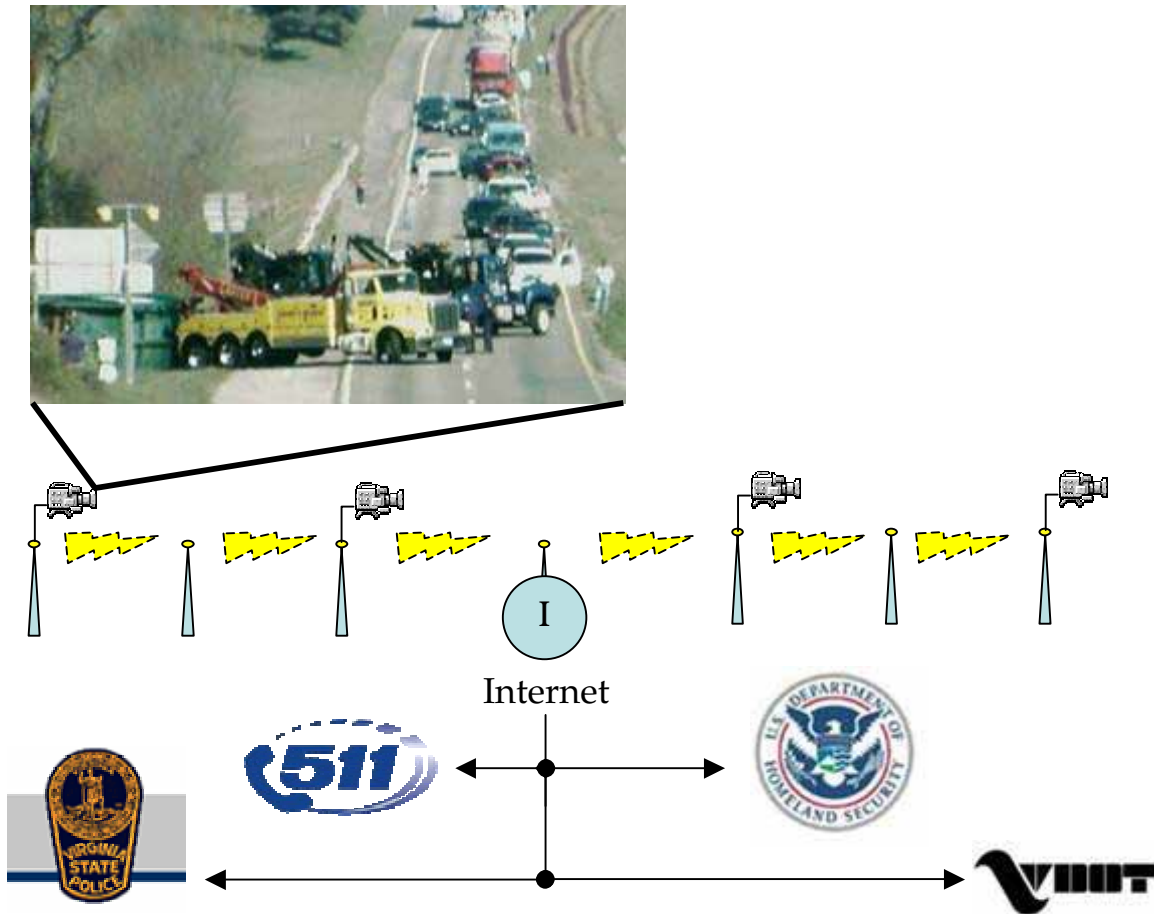


Figure 6 Conceptual Diagram of Highway Wireless LAN

### Wireless security issues

The issue of security comes up often during discussions of wireless. The main difference between wireless and a wired network is that one cannot control access to the physical medium with wireless. A DOT can lock the doors to an Ethernet closet but cannot shut down access to the air waves. In order to discuss security, the first step is to not think in terms of absolutes. Network security can only be addressed in relative terms, like a stair step, with each step more secure than the next. The Network owners develop a security plan by determining what they are trying to protect, who they are protecting it from and how much they are willing to pay in terms of time and money to protect it. For example, is it worth spending a lot of effort securing a camera image that the DOT is going to publish on the Internet anyway? In contrast, it is paramount to protect access to a VMS or a changeable HOV lane.

In general terms, there are two specific areas that need to be addressed with securing a wireless LAN: 1) Encrypting the actual wireless transmissions; 2) securing the routing and networking aspect of the LAN. Each type of wireless protocol has its own encryption techniques for securing the wireless transmissions. For 802.11b, Wired Equivalent Privacy (WEP) was the first version of encryption. Very soon after release,

techniques were developed to crack WEP-based encryption using specialized equipment that required a few hours of “sniffing” the airwaves. The industry is well aware of the deficiencies of WEP and is rolling out replacement encryptions, such as WPA and AES this year.

The network portion of security for a WLAN is almost identical to a wired network. The same protocols that are in use every day on the Internet can be applied to a wireless network. Protocols such as SSL and Virtual Private Networks (VPN) are suggested to provide the best network security on WLAN.

