WHITE PAPER

Toward Next-Generation Access Networking Technologies in Industrial/Enterprise Internet of Things

Sponsored by: Peplink

Bill Rojas
October 2015

IN THIS WHITE PAPER

Next-generation access networking for the Internet of Things (IoT) will need to provide cost-effective, high-reliability, secure edge/access networking communications in combination with cloud computing for industrial/enterprise applications. In this IDC White Paper, we discuss a new set of access networking technologies that is entering the market at significantly lower price points than previously available and provides higher uptime and lower total cost of ownership (TCO). The paper also investigates how these new access networking technologies will play an important role in realizing a wide range of IoT industrial/enterprise applications through the utilization of cellular/wireline bandwidth aggregation via multiple broadband and Long Term Evolution (LTE) links to realize multi-link WAN bonding, VPN bonding, and WAN smoothing.

SITUATION OVERVIEW

IoT Vision and Ecosystem

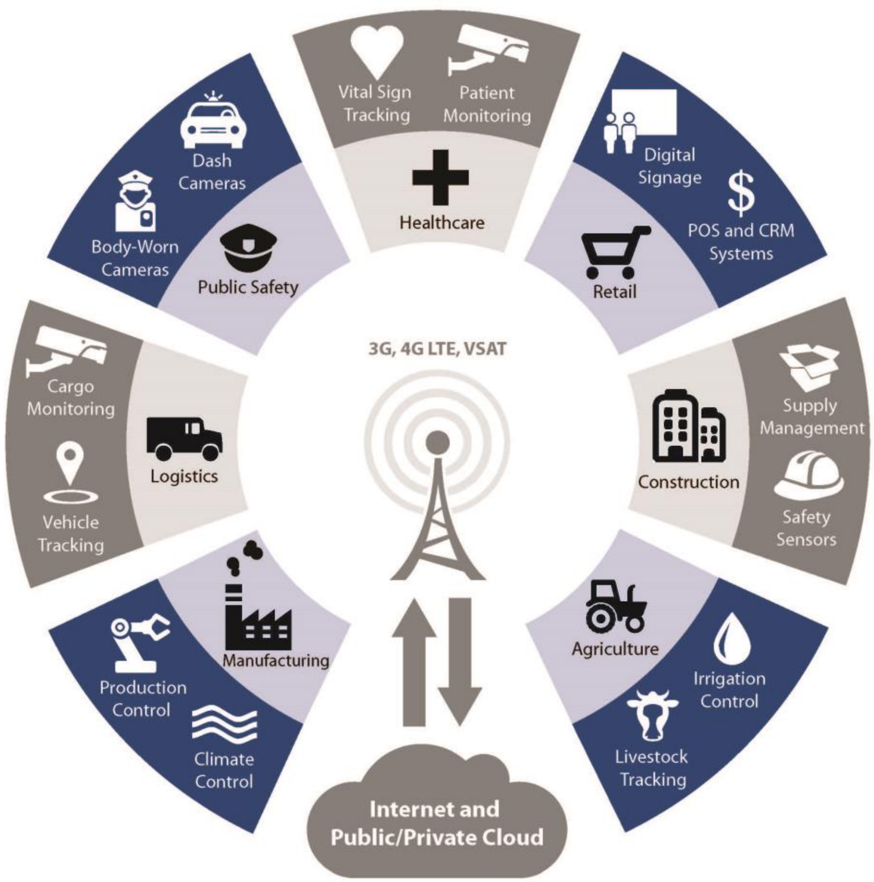
IDC defines the Internet of Things as a network of networks of uniquely identifiable endpoints (or "things") that communicate without human interaction using IP connectivity — whether locally or globally.

- The IoT brings meaning to the concept of ubiquitous connectivity for businesses, governments, and consumers with its innate management, monitoring, and analytics of traditionally unconnected "things".
- With uniquely identifiable endpoints integrated throughout enterprise networks, providing operational, environmental, and location intelligence, an IoT system is managed and monitored by an intelligent or traditional embedded system that acts as a gateway between local sensors/actuators and an IP network that is connected to the Internet and made part of a wider IoT solution that collects and acts upon the collated data from the endpoints. The result is that IoT can provide real-time and historic data-enabled strategic and tactical advantages for businesses, governments, and consumers.
- IoT is composed of technology-based connected solutions that allow businesses and governments to gain insights that help transform how they engage with customers, deliver products/services, and run operations.

Industrial IoT is the Internet of Things applied in industrial/enterprise use cases such as manufacturing and operational resources, retail distribution, public sector, and healthcare industries, energy and minerals including oil and gas, and mining. Thus, IoT is a pervasive vision (see Figure 1) for the ICT-based society that will impact virtually all vertical sectors and industries including local/state/national government and citizen services, public and utilities infrastructure, manufacturing operations, transportation and logistics, healthcare, education, and consumer services. IoT solutions will typically deploy multiple ICT technologies and use vertical-specific software to implement an intelligent automated system that collects data from remote sensors and stores it centrally. The data is then processed with analytics software using business logic rule-sets which then make decisions that could include sending instructions downstream to actuators in machines and instruments, or to operational resources such as business unit managers and field engineers.

FIGURE 1

IoT Vision



Source: IDC and Peplink, 2015

Drivers of Growth in Industrial IoT

The drivers of IoT adoption include:

- The need to drive operational efficiencies, including reducing machine downtime and maximizing throughput, in manufacturing.
- Specific demographic trends in verticals such as healthcare where IoT could provide many benefits in both clinical and nursing home care as well as remote healthcare.
- The emergence and widespread proliferation of 4G LTE network coverage is enabling new market opportunities/services/applications that will be able to take advantage of LTE's high-bandwidth and low-latency connectivity. The ability to resolve dead spots via multi-mobile network operator (MNO) LTE links will enhance coverage and service quality.
- Changing enterprise customer behavior — in which customers want the assurance of the service of the equipment, but do not want to own the equipment and the associated maintenance and service commitments. IDC estimates that just the process manufacturing, discrete manufacturing, upstream energy production, and resource industries will already account for 40% of IoT spend in Asia/Pacific excluding Japan (APEJ) in 2020.
- The continuous improvements in availability of broadband, fixed and wireless coverage even in remote areas where key energy and resources, and agriculture production take place.
- Government initiatives as governments come to believe the strategic importance of industrial IoT and their willingness to assist enterprises and industry in funding the necessary infrastructure for smart grid, online learning, smart city services, and environmental and resources monitoring and management. Governments in South Korea, China, Taiwan, Australia, Malaysia, New Zealand, and India are also taking steps to improve 4G wireless broadband coverage and optical fiber access in smaller cities and towns to ensure that broadband, fixed line, and/or cellular cover all the population including strategic rural areas.

