MISSION CRITICAL COMMUNICATIONS FOR TRAFFIC MANAGEMENT SYSTEMS

Introduction

A basic tenet of smart city programs is the deployment of technology to manage assets and resources more efficiently. Within this movement, city transportation infrastructure is often a top priority, given its extensive use and impact on residents, businesses and emergency response. Now with the growth of smart transportation systems, the arrival of connected vehicle technology and the future of autonomous vehicles, there is an increasing demand for maximum network bandwidth and high availability communications.

The enormous advances we are seeing today in technology, network speed and life-saving applications are enabling municipalities to address those challenges in intelligent, efficient and economical ways.

What we'll cover

The focus of this document is the critical communications network required to support a traffic management system. In traffic management, and broadly in Intelligent Transportation Systems (ITS), municipalities are deploying an increasing variety of applications and technologies. Examples include systems support signal priority, adaptive control, travel time and congestion pricing as well as connected vehicle technology for safety on city streets. We describe the underlying network requirements of these systems, including their interface with and reliance on a dependable communication network for their operation and performance.

Solving your city's challenges and preparing for the future

City managers face many challenges, especially with the trend toward urbanization. Surface transportation infrastructure capacity must increase to support new residents and businesses. However, widening the roads is costly and disruptive.

A better approach is to increase capacity using intelligent traffic management technology. These adaptive systems gather more citywide data and exert additional control at intersections. A dependable, high-speed communications network is critical for the traffic management system to function more efficiently.

Existing traffic management systems typically make use of a communications network for traffic signal coordination and system management. There are many legacy types, both narrowband and broadband, consisting of ISM-band radios, microwave, twisted pair and leased line.

Historically, the core requirements of these systems have not included real time, reliable communications, as the traffic controllers installed at intersections can operate autonomously at a basic service level using pre-programmed time-of-day schedules. Cities can build on this existing infrastructure, with updates to the communications infrastructure, for a significant improvement in traffic control.

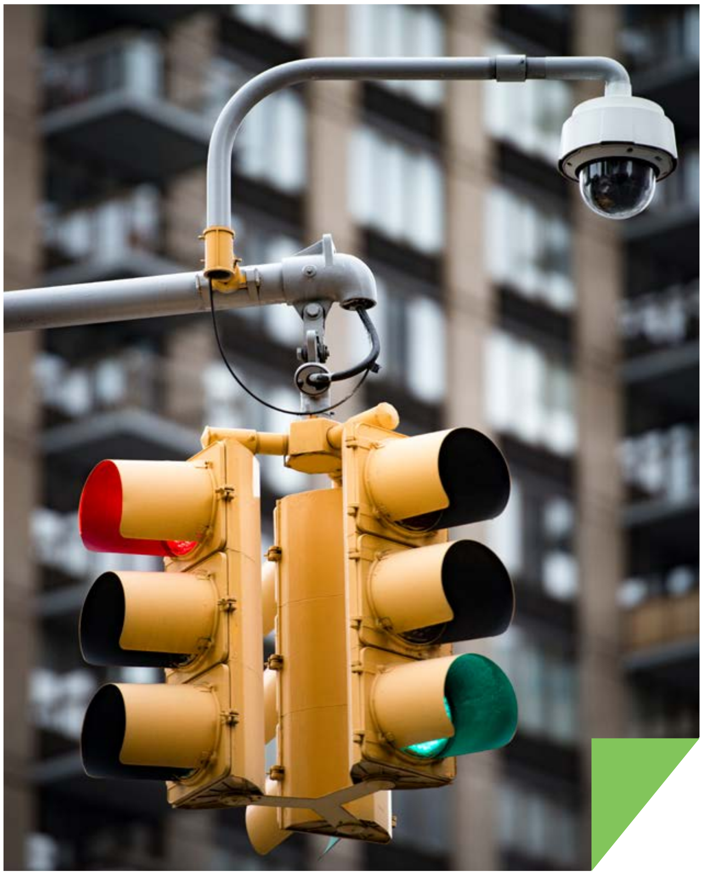
Smart city paradigm shift

The smart city movement has brought about a paradigm shift, where basic pre-programmed operation is no longer sufficient. At the same time, new applications and technologies requiring reliable broadband communications have been proven to deliver benefits to the community served. A few example solutions are described below.

- **Congestion detection:** Traditional single-vehicle detector loops are replaced with radar and camera systems, enabling detection of entire vehicle queues and city congestion.
- **Adaptive control:** Detected vehicle congestion triggers changes to traffic signal timing to optimize traffic throughput in real time.
- **Connected vehicle:** Installations are happening now to meet the objective of this technology: to prevent accidents through real time communication between vehicles, pedestrians (via smart phone detection) and the traffic control system.
- **Bus rapid transit:** Traffic signal timing is adjusted to maintain schedules of BRT transit buses.
- **Emergency routing:** A path through the city is coordinated for first responder vehicles, using congestion data and vehicle location to adapt route guidance and traffic signal timing.