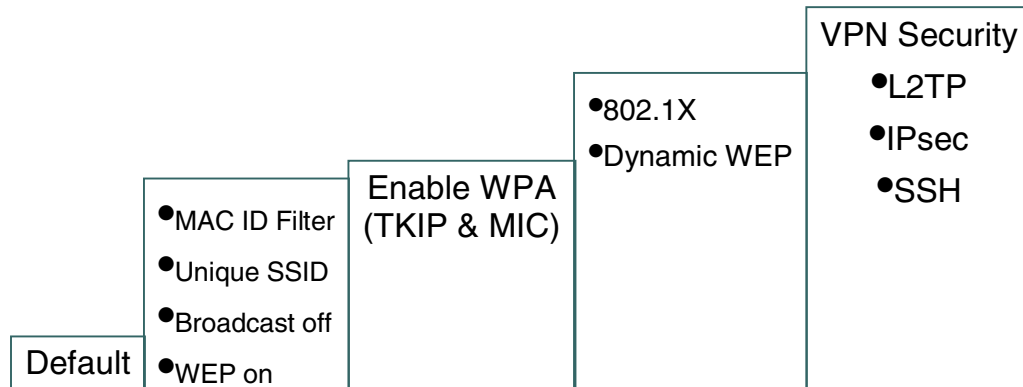


Figure 7 802.11b example of security steps<sup>2</sup>

## Real world deployments and current research

### Route 460 WLAN

The Virginia Tech Transportation Institute (VTTI) installed its first serial WLAN with VDOT over two years ago along route 460 in Christiansburg and Blacksburg, Virginia. The system was designed to provide a communications infrastructure for digital IP cameras for traffic monitoring purposes. The wireless network extends in three directions from the VTTI Smart Road Control room. The entire WLAN is networked as a stand-alone private system. It interfaces with the Virginia Tech Internet network via a router. This particular system has a maximum of five wireless hops away from the base node. At the three endpoints of the system, a wireless access point is available for client access into the system. These APs are disabled unless required for use by field personnel.

802.11b COTS products by Orinoco were used along with JVC network PTZ cameras. Most of the cameras utilize MJPEG compression; however, there is one newer model camera that has the option of MPEG1 or MJPEG. MJPEG, as will be discussed in more detail later, is not a very bandwidth efficient algorithm. With a serial wireless network, all devices on the network share the available bandwidth. Streaming video from all the cameras at the same time places a significant draw upon the WLAN. VTTI recommends grabbing JPEG stills on a timed interval, displaying them in a matrix, and then streaming from one camera at a time as needed. For a traffic monitoring concept of operations, this method is appropriate.