Inhibitors of Growth in Industrial IoT

The key inhibitors to growth in industrial IoT will be:

- Lack of an IoT vision for the business or organization that enables a complete revamp of the process used at all levels of the company.
- Lack of understanding about the CAPEX and OPEX implications.
- Cost of retrofitting equipment and tools in the factory setting.
- Cost of installing sensors, actuators, and other devices in the field.
- Lack of standards and propensity of large organizations to custom build their own solutions.
- Lack of and high costs of telecom broadband and 3G/4G wireless connectivity in some Asia/Pacific markets as well as lack of coverage in remote areas in both developed and emerging markets where much of the logistics, upstream energy transport, and long-distance electricity transmission take place.
- High operational costs of managing a much higher density of network connected devices and associated infrastructure to support multiple IoT sensor networks across an enterprise WAN.

IoT in Asia/Pacific — A Promising Outlook

IoT in the Asia/Pacific region has tremendous potential due to the breadth and depth of its industries coupled with government support for broadband fixed and wireless connectivity and coverage. For example, in Hong Kong, mobile operators such as SmarTone have installed 3G/4G towers to face the seashore along the container shipping areas so that ships can utilize offshore/nearshore 4G to upload data which in the past could only be done with very small aperture satellite (VSAT). In Australia, the government is providing co-funding in collaboration with two operators, Vodafone and Telstra, to install or upgrade 500 new cell sites in remote locations around Australia. The purpose of the A$365 million initiative is to provide coverage in over 5,700 km of black out routes for truckers and to cover an additional 68,000 sq km of rural areas including mining sites. In New Zealand, the government is working with Chorus and Vodafone to provide 3G/4G cell sites under the Rural Broadband Initiative. With the million plus 4G LTE cell sites that are being deployed by China's three telecom providers, machine to machine (M2M)/IoT developers in China will not find coverage to be a major obstacle in much of the Tier 1-3 cities. Moreover, fixed line broadband connectivity is available in most of China's factory zones today, which means that cloud-based, low-latency IoT processes can be implemented much more easily.

Access Networking for Industrial IoT

A number of network equipment providers (NEPs) are developing various WAN optimization solutions to provide alternatives to legacy multiprotocol label switching (MPLS)-based WANs. However, a newer trend is to try to provide enterprise-class security and connectivity over existing private-WAN MPLS, xDSL, fiber optic FTTx, and 3G/4G cellular connections that will enable the construction of lower cost multi-WAN VPN backbones that can replace or supplement the more expensive MPLS network technologies; oftentimes enterprises will use commodity links alongside MPLS in order to offload bulk traffic and minimize the cost of bandwidth expansion. In order to realize the aforementioned vision, early NEP participants are deploying a portfolio of technologies including Layer 2 interception, sub-second path decisions, and congestion detection via deep packet inspection, hot failover, cellular bandwidth aggregation or bonding, caching, dynamic load balancing, and multi-path bandwidth smoothing.

Figure 2 provides the networking ecosystem view from the perspective of industrial IoT deployments. Semiconductor and sensor companies provide a wide range of processing, semiconductor memory, radio and Ethernet modems, and microelectronic sensors that are used to construct generalized and vertical/use case specific modules that are installed in various systems and structures including automobiles and trucks, IP CCTV cameras, homes (e.g., healthcare, smart meters, smart appliances), utilities grids, streetlights, parking meters, ATMs, point of sale (POS) terminals, and so on. Edge routers and edge/access networking are paramount to achieving high reliability, cost-effective scalability as bandwidth increases, and the remote control of networking assets. Core network routers and Ethernet switches provide the connectivity in telecom networks and large enterprises back to the public or private-cloud connected datacenters where servers running vertical applications, analytics, databases, and warehouse software will log, analyze, and issue control instructions to the devices and sensors in the field.

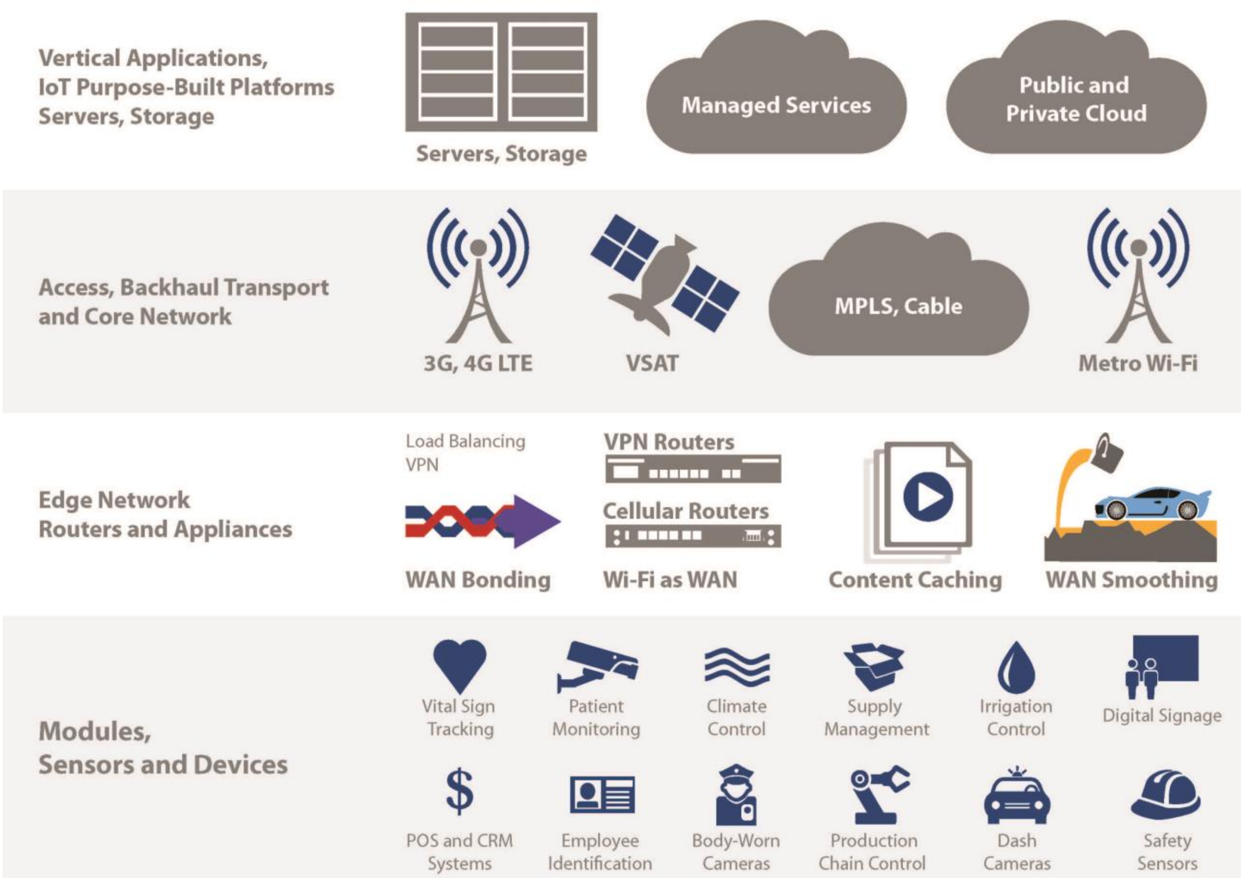
Some of the early entrants in this space include:

- **Cisco Systems:** Multi-WAN VPN router; has been a leading player in WAN optimization solutions.
- **Peplink:** Founded in 2007; products include multi-WAN routers, cellular routers, WAN bonding, bandwidth aggregation, and WAN smoothing.
- **Barracuda Networks** (NYSE: CUDA): Founded in 2003; products include cloud-based networking security, application delivery controller (ADC) and load balancing.

- **Fortinet** (NASDAQ: FTNT): Founded in 2000; products include network security, unified threat management (UTM), and WAN optimization including ADC.
- **Talari Networks:** Founded in 2009; products include software defined WAN (SD-WAN) and adaptive private networking (APN) appliances.
- **Elfiq Networks:** Founded in 2004; products include link balancing and bandwidth management appliances including Layer 7 traffic shaping and deep packet inspection (DPI); multipath routers.
- **Mushroom Networks:** Founded in 2004; products include load balancing appliances, wireless bandwidth aggregation, WAN orchestration, and VoIP/SIP bonding for WAN to cloud.

FIGURE 2

IoT Access Networking Ecosystem



Source: IDC and Peplink, 2015

The key specific technical design goals that IDC has identified as requirements for edge/access networking, wireless, and IoT enterprise/industrial deployments include the following.

Network and Operator Link Path Redundancy

There are multiple reasons for a requirement that takes advantage of the presence of multiple MNOs and Internet service providers (ISPs) including:

- Cost
- Higher uptime
- More bandwidth
- Enhanced coverage including resolving dead spot zones

Wireless Network Diversity

Population coverage of 4G LTE has already surpassed 70-80% by many leading MNOs across Asia/Pacific in Australia (87%), New Zealand (84%), Hong Kong (>95%), Singapore (>95%), China (71%), Taiwan (93%), South Korea (99%), and Japan (>93%). In some of the emerging markets in Asia/Pacific such as Malaysia, LTE penetration is approaching 25-35% of the population to complement 3G coverage that is reaching 80-95% of the population. According to the GSMA, by 2020 the population coverage of LTE globally will reach 64% with roughly 2.5 billion frequency division duplex (FDD)/time division duplex (TDD) LTE connections. LTE spectrum in the sub-gigahertz bands, such as Band 28 700 MHz and Band 850 MHz, and new technical features included in 3GPP Releases 10–13, such as LTE-Advanced (LTE-A), carrier aggregation (CA), and machine type communications (MTC), when combined with the low-priced <US$20 LTE modems from companies such as Sequans, is making LTE increasingly attractive as the access medium for both stationary and medium/high-mobility IoT deployments. When combined with low-power WAN (LPWAN), LTE will be even more powerful as a backhaul for endpoint devices and gateways.

4G LTE cellular bonding and automatic failover are important features that can be used to provide session persistence (OSI Level 4-7) (see Figure 3) even when doing large file transfers, VoIP, and video conferencing/streaming sessions. Use cases abound that would benefit from 4G LTE cellular bonding including law enforcement surveillance, property and assets surveillance, transportation logistics and high-value cargo fleet management, live TV journalism, and other digital media applications.

FIGURE 3

Mobile Bandwidth Aggregation

Source: IDC and Peplink, 2015

Seamless Network Failover and Backup

In the consumer space this would not normally be a requirement but in the enterprise/industrial setting seamless sub-second failover, uninterrupted sessions, and backup are mission critical for many if not most use cases. For example, in the highly volatile environments of oil and gas exploration and production, oil and gas companies go to great lengths to ensure that VSAT backup and failover are put in place in remote locations. However, as the 4G LTE and fiber optic access situation improves in remote areas and coastlines such as Barrow Island in Western Australia, the need for VSAT will still be there but much less so. Other use cases that require seamless network failover, session persistence, and backup include retail POS terminals, telemedicine, and police command and control center vehicles.

WAN Load Balancing and Failover

WAN load balancing and failover can be realized using a single device with multiple WAN links. WAN diversification is a big driver for its use, allowing multiple WAN technologies from multiple providers to be used simultaneously or in an active/standby configuration providing additional bandwidth and also approximating 100% uptime. The ability to do intelligent IP session-based load balancing across multiple physical links requires a fair amount of expertise and know-how which is why IDC considers this a next-generation technology for access networking. WAN failover is a low-cost method of improving remote site availability, particularly between fixed line connectivity and cellular where cellular is used as a standby WAN link. WAN load balancing has been found to be very useful in schools, rural businesses, resort hotels, ferries and luxury yachts, and container ships, just to name a few. WAN failover from fixed line to cellular is an attractive proposition in retail for POS and businesses that are reliant on cloud-based services where any lack of connectivity has an immediate operational impact.

WAN Bonding

WAN bonding is a two-ended technology — similar to the way symmetrical WAN optimization is deployed — that enables the use of multiple WAN connections to augment or replace individual private WAN connections. Those connections can be existing private WANs, such as MPLS, or Internet WAN links, like DSL, cable, and cellular. WAN bonding performs bandwidth aggregation, allowing all links to be used almost all of the time (even by a single IP session), and performs real-time traffic engineering, with sub-second reactions to WAN link failure and congestion. This enables enterprises to build much higher bandwidth WANs for a much lower cost and provides higher levels of resilience due to combination of WAN link diversification and packet level failover that enables traffic from a single active session (such as a VoIP call or a file download) to be rerouted at a packet level when a WAN link fails via an alternative healthy WAN link. This sub-second response on WAN failure providing session persistence has many applications, particularly when real-time services (such as VoIP, radio over IP, and CCTV/video) are required including emergency disaster recovery, mining and gas exploration, ambulances, and police vehicles.