The time is now to deploy the communications technologies that support these fast moving smart cities initiatives. Cities on the cutting edge of this movement will see better traffic flow, improved emergency response and a reduction in traffic accidents and pedestrian fatalities. The heart of these deployments is a Smart Traffic Management System.

> Widening roads is costly and disruptive. A better approach is to increase capacity using intelligent traffic management technology.



Architecture of a smart traffic management system

Smart traffic is not complex. But it is critical to integrate system management and high performance cellular technologies into existing infrastructure to establish flawless operation. The system architecture described below is designed for fast, secure communications as well as automation of critical systems and central visibility and control.

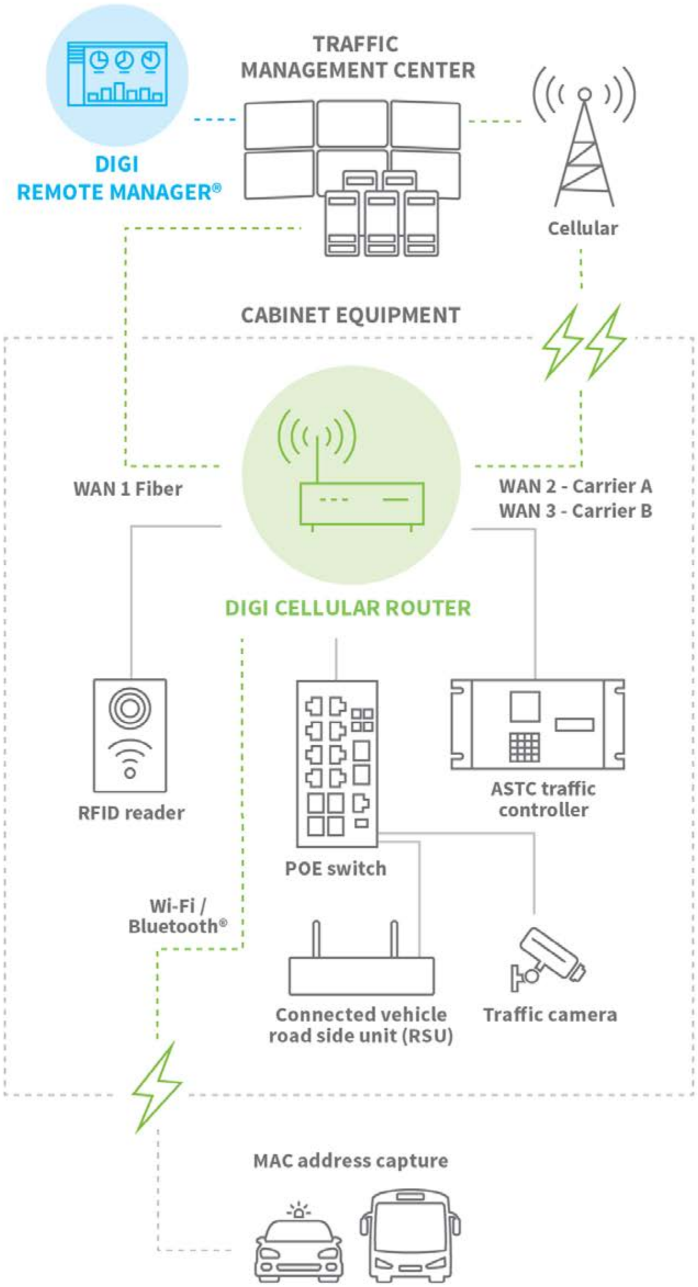


Figure 1: Traffic Cabinet Communications

The Traffic Management Center (TMC) is the central facility where vehicle and pedestrian movement is monitored and controlled. The Digi router provides secure and reliable communications between intersection equipment and the TMC, while Digi Remote Manager® (Digi RM) provides central control over the communications infrastructure. The Traffic Cabinet Communications diagram presents the various entities and their connections. The principal system functions are as follows:

- **Backhaul communications:** Multiple concurrent cellular and fiber links ensure continuous communications with the TMC. IPsec VPNs ensure secure passage through any network.
- **Local network:** The router's built-in four-port Ethernet switch supports connections to IP-enabled equipment within the cabinet. A Power-over-Ethernet (POE) switch expands the port count and supplies power to multiple IP cameras.
- **Legacy equipment:** A serial port is provided for connection to legacy devices such as an RFID Reader. Typically, a server application accesses the device using virtual comm port redirection.
- **Local management:** The router supports simultaneous client and access point Wi-Fi operation. Nearby authorized personnel can download heavy data such as stored video files or manage cabinet equipment using a laptop or handheld device.
- **MAC address capture:** MAC addresses from passing Wi-Fi or Bluetooth devices are sent anonymously to a central server for travel time analysis and displays, providing drivers with an estimated driving time to key locations.
- **Additional functionality:** An available USB port allows for accessories and expansion, and GPS/GNSS provide additional options (not shown). The Digi router includes indicator LEDs for power, WAN signal strength, WAN service and GPS/GNSS (which can be reprogrammed for other functions).

