Leveraging Public Networks to Compliment Delivery of High-Performance Private Networks

A technical paper prepared for presentation at SCTE TechExpo24

Kamaljit Bal
WPN Architect, Enterprise Customer Solutions
Rogers Communications Inc.
Kamaljit.bal@rci.rogers.com

Table of Contents

List of Figures

1. Introduction

In today's digital age, seamless and reliable wireless connectivity is paramount for enterprises across various industries. The proliferation of Internet of Things (IoT) devices, the growth of mobile and remote workforces, and the increasing reliance on cloud-based applications and services necessitate robust and high-performance communication networks. High-performance wireless private networks (HPWPNs) have emerged as a vital solution, offering dedicated resources, enhanced security, and tailored performance to meet specific business requirements. However, these private networks face significant challenges, including limited coverage, scalability issues, high costs, and security concerns.

The advent of advanced public network technologies, such as 5G, Wi-Fi 6, and future innovations like Wi-Fi 7, presents a unique opportunity to address these challenges. Public networks offer extensive coverage, high capacity, and ongoing technological enhancements, making them a valuable complement to HPWPNs. By strategically integrating public networks, enterprises can create a hybrid network model that leverages the strengths of both public and private networks, maximizing performance, reliability, and cost-efficiency.

2. Challenges in Current HPWPNs

High-Performance Wireless Private Networks (HPWPNs) provide essential connectivity solutions tailored to specific business needs. However, these networks face several significant challenges that can impede their effectiveness and scalability. Below are the primary challenges:

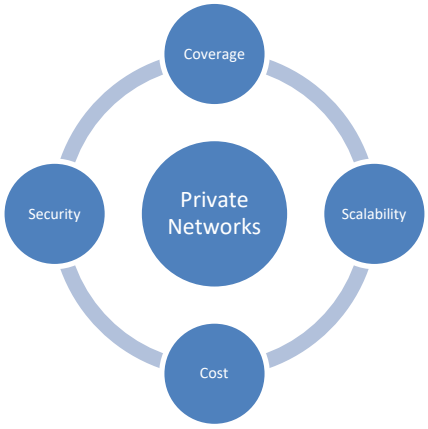

Figure 1- Challenges in Current HPWPNs

2.1. Limited Coverage

Private networks are commonly designed to serve specific, localized areas similar as commercial premises, artificial installations, or designated civic zones. Extending these networks beyond their original boundaries presents significant logistical and fiscal challenges. Expanding content requires substantial investment in structure, including fresh base stations, repeaters, and expansive cabling. For enterprises with geographically dispersed operations or those seeking to give content in remote or underserved areas, this expansion is frequently impracticable and cost- prohibitive. The limited content of HPWPNs can hamper business operations that calculate on wide- area connectivity, similar as force chain logistics, remote monitoring, and field services.

2.2. Scalability Issues

As businesses expand and the number of connected devices increases, extending HPWPNs to accommodate this growth can become increasingly complex and costly. Each new device demands a portion of the network's bandwidth, as well as security measures and operational resources. This surge in demand can lead to potential bottlenecks and performance degradation. The dynamic nature of modern business environments, where the number of connected devices can fluctuate significantly, further complicates scalability. Additionally, the introduction of new technologies and applications may necessitate substantial upgrades to the existing network infrastructure, adding to the complexity and expense.

2.3. Cost Constraints

The deployment and maintenance of a dedicated private network involve substantial capital expenditures and ongoing operational costs. Initial investments include the purchase of hardware, software, and other necessary equipment. Additionally, there are costs associated with installation, configuration, and integration with existing systems. Operational costs encompass routine maintenance, updates, and the salaries of skilled personnel needed to manage the network. For small to medium-sized enterprises (SMEs), these costs can be particularly burdensome.

2.4. Security Enterprises

While private networks offer enhanced security through dedicated resources and control, they are not immune to threats. Ensuring robust security measures such as encryption, intrusion detection, and access control is essential to protect sensitive data and maintain network integrity. However, integrating public networks to expand coverage and improve scalability introduces new vulnerabilities that must be addressed. The hybrid nature of these networks can create complex security landscapes where the risk of unauthorized access, data breaches, and other cyber threats is heightened. Enterprises must implement comprehensive security strategies that address both the private and public aspects of their networks, requiring ongoing vigilance, advanced security tools, and skilled personnel to manage and mitigate risks.