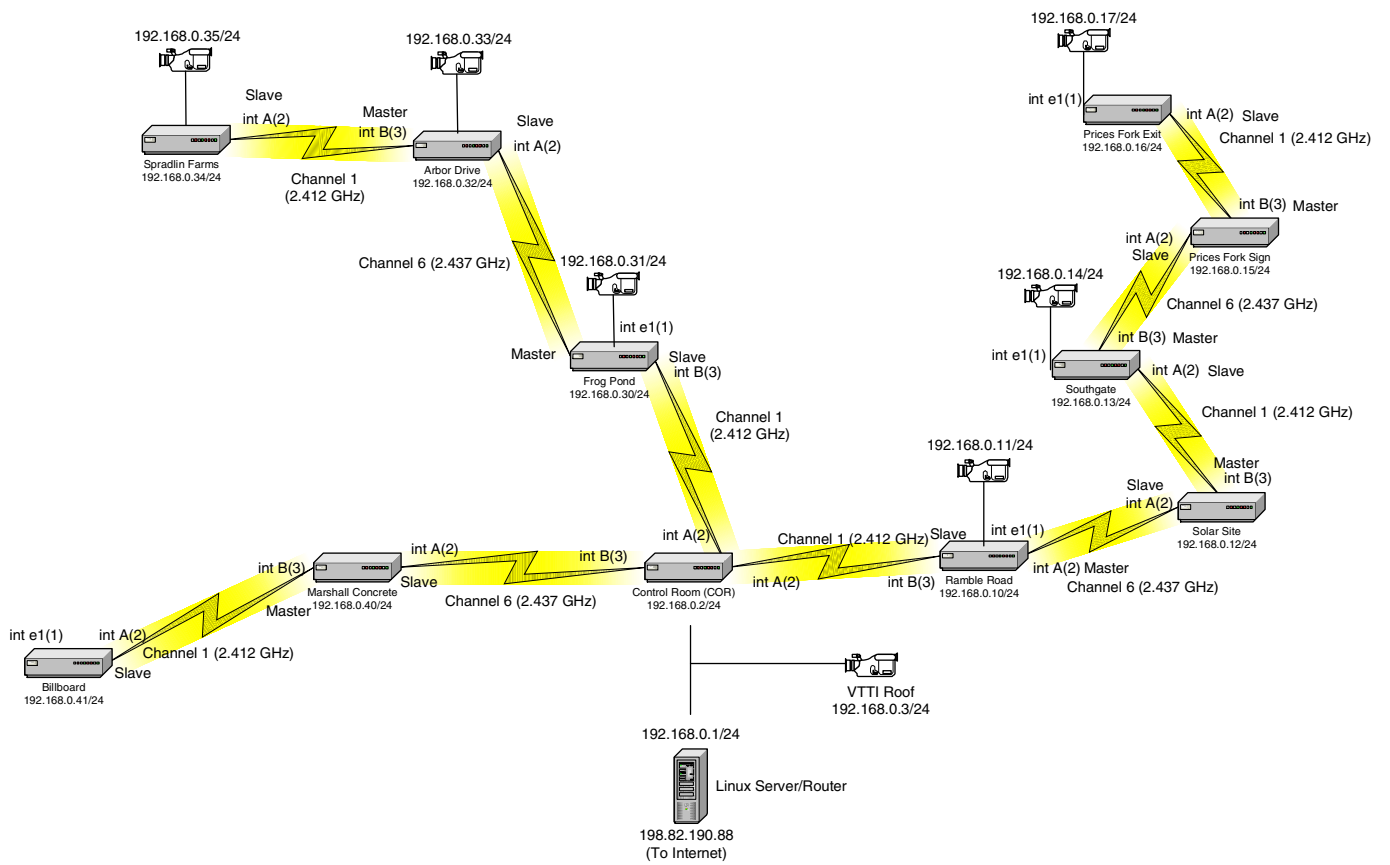


Figure 8 Schematic of Route 460 Wireless LAN

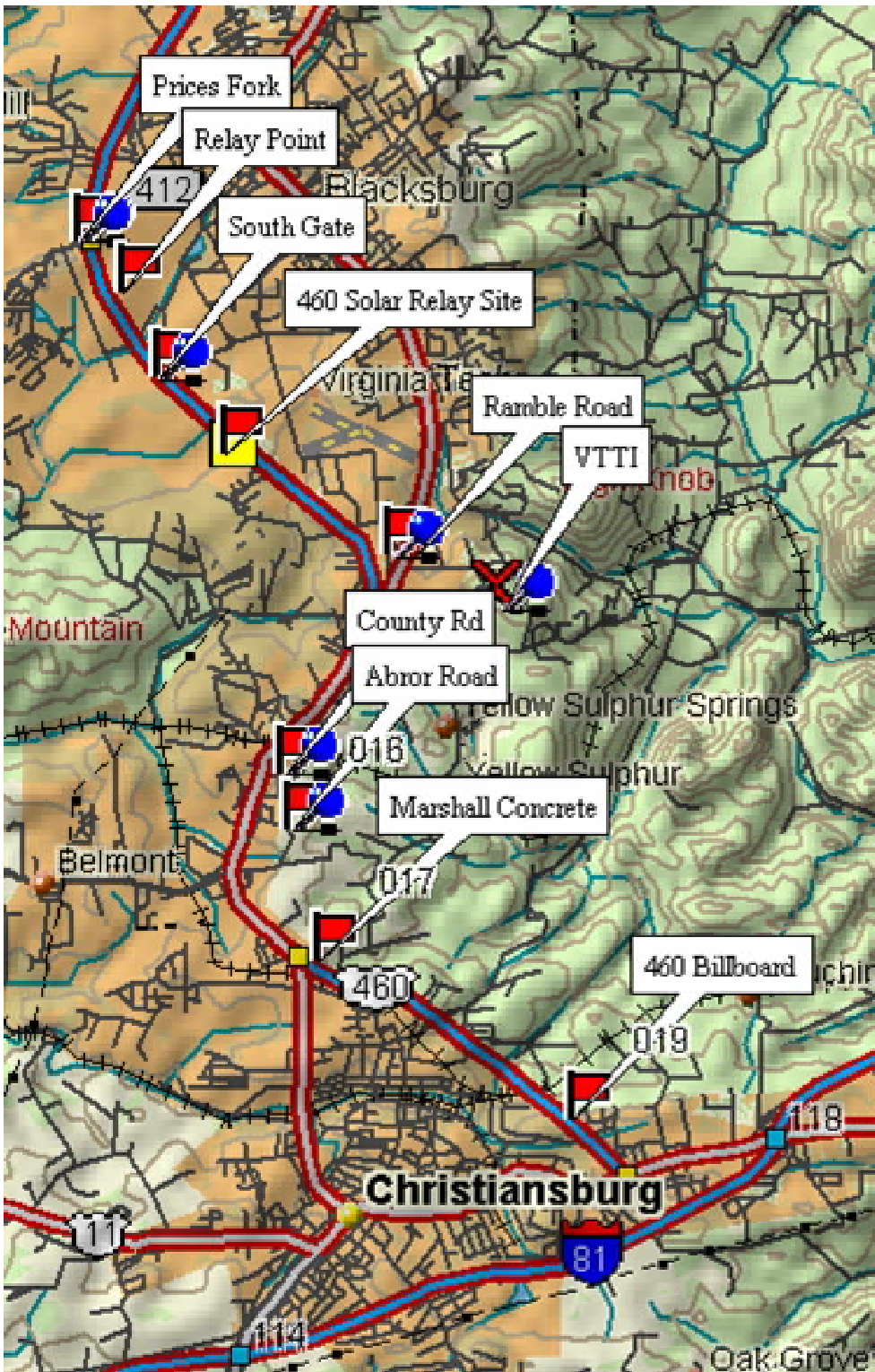
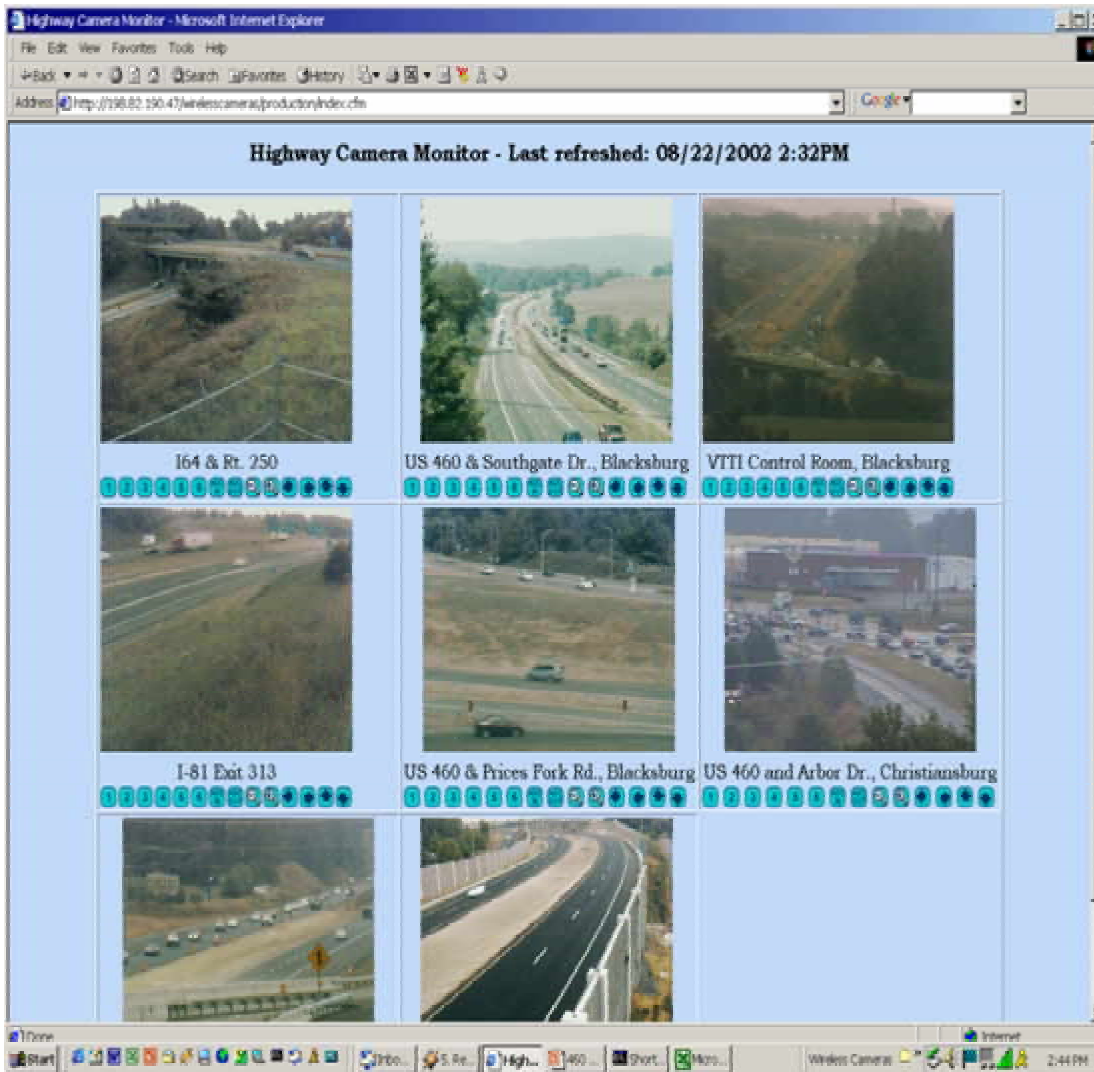


