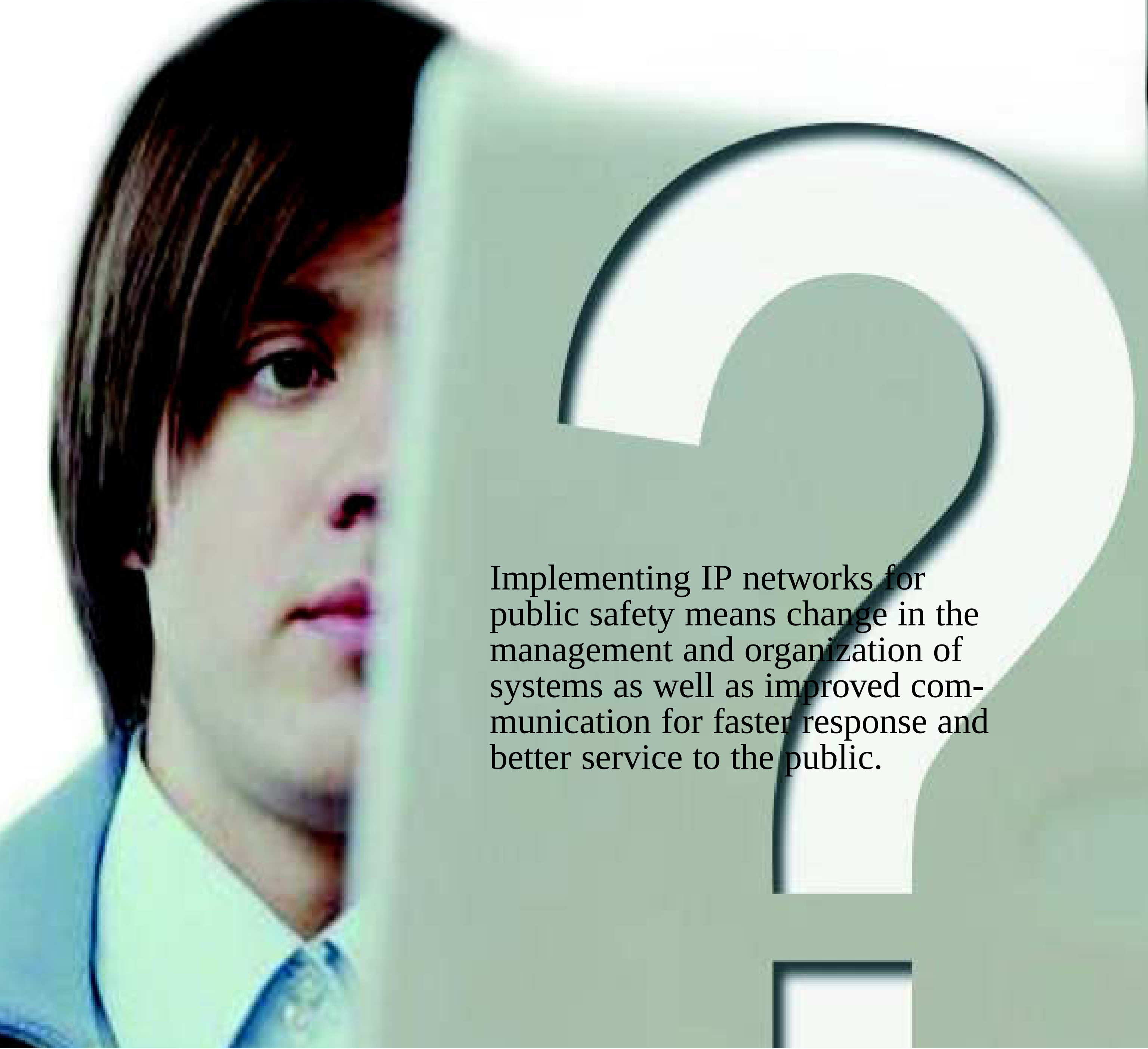
WHAT YOU NEED TO KNOW ABOUT INTERNET PROTOCOL NETWORKING AND SECURITY

By Pierre Olivier, Chief Architect, CML Emergency Services



Implementing IP networks for public safety means change in the management and organization of systems as well as improved communication for faster response and better service to the public.

If there is a protocol that has had its share of attention lately, it is the ubiquitous Internet Protocol (IP). Offered as an integrated solution for data, voice, video and a wide range of multimedia applications, it seems as if all networking and transmission needs can be met by employing the mighty IP.