2.5. Regulatory

The 5G spectrum allocation and licensing are still not completed in many countries. This hampers the final design and deployment of several potent solutions that are ready for the market. Also, there is a significant price for the usage of a dedicated spectrum.

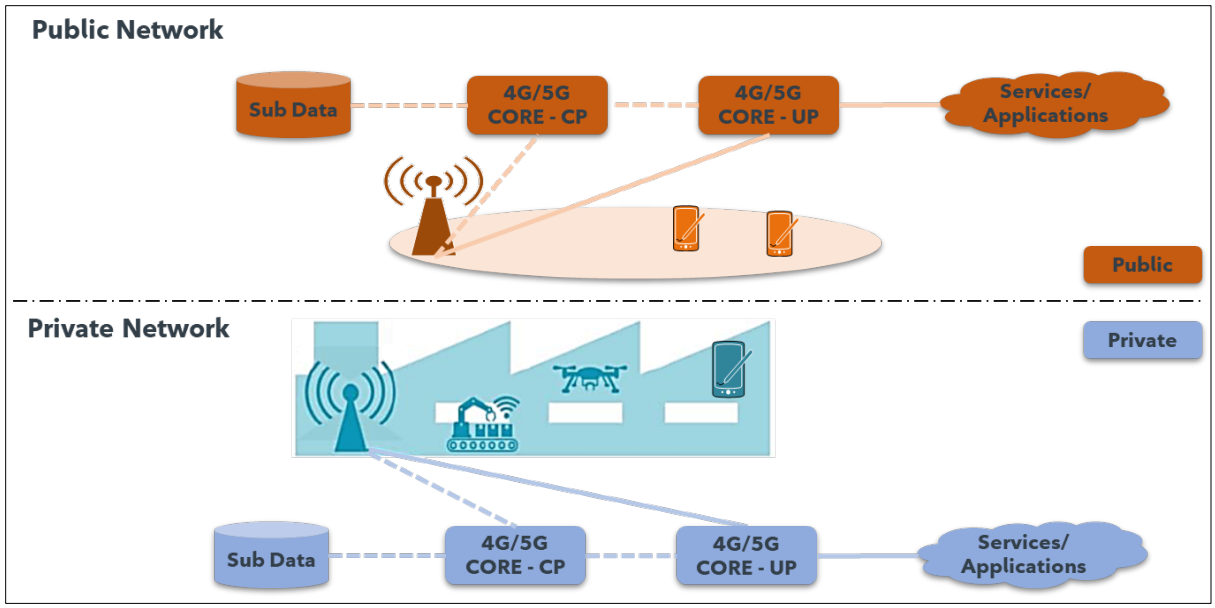

Figure 2- Independent Network

3. Benefits of Integrating Public Networks

3.1. Expanded Coverage

Public networks, particularly those powered by 5G and advanced Wi-Fi technologies, offer extensive coverage that can complement the limited reach of private networks. This integration allows enterprises to extend connectivity to remote locations, field operations, and mobile workforces without significant infrastructure investment.

3.2. Improved Redundancy and Reliability

Combining public and private networks enhances redundancy, ensuring continuous connectivity. In the event of a private network failure, traffic can be seamlessly rerouted through public networks, minimizing downtime, and maintaining operational continuity.

3.3. Cost Efficiency

Utilizing existing public network infrastructure reduces the need for extensive capital expenditure on private network expansion. Enterprises can leverage the scalability and reach of public networks, paying only for the resources they consume, thus optimizing operational costs.

3.4. Enhanced Scalability

Public networks are designed to handle large volumes of traffic and a high number of connected devices. By integrating these networks, enterprises can scale their operations more efficiently, accommodating growth without significant changes to their infrastructure.