Figure 9 Map of Wireless LAN nodes



**Figure 4 JPEG Still viewing matrix**

VTTI is currently tracking all operations and maintenance of the Route 460 WLAN to track the long term costs of the system. As part of this analysis, Knowledge Skills Assessments (KSAs) are being developed for the design, deployment and maintenance of the system to help VDOT determine what skills they have in house and what skills they will need to contract or hire to make use of WLANs in their operations.

In addition to the 460 network, VTTI has worked with VDOT to deploy several individual cameras in the I-81 and I-64 cameras that connect to the Internet through a shared state Fiber Optic network.

VTTI is currently under contract with the Salem District of VDOT to design and install two 5-mile sections of WLAN along Interstate 81. The system consists of 21 nodes, 12 cameras, 7 acoustic sensors and 2 T1 Internet backdrops.

### **Smart Road 2 mile wireless backbone with seamless AP coverage**

Virginia's Smart Road is located at VTTI in Blacksburg. This highway is a closed test track used for various types of controlled transportation research. VTTI deployed a backbone serial wireless LAN down the highway and added access point coverage to create seamless coverage across 2 miles of 2 lanes and shoulders of the Smart Road. 802.11b technologies are not designed for mobile applications, and the intent in developing this system was to analyze the ability of the 802.11b standard to operate in a mobile environment.



**Figure 11 Aerial view of the Smart Road**

The wireless backbone was created using Orinoco ROR-1000 outdoor routers, as used on the Route 460 WLAN. Directional Yagi antennas were mounted on the top of existing light poles to transmit the backbone signal up and down the road. Two 120° sector antennas were mounted lower on the light poles to provide AP coverage up and down the road.