WAN Smoothing

WAN smoothing greatly enhances the operations of use cases in mobile environments where coverage or signal strength varies widely such as emergency response, law enforcement vehicle management and surveillance, radio and TV broadcasting, and news gathering that need VoIP and/or audio/video streaming. WAN smoothing is a feature where the network router/appliance can smooth out traffic flows across multiple VPN-WAN links to mitigate IP packet loss that might occur in VoIP and video conferencing/video streaming. Vendors can do this by deploying proprietary packet loss reconstruction algorithms but will typically need to use more bandwidth than is required for bandwidth aggregation/bonding alone in order to realize connection consistency of time-sensitive traffic.

VPN Security and Bonding

VPN uses encryption to provide data confidentiality by using tunneling protocols such as IPsec, Layer 2 Tunneling Protocol (L2TP), Point to Point Tunneling Protocol (PPTP) and Secure Sockets Layer (SSL) to create a tunnel to encapsulate encrypted payload data. Although the headers can be openly read since they cross the public network, the encrypted data is thus secured and can only be read if the user has the decryption key. In the multi-WAN setting, the ability to keep the VPN tunnel operating even when an ISP link fails is important — this is known as VPN resilience.

With VPN bonding (see Figure 4) it is possible to create a single logical VPN connection across multiple WANs that aggregates bandwidth and allows for packet level failover for a single user session. Rapid VPN failover of 1 second or less would also typically be required in VPN bonding deployments including VoIP services. One of the main attractions of VPN bonding in the edge is to reduce significantly the overall cost of traditional MPLS deployments.

FIGURE 4

VPN Bonding

Source: IDC and Peplink, 2015

Local Content Caching

Local caching of requested Internet resources, where the first request for content is downloaded once over the available WAN link(s) and subsequent requests for the same content is served from local on device storage, reduces both the amount of WAN bandwidth consumed by LAN client activity as well as improving response times for content delivery. This can be very useful in circumstances where WAN bandwidth is both expensive and/or has high latency characteristics (such as when VSAT connectivity is used) and when large numbers of LAN clients are requesting the same content at the same time — reducing WAN link congestion. Content caching has been proven to be very useful in educational settings (where tens of students can be accessing the same online content for a class activity at the same time on multiple devices) as well as in mobile deployments where cellular bandwidth availability can be highly variable as the vehicle moves in and out of provider coverage areas. The amount of caching needed varies with each use case but we are seeing typically 125–250 GB as the starting requirement.

Wi-Fi as WAN Functionality

Wi-Fi clients are of particular importance in manufacturing operations and asset management where factory owners want to transform their legacy machine tools and robots into participants in an IoT network by enabling Wi-Fi connectivity for each machine/robot.

The ability of some multi-WAN capable routers to treat Wi-Fi as an additional WAN link also allows for additional connectivity to be added automatically on demand, with intelligent devices capable of automatic prioritization of the Wi-Fi WAN using a lowest cost routing approach. This can be useful for example, where a multi-WAN cellular router is installed in a vehicle that regularly returns to a fixed location (such as a marina, bus depot, or service station) with Wi-Fi infrastructure in place, as it enables the seamless transition of WAN traffic to the Wi-Fi WAN when in range and then back again to cellular as the vehicle leaves the Wi-Fi coverage area.

Virtualization and Central Management in the Cloud

As more network-based services are deployed in public, private, and hybrid cloud architectures, the demand for completely virtualized core network services is increasing. IDC considers the availability of a virtual WAN bonding appliance a necessity for vendors in this sector for them to achieve penetration into the increasing number of customer infrastructure deployments where the use of virtualized appliances is either mandated or at the very least presented as a strong preference over physical appliances by the company’s management teams.

The ability to offer cloud-based device management, traffic analysis, and cloud-based security management is becoming not "nice to have" but rather "must have" in the implementation of enterprise/industrial IoT solutions, especially as the number of remote devices deployed in the field and the resultant WAN complexity increases. The benefits of cloud-based edge-network device management systems include simplifying configurations, streamlining deployments and firmware upgrades, and facilitating repairs and replacements, which improve operational efficiencies especially for managed service providers.

Use Case Examples

The following section presents several use cases where IDC is aware that next-generation edge/access networking technology is being deployed.

I. Government

Law Enforcement Surveillance and Video Streaming

From time to time, law enforcement would need to conduct ad-hoc undercover video surveillance of target persons and/or assets and property. The command center might be mobile, such as a mobile command vehicle, or fixed in a command center with a centralized server that can be connected via the public Internet or through a private WAN. If the connection needs to be the most secure possible, network appliances would need to be used with strong VPN authentication and payload encryption. In some cases, the law enforcement operations team will select, due to timing and unpredictability of the duration of the surveillance, to use VPN over a public (telecom) network back to the datacenter.

Live video streaming is an increasingly important use case in law enforcement (see Table 1). Cellular bonding, VPN bonding, and local caching are key technical requirements in this class of use cases.

TABLE 1

Government Use Cases — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
LAW ENFORCEMENT SURVEILLANCE	Needed by local, state, and federal law enforcement agencies including homeland security, immigration, and customs
Bandwidth (Mbps)	1-2 Mbps (HD video)
Frequency of uplink	Continuous or activated by remote control
Frequency of downlink	Ad hoc such as camera positioning
Latency (ms)	<100 ms for most LTE networks
Security	Extremely important
Redundancy of links	Extremely important, needs close to 100% availability and to maximize coverage
VPN	3G/4G bonding, multi-WAN
Key sensors	IP CCTV, audio, motion detection, heat
Physical mobility requirements	Stationary, field-based, and in vehicle
Wireless connectivity	3G/4G to WAN (cellular operators), Wi-Fi to client devices, cameras, etc.
Additional applications	Radio over IP, automatic number plate recognition (ANPR), image recognition, language translation
Location-based services	GPS accuracy
Central command architecture	Cloud or mobile command center
POLICE FIELD MONITORING	
Bandwidth (Mbps)	1-2 Mbps (HD video)
Frequency of uplink	Continuous
Frequency of downlink	Frequent: such as email communications, operating instruction documents
Latency (ms)	<100 ms for LTE networks
Security	Extremely important
Redundancy of links	Extremely important, needs close to 100% availability and to maximize coverage
VPN	3G/4G bonding, multi-WAN
Key sensors	On-person video camera, on-vehicle video camera (internal and external views)
Physical mobility requirements	Stationary, field-based, and full mobility
Wireless connectivity	Wi-Fi, 3G/4G
Additional applications	Radio over IP, ANPR, image recognition, language translation
Location-based services	GPS accuracy
Central command architecture	Cloud or mobile command center
DISASTER EMERGENCY RESPONSE	
Bandwidth (Mbps)	1-2 Mbps (HD video)
Frequency of uplink	Continuous
Frequency of downlink	Frequent: such as email communications, operating instruction documents
Latency (ms)	<100 ms for LTE networks
Security	Extremely important
Redundancy of links	Extremely important, needs close to 100% availability and to maximize coverage