Technology trends

The following are some of the key advances in Information and Communications Technology (ICT) relevant to traffic management systems. Digi cellular routers incorporate these technologies to support smart cities in deploying the most robust, forward-thinking traffic management, transit system and emergency response applications.

Cellular communications

Cellular communications are advancing at a rapid pace. Each new generation offers increased bandwidth, reliability and services. Much of the credit is attributable to 3GPP, a global consortium of standards organizations created in the late 90's with a vision for a wireless Internet. The advances are delivering key benefits to traffic management systems:

- **Service reliability:** Priority transmission even in shared spectrum is now available for eligible mission critical services such as traffic management systems.
- **Network capacity:** Higher density modulation enables increased data transmission speed without additional spectrum, reducing network operator costs and therefore service costs.
- **Lower latency:** The transmission delay of data packets continues to drop and is now in the range of a few tens of milliseconds, on average.
- **Equipment costs:** The global standard has resulted in economies of scale worldwide in technology deployment, product development and production.
- **Service costs:** The increasing market size, network expansion and open system established by 3GPP has reduced infrastructure costs for network operators.
- **Broadband communications:** Enables simultaneous transmission of both data and video.

With the availability of these benefits, cellular is now often deployed instead of fiber as the primary communications backhaul in traffic management systems. It is also used in conjunction with fiber as a secondary backhaul, or "failover," since a fiber cut can result in an extended network outage.

The impact of 5G

The long-term evolution of cellular infrastructure from 4G to 5G is certain to benefit traffic management systems in urban environments. For example:

- Multi-gigabit speeds will allow higher-resolution video surveillance to identify and resolve traffic incidents more quickly.
- Single-digit latency combined with V2X (vehicle to vehicle, vehicle to infrastructure and vehicle to pedestrian) will improve driver, passenger and pedestrian safety and reduce accidents and deaths.
- The massive amount of IoT devices deployed across a city will reduce excess traffic by enabling drivers to find a parking spot more quickly and get to their destination via the most optimal route available.

Keep up with 5G network news and migration planning by visiting our 5G Standards and Technologies page: http://www.digi.com/resources/standards-and-technologies/5g

Cloud computing

Not that long ago, cloud computing was considered to be an interesting fad — at most an option for hosting generic non-essential applications. Now it is generally acknowledged by industry experts as a key force in the evolution of the global IT infrastructure.

Cloud computing is profoundly changing the way governments and businesses operate, due to the core function of IT today. Government and industry entities worldwide are using cloud-based software, platforms, and infrastructure to improve access, streamline processes, lower IT complexity and reduce costs.

Deployment approach for traffic systems

Fortunately, modern infrastructure systems such as traffic management are predominately IP-based, so the operation of one subsystem is often independent of other subsystems. This is the case for the communications network. Field service contractors supported by vendors can often upgrade communication network equipment without disruption to existing traffic management systems.

Installation of field equipment such as the router, power supply and antenna is straightforward. The router and power supply are situated on a shelf within the cabinet, and connect to existing equipment by Ethernet, serial or USB cable. The antenna is fixed to the cabinet roof, with the RF cables entering the cabinet via a threaded through-hole stud mount, sealed to prevent water ingress into the cabinet.

Digi RM provides a management interface for automated configuration during the site activation process. Any site-unique parameters are preloaded into Digi RM, and automatically download when the router connects. The Digi RM dashboard shows connection status and key performance data to help spot any issues that occur. You can also perform a quick speed test to confirm full operation in preparation for site commissioning.

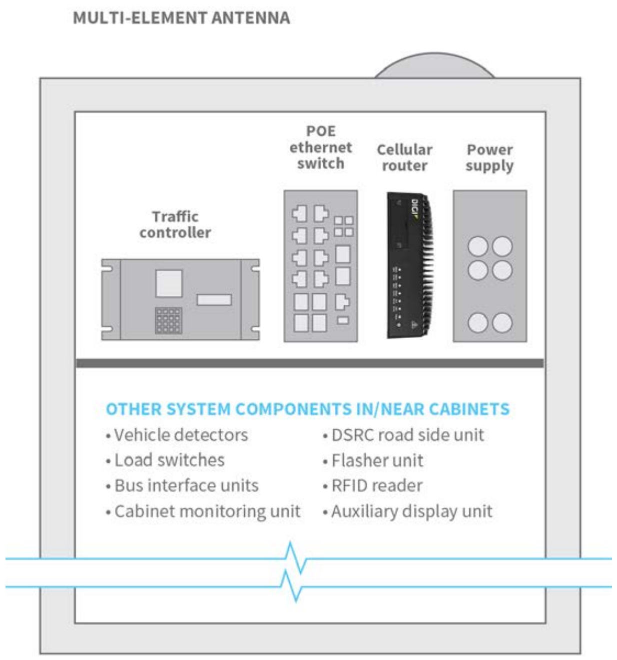


Figure 2: Traffic Cabinet Components

Equipment description

The core components used in the communications network are described below. Depending on system requirements, the communications network may be extended to include an Ethernet switch in the cabinet and a network appliance in the TMC.

