

# Ethernet in Intelligent Transportation System Applications: **Intelligence is Essential**

In order to decrease congestion on the roads and save lives, Departments of Transportation (DOT) are investing in solutions that make highways “smarter.” By using intelligent transportation systems (ITSs), DOTs are able to monitor and react to traffic-flow issues, speed emergency communications and response, better inform the public of traffic issues, and expedite traffic by using automated toll collectors. Networked applications are critical to the success of ITS solutions, and they require the ability to handle many types of data and performance requirements. Ethernet is a cost-effective, high-bandwidth, intelligent technology that gets the most out of the ITS network infrastructure.

Performance requirements of intelligent transportation system (ITS) networks are increasing dramatically. Many new ITS projects are using video monitoring, which increases bandwidth demands from thousands to tens of millions of bits per second. Mission-critical data coexists on the same network as lower-priority monitoring data, creating the need for bandwidth optimization. Wireless access is being considered for deployment at city intersections. Information is shared with many end users, including users on the Internet, generating the need for logical network partitioning and security.

Traditional networks are being upgraded to meet these requirements, using fiber, wireless technology, lower-cost endpoints,

and scalable architectures. Transmission Control Protocol/Internet Protocol (TCP/IP) represents an excellent end-to-end solution for these requirements, and as a result, Ethernet is being deployed as an underlying architecture in many ITS networks.

Transportation network infrastructures are historically a collection of many traditional networks. These networks are stable and reliable, but often lack the economies of scale necessary to deliver the performance requirements of today’s ITS solutions. A top priority of a network upgrade is to deliver an infrastructure built on a single, standards-based, scalable technology. Ethernet, the most widely recognized networking standard today, is an obvious consideration. It is prevalent in most networks worldwide, is extremely cost-effective (due to a supplier base that is shipping millions of ports a month), and is easy to deploy and manage. As such, it is the technology of choice for many next-generation ITS networks.

The shift to a single underlying technology in the ITS network infrastructure is a natural convergence, completed in the corporate network a decade ago and rapidly moving into many new applications today. Manufacturing (industrial Ethernet), telecommunications (metro Ethernet), and ITS networks are migrating to Ethernet as an underlying technology.