TABLE 1

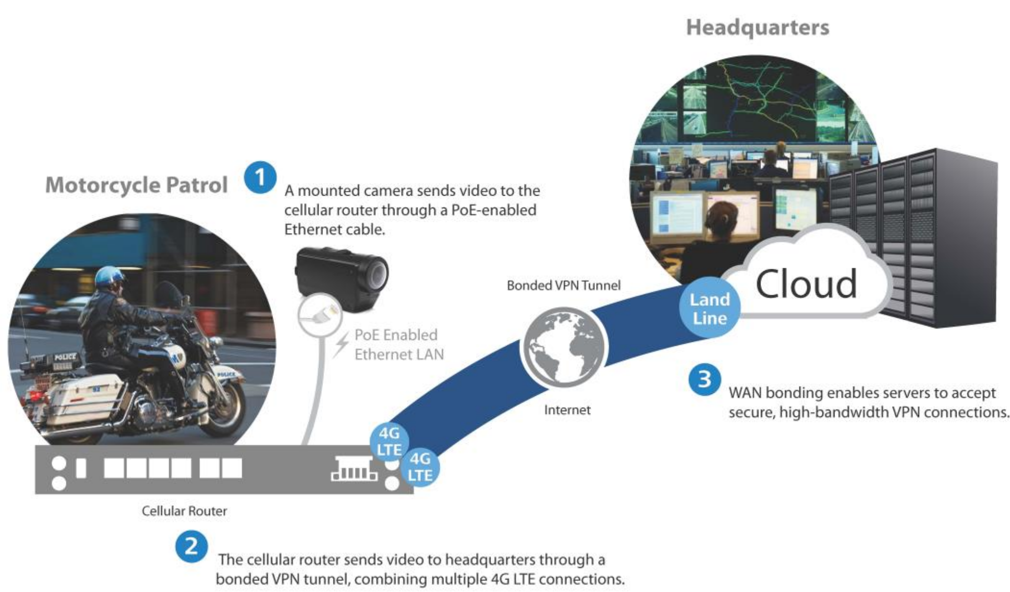
Government Use Cases — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
VPN	3G/4G bonding, multi-WAN
Key sensors	IP CCTV (the main requirement), audio, motion detection, heat
Physical mobility requirements	Stationary, field-based, and full mobility
Wireless connectivity	Wi-Fi, 3G/4G
Additional applications	Radio over IP, image recognition, public address
Location-based services	GPS accuracy
Central command architecture	Cloud or mobile command center

Source: IDC, 2015

FIGURE 5

Use Case: Police Vehicle Video Streaming



Source: IDC and Peplink, 2015

Disaster Emergency Response

The key requirement for disaster emergency response includes the ability to quickly deploy multiple WAN links to enhance uptime and reliability while at the same time providing excellent network security (see Table 1). In emergency response and recovery operations it becomes necessary to provide uptime as much as possible and to provide as much bandwidth as possible. In some of the most severe earthquakes, typhoons, and flooding that have occurred, operators had to struggle to get cellular service back online. In some cases VSAT is the only available backhaul and VSAT can also be used as a backhaul for cellular base stations.

WAN bonding can provide near 100% uptime connectivity for disaster emergency response anytime, anywhere by bonding cellular and VSAT in order to provide the versatility and mobility needed in rapid deployments. A recent example of where WAN bonding was used in disaster emergency response was the Dawlish Rail Disaster in the U.K. in which the very remote town on the sea was put in danger by 80 meters of sea wall that collapsed due to violent storm sea waves. When the sea wall fell, the incident was quickly declared a national emergency. The U.K.'s "Cobra" crisis management committee was brought in to handle the situation, with Prime Minister David Cameron eventually taking over the chairmanship. Over 300 homes were evacuated due to the flooding that followed. The power was out and public transportation cut off. The area was not only uninhabitable but still faced unpredictable weather. Cobra ordered train services to resume within two months and they brought in a construction contractor and wireless networking experts to do the urgent repair work and manage the site network since the construction company needed to access its headquarters datacenter and transfer large blueprint files and other architectural data. WAN bonding was deployed with 8 SIM cards to provide the large bandwidth needed over a secure VPN link back to the construction company's datacenter as well as providing secure links for members of the press and the Prime Minister's Office.

II. Healthcare

Mobile Healthcare Services

Emergency healthcare can be greatly enhanced if the doctors waiting in the emergency room for a patient to be brought by ambulance can view the vital biodata of the patient while he/she is being transported and that includes live video feeds. In this type of use case, the more 4G LTE bandwidth available the better, and thus WAN bonding becomes a highly desired feature; this is not a use case where 3G would be very effective. A recent example of a use case is a mobile mammography service operated by LSU Health Shreveport in North Louisiana in the U.S. The areas served are rural and remote with poor cellular coverage and effectively transmitting medical images back to the university is especially challenging in this environment. When lives depend on timely diagnosis, the connection between the mammography vehicle and the university must be fast and reliable. Faced with this challenge, LSU Health and its systems integration partner used 4x cellular bonding to provide a reliable, high-bandwidth VPN connection back to LSU enabling patient registration and database lookup, VoIP, and secure transfer of high-resolution mammogram images to the LSU doctors.

Automated Medicine Dispensers

Depending on the level of authentication needed to verify that the person attempting to purchase medicine has the proper prescription and identification, this use case can be served by 2G, 3G, or 4G. If video cameras are required, then 4G radio access and caching would be more ideal as well as store and forward.

III. Construction

Construction Site Management

Construction companies are requiring more and more bandwidth for their daily operations as well as worker/crew welfare services (see Table 2). In very remote areas, VSAT has been the only way to provide any sort of connectivity for shipping vessels, mining, and gas exploration and production. There is also an important application that exists in the larger mining sites and that is autonomous vehicles (trains and trucks) that might be controlled via a Wi-Fi or cellular link. In some markets such as Australia, the local mobile service providers are expanding their 4G LTE coverage through a combination of low-band (700 MHz, 850 MHz) service and construction of 4G LTE cell sites in areas where many remote campsites might be set up.

For construction sites in large cities or in surrounding suburban areas, wireless broadband is also very attractive as opposed to asking the fixed line provider to lay an optical fiber to the site. In Hong Kong SAR territory, telecom operators have been wary of provisioning the fixed line broadband connections to construction sites as the costs are typically over US$38,000 per link and the ROI is not attractive due to the temporary nature of the business. With cellular bonding everything has changed and it is now much more cost effective for telcos to offer the temporary broadband connectivity via 4G LTE bonded connections to provide the necessary high bandwidth needed by the architects and engineers.

