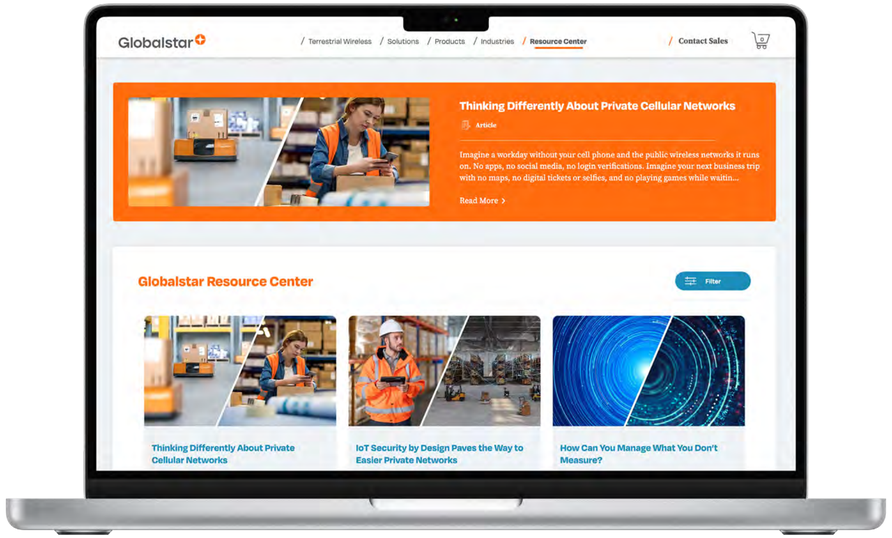
Globalstar

EBOOK

Thinking Differently

About Private Wireless Networks

Table of Contents



Share Our Blog Series

Each of the articles in this ebook are easily sharable as as blog posts on the Globalstar website.

ACCESS THE SERIES HERE

Get to Know Globalstar

Globalstar's technology and services extend from low Earth orbit to mobile networks and leading-edge industrial and business facilities on the ground. We provide satellite-based IoT and asset tracking, licensed RF spectrum ideal for 4G/LTE and 5G networks, and the most advanced 5G private network technology on the market.

Learn more at www.globalstar.com.

Cellular Evolution

Adaptation has always been humanity's superpower.

Adaptation happens at the level of the cells in our body. It happens in ideas, our societies, and our ways of life. It races ahead in our technologies, so that one generation's best solution turns into the next generation's nostalgia tour.

And it's happening now in cellular communications, where it supports the evolution of business and industry as they adapt to future opportunity.

The future is available now

Private wireless networks have become critical assets in warehouses, factories, ports, energy platforms, mines, stadiums and countless other facilities where physical meets digital under demanding conditions. Wi-Fi, which came to market nearly 50 years ago, has served many generations of private networks. More recently, public cellular has been adapted for private use, bringing greater reliability, performance and protection from interference.

But neither technology is equal to many of the demands being placed on private wireless networks today. Autonomous mobile robots roaming through distribution centers and factories. Automated mining equipment navigating deep underground or across massive open pits. Digital twins needing continuous connectivity from hundreds or thousands of sensors in heavy industrial or utility environments. Vast networks of smart cameras generating interactive digital traffic that can be critical to safety and security.

Capacity fluidity

In this ebook, you will meet a technology that can master those requirements and much more. It is based on a simple but profound idea: that a network made up of individual, independent cells has a built-in weakness that affects coverage, capacity and interference. In an average public mobile network, it rarely causes more than minor annoyance. But in business-critical applications on private networks, it can seriously affect performance, reliability and cost.

Overcoming them takes "capacity fluidity" – a breakthrough in cellular network design that goes by the name XCOM RAN. Read on to explore the next generation of cellular evolution. You will come away understanding how high-demand applications challenge today's private cellular networks, how XCOM RAN overcomes the challenge, and what it takes to deploy a next-gen private cellular network.

Private Networks? Who Needs Them?

In 2023, Robert Metcalfe received the $1 million Turing Award for a milestone he achieved in the 1970s. It was called Ethernet, a technology that used digital packets to transmit data over cables connecting computers. Metcalfe went on to found 3Com to commercialize it and launched the networking revolution.

A decade later, two computer science professors at Stanford realized that something their students developed, a routing technology based on Ethernet, could be used to connect their offices together in what became known as a local area network or LAN. They started a company to commercialize routers, naming it after San Francisco, the city where they lived. Cisco Systems sold its first product in 1985, went public in 1990 and started a furious pace of innovation and investment that bravely continued through the darkest days of the dotcom bust, from which Cisco emerged far ahead of its competition. From 1987 sales of $1.5 million, the company grew to $53 billion in 2023. Each innovation created major increases in the speed, efficiency and capacity of data routing.

Along the way, Cisco's technology became the basis of every LAN, metropolitan-area and wide-area network, including one we know by a different name: the internet. Together, Ethernet and Cisco's routing technology transformed the traditional business of telecom into what would be more accurately called "datacom" today.

The Evolution of Private Networks

The internet is a public network that interconnects us all. But the private enterprise networks that 3Com and Cisco Systems invented are still vital. They are secure and

deliberately isolated from the internet or public cellular, and they only allow authorized devices and apps to connect and share data. Analysis Mason predicted that enterprise spending on LTE/5G private networks will reach $9 billion in 2028, up from only $1 billion in 2022. The 4,000 private cellular networks operating in 2022 will grow to more than 60,000 for the same reason that Ethernet and Cisco were so successful: the use cases and applications for them are limited only by our imaginations.

As wireless technologies evolved, enterprise networks have gone wireless. Wireless networks in our homes and workplaces provide the last few meters of the last mile for digital traffic that is part of our daily lives: email and chat, social media and video, web browsing and powerful cloud-based applications. But they also meet much more specialized needs: the monitoring and management of industrial equipment, logistics, video surveillance and security systems, medical diagnostic systems, sensor networks and much more. They are critical to driving the automation and process virtualization that maintains growth in efficiency, productivity and return on investment. In doing so, they are also helping to drive the growth of our economy.