Digi cellular router

Digi's growing offering of routers are purpose-built for smart traffic management and emergency traffic routing.

The flagship product in this series, the FirstNet Ready™ Digi WR54, will serve as an example for the purposes of this white paper. Contact Digi to identify the right solution for your needs.

The cellular router functions as a central communications gateway, using multiple WAN interfaces to maintain an active link to the central traffic management center.

Digi WR54 is well-suited for any application requiring continuous connectivity, field longevity and edge computing. This industrial-class router is designed to provide secure routing and gateway functions across traditional and wireless communications networks, protocols and interfaces. It bridges local private wired or wireless subnets across a public or untrusted network, ensuring message privacy and integrity, using trusted channels with authenticated systems.

The router's advanced capabilities enable mission critical communication through concurrent and independent dual cellular and dual WLAN interfaces. The device is designed and verified to relevant industry standards including the NEMA TS2 temperature rating to ensure reliable, high performance operation in challenging environments. In addition, an embedded Python environment enables quick adaptation to future evolving system requirements.

The Digi WR54 cellular router is supported by Digi Remote Manager (Digi RM), a customized dual output power supply and antenna. Next, we will discuss the features at a high level.

Digi Remote Manager

Digi RM is a cloud-based device management, security and data enablement platform. The data enablement functions permit integration of legacy systems into the communications network. The platform includes various dashboards and reports as well as a data repository, enabling other agency systems to generate comprehensive reports that integrate device and performance data. The Digi RM reports range from daily summaries to detailed time-based charts of individual system metrics such as link uptime, network response and data throughput. The Digi RM API enables transfer of device and performance data to other systems using a restful API and JSON formats.

Digi RM's security feature provides a range of security insights as well as automated configuration management. Once Digi devices are configured, Digi RM acts as a watchdog over the network. It not only monitors for anomalies but also automatically resets configurations back to their prescribed settings in the event of an unauthorized change, to thwart cyber threats.

The device management capabilities enable personnel to perform a range of tasks for efficient and effective operation. For example:

- Proactively keep all devices up to date with the latest security patches, firmware and configurations.
- Set up health metrics to track the state of the system at a high level, and then drill down to assess any issues.
- Set up alerts to inform system administrators or other connected systems of any warning or alarm conditions.
- Manage remediation automatically, if any router falls out of compliance for any reason.

Power supply

The industrial-grade power supply unit (PSU) supports both the Digi WR54 router and a POE switch in its default configuration. Its modular design is expandable up to five different voltage outputs. The PSU is rated for industrial environments and customized for the unique application requirements, as highlighted:

- Dual 24 VDC and 56 VDC isolated outputs (expandable to five outputs)
- Agency safety approvals
- Operates at low line voltage and across line sags
- Fanless operation for added reliability
- Operates across NEMA TS2 temperature range
- Conformal coating
- Power-over-Ethernet (POE) electrical isolation ratings
- Monitoring and control using PMBus standard
- Auxiliary 12 VDC output for accessories

Antenna

The antenna is actually multiple antenna elements housed within a single radome. Each element is tuned to transmit and receive in the appropriate frequency bands:

- Cellular: 698-960 MHz and 1710-2700 MHz
- Wi-Fi: 2.4-2.5 GHz and 4.9-5.9 GHz
- Bluetooth: 2.4-2.5 GHz
- GNSS: 1565-1608 MHz (receive only)

The radome is constructed of water resistant, UV stable, impact resistant, fiberglass-reinforced composite. Cable egress is through the bottom plate, where VHB adhesive and a threaded mount make for a vandal-resistant installation.

System features

The following sections highlight some of the key traffic management features built into the Digi WR54 and Digi RM.

VPN failover and fallback

The least cost-active link carries the IPsec VPN, which is typically fiber, if available at the site. The IPsec VPN moves to other active links within a couple of seconds if its current link fails or is not sustaining a sufficient level of service quality. It will then fall back when the lower cost link becomes available and stable.

A low-level WAN probe function provides end-to-end confirmation of link performance and availability. The probe is an ICMP echo request packet transmitted to a TMC server that returns an ICMP echo response packet. The response arrival confirms the link is up while the response timing indicates the speed and therefore performance of the link.

The VPN has a dedicated probe function as well. Like the WAN probe, it confirms VPN performance and availability. The system will automatically move the VPN to a higher-cost link if the performance drops below a threshold.