In fact, large enterprises, banks and the military are deploying reliable, secure IP networks with great benefit. Meanwhile, public safety organizations largely still rely on telephony and point-to-point data exchange circuits. As a result, public safety has lagged behind business when it comes to receiving, sharing and exchanging information.

The first step in moving into the IP era is to understand IP. What makes it so versatile? How is it deployed in local and global networks? From a public safety point of view, is it secure and reliable?

What Is the Internet Protocol?

At the most elementary level, IP is a networking protocol that allows datagrams (blocks or packets of data) to be sent from one computer to another. The origins of IP can be traced to the Department of Defense's ARPAnet (Advanced Research Projects Agency Network) in the late sixties. The intent of ARPAnet was to design a computer system that would be failure-resilient. To achieve this, the scientists opted for a distributed network of computers, interconnected through a packet-based network.

ARPAnet went live in October, 1969, with host computers in UCLA and Stanford. Eventually, ARPAnet was turned over to the public domain and became what we know as the Internet today—a global network of computers interconnected using IP.

As the use of public and private networks expanded, the underlying protocols progressively were refined. In 1981, what we now know as IP—or IP version 4 (IPv4)—was codified in RFC 791. It was specified later, in 1983, as DoD MIL-STD-1777.

Within the construct of IP, each computer is assigned an address. An IPv4 address is defined as being composed of four eight-bit octets (i.e., "192.168.1.1"). Thus, IPv4 theoretically supports four billion individual addresses.

With proper planning, a reliable, secure, highly available IP network is an easily achievable goal.

Despite this large number of addresses, address exhaustion fast is becoming a reality, much like numbering plan area (NPA) exhaustion. This fact alone is a testament to the popularity of IP.

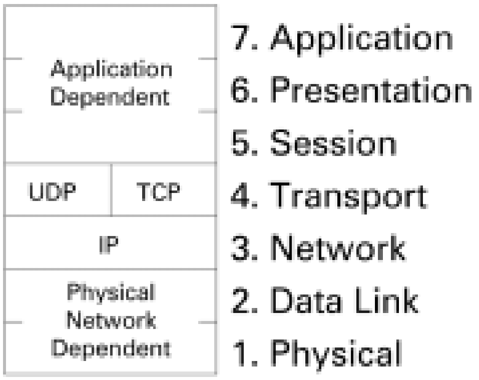
Today, IP version 6 (IPv6) is replacing the thirty-two–bit address of IPv4 with a 128-bit address, or a theoretical 340 undecillion (340 followed by 36 zeros!) addresses. The transition to IPv6 is a complex exercise that has started only recently. Let it suffice to say that it will take years to complete.

IP in the Network

The Open Systems Interconnection (OSI) model defines a communication platform as consisting of seven layers (see **Figure 1**). IP is a network protocol, occupying and operating in layer 3. At this level, IP is independent of the hardware and data links on a network. It's important to understand this basic fact, because it affects where issues such as security and reliability come into play.

The most common transport (layer 4) protocols using IP are the transport communication protocol (TCP)—a connection-oriented protocol—and the universal datagram protocol (UDP)—a connectionless protocol. IP also uses one of many different data link (layer 2) protocols that interface in turn through various physical (layer 1) links to deliver information.

Figure 1 IP in the OSI model.



Figures 1 and 2 courtesy of CML Emergency Services.

Types of Networks

The simplicity of IP and the versatility of its accompanying transport protocols, TCP and UDP, have made IP a logical choice for bridging heterogeneous networks (i.e., networks made up of different types of computers, switches and routers), as well as wide-area networks (WAN). That's one of the primary reasons IP has been adopted wholeheartedly by the business community.

In a public safety environment, IP makes it possible to replace the multitude of individual circuits that now exist with one infrastructure, linking different public safety organizations at the federal, state and local levels. It also facilitates access to 9-1-1 from the public using e-mail, computers and other devices.