Use Cases for Private Networks

In October 2002, a Lufthansa 747-400 took off from Frankfurt on its way to Washington. Unknown to the rest of the passengers, members of a project team from Lufthansa and Boeing were aboard to test the first airborne private wireless network. They successfully connected a standard laptop to the onboard network, which gave it access via satellite to a secure, firewalled internet connection and, via a VPN, the Lufthansa corporate intranet.

Today, when a commercial aircraft pulls up to its gate, it connects over a private wireless network with the airline's central server to exchange data on flight plans, weather and system diagnostics, typically using Wi-Fi. But where Wi-Fi was once the standard, cellular has come into its own, particularly with LTE and 5G capacity and speeds. As a result, private wireless is showing up in some unexpected places. In US Formula 1 racing, teams are permitted to have only 60 engineers and technicians trackside at each race. To ensure they have all the expert analysis they need, the cars have private wireless connections to their pits, where trackside compute clusters typically link at over 80Mbps to "mission control" at HQ.

Formula 1 racing, however, is a narrow niche. Opportunities for private cellular networks with greater scale include –

- **Manufacturing and industrial facilities**, where interference creates serious issues for Wi-Fi.
- **Healthcare** in support of life and health support devices, patient tracking, inventory management, surveillance and security.
- **Campuses for corporate offices and higher education**, where a private cellular network offers blanket coverage that brings all operations under one network for greater control, security and reliability.
- **Stadiums, arenas and convention centers**, where capacity crowds make public cellular networks too congested to be useable but customer satisfaction, not to mention public safety, depend on reliable wireless.

At the extreme end are very high-capacity requirements in challenging environments where wired infrastructure isn't feasible. These include:

- **Autonomous mobile robots**. Once kept in steel cages to protect workers, robots are increasingly mobile and autonomous in factories, warehouses and logistics facilities. They have come to dominate investment in warehouse automation – Amazon alone has grown its fleet of autonomous mobile robots 24x from 30,000 in 2015 to 750,000 today. In Micro Fulfillment Centers (MFC), they typically operate in multi-level metallic structures, navigating through ramps and vertical lifts among thousands of storage bins. To do their jobs, they need continuous connectivity with the management system wherever they travel.
- **Digital twins.** Digital twin applications are revolutionizing the cost and complexity of operating and upgrading major process plants, drilling platforms and urban infrastructure. Running in a virtual environment that duplicates the real one, they enable changes to be designed, tested and proven in software before the trial-and-error of costly real-world implementation. But the digital twin is only as good as the real-time data that drives it. That demands continuous connectivity for hundreds or thousands of sensors operating in heavy industrial and urban environments.
- **Edge video.** Video technology once meant a set of feeds from static video cameras, which sent either real-time video or a series of still frames, depending on available bandwidth. Today, real-time video is growing at double-digit rates to meet demand for safety, security and transparency in the public sphere. Cameras are everywhere, and they are increasingly capable of two-way communication to control what the camera sees and provide edge-processing for image recognition and the ability to generate alerts to activity that may demand action. One-way traffic has become interactive exchange, boosting bandwidth demand as networks expand their footprint.

Designing for Performance

Use cases offering scale have one thing in common. They take place – not within the calm and sheltered walls of an office – but in the rugged and dynamic environment of factories, warehouses, ports, industrial plants and urban infrastructure. Wireless private networks are the default choice for such locations and network design must answer a long list of questions, including:

- Where do the wireless radio units need to be positioned and how will they be powered?
- What walls, metal structures and radio signals may cause RF interference, and how will the network design deal with it?
- What spectrum is available for the network and how does its performance match capacity, reliability and interference requirements?
- How will the network provide adequate information security, given the mission-critical nature of its traffic?
- How simple and cost-effective will it be to make changes and updates to the network as requirements change?
- What economics do the different technology options offer, not only for initial installation but total cost of ownership over years?

The evolution of Ethernet and routing technology has no doubt surpassed the wildest imaginings of their inventors. The technology for private wireless is advancing at similar speed, and in our next post, we'll go into detail about the options for network technology, design and spectrum that can deliver on the promise of that revolution that began so many decades ago.

Can your private wireless network meet extreme bandwidth demand with less spectrum? Let us show you how.

Network Planning? Why Bother?

Private networks are the last mile –a protected connectivity environment at the end of the transmission chain where authorized devices and apps can exchange data securely. Enterprises typically deploy one of two technologies for them: **Wi-Fi**, relying on unlicensed spectrum, and **distributed antenna systems or DAS**, which are most often used to extend cellular service into large, enclosed facilities such as malls and casinos.

Both are popular. Both are proven. And both are a pain in the neck, at least when it comes to designing and deploying the last-last mile. Somebody should really do something about that, shouldn't they?

Designing Wi-Fi and DAS networks

To design a Wi-Fi network, experts recommend a serious planning exercise.

Coverage planning is the first step to ensure that there will be sufficient signal strength for Wi-Fi devices to connect. Poor design can result in too many access points – which increases both cost and network contention – while too few will leave coverage gaps.

Capacity planning accounts for the different types and number of devices and applications that will connect. Here, poor advance planning can produce intermittent connectivity and slow speeds as the network struggles to meet demand with too little capacity. Poor performance can also be a sign of growing pains: a successful network can begin to degrade when new users and devices are added over time.

Radio frequency planning is another step. Avoiding in-network or out-of-network interference requires a comprehensive site survey and frequency planning, proper antenna placement, careful network design and the shielding of sensitive equipment. Careful analysis of wall materials and physical obstacles like metal structures, signage and columns can ensure that access points are placed to maintain a link wherever devices try to connect, but they are very expensive and time-consuming.

When dealing with public networks, DAS networks require a higher level of detailed planning to avoid "near-far" interference, in which an access point connects to a cell tower far away and forces the network to work overtime to transport data. Notoriously difficult to test, optimize and maintain, DAS networks require serious engineering skills from the original design through maintenance and upgrade.

Who Needs a Plan?

Should it really take this level of effort and cost to design, maintain and change a private network? At Globalstar, we don't think so.