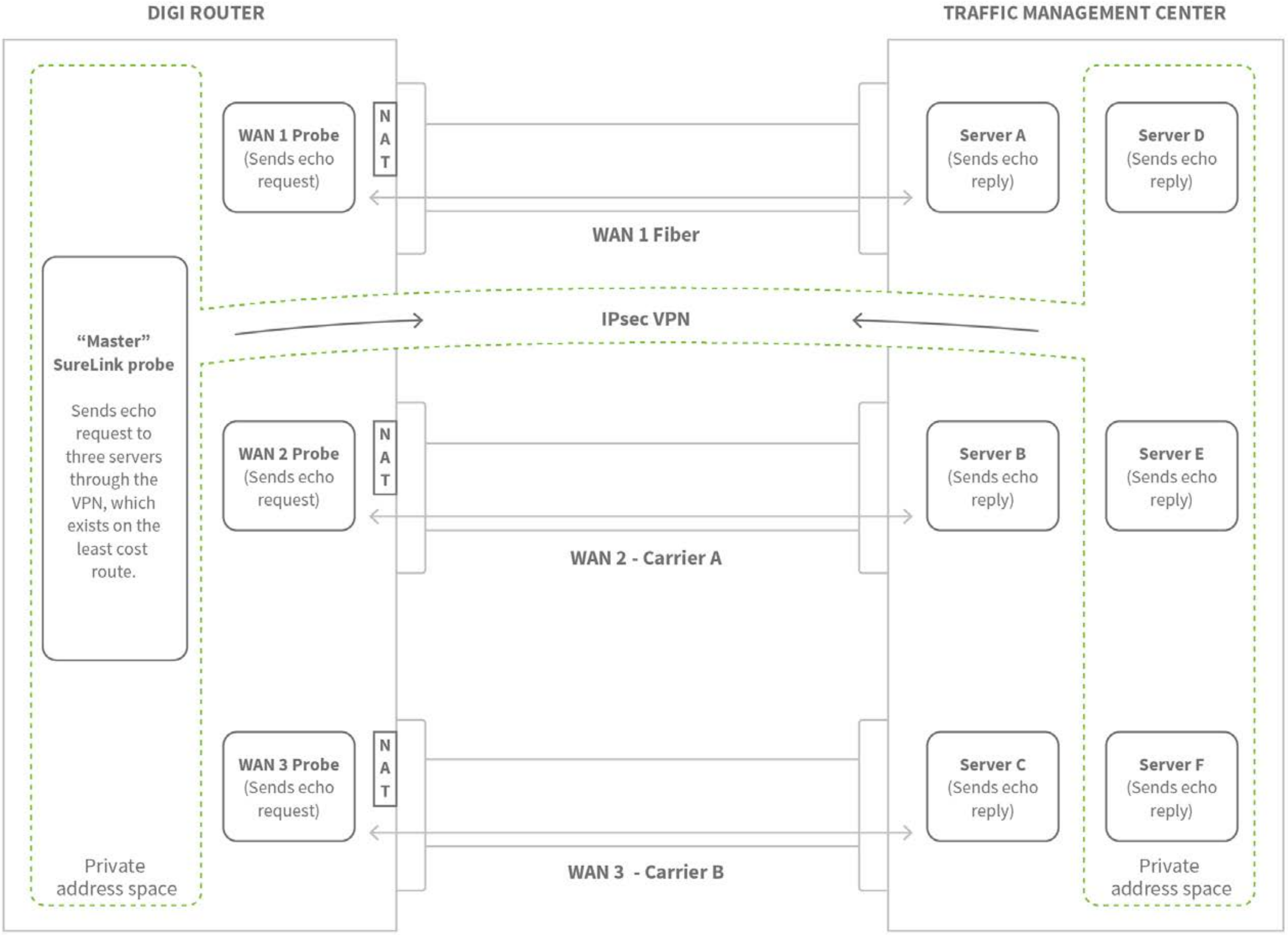

DIGI ROUTER
TRAFFIC MANAGEMENT CENTER
WAN 1 Probe (Sends echo request)
NAT
Server A (Sends echo reply)
Server D (Sends echo reply)
WAN 1 Fiber
"Master" SureLink probe
Sends echo request to three servers through the VPN, which exists on the least cost route.
IPsec VPN
WAN 2 Probe (Sends echo request)
NAT
Server B (Sends echo reply)
Server E (Sends echo reply)
WAN 2 - Carrier A
WAN 3 Probe (Sends echo request)
NAT
Server C (Sends echo reply)
Server F (Sends echo reply)
WAN 3 - Carrier B
Private address space
Private address space

Figure 3: VPN Failover and Fallback

Cybersecurity

The high-level functions in the Digi router, such as bridging, management, data transfer and routing, make use of the many built-in protocols and cryptography to support message integrity, authentication and encryption. The security functions can be grouped into three categories:

- Encryption of packets prevents snooping and tampering by an unauthorized source.
- Message integrity ensures that a packet has not been tampered with in transit.
- Authentication verifies that the message is from a valid source.

A typical secure configuration includes an IPsec VPN tunnel established between the router and the application server. This is best accomplished using AES-256 encryption, Diffie-Hellman IKEv2 key agreement and RSA/PKI authentication.