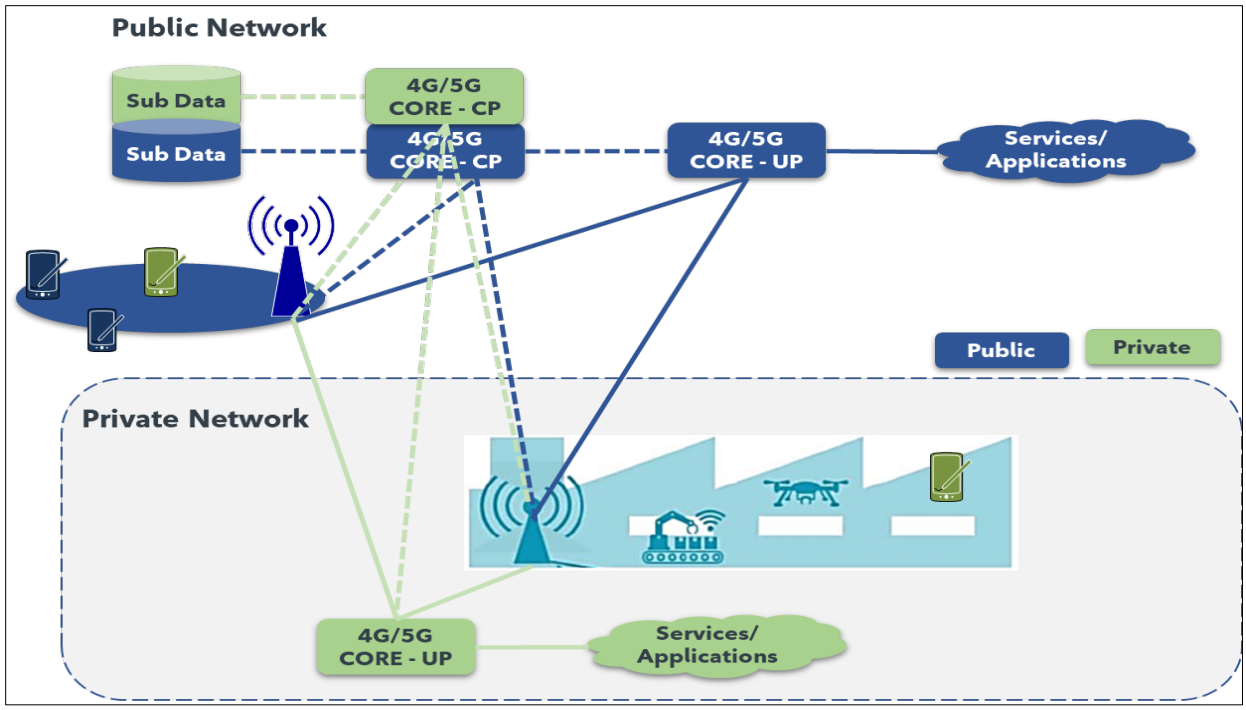

Figure 3- Integrated Network

4. Technological Advancements Facilitating Integration

Integrating public networks with high-performance wireless private networks (HPWPNs) requires leveraging several technological advancements to ensure seamless, secure, and efficient connectivity. The evolution of these technologies has enabled businesses to overcome challenges related to network integration and enhance their overall network performance. Here's an expanded look at key technological advancements facilitating this integration:

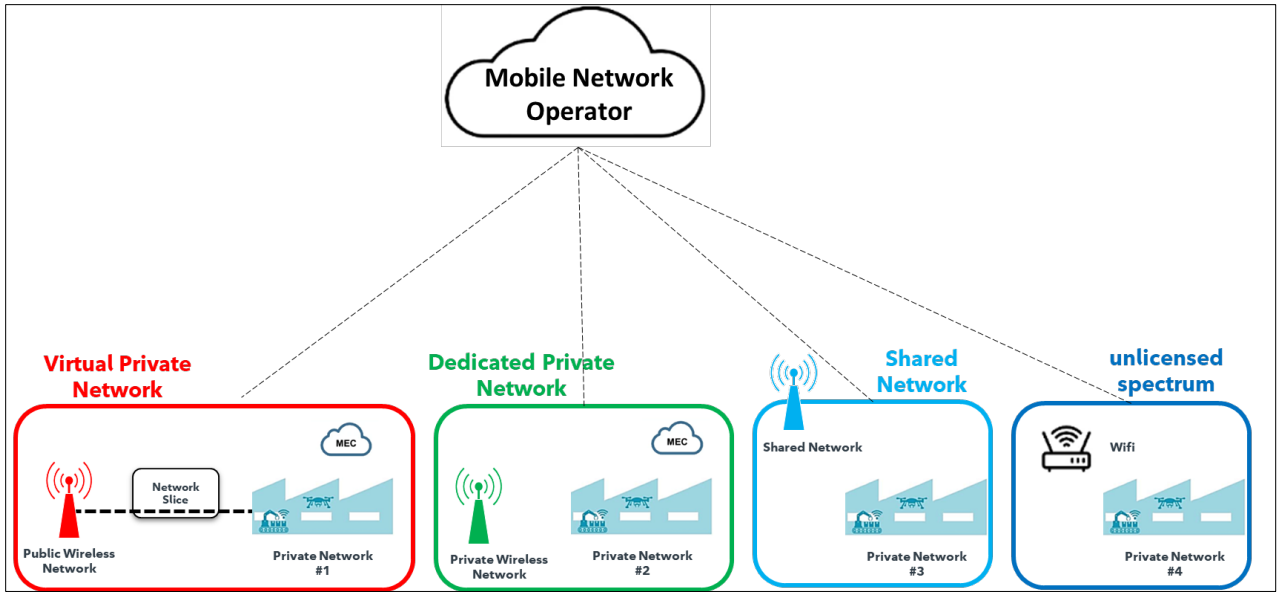

Figure 4- Integrated and efficient network landscape.

4.1. 5G Technology

The fifth generation of mobile networks brings substantial advancements compared to its predecessors in terms of speed, latency, and capacity. One of its key features is its ability to provide extremely high data transfer rates and ultra-low latency, which are crucial for enabling real-time applications and services. Additionally, 5G supports a massive number of connected devices simultaneously, a capability that is essential for the Internet of Things (IoT) and the development of smart environments. Another significant feature is network slicing, which allows for the creation of multiple virtual networks within a single physical 5G network, thereby offering tailored services for various applications.

The integration of 5G technology offers numerous benefits. It enhances the performance of both public and private networks, leading to faster and more reliable connectivity. Furthermore, 5G facilitates the seamless incorporation of IoT devices into these networks, enabling advanced use cases and smart applications. The technology also supports flexible network management through network slicing, allowing organizations to design virtual networks with specific attributes to address diverse business needs and integrate effectively with private network requirements.

4.2. Wi-Fi 6 and Wi-Fi 7

Wi-Fi 6 (802.11ax) and the forthcoming Wi-Fi 7 (802.11be) represent the latest advancements in Wi-Fi technology, delivering significant improvements in performance and efficiency. Wi-Fi 6 enhances data rates and capacity compared to previous Wi-Fi standards, while Wi-Fi 7 is expected to offer even greater advancements. Both technologies feature increased throughput, with Wi-Fi 6 incorporating innovations such as Orthogonal Frequency Division Multiple Access (OFDMA) and Target Wake Time (TWT) to boost network efficiency and reduce latency. Additionally, they offer improved performance in environments with a high density of connected devices, such as offices and public spaces.

For integration, these Wi-Fi technologies offer several benefits. They provide high-speed and reliable wireless connectivity that complements private networks. The enhanced network efficiency afforded by these technologies helps improve overall performance and reduces congestion in hybrid network environments. Wi-Fi 6 and Wi-Fi 7 are also particularly effective in high-density areas, such as airports and shipping yards, where many devices are connected simultaneously, ensuring effective and reliable connectivity.

4.3. Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is an innovative network architecture approach that enables centralized management of network resources and traffic. It operates by providing a centralized control plane that manages network traffic and policies, distinctly separate from the data plane. This architecture allows for the dynamic configuration of network resources and policies through software applications, offering substantial programmability. Additionally, SDN provides flexibility and agility, allowing for rapid adjustments to network configurations and optimizations based on real-time requirements.

In terms of integration, SDN offers several notable benefits. It facilitates the dynamic management of both public and private networks by enabling the reconfiguration and optimization of network resources in response to changing needs. This capability improves visibility into network performance and traffic, which is valuable for troubleshooting and management purposes. Moreover, SDN supports the integration of diverse network technologies and services, enhancing the overall flexibility and adaptability of hybrid networks.