TABLE 2

Construction Use Case — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
CONSTRUCTION SITE MANAGEMENT	Major challenges for planned construction sites: telcos' unwillingness to provision broadband, exorbitant provisioning costs, very long lead times; cellular WAN bonding routers solve all that. Instant "unbreakable" connectivity.
Bandwidth (Mbps)	2-10 Mbps
Frequency of uplink	Continuous
Frequency of downlink	Ad hoc or continuous
Latency (ms)	250-500 ms
Security	Preferred with VPN
Redundancy of links	Important with cellular solutions
VPN	3G/4G bonding, multi-WAN
Key sensors	Stationary IP CCTV
Physical mobility requirements	Stationary, but easily moved both around the site and to new sites when the construction project is complete
Wireless connectivity	Wi-Fi, 3G/4G, Zigbee, Bluetooth
Additional applications	CCTV, building information modeling, large CAD file downloads/uploads
Location-based services	GPS accuracy
Central command architecture	Cloud or mobile command center

Source: IDC, 2015

IV. Transportation

Fleet Management

Fleet management is a well-known use case that has in the past operated typically with 2G GPRS services in markets such as North America (see Table 3). The emerging pervasiveness of 4G LTE in many markets in Asia/Pacific and North America is encouraging application developers to look at additional functionality such as geo-fencing and central vehicle and cargo health/quality control management that would take advantage of the bandwidth offered by 4G LTE, including video streaming, store and forward video, and so forth. For example, for trucks that transport cash and other highly valuable goods the ability to stream online video could be an important deterrent to criminals, and insurance companies could start requiring such functionality in future commercial insurance coverage contracts.

Ferry Boat and Luxury Yacht Communications

Ferry boats that provide services between nearby islands need to provide scalable bandwidth for passengers who nowadays expect Internet connectivity for their smartphones and tablets. Gone are the days when passengers were willing to wait at airports and sit on ferry boats or even ride long-distance bus routes without Wi-Fi and Internet connectivity (see Table 3 and Figure 6). The ability to provide VPN for ferries and luxury yachts is also an important requirement for operational purposes and onboard secure communications. IDC has seen reports that daily traffic through cell sites posted along the shore of ferry routes can see traffic of over 500 GB-1 TB per day.

There has been quite a lot of effort in certain geographies on the part of mobile operators to take advantage of the 15–30 km coverage of 3G and LTE by placing base stations with antennas facing out to shore. In places such as Manila Bay, Hong Kong's Victoria Harbor, Tokyo Bay, Pusan Port, Cebu Port, and along the offshore coastline, 3G/4G connectivity has become an important requirement for consumers where in the past it was exclusively for near-shore gas and oil exploration/production in places such as Taranaki coastline in New Zealand.

TABLE 3

Transportation Use Cases — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
FLEET MANAGEMENT	
Bandwidth (Mbps)	128 kbps-1 Mbps; 2 Mbps for HD video anti-theft protection
Frequency of uplink	Ad hoc and regular intervals
Frequency of downlink	Ad hoc and regular intervals
Latency (ms)	250-500 ms
Security	Important
Redundancy of links	Two wireless links + Wi-Fi
VPN	3G/4G bonding, multi-WAN
Key sensors	GPS and CCTV (majority for now); emerging requirement – temperature, pressure, humidity, weight sensors for luxury goods or food transport
Physical mobility requirements	Predominantly cellular; Wi-Fi might be used when the vehicle is undergoing maintenance
Wireless connectivity	Wi-Fi, 3G/4G
Additional applications	Navigation, voice activation, language translation

TABLE 3

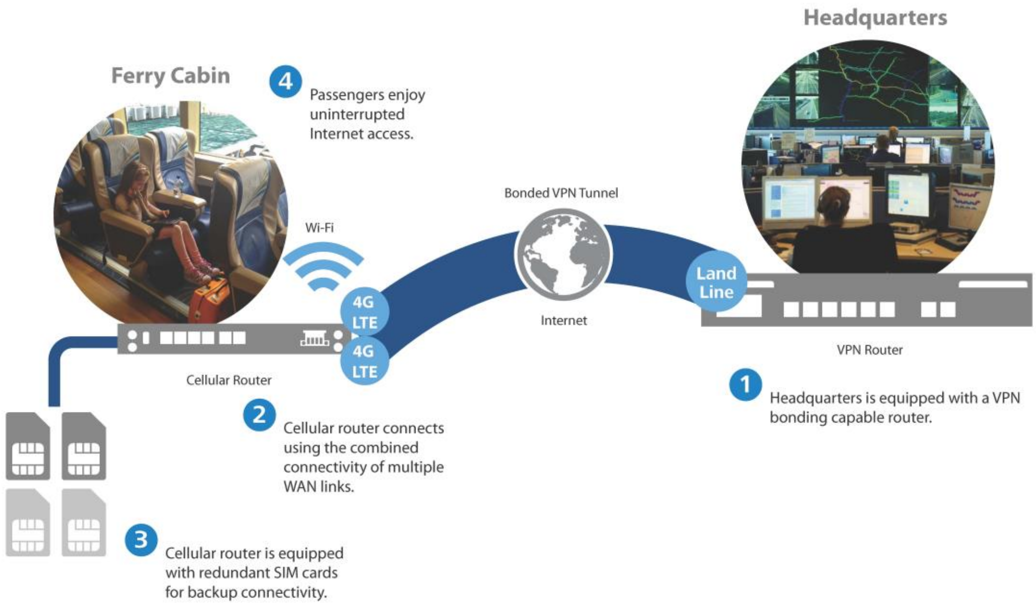
Transportation Use Cases — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
FLEET MANAGEMENT	
Location-based services	GPS accuracy
Central command architecture	Cloud datacenter (multiple datacenters if more than one application such as usage-based insurance and engine monitoring)
LUXURY YACHT & FERRY BOAT SERVICES	Onboard CCTV, GPS location tracking; oftentimes, also providing guest Internet Wi-Fi
Bandwidth (Mbps)	1-2Mbps (HD video) 10M+ (also Internet Wi-Fi)
Frequency of uplink	Continuous or activated by remote control
Frequency of downlink	Very frequent, general application traffic, IP TV streaming, email, general Internet traffic
Latency (ms)	100 ms
Security	Customer specific
Redundancy of links	Extremely important, needs close to 100% availability
VPN	3G/4G bonding, multi-WAN (marina Wi-Fi when close to shore, cellular when coastal, VSAT when offshore)
Key sensors	GPS
Physical mobility requirements	Vessel mounted
Wireless connectivity	Wi-Fi, 3G/4G, Zigbee, Bluetooth
Additional applications	Guest Internet, CCTV, Radio over IP, VoIP
Location-based services	GPS accuracy
Central command architecture	Cloud