That's why we developed XCOM Radio Access Network. XCOM RAN is a 5G wireless technology designed by innovators who made fundamental contributions to mobile technology from LTE to femtocells. Tossing out the Wi-Fi and DAS rulebook, we created a technology that offers true ease of deployment without complex network design, with 4 times the capacity of baseline 5G and a large supercell with no handover boundaries.

How is that possible? Instead of antennas or cell sites, XCOM RAN uses basic Remote Radio Units (RRUs) that deliver signals simultaneously to commercial-off-the-shelf hardware running XCOM RAN software. Every RRU added to the network increases both coverage and capacity – because the entire network acts as one supercell, with no need for additional spectrum or cell handovers. Intelligent base-band processing ensures Radio Units never interfere with each other. That lets you place them for best coverage rather than minimization of interference. Yet the RRUs are as easy to install as Wi-Fi access points.

But don't take our word for it. After testing XCOM RAN, research firm Signal Research Group wrote, "The XCOM technology provides extremely high capacity within a single logical cell comprised of multiple radio units. Inter-cell interference is nonexistent and there are no interruptions due to cell handovers."

Add up all the benefits – performance, capacity and ease of deployment and upgrades – and XCOM RAN is more than a private network. It's a cure for that pain in your neck that just won't go away.

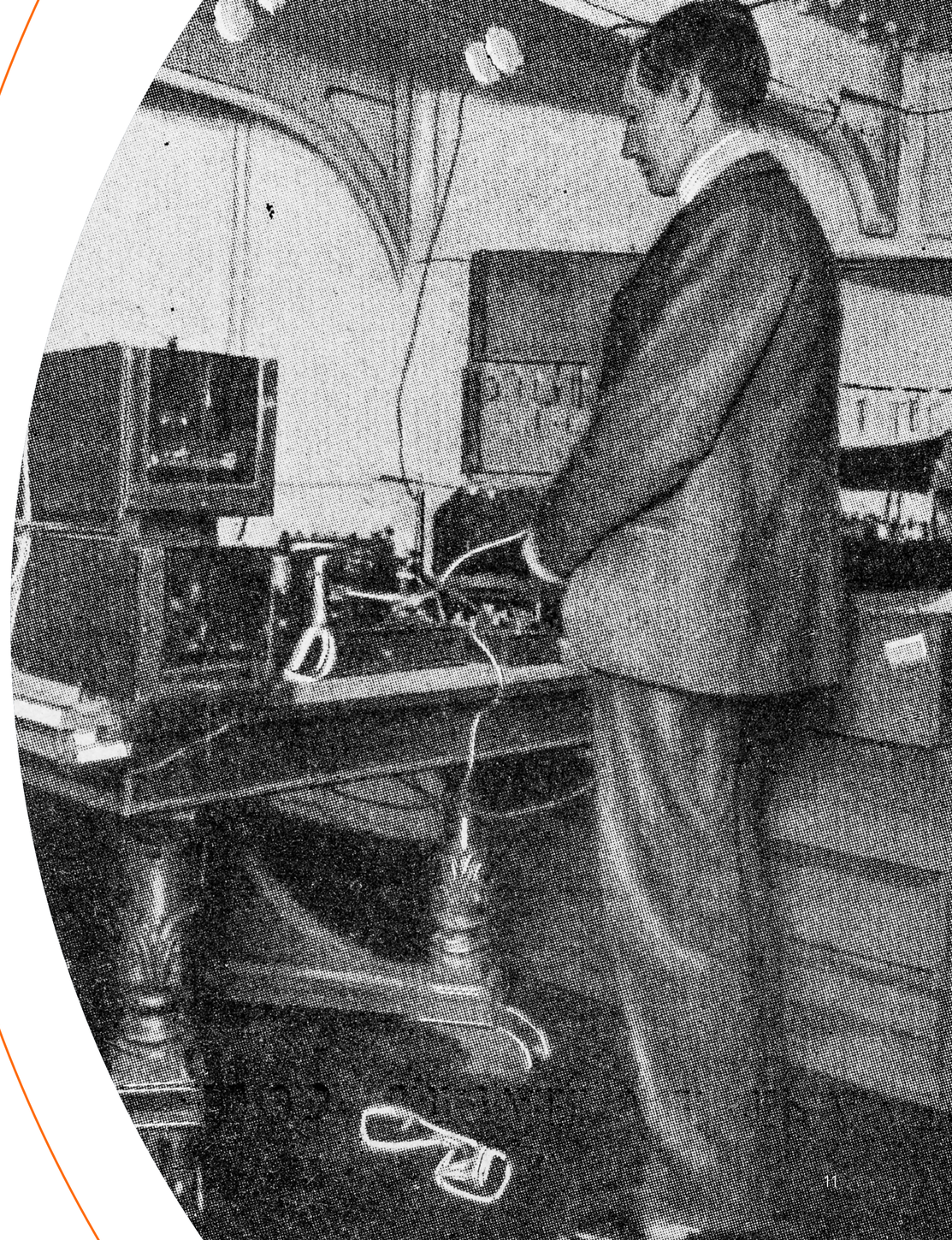
Want to see XCOM RAN in action? See the video on our website.

The Endless Search for Spectrum

The next time you connect to a wireless network at home or in a hotel, you can thank a 19th Century Italian aristocrat. The guy never needed to work a day in his life, but he laid the foundations of the wireless world we live in.

In the second half of the 19th Century, scientists were fascinated by invisible forms of electromagnetic radiation that we call radio waves. Inventors also tried to find a use for them, but none proved successful – until Guglielmo Marconi developed the first workable system for sending information over the airwaves. In 1894, the 20-year-old, home-schooled Marconi pushed a button on one side of a room in his villa and wirelessly rang a bell on the other side of the room. His Mom was amazed. Just seven years later, Marconi was transmitting a wireless telegraph signal across the Atlantic from the UK to Newfoundland, and his reputation as an inventor began spreading around the world.