**Figure 52 Yagi Antennas for wireless backbone**



Figure 13 Sector Antennas for AP coverage

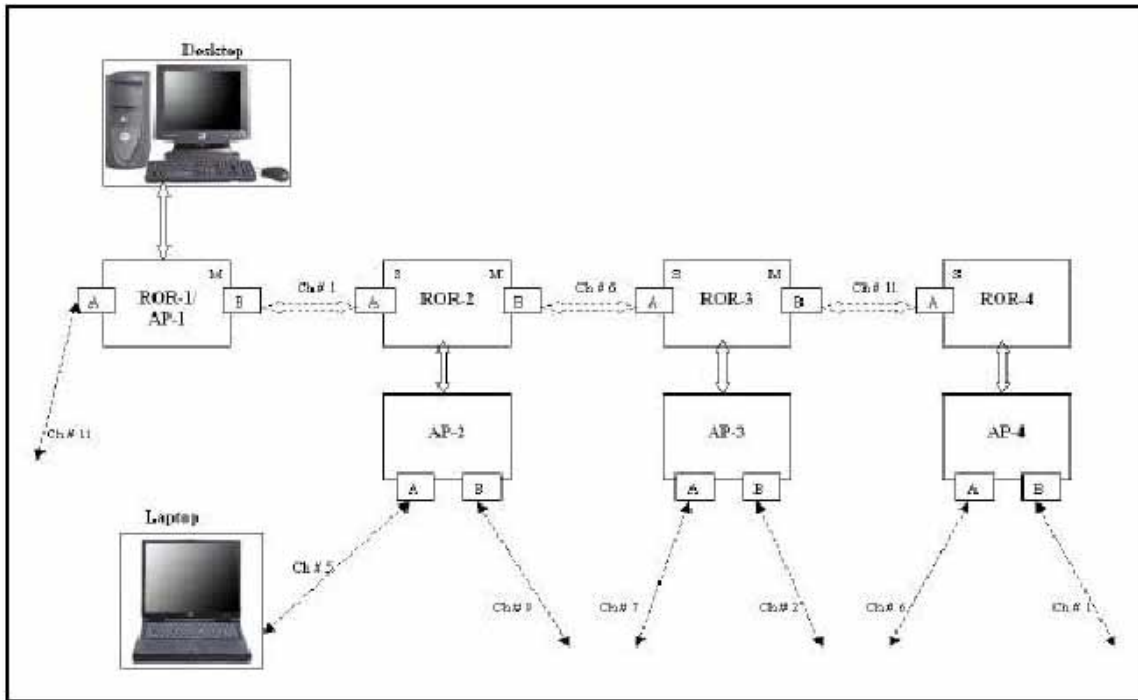


Figure 14 Smart Road Wireless Architecture<sup>3</sup>

While the technology was not designed with mobile applications in mind, the system works admirably at speeds ranging from 5mph up to highway speeds of 60mph. A client laptop inside the vehicle connected to the first AP upon entering the roadway. As the vehicle continued down the roadway, the client computer would associate with a new AP further down the road as the signal strength from the first AP grew weaker and reached a

threshold level where the client looks for stronger signal. This re-association to new APs continued through the length of the roadway. During mobile tests, VTTI used network analyzing software to measure throughput from the client computer to a stationary computer back at the command center. As mentioned earlier, the available bandwidth degrades as the number of hops away from the base node increases. The table below shows that when connected to APs further down the road, the throughput decreases. This will be discussed in more detail later; however, the important issue is that these readings were taken in a mobile environment.

**Table 5: Throughputs at speed along Smart Road testbed**

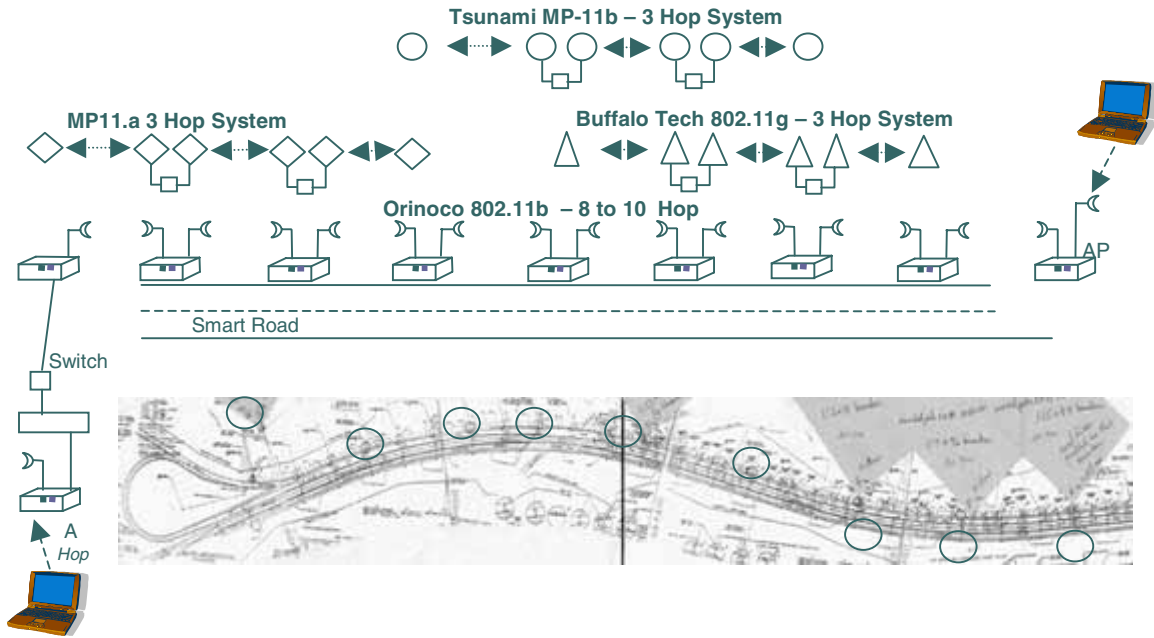
Laptop connected to:	Static (Mb/s)	20 mph (Mb/s)	40 mph (Mb/s)	60 mph (Mb/s)
AP-1	4.337	4.4023	4.1322	4.2823
AP-2	3.383	3.3654	3.1561	3.1568
AP-3	2.233	2.1893	2.1543	2.2058
AP-4	1.049	1.1986	1.1940	0.9824

### **Current Research and Preliminary Results**

Currently, VTTI has developed a reconfigurable wireless test bed on the Smart Road. Using temporary antenna poles that are easy to move, networks of over 8 “hops” can be created. In addition, an AP can be added at each end of the system to connect to a client to simulate an additional two hops. At each node, custom-designed Single Board Computers (SBCs) have been installed. These mini computers are used with the top-of-the-line network simulation software to allow benchmark readings of the wireless network performance to be taken.

Presently, VTTI has installed an 8-hop backbone Orinoco 802.11b system on the roadway that can be expanded to 10 wireless hops with the addition of APs on either end. A pair of Proxim Quick Bridge 20s and a 3-hop Tsunami MP.11b system have also been installed. VTTI is currently procuring a 3-hop Tsunami MP.11a system. Other devices that researchers wish to test include Smart Sight Networks Tri band 802.11b radio.