4.4. Network Functions Virtualization (NFV)

Network Functions Virtualization (NFV) is a network architecture concept that leverages virtualization technologies to implement network functions as software applications running on standard hardware. This approach enables the deployment of network functions such as firewalls, load balancers, and routers as virtualized software instances. NFV enhances resource efficiency by reducing the need for dedicated hardware and optimizing resource use through virtualization. Additionally, it provides scalability, allowing network functions to be easily scaled up or down according to demand.

The integration of NFV brings several benefits. It reduces the cost of deploying and managing network functions by utilizing standard hardware and virtualization technologies. NFV also facilitates the integration of public and private network functions through the flexible and dynamic deployment of virtualized services. Furthermore, it accelerates the deployment of new network services and functions, supporting quicker adaptation to evolving business needs.

4.5. Edge Computing

Edge computing focuses on processing data closer to its source rather than relying solely on centralized cloud data centers. This approach minimizes latency by processing data locally at the edge of the network. It also optimizes bandwidth usage by reducing the amount of data transmitted to central data centers and supports real-time data processing and analytics for applications that require immediate responses.

The benefits of integrating edge computing include improved performance for applications and services by processing data nearer to the source, which reduces latency and enhances responsiveness. It also facilitates efficient data handling by decreasing the load on central networks and cloud services. Additionally, edge computing supports the integration of IoT devices and applications by providing local processing capabilities, thus reducing reliance on centralized resources.

4.6. Advanced Security Technologies

Advanced security technologies, including next-generation firewalls (NGFWs), Security Information and Event Management (SIEM) systems, and threat intelligence platforms, are designed to enhance network security. NGFWs offer advanced threat detection and prevention capabilities, including deep packet inspection and application awareness. SIEM systems collect and analyze security event data from various sources, providing insights into potential threats and incidents. Threat intelligence platforms utilize threat intelligence feeds to stay informed about emerging threats and vulnerabilities.

The integration of advanced security technologies brings several benefits. It enhances network protection by providing sophisticated threat detection, prevention, and response capabilities. These technologies also offer comprehensive visibility into network security events and potential threats, aiding in proactive management. Moreover, they support adaptive security measures based on real-time threat intelligence and analytics, thereby enhancing overall network protection.

5. Implementation Strategies

Implementing a hybrid network model that leverages public networks to complement high-performance wireless private networks (HPWPNs) requires a well-planned and structured approach. This section outlines the key strategies and phases involved in successfully integrating public networks with HPWPNs, ensuring enhanced performance, reliability, and security.

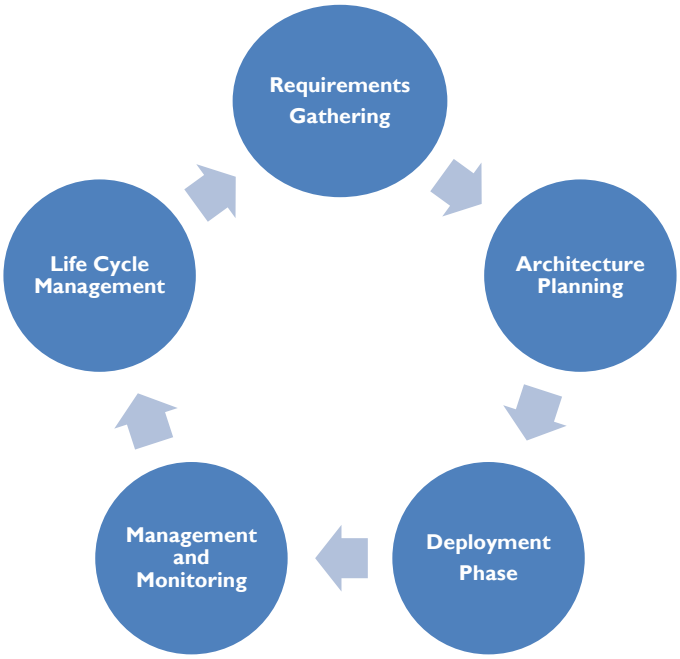

Figure 5- Implementation Strategy

5.1. Architecture Design

A well-designed network architecture is the foundation of a successful hybrid network. The architecture should seamlessly integrate public and private network components, optimizing the strengths of each.