Source: IDC, 2015

FIGURE 6

Marine Vessel Bandwidth Aggregation



Source: IDC and Peplink, 2015

V. Utilities

Smart Metering and Smart Grid

Smart metering for consumer homes is an excellent example of engineering compromises that have to be made to support a wide range of rugged and outdoor environments. As a result, smart meter manufacturers such as EDMI have developed an array of solutions and in particular low-power solutions that can run on a single battery for 3-5 years or longer and uses 2G or 3G access to upload the data once or twice per day. The Chinese government has announced plans to install over 300 million smart meters by 2016-2017. New Zealand with a population of around 4 million people already has 1 million smart meters in operation. In places like China, Hong Kong, Singapore, Taiwan, and South Korea, where much of the population live in high-rise apartments and condominiums, a combination of Wi-Fi or Zigbee (due to its hopping capabilities) can be used to aggregate the data from the smart meters on several floors that are then further aggregated to send via an edge router that has either an Ethernet port or 3G/4G port, or both. At the WAN level, VPN will also be an important requirement to protect the commercial interests of the electricity provider.

Advanced metering infrastructure (AMI) is used by gas pipeline, water, and electricity companies to monitor their assets, which are often in remote areas, along the transmission routes. One example is Energy Transfer in the U.S. which owns a number of interstate gas pipelines. The company deploys digital supervisory control and data acquisition (SCADA) controllers with sensors along its pipelines that measure pressure, temperature, flow rate, and leakage. In these types of infrastructure systems it is important to be able to provide a reliable link all the time and to reach all remote areas either through VSAT or a combination of VSAT + 3G/4G cellular. Electricity companies will oftentimes lay optical fiber along the transmission system but VSAT + cellular WAN bonding provides redundancy and backup especially in the remote areas.

VI. Retail

Retail holds tremendous promise for IoT deployments due to the promise that IoT can provide or enhance the following attributes needed in modern retail: traceability, mobility, big data analytics, business operations analytics, identity, and capture.

Omni-channel retailing is a concept that provides multiple ways for the buyer/consumer to purchase a product or service: brick and mortar store, website, mobile devices (NFC, QR reader, etc.), interactive TV, telephone order, direct mail/catalogue, and comparison shopping. IoT-based omni-channel utilizes item-level tagging via electronic product code (EPC)/RFID to improve the accuracy of inventory management and to provide real-time inventory visibility. GS1's Hong Kong IoT Center for Excellence for example has showcased four IoT solutions for retail: cold chain management, inventory management, genuine production authentication, and consumer mobile trusted sources management.

Wireless Points of Sale

Wireless POS terminals can be deployed in retail stores, temporary retail environments, and ad-hoc environments such as a flea market or farmers' market. The ability to provide redundancy with VPN security makes for an ideal use case for next-generation edge/access networking that includes in-store and perimeter security surveillance, POS operation, and intra-company VoIP services (see Table 4).

TABLE 4

Retail Use Case — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
WIRELESS POINTS OF SALE	LTE is positioned as a wireless "fixed" broadband, as an alternative to DSL/cable or business Internet lines
Bandwidth (Mbps)	256 Kbps-1 Mbps; 2 Mbps if HD video
Frequency of uplink	Event driven, regular intervals
Frequency of downlink	Regular intervals
Latency (ms)	500 ms
Security	Extremely important
Local caching (GB)	N.A.
Redundancy of links	3G/4G LTE backup
VPN	3G/4G bonding, multi-WAN
Key sensors	IP CCTV, POS terminals, VOIP
Physical mobility requirements	Stationary, field-based for ad-hoc selling
Wireless connectivity	Wi-Fi, 3G/4G
Additional applications	Magnetic or smart card swipe reader, fingerprint reader,

TABLE 4

Retail Use Case — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
	keyboard for pin input, language translation
Location-based services	GPS accuracy
Central command architecture	Cloud datacenter and/or local

Source: IDC, 2015

VII. Manufacturing

Manufacturing Operations and Asset Management

Machines used in discrete and process manufacturing, including robotics and tools such as lasers and milling machines, can be retrofitted at a cost with Ethernet connectivity and on-board control software can be modified if not already available to monitor or even record machine tool movements (such as measuring torque), usage statistics, and even images and video clips (e.g., aerospace production) that can be transmitted to a central server. The challenge of converting an automated machine tool floor in the factory to an IoT-connected machine tool ultimately comes down to the ability to quickly and cost effectively connect machines into a local area network that can then be connected to the WAN datacenter. Wi-Fi is being used extensively in many factory floors so the IoT connectivity has to at least be separated logically, and one way to do this is to use an edge router that is connected to one or more machines via Ethernet ports and that has a Wi-Fi client feature (see Table 5). Essentially, this allows the IoT part of the network to be managed as a separate VPN running over the same local area network access point (2.4 GHz and/or 5.8 GHz) infrastructure.

TABLE 5

Manufacturing Use Case — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
MANUFACTURING OPERATIONS & ASSET MANAGEMENT	This is Wi-Fi in production lines, keeping track of status at different machine tools and manufacturing stages
Bandwidth (Mbps)	1 Mbps or less (data captures)
Frequency of uplink	Continuous
Frequency of downlink	Continuous
Latency (ms)	20-100 ms
Security	Internal LAN as protected by Wi-Fi WPA2
Local caching (GB)	N.A.
Redundancy of links	Can be deployed for management across different factories
VPN	3G/4G bonding, multi-WAN
Key sensors	Optical, air quality, gas sensing, temperature, pressure, bio-sensing, current/power
Physical mobility requirements	Stationary or moving on production line
Wireless connectivity	Wi-Fi, Bluetooth, Ethernet, 3G/4G
Additional applications	N.A.

TABLE 5

Manufacturing Use Case — Networking Requirements

USE CASE	TECHNICAL SPECIFICATIONS/REQUIREMENTS
Location-based services	N.A.
Central command architecture	Cloud and/or local

Source: IDC, 2015

FUTURE OUTLOOK

IDC's Forecast for IoT in the Asia/Pacific Region

IDC forecasts that in 2020, Asia/Pacific will have 9.276 billion IoT units installed representing a total addressable market of US$853 billion (see Table 6). IDC estimates that as of the end of 2013, there were 2.45 billion IoT units installed in APEJ. IDC estimates the installed base of IoT units will grow at a compound annual growth rate (CAGR) of 18.9% over the forecast period to 8.22 billion in APEJ in 2020 or 17.8% to 9.28 billion units in Asia/Pacific including Japan. IDC predicts that consumer IoT will start to gain momentum by 2017-2018 with basic wearables as well as smart wearables, games, home appliances, and connected passenger cars. If the price points for edge/access networking devices and appliances are right then these enterprise solutions can also find enticing market opportunities in consumer IoT.