The test bed will be used to install varied devices in the field and then to benchmark their network performance. Criteria that will be measured include TCP and UDP throughput as well as ping delay times and signal-to-noise ratios in varied weather conditions. The UDP measurement is the most applicable for streaming digital video as it is a “connectionless” transfer. The research is not limited to just wireless devices: VTTI is also testing multiple digital video servers that assess their capabilities when used on serial wireless networks.



**Figure 15 Schematic of Smart Road WLAN Test bed**

As discussed earlier, one of the major issues to consider when dealing with serial wireless LANs is the bandwidth degradation that occurs at each node. When dealing with devices on a network, especially digital video, the main design criteria is the bandwidth draw of the device in relation to the available bandwidth of the system.

### **Analysis of Orinoco ROR-1000 802.11b Eight Hop Serial Wireless Network**

The network performance of an eight hop wireless LAN using Orinoco ROR-1000 802.11b radios was characterized using NET IQ Chariot, NET IQ Qcheck, and simple FTP transfers between laptop computers. Over 600 records per hop were taken with Chariot for UDP characterization. Chariot would not work with Orinoco ROR product line for testing TCP throughput, so FTP transfers were used instead. Using regression analysis it was determined that the UDP throughput decreases by 4% per hop. There was a linear relationship between throughput and number of hops that can be described by the equation:  $\text{Throughput} = 4.524 - 0.159 * (\# \text{ of hops})$ .

Figure 16 shows the linear degradation in UDP throughput over successive hops for the Orinoco test system. TCP data was gathered by placing laptops at each node and performing FTP transfers between laptops. As expected, UDP throughput is higher than TCP throughput due to the connectionless nature of UDP.