- **Network Topology**: Define the physical and logical layout of the network, detailing how public and private networks will interconnect. This includes the placement of base stations, access points, and edge devices to ensure optimal coverage and performance.
- **Integration Points**: Identify and plan the integration points between public and private networks. These points will manage traffic flow, ensuring seamless handoff between networks and maintaining performance and security standards.
- **Hybrid Infrastructure**: Develop a hybrid infrastructure that leverages both private network capabilities for critical applications and public network resources for extended coverage and scalability. This includes using technologies like network slicing to allocate resources dynamically based on application needs.
- **Security Framework**: Establish a robust security framework that encompasses both public and private networks. This includes implementing encryption, access control, and intrusion detection systems to protect data and network integrity.

5.2. Deployment Phases

The deployment of a hybrid network should be carried out in carefully planned phases to ensure smooth integration and minimize disruptions.

- **Assessment Phase**: Conduct a thorough assessment of the existing network infrastructure and identify areas where public network integration can enhance performance and coverage. This phase

includes evaluating current network performance, identifying bottlenecks, and determining the specific requirements of various applications and services.

- **Pilot Deployment**: Implement a small-scale pilot deployment to test the integration strategies. This phase allows for the identification and resolution of potential issues before full-scale deployment. Pilot deployments should include a representative subset of the overall network, including critical applications and diverse geographic locations.
- **Full Deployment**: Roll out the hybrid network across the entire enterprise, following the lessons learned from the pilot phase. This phase should be carefully managed to ensure minimal disruption to ongoing operations. A phased approach, starting with less critical areas and gradually integrating more vital parts of the network, can help manage risks.
- **Post-Deployment Review**: After full deployment, conduct a comprehensive review to evaluate the performance, reliability, and security of the hybrid network. This review should include feedback from users, performance metrics analysis, and security audits to ensure the network meets all objectives.

5.3. Management and Monitoring

Effective management and monitoring are essential to maintaining the performance, reliability, and security of a hybrid network. Implementing advanced tools and strategies can help enterprises achieve these goals.

- **Centralized Management**: Use a unified management platform to oversee both public and private network components. This platform should provide a single interface for monitoring, configuration, and management, simplifying administrative tasks and improving visibility.
- **Real-Time Monitoring**: Deploy advanced monitoring tools that provide real-time insights into network performance, usage patterns, and potential issues. These tools should offer capabilities such as traffic analysis, performance metrics, and alerting for anomalies.
- **Performance Analytics**: Utilize performance analytics to identify trends, optimize resource allocation, and improve network performance. Analytics can help in making data-driven decisions, such as adjusting network configurations, reallocating resources, or upgrading infrastructure.
- **Security Monitoring**: Implement continuous security monitoring to detect and respond to potential threats promptly. This includes using intrusion detection systems (IDS), security information and event management (SIEM) solutions, and automated response mechanisms to mitigate risks.
- **Automated Management**: Leverage automation tools for routine management tasks, such as network configuration, software updates, and performance optimization. Automation reduces the workload on IT staff, minimizes human error, and ensures consistent network performance.

6. Use Cases

6.1. Connected Cars

The connected car ecosystem relies on seamless, high-performance connectivity to enable various advanced features and services. Integrating public networks with high-performance wireless private networks (HPWPNs) can significantly enhance the functionality and safety of connected vehicles.

- **Vehicle-to-Everything (V2X) Communication**: V2X communication includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) interactions. Hybrid networks facilitate real-time communication between vehicles and surrounding infrastructure, improving traffic safety, reducing accidents, and enhancing traffic flow through features like collision avoidance and adaptive traffic signals.