Marconi's invention gave us access to the nearly 3000 GHz of Radio Frequency spectrum we use today, particularly for telecommunications. That sounds like a lot of invisible real estate: surely enough for all. Except it's not. RF spectrum has proved so useful for so many applications that demand exceeds supply, despite our efforts to commercialize more and more of it. Demand for high-bandwidth, ultra-reliable networks is accelerating as we put wireless to work in more applications where failure is not an option, from autonomous vehicles to Industry 4.0 facilities.



The challenges of private wireless networks

Nations manage the spectrum availability in each country licensing blocks of RF

frequency to telecommunications operators commonly named Mobile Network Operators (MNOs). Other parts of spectrum are determined unlicensed or so many devices co-work in the same frequencies. A new trend of shared spectrum started in the U.S. allowing industries to obtain spectrum grants for specific areas and for specific times.

Industries willing to take advantages of wireless communication to transform operations must determine how to obtain spectrum so must private networks rely on Wi-Fi (which operates in 2.4, 5, and 6GHz unlicensed radio bands). Wi-Fi access points (APs) are low-cost and easy to install but are subject to blocking or interfering with each other, especially as density of APs increases, because they share spectrum and Wi-Fi is widely deployed. These challenges can lead to intermittent connectivity and slow speeds, which makes it a poor choice for mission-critical applications. Its widespread deployment has also made Wi-Fi an attractive target for hackers, who have hundreds of thousands of networks to experiment on.

Among the most demanding private wireless networks are used in highly automated factories, process plants, ports and warehouses. They need very high data rates and resiliency in a dynamic environment full of metal machinery and structures that block radio signals. That motivated the increasing need for new private wireless networks based on 4G/LTE and 5G cellular standards. In the US, they typically rely on Citizens Broadband Radio Service (CBRS) frequencies in the 3.55 to 3.7 GHz band. CBRS does not require a license to use – but every CBRS network must register automatically with a central online database to avoid interfering with licensed users including the US Government and ISPs. Running on cellular standards, private networks are more reliable and have better security than Wi-Fi, but CBRS is also available only in the United States – and only if the government or other incumbent (ex. PAL user) has not received priority for the frequency in your area.

Spectrum to call your own

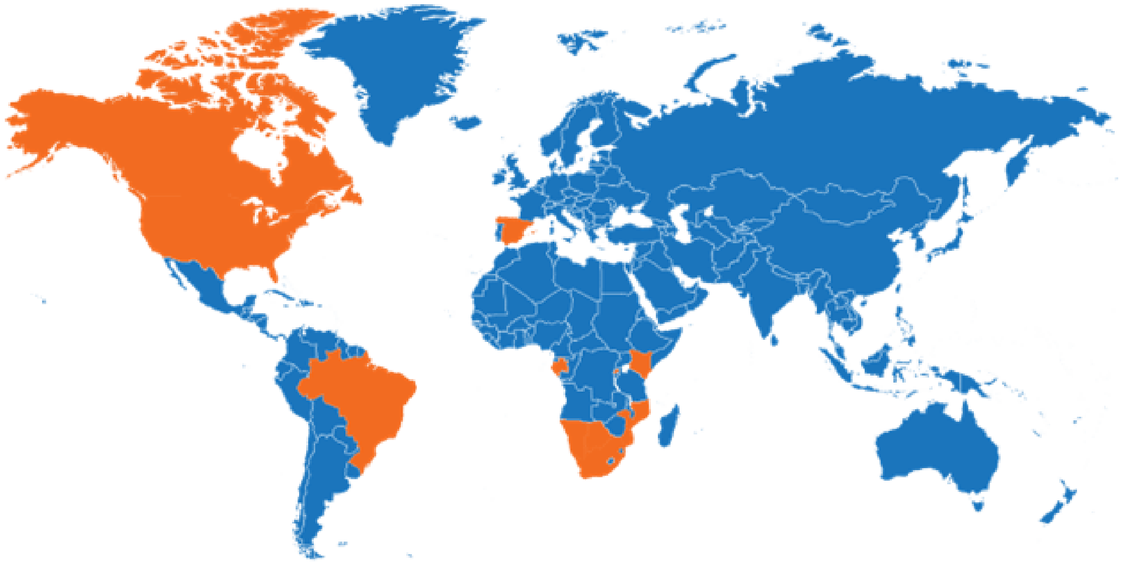
Wi-Fi unlicensed spectrum has long made obvious sense for private wireless networks in offices, retail stores and other places where cost and ease of deployment are the main goal. "Lightly licensed" CBRS offers the value of cellular standards with the potential to improve both the user experience and network security. For the best of both worlds, however, a private wireless network would operate on licensed, but private spectrum to guarantee a high availability and interference free environment. Only this combination can provide high availability for mission critical applications and high throughput to enable the industry transformation. In addition, there is strong preference from private network customers to have the data running on these networks locally hosted in the customer's facility as well as for the network to be simply deployable without the need to coordinate much internally within the APs of the private network or externally with other public networks.

The Third Generation Partnership Project (3GPP) has approved a new midband swathe of spectrum that fits the bill. Band 53 for 4G/5G networks is 10MHz of bandwidth located at 2.4GHz. Its availability and attractive features have led chipset manufacturers, RAN providers and device makers, such as Nokia, to commercialize it, with a focus on private networks. Any organization or network integrator can license it from Globalstar.

Unlike CBRS, band 53 is available globally. Globalstar is currently authorized to operate or license Band 53 for private wireless networks in 11 countries, including all of the United States and Canada as well as Brazil, Spain, South Africa, Botswana, Rwanda, Gabon,

Mozambique, Kenya and Namibia. Globalstar is seeking authorization in more countries as private wireless demand increases.

For organizations with worldwide operations, band 53 provides a single licensed band for all its networks, which unifies equipment and device characteristics across the organization. Many countries have allocated licensed spectrum for private wireless networks without any attempt at coordination with other nations.



The number of nations that have allocated any spectrum for private wireless is dwarfed by those that so far have not. The situation is fluid, with consideration of licensing going on in many places, but most of Latin America, Africa, the Middle East, and Southeast Asia have yet to approve a private wireless licensing regime. In some of these, licensed access to band 53 can close the gap.