## Accelerating Change

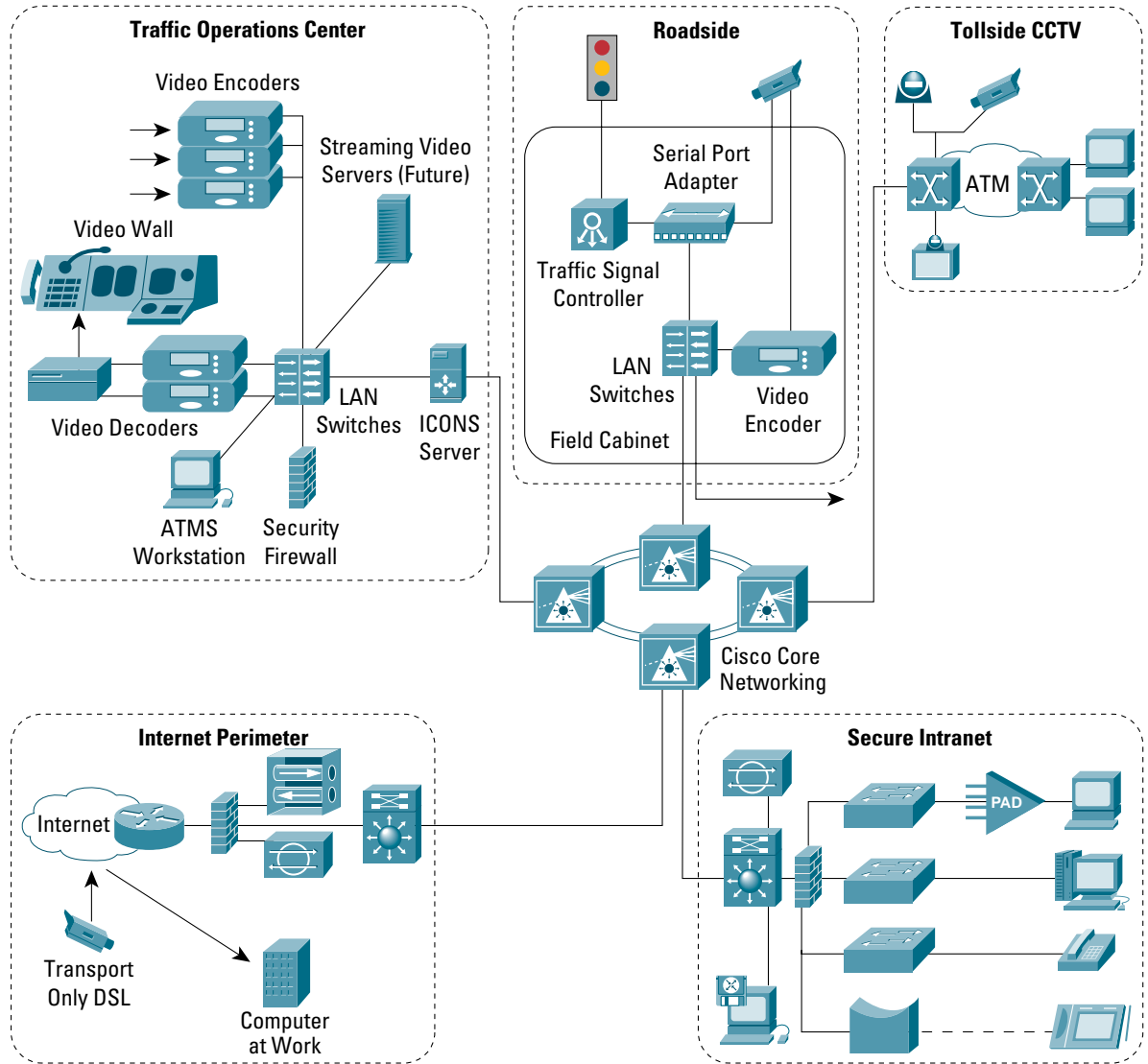
A closer look at the needs of today's ITS networks makes the benefits of Ethernet clear. ITS infrastructures demand the following to scale to today's services:

- *Commonality*—Network administrators are interested in deploying a single underlying technology for the network infrastructure. Ethernet is the most recognized networking standard today, and is a comfortable solution for many ITS network administrators.
- *High bandwidth and bandwidth optimization*—Video monitoring is becoming an important element of an ITS network. Ideally, project managers can provide the ability to monitor up to hundreds or even thousands of locations. A digitally encoded video-over-IP solution requires data streams of 500 kbps to 6 Mbps in size. Fast Ethernet and Gigabit Ethernet infrastructures allow cost-effective scalability to meet these needs.
- *Availability and scalability*—ITS networks need to be resilient. The network should be able to respond to unexpected bursts in traffic or the failure of a network component, and recover quickly in the event of a link failure. The network also must accommodate future needs, and be able to scale from tens of end devices to hundreds or thousands without the need for a major overhaul.
- *Network security*—A well managed ITS network carries data that is valuable to many end users. Police and fire departments can use ITS data for emergency response and monitoring. Local TV stations can use video streams to broadcast traffic conditions. Commuters would like access to traffic conditions via the Internet. To effectively deliver these services without compromising sensitive information or making the network susceptible to threats, network security is essential.

Figure 1 shows an end-to-end ITS infrastructure, based on IP. In the example, Ethernet is used as a backbone technology connecting the traffic operation center, traffic intersections, traditional closed-circuit TV (CCTV) over Asynchronous Transfer Mode (ATM) networks, and data handoffs to the Internet.