Up to 32 such tunnels can be established, enabling individual onboard subsystems to maintain isolated and secure communications with their associated servers. Also IKEv2 enables establishment of multiple subnets within a single tunnel, reducing the overhead of multiple VPN tunnels. The following diagram shows a typical system.

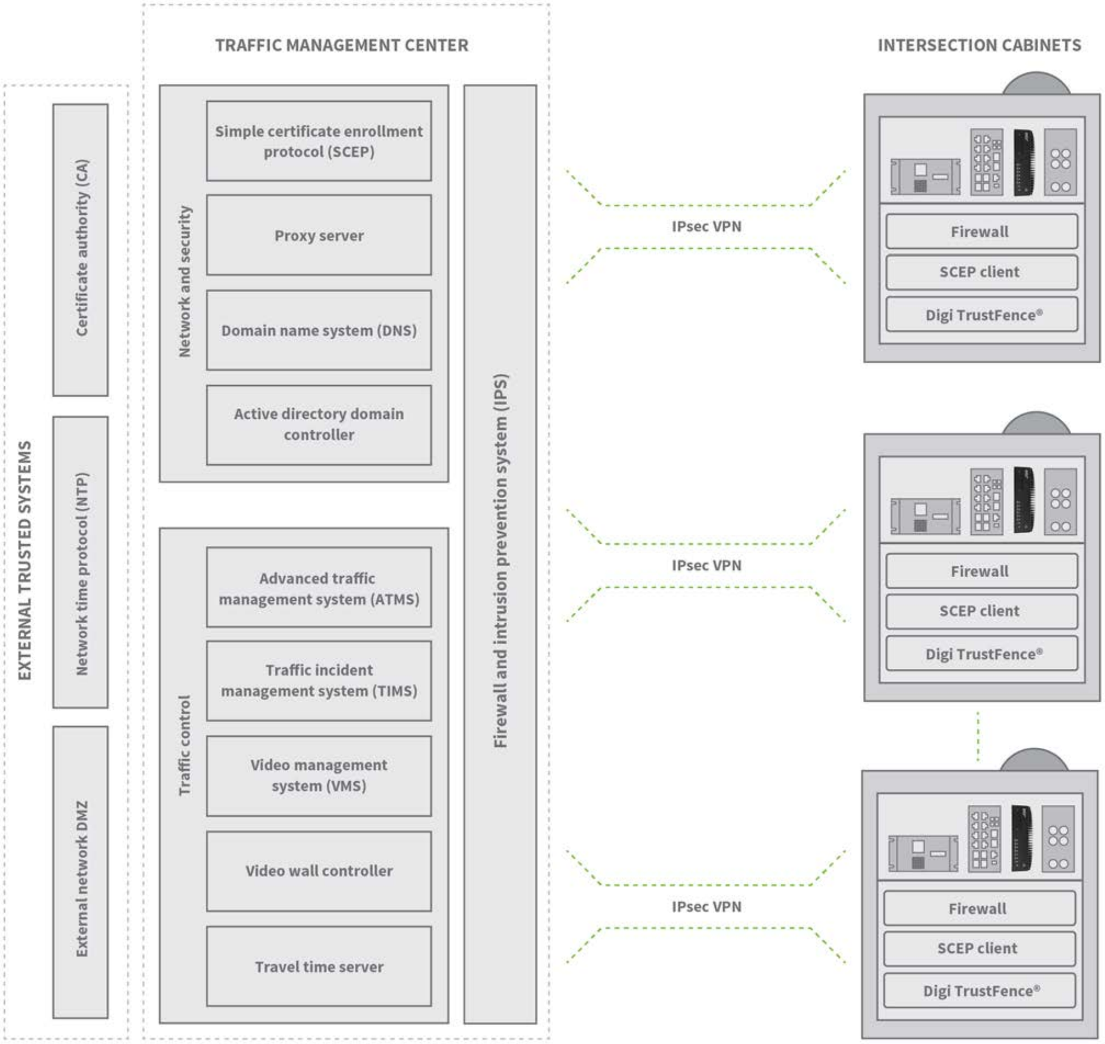

TRAFFIC MANAGEMENT CENTER
INTERSECTION CABINETS
EXTERNAL TRUSTED SYSTEMS
Certificate authority (CA)
Network time protocol (NTP)
External network DMZ
Network and security
Simple certificate enrollment protocol (SCEP)
Proxy server
Domain name system (DNS)
Active directory domain controller
Traffic control
Advanced traffic management system (ATMS)
Traffic incident management system (TIMS)
Video management system (VMS)
Video wall controller
Travel time server
Firewall and intrusion prevention system (IPS)
IPsec VPN
IPsec VPN
IPsec VPN
Firewall
SCEP client
Digi TrustFence®
Firewall
SCEP client
Digi TrustFence®
Firewall
SCEP client
Digi TrustFence®

Figure 4: IPsec and PKI Aided by SCEP

Firewall

The stateful firewall keeps track of the state of network connections traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected. All rejected packets increment an easily viewed counter and are logged for analysis purposes.