Band 53 can even be combined with CBRS in a 5G private network, with Band 53 providing robust and secure bandwidth and CBRS boosting network performance with best-effort SLAs. Additionally, XCOM RAN can be deployed in Band 53, further increasing the available throughput for indoor applications up to 4x over classical 5G networks.

In our spectrum-challenged world, it is rare to find a swathe of midrange bandwidth that is not already taken up by incumbents. With a long history in satellite messaging and IoT, Globalstar is now expanding its technology and services to serve organizations with high-demand operations on the ground.

Wi-Fi spectrum first came to market in 1977 and for decades was the only realistic option for private wireless networks. CBRS cellular was opened for private wireless use in 2019. Just four years later, XCOM RAN entered commercial service to deliver a step-change in capacity, coverage and simplicity, taking 10 MHz of spectrum today and enabling it to work like 40 MHz, and in a few years even higher, thanks to the unique technology multiplying spectral efficiency. And so, the wireless innovation engine shows no sign of slowing down,

with the story that began when Marconi amazed his Mom by ringing that bell continues, supporting new generations of wireless technology and delivering benefits Guglielmo could only dream of.

For more information on Band n53, visit https://www.globalstar.com/en-us/terrestrial-wireless/band-n53.

Redesigning Private Wireless from the Ground Up?

In previous pages, we wrote about the power of private wireless networks to solve real-world problems in manufacturing, warehousing and safety – and the rising challenge of deploying those networks using today's established technologies and frequencies. That's why it is time for "capacity fluidity" – a new wireless architecture that overcomes the challenge.

The Incumbent Technologies

Wi-Fi is familiar to almost everyone – commercialized nearly 50 years ago and with 600 million devices in the field. But for mission-critical, high-demand applications, it's not ideal. Interference among nearby Wi-Fi systems is a real issue that affects performance. Widespread deployment has also given hackers years of experience at penetrating Wi-Fi networks. And if you are covering a wide area, you need roaming capability, where Wi-Fi is weak.

These shortcomings are behind the rising popularity of Citizens Broadband Radio Service (CBRS) 4G/5G cellular for high-demand private networks. Cellular standards make these networks more secure and less vulnerable to interference than Wi-Fi. Like Wi-Fi, the bandwidth is free, but networks must register with the online Spectrum Access System, which gives licensed CBRS users priority. Even when the band is available, the SAS system can disrupt some applications if the wireless link is interrupted to change frequency.

Both technologies are challenged when operating in complex spaces full of radio-absorbing metal structures and machinery. Getting high performance there requires extensive planning of coverage, capacity and interference, which has to be repeated with each significant change to the facility. It is past time for a complete rethink of private wireless networks to make them a reliable, high-performance asset for mission-critical operations.

The New Contender

Standard cellular design calls for many radios spaced so that they form overlapping cells of radio frequency. That has proven its value for public mobile networks. But in dense interior and exterior deployments that require uninterrupted high capacity, the handovers between cells become complicated, and the boundaries between cells generate interference at the edges. These issues can cause user equipment (UEs) to bounce back and forth between cells during a handover or fail to complete the handover at all.

The cell-based design also comes with a built-in disadvantage. When multiple UEs are at work within a single cell, the cell responds by dividing its available bandwidth among them. That's eminently fair to all concerned – but it means that throughput goes down while latency rises. Meanwhile, adjacent cells may have plenty of available bandwith that is largely going to waste.

A cellular network designed from the ground up for private wireless would take a completely different approach. Instead of many cells, it would consist of a single "supercell" with no handovers, in which all radios transmit to and receive from all UEs at the same time without interfering with each other. It would deliver far greater reliability and would give each UE the potential to access the total capacity of the network, with no congestion in a single cell. The same ideal network would use radio units already available in the market and interface seamlessly with established user devices.

That is the design of XCOM RAN. It uses standard radio remote units (RRUs) that have four transmit and four receive antennas, all independent. They connect to XCOM RAN software compatible with the ORAN and 3GPP standards, and that's where the magic happens. The software synchronizes and calibrates the connections with the RRUs so that all are transmitting the same information at the same time on the same frequency. Once the system is synched, it exchanges streams of data with every UE, calibrating the parameters for each one separately. Instead of a UE exchanging signals with one of many cells, it receives signals from all RRUs, perfectly synchronized to prevent interference. We call it "capacity fluidity," because it eliminates the need to plan coverage and capacity cell by cell.

Stop the Noise

The signal-to-noise ratio (SNR) is fundamental to communication technology. It measures the level of a desired signal against the level of background noise. Every network has a noise floor generated by the electronics in the terminals. More noise is typically generated by interference in the same frequency, either from within the network or outside. The more noise in the network, the lower the throughput, which confuses the decoders and generates errors. Errors trigger error correction software, which further reduces throughput. Modems respond by stepping down to a lower modulation to reduce errors, at the cost of still more throughput.

The XCOM RAN design sidesteps this downward spiral. Because all RRUs are transmitting the same stream of data in precise synchronization, interference-generated noise is absent. Because UEs are exchanging traffic with multiple RRUs, signal power is higher than it would be in one of many independent cells. By combining all the signals, XCOM RAN's SNR is always high: boosting power and eliminating interference combine to achieve high bandwidth. Within that high capacity, XCOM RAN can support 16 independent MIMO (multiple in, multiple out) layers between the UEs and RRUs.

XCOM RAN is in commercial deployment keeping autonomous mobile robots moving in advanced, automated warehouses. It is uniquely suited to such high-demand applications. Its high SNR delivers minimal degradation at the outer edges of each's RRU's coverage compared with Wi-Fi or conventional cellular. That provides consistent coverage even across sites with complex metal structures, from warehouses to factories and stadiums.

These are just some of many use cases for a technology that unlocks the true potential of private wireless and takes digital transformation where it has never been able to go before.

Learn more about how XCOM RAN can apply to your operational challenges at the Globalstar website.

How Can You Manage What You Don't Measure?