**Figure 1**  
An Ethernet ITS Infrastructure



### Intelligent Ethernet—The Key to Scalable Ethernet ITS Systems

ITS project managers should be careful to select Ethernet products that add vital intelligence to their networks. Ethernet has many advantages over traditional technologies that exist in ITS networks today. It is important to know, however, that not all Ethernet solutions are the same. An effective ITS network needs to take advantage of intelligent Ethernet, a suite of features that allows the network infrastructure to meet its data service requirements.



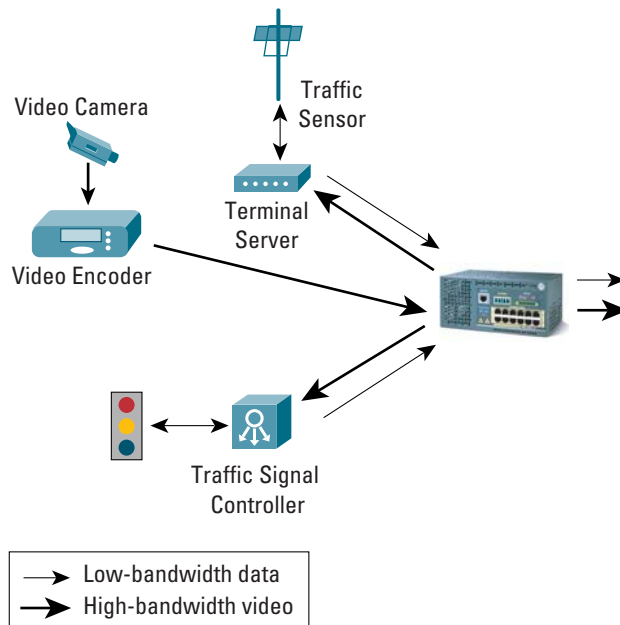
What is meant by “intelligence?” Specifically, an Ethernet solution should provide additional services that make the network highly functional, manageable, and secure. For ITS environments, these intelligent services should include:

- *Multicast support featuring IGMP snooping*—The Internet Group Multicast Protocol (IGMP) defines the rules used to deliver multicast traffic, such as video, over an IP network. IGMP snooping is an Ethernet switch feature that prevents the multicast traffic from reaching devices that have not requested it. Without this feature, other equipment colocated with the video equipment will experience a constant flood of unwanted, high-bandwidth data.

In the example in Figure 2 below, a roadside cabinet is configured with a traffic signal controller, video camera with encoder, and terminal server for a traffic counting sensor. An intelligent Ethernet switch is used as the interface to the network. The signal controller and traffic counter deliver low-bandwidth data back to the traffic control center via the switch, while the encoder delivers high-bandwidth video streams. Without IGMP snooping, the switch will forward all multicast traffic, or video, to its other ports. This activity could potentially flood the other equipment with incoming data and prevent it from sending its own information. This problem becomes worse in multiple-camera configurations.

**Figure 2**

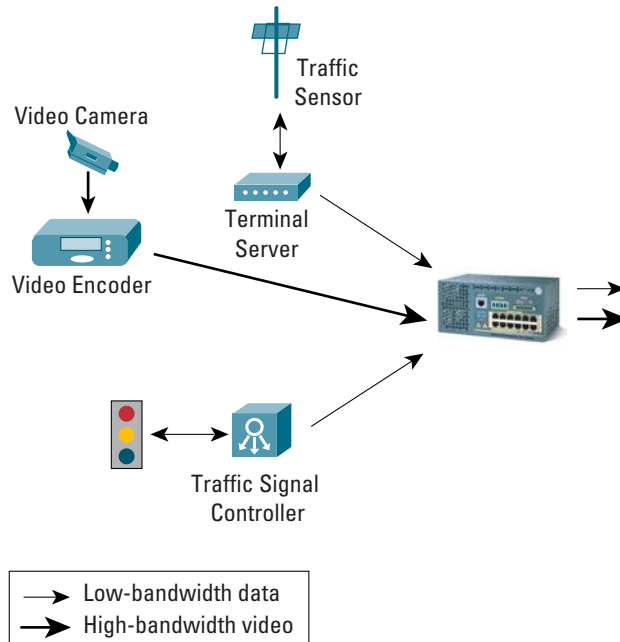
Without Multicast Control, Video Traffic Floods Other Devices