Automated PKI

The Simple Certificate Enrollment Protocol (SCEP) automates and simplifies the process of Public Key Infrastructure (PKI) certificate management. The Digi WR54 SCEP client requests and retrieves a certificate over HTTP directly from the SCEP server. The SCEP server manages the signing of Certificate Signing Requests (CSRs), provides Certificate Revocation Lists (CRLs), and distributes valid certificates from a Certificate Authority (CA).

Digi TrustFence

Digi cellular routers include Digi TrustFence®, a suite of hardware and firmware features that protect the device from tampering and ensure the reliability and integrity of its security functions. It uses a cryptographic co-processor to protect particularly sensitive data such as stored passwords and encryption keys so that they are not accessible, even by an administrator. It also includes mechanisms so that the router itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes.

Prioritized traffic

Should there be a need to prioritize the signal controller data over camera video, the best way to accomplish this is using the IETF standard for Differentiated Services (RFC 2474). Critical traffic is given priority over other traffic. The method involves the setting of importance in the IP header, specifically the 6-bit differentiated services code point (DSCP) value. Then controller traffic will always have the lowest latency and highest priority over camera video, for example. This method is universal, so the IP packet is given priority throughout its journey beyond the cellular network to routers/switches in the private or public networks, as the case may be.

Fast, automatic configuration

Digi RM automates device configuration management to gain efficiencies and to ensure consistency across fielded devices with similar functionality. An administrator can establish reference configuration profiles in Digi RM and associate them with device groups and/or individual devices. When a device first comes online, or when scanned according to a schedule, its configuration is checked against the associated reference. A difference is considered a compliance deviation, which generates an alarm and/or triggers an automatic update to remedy. System administrators make that choice in Digi RM settings, and they can be modified anytime.

The system also provides automated configuration of replaced devices. Digi RM is made aware of the replacement by a shift of an established Digi RM Device Name to a different physical device. For example, if an installed Digi router has a Digi RM device name of Site 1234, and the device named Site 1234 is shifted to a different Digi router within a swap move, Digi RM will update the new Digi router with the exact configuration of the original device.

Often fielded devices have site-unique settings. This is also managed within Digi RM by identification of those specific parameters and uploading the actual values, indexed by device name in Digi Remote Manager.

> Digi RM automates device configuration management to gain efficiencies and to ensure consistency across fielded devices with similar functionality.

Digi support teams can provide installation and programming support to assist with every aspect of the system setup.

System performance

The assessment of system performance typically includes three measurements: availability, network response and capacity. Availability is presented as a percentage of time in which the network is able to transmit and receive data. Network response is presented as a latency value, indicating the amount of time required for a data packet to traverse the network as a round trip time (RTT). And capacity is presented as peak throughput: the maximum rate of transmitted and received data.

The Digi router has automated the measurement of availability and network response, using the WAN and VPN probes described earlier. The router records the arrival and round trip time (RTT) of each probe, then uploads to Digi Remote Manager for dashboard presentation and reporting.

A measurement of peak throughput (aka “speed test”) is a good diagnostic tool for isolating network performance problems. Multiple peak throughput measurements gathered at regular intervals is a method to characterize network performance over a period of time, perhaps to confirm if network infrastructure upgrades are effective.

The throughput measurement system makes use of iPerf, a well-established industry method for network throughput measurement. The Digi router runs iPerf Server, which enables it to be ready to accept a request to initiate a throughput test on any interface including the VPN. A TMC server running an iPerf multi-client instance would initiate a throughput measurement with any fielded router.

It is of course desirable to obtain an accurate measure of peak throughput. However, this comes at a cost, as the only way to measure peak throughput is to transmit a relatively large block of data in each direction. Accuracy improves with larger block sizes, longer transmit durations and when the system is relatively idle (for example, when it is not transmitting other data such as a camera video feed). The right balance of accuracy vs. cost is a choice for operations and is adjustable over time. A longer transmission time improves the accuracy of the measurement, but increases data use and possibly usage fees.

Cloud-hosted management

Digi Remote Manager is hosted in Amazon Web Services (AWS) Virtual Private Cloud (VPC). All communications between the router and Digi RM are protected using TLS v1.3. No traffic system communications are routed to AWS, only system performance and configuration data. Traffic operations personnel access Digi RM using secure HTTPS. Optionally, a VPN connection can be established between AWS and the Traffic Management Center for an extra layer of security.

Should there be a loss of connection to AWS, the traffic system continues to operate normally. Management of routers is less efficient under these circumstances, but can be preserved using traditional SSH and HTTPS from the Traffic Management Center.