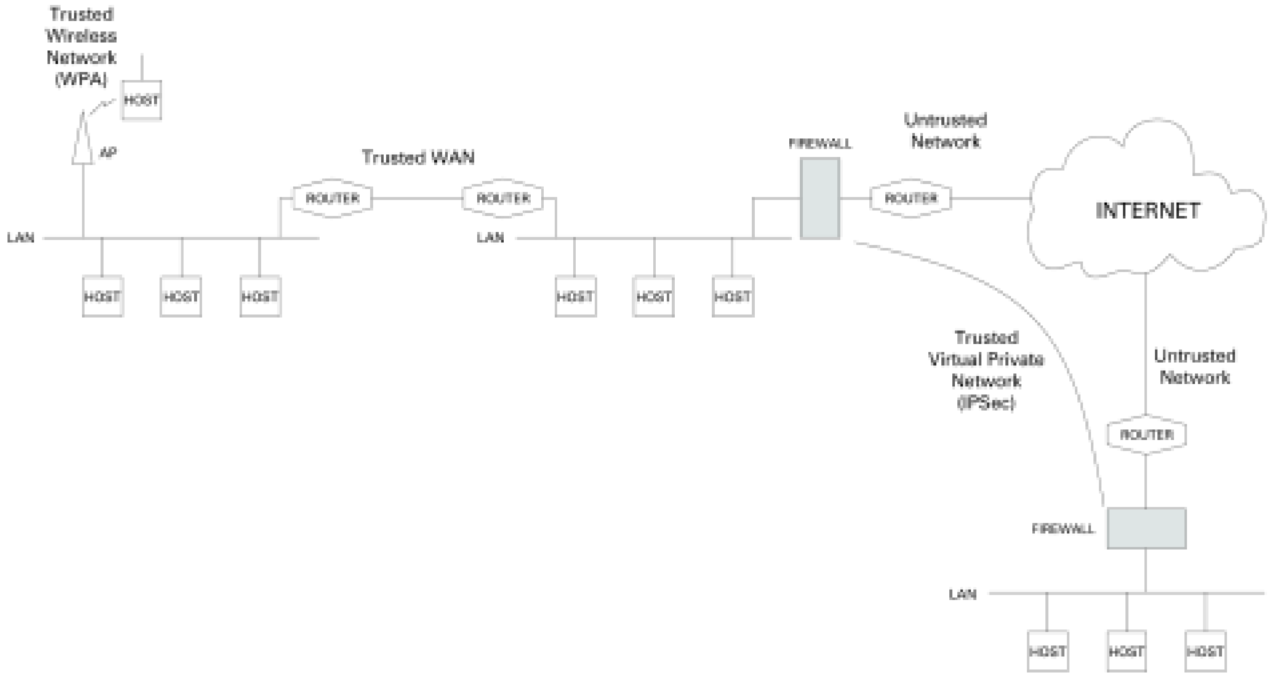
As illustrated in **Figure 2** (**page 38**), typically there are three kinds of WANs:

1. Leased-line WANs are networks in which only the physical layer is shared. For instance, point-to-point protocol (PPP) running over a leased T1 facility spanning two buildings would constitute a leased-line WAN.

2. Layer 2 virtual private network (VPN) WANs are networks in which layer 2 and below use a shared infrastructure. For instance, frame relay and automated teller machine (ATM) networks are layer 2 VPNs.

3. Internet-based VPN WANs are built on a shared IP network: the Internet.

Figure 2
The global IP network.



When using IP over a WAN for public safety, it also is important to know whether the network is *trusted* or *untrusted*.

• Trusted networks are networks in which all access points are controlled. Local area networks (LANs) usually are considered to be trusted networks.

• Untrusted networks are networks in which not all access points are controlled. The Internet is an untrusted network.

Leased-line WANs and layer 2 VPNs usually are considered trusted networks; Internet-based VPNs, on the other hand, operate on an untrusted network, and therefore must have special features to handle security. This is accomplished through IP Security (IPSec). IPSec uses data encryption standard (DES) or 3DES encryption to secure the data transmission. The resulting *tunnel* can be considered trusted.

Wireless networks pose an interesting challenge because they usually are intended to be extensions to the LAN (the trusted network) and yet, by their very definition, are untrusted (i.e., physical access cannot be controlled). Again, special security precautions apply to wireless networks. Much like Internet-based VPNs, wireless networks use encryption. The latest standard is Wi-Fi Protected Access (WPA).

Security Threats

A public safety network should employ trusted technologies right from the very start. Even so, security is one of the biggest concerns that public safety officials have when the subject of IP comes up.