With IGMP snooping enabled, the switch “snoops” the incoming data, looking for devices that specifically request the multicast information. The switch will only forward the video to those devices. Figure 3 shows how an intelligent switch protects devices in the cabinet from video flooding.

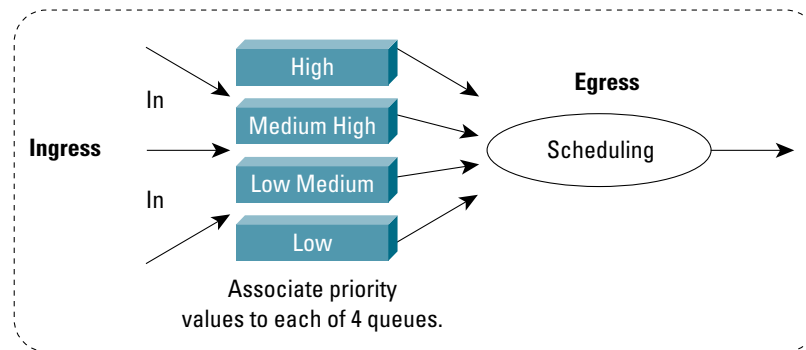


**Figure 3**  
IGMP Snooping Prevents Video Flooding



*Quality of service (QoS)*—An Ethernet ITS network may transmit many different types of data—from highway monitoring information to mission-critical health alerts to bandwidth-intensive video. The network must be able to distinguish among, and give priority to, different types of traffic. QoS mechanisms do just that. They ensure all traffic receives the required bandwidth, priority, and latency so the network runs smoothly and efficiently.

**Figure 4**  
QoS Traffic Shaping and Prioritization



*Virtual LAN (VLAN)*—VLAN support provides reliability, network security, and isolation by logically segmenting end devices from the network. A device assigned to a particular VLAN will not share traffic with a device assigned to a different VLAN. Using VLANs on a switched network, network ports and end devices do not have to manage unwanted traffic, improving their availability.

Port security and access control lists (ACLs). This capability at different layers provides granular and secure filtering, and allows a network administrator to prevent or allow access to information based on its source, destination, and type of application. Access can be based on physical parameters (for example, port number or MAC address), IP address, or TCP/User Datagram Protocol (TCP/UDP) port (essentially determining if the packet is from an application that should be running on the network). This is particularly effective when sensitive data is sent on the network (for example, emergency response data) alongside data that will be shared with a large community of end users (for example, traffic reports on the Internet).

*Redundancy featuring Rapid Spanning Tree*—The Spanning Tree Protocol permits the rapid convergence of a network during a network failure. When a problem occurs on a network node, a redundant link will automatically become active to bring the network back online. With Rapid Spanning Tree (IEEE 802.1w), networks converge very quickly—usually in less than one second.

*Simple Network Management Protocol (SNMP) support*—SNMP forms the basis of virtually every major network-management system. Intelligent Ethernet devices must support SNMP, allowing them to interface with an existing management system or with commercially available management systems.

## Looking Ahead

For project managers, ITS networks must be highly available, reliable, and secure. At the same time, network elements must provide highly intelligent features that allow end users to take advantage of the flow of information available. Intelligent Ethernet fulfills these requirements and more, resulting in a migration to this robust platform. Due to its obvious advantages, intelligent Ethernet adoption will only accelerate over the next few years as ITS administrators choose to consolidate their operations under a single, intelligent network.



### Corporate 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: 408 526-4100

### European Headquarters

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0304R) 203104/ETMG\_07/03