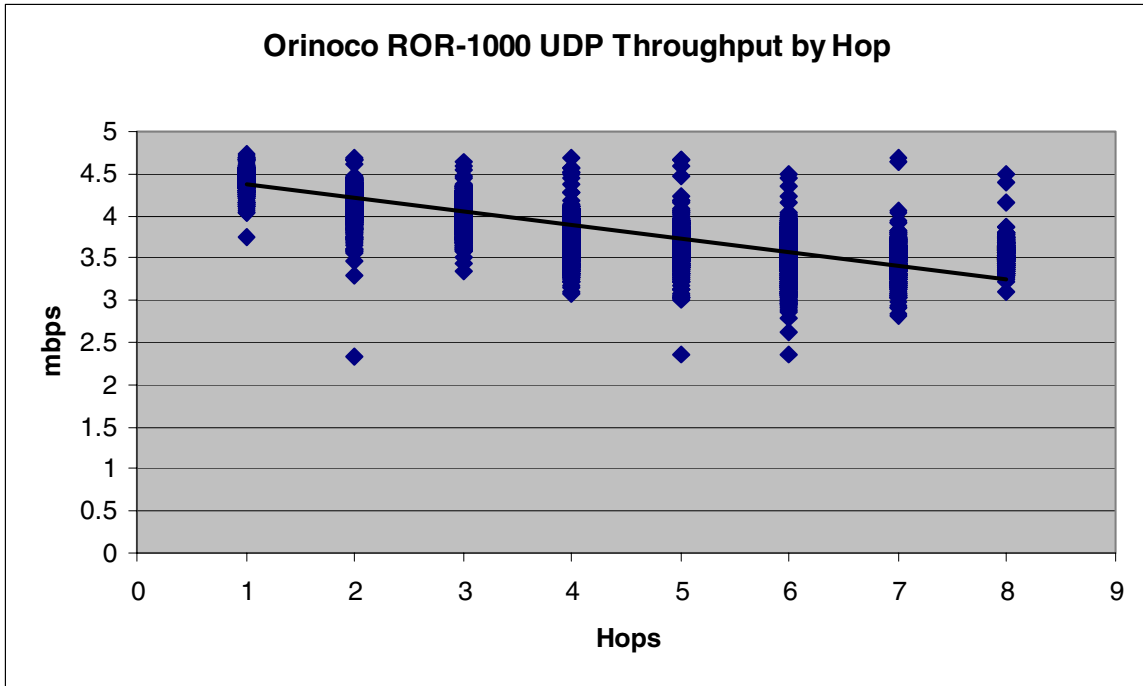


Figure 16 Orinoco UDP throughput

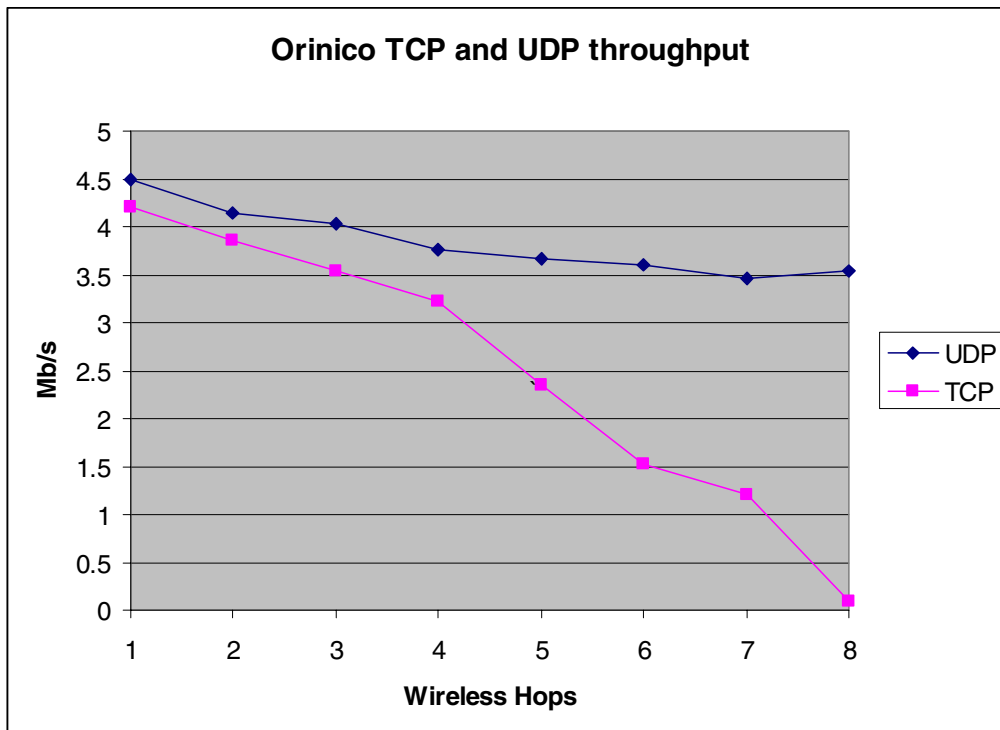


Figure 17 Orinoco TCP and UDP throughput

### Analysis of other systems in 3 hop configurations

We have procured several other radios and set them up in 3 hop configurations in order to determine if they are suitable for a serial type of architectures. Some radios, such as the Tsunami Quick Bridge products would not operate in a serial configuration over multiple hops and are more suited for individual point to point or single link point to multipoint architectures. Currently we are testing the Proxim MP.11a 802.11a radio, the Proxim MP.11 802.11b radio that has replaced the Orinoco product line, and the Buffalo Tech 802.11g wireless bridge/AP radio.

Below are summary results from our throughput analysis of 3 hop configurations of the above systems. Our goal is to develop similar formulas to our Orinoco analysis to help in specification development.