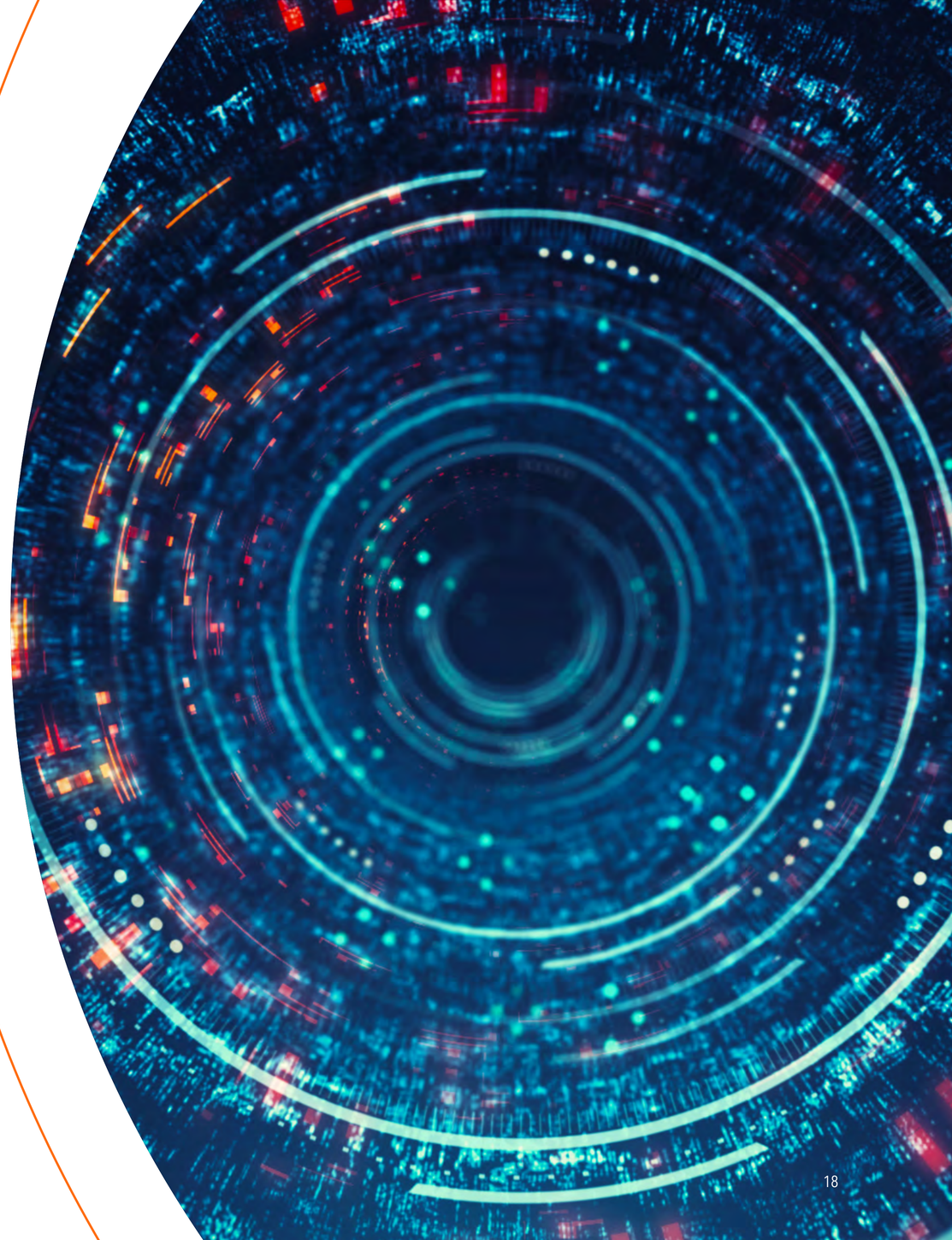
We have taken you inside a radical advance in private wireless network design that accelerates the benefits and eliminates the limitations, opening powerful new use cases. The next challenge is to manage that connectivity for optimal performance.

The Improvement Machine

You surely know the bit of business wisdom that says, "you can't manage what you don't measure." It is attributed to W. Edward Deming, the engineer, consultant, and business theorist who introduced Total Quality Management to manufacturing.

But Deming never said it. In fact, he called the idea a myth. The person that we are all misquoting is legendary business writer and consultant Peter Drucker, who wrote, "If you can't measure it, you can't improve it." There is a world of difference between managing a process and improving it.

Most private wireless networks come with network management systems (NMS) that let managers configure, monitor and manage the network. You can acquire an NMS for a Wi-Fi or private cellular network. Savvy customers make sure that the NMS can integrate a variety of software and hardware, provide scalability, and offer reliable performance management capabilities. Those factors become part of the purchase decision along with the characteristics and costs of the network itself. But is it enough just to manage the network? For a typical office or campus network, probably so.



When that network serves a complex environment and is mission-critical to operations, probably not. Certainly not for an automated factory or warehouse where machines need to exchange data and robots roam. Nor for an operating theater where surgeons wear augmented reality goggles to precisely visualize what they are doing in the patient's body. Nor for a high-pressure process plant linked to its digital twin or for security surveillance and personnel at a crowded stadium, where uninterrupted data and voice service is essential.

Those are applications for which XCOM RAN was designed: facilities with challenging environments for RF signal propagation, and facilities where the network must adapt to frequent change. For these places, the XCOM RAN NMS becomes a real operational improvement.

Knowledge is Power

XCOM RAN NMS does the things you would expect. A single pane of browser-based glass lets you manage network configuration, user equipment (UE), operations and software. The NMS simplifies network setup and the addition of remote radio units. It monitors performance, sets rules for quality of service, and sends alerts to faults. It even supports integration with 5G Cores and runs on its own separate CPU to keep it from affecting network performance.

What turns our NMS into a network improvement system is its ability to measure and display over 300 3GPP-defined metrics captured from the DU and CU, and to compare them with KPIs. This gives you truly granular control and the ability to tweak network layout and coding for best performance as conditions change. Statistics on aggregate cell levels, both current and historical, give you a 50,000-foot view of capacity across the network. And with XCOM RAN, that cell data tells a big story, because its unique technology combines multiple radio units into one high-capacity "supercell" that covers your entire operation without handovers or interference.