Digi RM includes a range of dashboards and reports as well as a data repository, enabling other systems to generate comprehensive reports that integrate device and performance data. The Digi RM reports range from daily summaries to detailed time-based charts of individual system metrics such as link uptime, network response and data throughput. The Digi RM API enables transfer of device and performance data to other systems using a restful API and JSON formats. Such systems are often located in AWS as well. For example, these include things like service delivery and business intelligence applications.

Digi teams consult closely with each municipal entity as they identify the right setup for their needs and prepare to deploy. You can start the conversation from our Contact Us page on Digi.com.

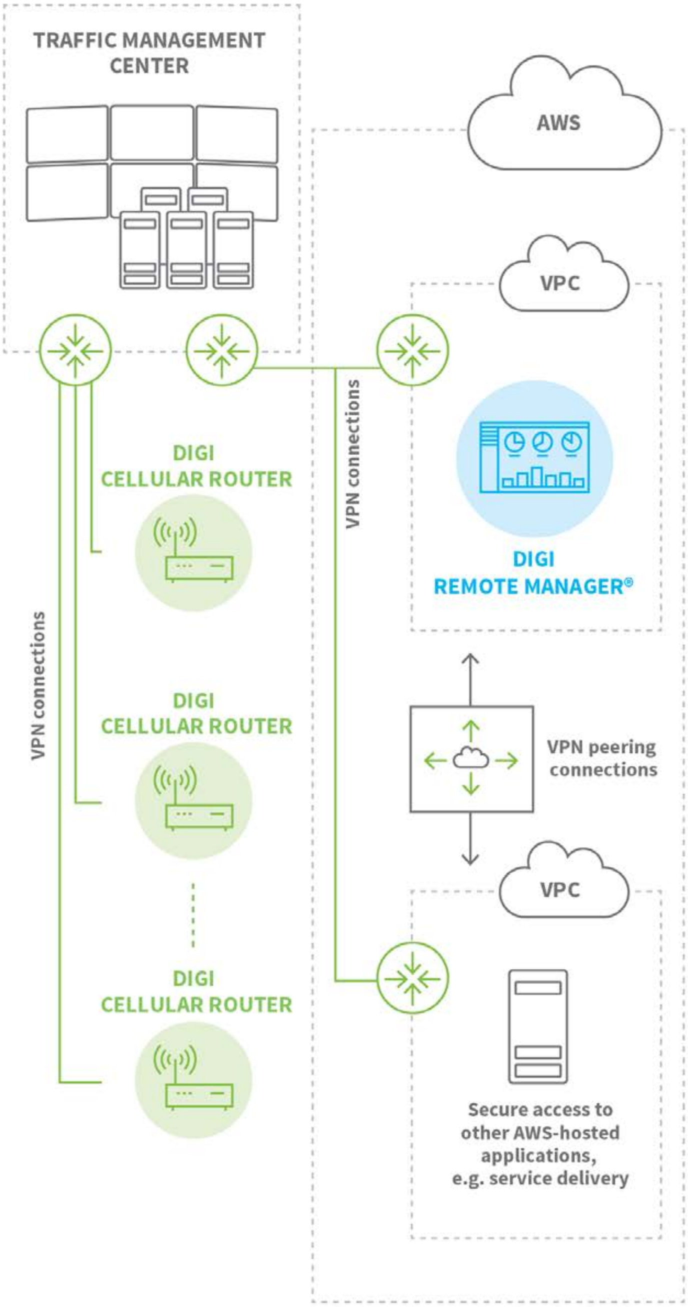


Figure 5: Digi Remote Manager cloud architecture

Why Digi?

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission-critical communications equipment to professional services to get your application designed, installed, tested and functioning securely, reliably and at peak performance.

Digi builds its products for high reliability, high performance, and versatility so customers can expect extended service life, quickly adapt to evolving system requirements and adopt future technologies as they emerge. Digi cellular routers, servers, adapters and gateways support the latest applications in traffic, transit, energy and smart cities.

Our solutions enable connectivity to standards-based and proprietary equipment, devices and sensors, and ensure reliable communications over virtually every form of wireless or wired systems. An integrated remote management platform helps accelerate deployment and provide optimal security using highly efficient network operations for mission critical functions such as mass configuration and firmware updates, including system-wide monitoring with dashboards, alarms and performance metrics.

Company Background

- Digi is publicly traded on the NASDAQ stock exchange, symbol DGII
- Founded in 1985, Digi has 30+ years of experience connecting the “things” in the “Internet of Things” — devices, vehicles, equipment and assets
- Headquartered in the Twin Cities of Minnesota, Digi employs over 550 people worldwide
- The business has been profitable for 15 consecutive years
- Digi’s annual revenue is around $250 million
- The company has 285 patents issued and pending (150 issued)
- In our three decades in business, we have connected over 100 million devices

As a communications equipment manufacturer, Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that’s relentlessly reliable, secure, scalable, managed — and always comes through when you need it most. That’s Digi.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international @DigiDotCom /digi-international

While every reasonable effort has been made to ensure that this information is accurate, complete, and up-to-date, all information is provided “AS IS” without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.