- **Real-Time Navigation and Traffic Updates**: Connected cars require continuous updates on traffic conditions, road closures, and navigation. Hybrid networks ensure reliable, high-speed data transmission for real-time navigation services, improving route planning and reducing travel time.
- **Autonomous Vehicles**: Autonomous vehicles depend on high-bandwidth, low-latency communication for sensor data processing and decision-making. Hybrid networks provide the necessary connectivity to support the data needs of autonomous vehicles, including real-time communication with other vehicles and cloud-based processing.
- **Remote Diagnostics and Over-the-Air (OTA) Updates**: Connected cars can benefit from remote diagnostics and OTA updates, reducing the need for physical service visits. Hybrid networks facilitate the secure and efficient transmission of diagnostic data and software updates, enhancing vehicle maintenance and performance.
- **Fleet Management**: For commercial fleets, hybrid networks enable real-time monitoring and management of vehicle performance, location, and driver behavior. This improves fleet efficiency, reduces operational costs, and enhances safety through features like route optimization and predictive maintenance.

6.2. Transportation

The transportation sector benefits significantly from the integration of public and private networks, enhancing efficiency, safety, and customer experience across various modes of transport.

- **Intelligent Transportation Systems (ITS)**: ITS applications use data from various sources, including traffic sensors, cameras, and GPS, to optimize traffic flow and reduce congestion. Hybrid networks provide the connectivity needed for real-time data integration and analysis, supporting dynamic traffic management and improved commuter experience.
- **Public Transit Management**: Public transportation systems rely on real-time data for scheduling, routing, and passenger information. Hybrid networks enable seamless communication between transit vehicles, control centers, and passenger information systems, improving service reliability and passenger satisfaction.
- **Cargo and Freight Tracking**: The transportation of cargo and freight involves tracking and monitoring throughout the journey. Hybrid networks facilitate real-time tracking of shipments, optimizing logistics, and providing visibility to shippers and recipients. This improves supply chain efficiency and reduces delays.
- **Smart Ticketing Systems**: Smart ticketing systems use mobile apps and contactless payment methods to streamline the ticketing process for passengers. Hybrid networks ensure reliable connectivity for real-time transaction processing, ticket validation, and account management.
- **Fleet Management and Optimization**: Fleet management systems use GPS and telematics to monitor and optimize the performance of transportation fleets. Hybrid networks support real-time data transmission for fleet tracking, route optimization, and maintenance scheduling, improving operational efficiency and reducing costs.

6.3. Industrial IoT (IIoT)

The industrial sector can significantly benefit from the hybrid network model, which supports the connectivity needs of complex and large-scale operations, improving efficiency, safety, and productivity.

- **Manufacturing**: Smart factories use interconnected machinery, robotics, and sensors to automate and optimize production processes. Hybrid networks ensure seamless communication between devices, enabling real-time monitoring, predictive maintenance, and immediate response to anomalies.

- **Supply Chain Management**: Tracking goods throughout the supply chain requires extensive connectivity, from warehouses to transportation networks. A hybrid network provides continuous coverage and reliable data transmission, enhancing visibility and management of the supply chain.
- **Remote Monitoring and Control**: Industrial facilities often have remote or hazardous areas that require monitoring and control. Integrating public networks with private networks extends connectivity to these areas, allowing for real-time data collection and remote operations, improving safety and efficiency.
- **Energy Management**: Industrial IoT applications monitor and manage energy consumption and optimize usage patterns. Hybrid networks facilitate the transmission of energy usage data from various sensors and meters to central management systems, enabling effective energy management.

6.4. Smart Cities

Smart cities rely on a multitude of interconnected devices and applications to improve urban living and enhance operational efficiencies. The hybrid network model can support the vast and varied connectivity needs of smart cities by providing robust and scalable network infrastructure.

- **Traffic Management**: Real-time traffic monitoring and management systems require seamless connectivity across wide urban areas. Integrating public networks with private networks ensures reliable data transmission from traffic sensors, cameras, and IoT devices, enabling dynamic traffic control and reducing congestion.
- **Public Safety**: Smart cities deploy numerous surveillance cameras, emergency response systems, and public alert systems. A hybrid network ensures uninterrupted connectivity for these critical systems, providing real-time data to law enforcement and emergency services.
- **Environmental Monitoring**: Sensors deployed across cities to monitor air quality, noise levels, and water quality need reliable connectivity to transmit data to central systems for analysis and action. Hybrid networks extend coverage to all sensor locations, ensuring consistent data flow.
- **Smart Lighting**: Connected streetlights equipped with sensors can adjust brightness based on traffic and pedestrian activity, reducing energy consumption. Hybrid networks provide the necessary bandwidth and reliability for real-time adjustments and remote management.