Our XCOM-RAN has been instrumented with a code that outputs detailed metrics about the performance of various parts of the installation. These metrics are then streamed through an Open Telemetry protocol to a time series database. The NMS Dashboard queries this database frequently to display various performance statistics.

On the main dashboard, we have Cell Uplink Scheduled Throughput and Cell Downlink Scheduled Throughput, so that end users can see how much data is being sent over the air. This enables the end user to quickly be able to see if there are spikes or drops in throughput. On the main page, we have many other indicators including:

- SAS Status – are we authorized to transmit currently?
- Core connectivity – Is the connection with the NGC up and does the NGC report that the connection is healthy?
- BBU Health – Is the BBU up and running, and are all components reporting that they are healthy?

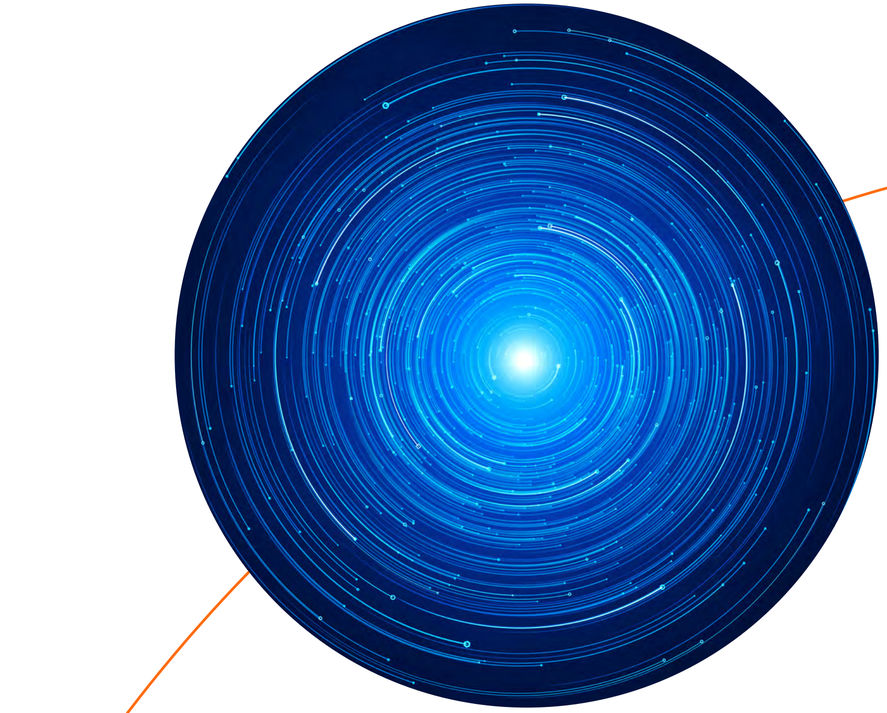
In addition to these indicators, there is also live subscription information such as:

- How many licenses have been used
- How many devices are online and/or active at the current time

We also have a set of Grafana dashboards that utilize the metrics that are being set to our time series database. Using these dashboards and metrics makes it possible to drill deep into system performance and even diagnose common issues.

XCOM RAN NSM Dashboard

Mr. Deming may have been right that trying to measure everything in a business can be futile. Business is not driven just by metrics but by the human qualities of vision, passion, persistence, and teamwork. But when it comes to getting optimum performance from a mission-critical wireless network, Mr. Drucker had it right. The better you can measure it, the more likely your NMS is to deliver the improvements you need.



IoT Security by Design Paves the Way to Easier Private Networks

IoT Device Security

As digital transformation accelerates, the world is increasingly becoming interconnected through IoT (The Internet of Things). According to an article written by IoT Analytics, the number of connected IoT devices is expected to grow to 18.8 billion by the end of 2024 and is estimated to reach 40 billion by 2030.

Enterprises around the world and across industries such as smart manufacturing, construction, transportation, government, public safety, agriculture and more, are relying heavily on connected devices, widening the opportunity of potential cyberattacks and threats of malicious activities. This has made organizations more susceptible, presenting them with security challenges that they must be aware of and address. With the number of cyberattacks increasing and becoming more frequent, old-school cybersecurity is no longer an option.

Because technology is forever evolving, hackers have gained access to more tools and improved their cyberattack skills. To prevent these advanced cyberattacks, businesses must understand their IoT devices behavior to detect any abnormalities. Implementing robust security practices across all elements of the IoT device can allow it to notify and alert administrators when an unexpected change in behavior is detected. This helps protect an IoT ecosystem from potential threats and vulnerabilities, as well as mitigate risks. Some of these security practices include role-based access controls (RBAC), encryption keys, VPN solutions and multi-factor authentication.

Security Across Device Communication Over Networks

While this is a no-brainer, IoT devices require network connectivity to operate and transmit data. When it comes to the communication aspect between IoT devices, having a highly secure and reliable network infrastructure is paramount – but not to just any network.

Private networks are much more secure than public networks as they are isolated from the public internet, making them less vulnerable to outside cyber threats and malware. To access a private network, they require authentication of some sort (i.e. password) and make it challenging for hackers to access data transmitted across the network. With private networks, organizations are in control of their data and where it goes.

Most private wireless networks come with network management systems (NMS) that allows employees to configure, monitor, and manage the network the device is connected to, as we discussed in our last blog post. Ensuring that the device is securely connected to the network is vital in order for the devices to communicate, especially when it serves a complex environment where uninterrupted data is essential, and is mission-critical to operations.

This is where Globalstar's XCOM RAN NMS shines, as it was designed for these types of applications: facilities with challenging environments for RF signal propagation, and facilities where the network must adapt to frequent change. With XCOM RAN NMS, one can manage network configuration, user equipment (UE), operations, and software, as well as remote radio units (RRus). On top of this, it monitors performance, sets rules for quality of service and sends alerts when faults are detected. By delivering data with optimum performance to your mission-critical network, XCOM RAN NMS enables configurability and the ability to measure your network to achieve the security and performance that your organization needs.