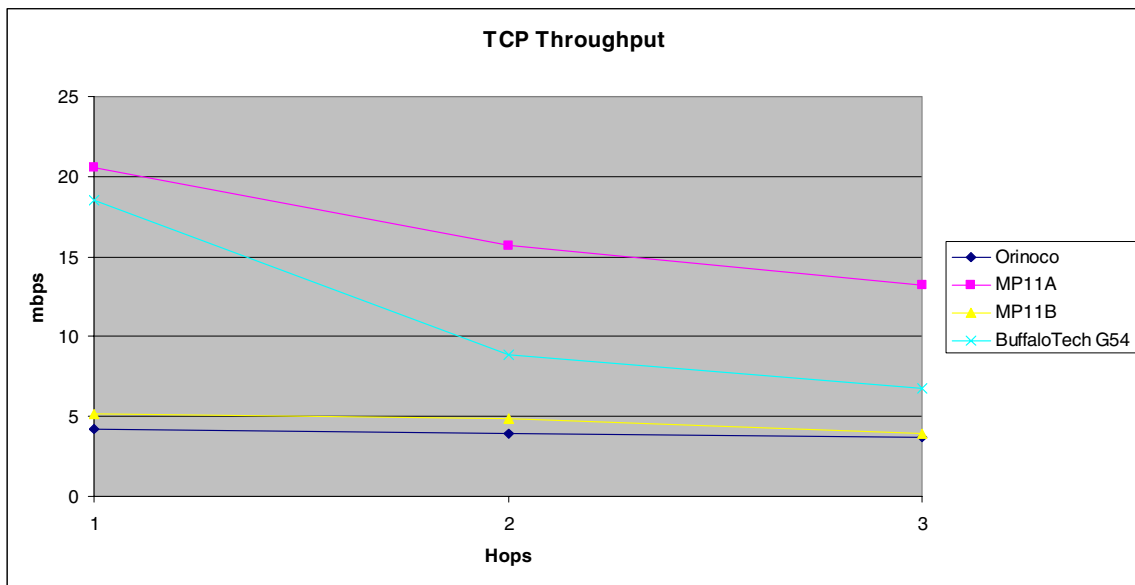


Figure 17 TCP Throughput Comparison for 3 Hops

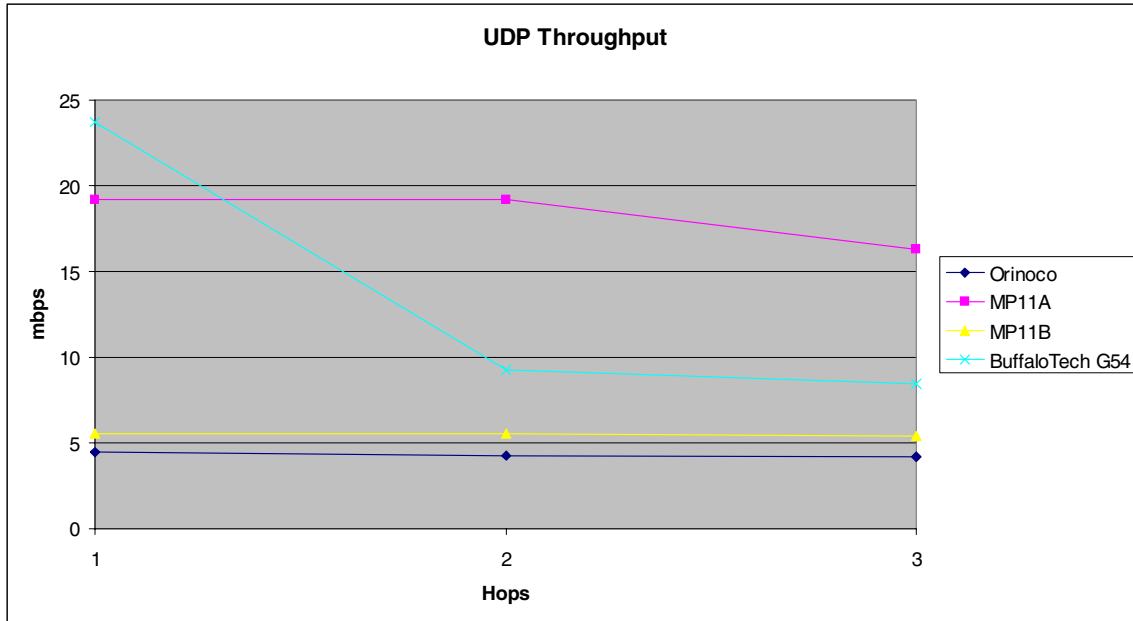


Figure 18 UDP Throughput Comparison for 3 Hops

### Design Methodology

The first steps required for designing a wireless LAN are to determine the quantity and type of devices that will be placed on it and that will be sharing the bandwidth. Cameras are by far, the most bandwidth-intensive devices that will most likely be used in the field. Therefore, they tend to be the driving force in defining the requirements of a WLAN.

Once the number of cameras is determined, the next step is to define what type of image is required and where it will be viewed. In other words, what kind of clarity, picture size, and streaming quality is required? Is a delay between when a PTZ command is issued and when the command is realized on screen acceptable? For example, in a security application where one must have the ability to pan and follow a specific vehicle or individual, a delay on the front-end compression or delay in transmission of a pan/tilt command might be unacceptable. However, this delay is perfectly acceptable in a strictly traffic monitoring application, where the defining questions are: Is traffic moving? If not, why?

Common digital video compression algorithms include MJPEG, MPEG1, MPEG2, and MPEG4. Each compression method will have a range of bit rates that the camera uses when streaming video. The chosen bit rate will affect the clarity of the picture, and depending on the specific compression method and manufacturer it may affect the frame rate. Larger pictures sizes will naturally require more bandwidth because they are sending more information.

All of these factors need to be taken into account to determine the optimal design of the WLAN. One suggestion is to make use of JPEG stills as opposed to streaming video for

general monitoring applications where several cameras are sharing wireless bandwidth. For example, if a network has 9 cameras on it, it is more bandwidth efficient to grab 9 JPEG stills every 30 seconds than it is to stream video from all 9 cameras at the same time. Cameras can be streamed continuously as needed for more detailed monitoring. If the terrain allows it, creating point to point links between each camera and a central location is the equivalent of home run fibers to each camera.

### **Next Steps**

VTTI is continuing its wireless research and plans to publish a full report on the results of the network benchmarking later this year. The goal is to begin testing several more products within the coming year. VTTI's experiences with the development of the Salem I-81 WLAN will help further the current knowledge base in WLANs and their use with digital video. We are available to help any state DOT with wireless and digital video training, specification development and wireless design.

There seems to be no slowdown for the wireless industry in the near future, and new products are being developed yearly. On the national-standards level, a new standard is currently in development called 802.16. This standard is specifically for backbone point-to-point applications. It will have its own dedicated spectrum and will be designed with higher throughputs and with the demands of long-distance point-to-point communications in mind. In addition, non-line-of-sight and near-line-of-sight systems will certainly come down in price, making them more available for large-scale deployments. In addition a DSRC (Dedicated Short Range Communications) standard is in development specifically for vehicle-to-vehicle and vehicle-to-roadside communications.

### **Conclusions**

Security, safety and mobility are the driving forces in ITS today. Infrastructure assets of the DOT are now considered targets and require monitoring that was never dreamt of before. The driving public craves more information, especially video to make its traveling decisions. DOTs need to place devices in the field to gather this information, which requires two main items: power and communications. Power can be accommodated with solar: however, communications can be the show stopper when it comes to deploying a field device.

The time for accepting wireless as a viable alternative is here. The costs are well within the means to deploy systems on a permanent or temporary basis. The speed in which they can be installed means that the field device can be placed within months instead of years. While it is by no means an end-all solution, wireless is definitely a viable option for DOTs to extend their communications network.

## Endnotes

1. Proxim Corporation
2. The Mansfield Group
3. F. Aziz, "Implementation and Analysis of Wireless Local Area Networks for High-Mobility Telematics," Masters Thesis submitted to Virginia Tech University, p. 124, May 2003.

## List of Tables and Figures

Table 1 Comparison of Communication Alternatives

Table 2 Frequency Bands of Unlicensed Spectrum

Table 3 Aggregate Throughput of COTS products

Table 4 Distance Chart for 802.11b radios

Table 5 Throughputs at speed along Smart Road test bed

Figure 9 Typical application of Wireless

Figure 10 Initial costs for mock scenario

Figure 11 Wireless compared to Telephony over time

Figure 4 Wireless Architectures

Figure 5 Wireless LAN connected to the Internet

Figure 6 Conceptual Diagram of Highway Wireless LAN

Figure 7 802.11b example of security steps<sup>2</sup>

Figure 8 Schematic of Route 460 Wireless LAN

Figure 9 Map of Wireless LAN nodes

Figure 12 JPEG Still viewing matrix

Figure 11 Aerial view of the Smart Road

Figure 13 Yagi Antennas for wireless backbone

Figure 13 Sector Antennas for AP coverage

Figure 14 Smart Road Wireless Architecture<sup>3</sup>

Figure 15 Schematic of Smart Road WLAN Test bed

Figure 16 Orinoco UDP Throughput

Figure 17 TCP Throughput Comparison for 3 Hops

Figure 18 UDP Throughput Comparison for 3 Hops