There are two main types of security threats to a network:

1. The risk that an unauthorized user may acquire confidential information
2. The risk that the network infrastructure itself will be put in jeopardy

Although security is a concern not to be overlooked, the widespread deployment of IP networks also has seen a comparable development in network security measures. First and foremost, the best policy is to have a policy!

Here are simple measures that have proven over time to be reliable and effective.

If for public safety networks, the question is no longer whether IP should be embraced, but rather when, the key question is not Can you build a reliable IP network? but How do you build a reliable IP network?

At the individual system level:

- Use operating systems that are developed for use in an enterprise environment, not personal or home versions.
- Keep operating systems up to date. Most vendors issue regular patches; many of those patches are intended to reduce security risks.
- Run antivirus software on every system and keep the software up to date.
- Implement password access on every host system.

At the LAN level:

- Ensure access to servers, switches, routers, etc. is physically secure.
- Keep the operating systems in all servers, switches and routers up to date.
- Run up to date antivirus software on each server.
- Monitor the network. If the network is designed properly, it will recover from minor failures without a noticeable difference in service to the end-user. Ensure that the system administrators are aware and notified of all problems and noticeable changes in network operation.

At the trusted WAN level:

- Ensure access to data lines is physically secure.
- If the WAN is mission-critical, diversify the infrastructure (routers and data circuits). Ensure it is diversified all the way through the circuit provider network.
- Make sure the remote end of the circuit is trusted as well. If the remote user(s) involved do(es) not apply adequate and equivalent policies, the WAN should not be trusted and should be augmented with firewalls.

At the Internet-based VPN level:

- Do not depend on an Internet-based VPN for mission-critical operations.
- As for trusted WANs, make sure the remote end of the virtual circuit is trusted as well.

At the untrusted network level:

- Implement and maintain a firewall on the circuit.
- Install mail servers, web servers, domain name servers, etc. on an isolated perimeter network, not on the trusted network.
- Monitor the firewall. Intrusion attempts, even when successfully blocked, should be acted upon.

Public Safety Implications

In a recent address to a CML forum held in North Carolina, NENA President Richard Taylor remarked, "In the recent FCC initiative, it was stated that wireless 9-1-1 is over with. It's just a matter of putting the pieces into place." Also, Taylor pointed out that IP is the next wave, and, in his opinion, it's going to be a big one. "As 9-1-1 leaders, we have to embrace this change," he stated.

Calls from Internet communication provider networks will need to be handled sooner rather than later. 9-1-1 e-mail will become a reality as well. IP already is used to exchange information between the MPC and the ALI database and is a logical candidate for delivering ALI to the PSAP as well. Furthermore, the ability to pass multimedia information (audio, video, data) in the same channel makes it a technology of choice for networking PSAPs together.

If, for public safety networks, the question is no longer whether IP should be embraced, but rather when, the key question is not "Can you build a reliable IP network?" but "How do you build a reliable IP network?"

The answer is clear. If an IP network is going to be mission-critical, it must be designed with redundancy, security, scalability and reliability in mind. Remember that IP was designed in collaboration with the Department of Defense as a military networking protocol and, even today, IP is a key component of the DoD’s operational networks—survivability was a requirement from the outset.

With proper planning, a reliable, secure, highly available IP network is an easily achievable goal. Here are some pointers to keep in mind as you ponder how to proceed with building your IP strategy:

- Consult an expert. Designing the appropriate IP network for your public safety operation and its future growth is a science, not an art.
- The same principles that apply to voice trunks and call-taking equipment (diversity, redundancy) apply to data circuits and networking equipment.
- Residential, small and home office (SOHO) equipment was designed for and is intended to be implemented in residences and home offices. Use enterprise-level systems.
- Design your IP network for security.
- Implement policies, and perform audits.
- Deploy in phases. Don’t try to turn up everything and everybody on day one.

Conclusion

IP is a universal, adaptable protocol. In conjunction with the global networking technologies available today, it enables seamless local and remote service deployment.

IP networks have been designed to be extremely reliable and trustworthy. Security threats are a reality; however, they are mitigated with proper network design and administration. The techniques discussed are available, effective and widely deployed.

Implementing IP networks for public safety will mean change in how systems are managed and organized; but it also means improved communication for faster response and, ultimately, better service to the public you serve.

Pierre Olivier has been involved in public safety product design at CML Emergency Services (Westchester, IL) for twelve years. He can be reached at polivier@cmles.com.