The Future of Security in The IoT Ecosystem

Regardless of what industry or vertical the IoT device is serving, each IoT device needs robust security to assure the data flowing into and out of them is protected, and that only those who are supposed to connect can do so. It's important to implement best practices such as data encryption and authentication to ensure that IoT data is protected as it moves through the network.

When looking at the future of security in IoT devices and how it can improve, it's important to first think about how to embed security in every single IoT device, and to do so in a way that can scale.

The main challenge to enterprises is securing communications between all their highly connected IoT devices distributed worldwide. Uniformity becomes a barrier when trying to build and establish a holistic environment, given that the IoT ecosystem in general includes a wide range of IoT devices from various a diversified set of manufacturers, that are built on diverse guidelines and communication agreements. This is where efforts within the industry from organizations such as the 3rd Generation Partnership Project (3GPP), and the GSMA come into institute what the common standards of the IoT ecosystem are.

Ultimately at the end of the day, successful deployments of IoT devices acknowledge the challenges within the IoT industry and utilize groundbreaking solutions to drive a secure, reliable and scalable IoT device ecosystem.

To learn more information about IoT security, private networks or XCOM RAN, please visit our Globalstar website, or contact our sales team here!

Thinking Differently About Private Cellular Networks

Imagine a workday without your cell phone and the public wireless networks it runs on. No apps, no social media, no login verifications. Imagine your next business trip with no maps, no digital tickets or selfies, and no playing games while waiting in line at Starbucks. Hard to imagine, isn't it?

The same thing has happened with private wireless networks. Since Robert Metcalf created Ethernet in the 1970s, private Wi-Fi networks have taken up residence in our businesses and homes, coffee shops, hotels and airports. Private networks have also adopted the same cellular technology that connects your phone, providing the reliability, performance and security of cellular standards. That has already made it essential in warehouses, factories, process plants, ports, mines and energy platforms – and its growth is set to explode.

That's because they overcome the weaknesses of Wi-Fi for business-critical applications. With 600 million Wi-Fi devices in the field, interference among adjacent Wi-Fi networks has become real problem that affects performance. That same widespread deployment has given hackers years of experience at penetrating Wi-Fi networks, as we explored in blog 6.

Cellular challenges

Private LTE/5G network deployments worldwide are set to accelerate from 4,000 in 2022 to more than 60,000 by 2028. Unlike other wireless technologies, private cellular's robust architecture provides coverage for extensive areas and supports massive device densities and multi-gigabit speeds. But private cellular struggles to deliver these benefits in some locations. Industrial spaces like warehouses, ports, and airports, as well as venues for high-density events, can be maze-like in their complexity, requiring higher signal resiliency, and reliability than conventional cellular can deliver. Take, for example, an autonomous mobile robot solution for warehouse automation. Warehouse environments are often metal and cross multiple sealed temperature zones. This creates coverage problems, and calls for multi-cell deployment. as In many deployments, robot's control and safety signals, are being blocked from one cell but cleared from another avoiding disruption of service. However, this becomes a dense deployment of cells which operates independently, creating boundaries in between. Boundaries in dense deployments mean interference at the edges, resulting in low data rates, and tricky handover. It is common to see in these settings where the device ping-pongs between few cells with incomplete handovers and that disrupts wireless connectivity. In addition, robots typically have many cameras and need to upstream the video for analytics, safety and performance reasons. All together, you end up with high interference/low-capacity system with crippling handover issues as bots move.

Cellular – but better

In our blog series, we introduced you an innovative architecture for private cellular networks. Its remote radio units (RRUs), installed throughout a facility, create a single "supercell". All radios transmit to and receive coherently with no handovers and without interfering with each other. Signal to the UE is boosted and interference minimized. Each UE in the network reaches almost peak rates, with no congestion in a single cell.

It's called XCOM RAN: a 3GPP 5G programable Radio Access Network, running on generic servers, which synchronizes and calibrates the connections with the RRUs so that all are transmitting the same information at the same time on the same frequency. Once the system is synched, it exchanges streams of data with every UE, calibrating the parameters for each one separately.

Transforming private networks

XCOM RAN offers a competitive cost for premium performance, with an entry level system cost comparable to existing DAS and small-cell solutions. Contributing to that cost are unique features of the system. Because critical processing takes place in software, it supports industry-standard RRUs and works with conventional UEs. Installation is also remarkably easy and low cost. As we discussed in our second blog on network planning, conventional private cellular networks require detailed and costly planning for coverage, capacity and interference to deliver good performance. Installation of XCOM RAN is far simpler. Because it operates as a single supercell, XCOM RAN scales with the number of RRUs deployed. If a new application requires more coverage or capacity, you simply add more radios and the server capacity will increase accordingly. All with the security you expect from cellular industry standards.

Like most private wireless networks, XCOM RAN provides a network management system to simplify configuration, monitoring and management. What sets it apart is the degree of granular control it delivers to maintain best performance as conditions change. The NMS can measure and display over 300 3GPP-defined metrics and compare with them KPIs. Statistics on aggregate cell levels give you the 50,000-foot view of capacity – and its supercell design means that data tells a big story.

Business journalists and consultants have been writing about the digital transformation of business since – well, it feels like forever. And there has been a lot to write about in recent decades. But the breakthroughs that matter seldom begin with strategy, finance or market reach. They start with thinking differently about the problem and finding a better solution than anyone else could. That's private networks with XCOM RAN – and why customers come to find they can't imagine operating without it.

Learn how it can provide the foundation for your own digital transformation at the Globalstar website.

Where Can You Go from Here?

Every high-demand, business-critical application is unique. It comes with its own requirements for total capacity, coverage, reliability and performance. We invite you to share your requirements with us and learn what price-performance advantages XCOM RAN can offer over the life of your network. You may discover the next step in the evolution of your business.

To learn more about how Globalstar can benefit your business, contact us at salesinfo@globalstar.com or visit www.globalstar.com.

Globalstar