TABLE 6

Asia/Pacific Internet of Things Install Base and Revenue, 2013-2020

	2013	2014	2015	2016	2017	2018	2019	2020	CAGR 14-20
Install Base (M)	2,950	3,618	4,375	5,205	6,098	7,019	8,060	9,276	17.8%
APEJ	2,452	3,061	3,750	4,506	5,322	6,157	7,104	8,219	18.9%
Japan	497	557	624	698	777	861	956	1,057	11.4%
Revenue (US$ M)	336,679	382,085	439,606	504,076	581,737	666,538	758,818	853,875	14.2%
APEJ	252,599	291,142	336,420	387,958	452,485	523,246	599,335	677,956	15.1%
Japan	84,080	90,943	103,186	116,118	129,252	143,292	159,484	175,919	11.1%

Source: IDC, 2015

CHALLENGES/OPPORTUNITIES

As the demand for (and number of deployed) IoT sensor networks increases, IoT solutions integrators and providers will need to get acquainted with the new agile features and capabilities that are entering into edge/access networking in order to design and implement secure, resilient, multi-path networks with cost effective and adequate amounts of bandwidth. The sheer size of the industrial opportunity will make such edge/access networking products high in demand, especially as IoT networks are deployed in those typically harder to reach locations that are distant from metro-based bandwidth and infrastructure, where the specialist multi-WAN aggregation capabilities and technologies will be most effective and add the most value.

IDC believes that a key challenge will come from the need to centrally monitor and manage complex connectivity solutions for these remote deployments. This would include remote device online status and bandwidth usage monitoring, as well as configuration management and automated processes for remote unit replacements and redeployments, especially when diverse network technologies and providers are used in combination — a requirement typically dictated by the lack of connectivity availability and capacity at remote and mobile locations.

There is significant opportunity for service providers and integrators who can deliver secure resilient IP connectivity quickly and efficiently as part of a managed service offering to enable remote IoT sensor network deployments. As IoT becomes pervasive in every vertical, demand will increase exponentially for easy to deploy and manage edge/access network solutions capable of delivering IP connectivity to rural, mobile, and other traditionally difficult to reach locations.

Additionally, as more IoT sensors are added to existing IoT networks that are already generating mission-critical data, more IP WAN bandwidth will be required at those locations. An edge/access network appliance that supports the easy addition of diverse WAN links to increase bandwidth capacity seamlessly with little or no downtime or interruption to data collection will be favored over the traditional rip and replace approach for bandwidth service upgrades.

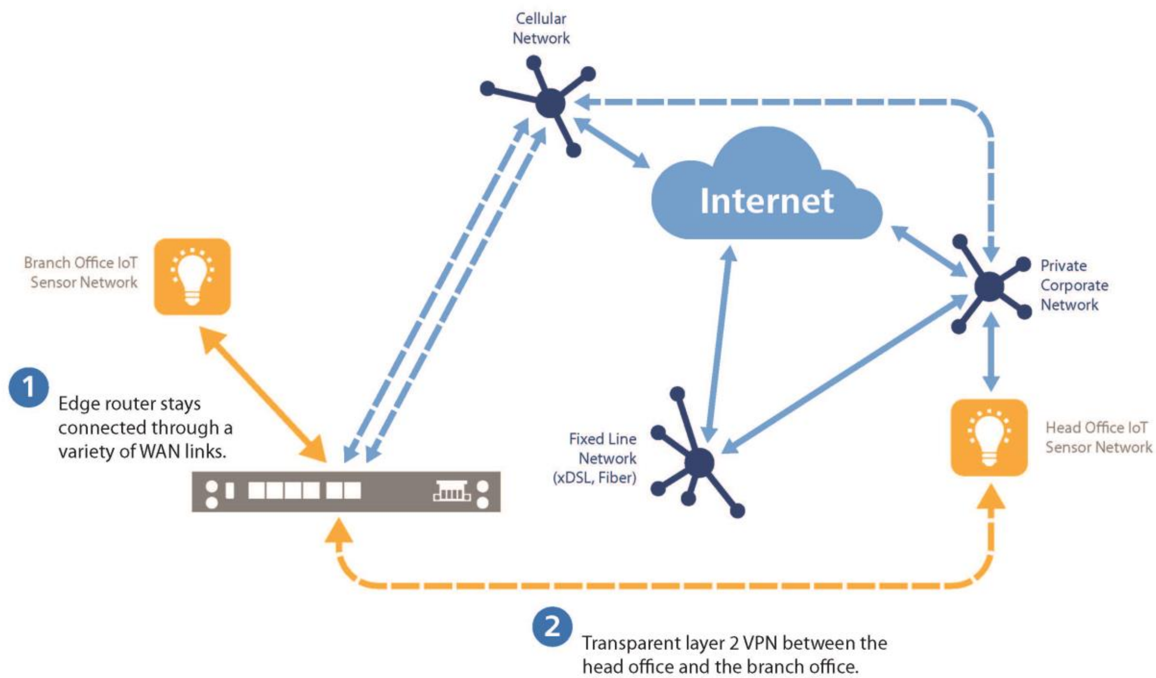
CONCLUSION

There has been a fair amount of activity by industry associations, research labs and various R&D partnerships to address the sensor and IoT device messaging and communications but not as much focus on how to best build secure, reliable, cost-effective IP access networking.

IoT network operators require a scalable, versatile edge/access networking solution that will allow enterprises/network planners to deploy IoT sensor networks anywhere quickly, efficiently and securely using diverse WAN technologies from diverse network operators as well as provide seamless integration over existing enterprise IP WAN infrastructures (see Figure 7).

FIGURE 7

Multi-WAN Network Provides Secure Access Network for IoT Sensor Deployments



Source: Peplink, 2015

IDC believes that there are considerable benefits and advantages to be found in the use of multi-WAN IP-based edge/access network gateways that are WAN technology and network operator agnostic to provide secure, diverse, highly reliable enterprise IP connectivity wherever IoT sensors are required.

The ability of this new generation of multi-WAN devices and supporting technologies to provide secure versatile connectivity anywhere, will for the first time enable the enterprise deployment of IoT sensor networks wherever they are needed, and so will become a key strategic enabler of enterprisewide fully inclusive IoT deployments.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com