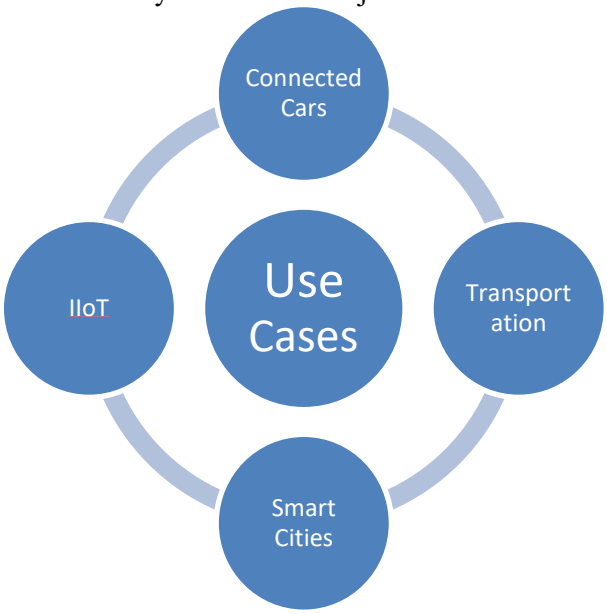

Figure 6- Use Cases

7. Security Considerations

In the context of integrating public networks with high-performance wireless private networks (HPWPNs), ensuring robust security is paramount. The hybrid network model introduces both opportunities and challenges in maintaining the confidentiality, integrity, and availability of data. Here are several key security considerations:

Figure 7- Security Considerations

7.1. Data Encryption

Data encryption involves converting data into a code to prevent unauthorized access and is essential for safeguarding data transmitted over both public and private networks. Its benefits include ensuring data confidentiality, which means sensitive information is only accessible to authorized users, thereby preventing data breaches and leaks. Additionally, data encryption aids in compliance with regulatory requirements such as GDPR, HIPAA, and other data privacy laws, and protects data integrity by safeguarding it from unauthorized modifications during transmission, thus maintaining its accuracy and reliability.

To implement data encryption effectively, one should use strong encryption protocols like AES (Advanced Encryption Standard) for data at rest and TLS (Transport Layer Security) for data in transit. End-to-end encryption should be applied from the data source to its destination to ensure protection throughout the entire transmission process. Robust key management practices, including regular key rotations and secure storage, are also crucial.

7.2. Network Segmentation

Network segmentation involves dividing a network into smaller, isolated segments to enhance security and control access. This practice has several benefits, including reducing the attack surface by isolating critical systems and data, enhancing control over network traffic and access, and containing security incidents within specific segments to prevent them from spreading across the entire network.

Effective network segmentation can be achieved by segregating public and private traffic using VLANs (Virtual Local Area Networks) or subnets. Implementing Access Control Lists (ACLs) helps control traffic flow between segments and enforce security policies. Deploying firewalls at segmentation points is also essential for monitoring and filtering traffic between network segments.

7.3. Access Control and Authentication

Access control and authentication mechanisms are vital for ensuring that only authorized users and devices can access network resources. These mechanisms prevent unauthorized access, track, and monitor user activity for accountability, and minimize the risk of insider threats and unauthorized access due to compromised credentials.

To implement robust access control, one should use Multi-Factor Authentication (MFA) to add an extra layer of security beyond traditional username and password combinations. Role-Based Access Control (RBAC) should be implemented to grant access based on user roles and responsibilities, ensuring that users only access necessary resources. Regular reviews of access permissions are also necessary to ensure they align with current user roles and responsibilities.

7.4. Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection and Prevention Systems (IDPS) are technologies designed to monitor network traffic for signs of malicious activity and respond to potential threats. The benefits of IDPS include early detection of suspicious activities or potential security breaches, automated threat mitigation actions, and enhanced visibility into network activity and vulnerabilities.

For effective implementation, network-based IDPS should be deployed to monitor traffic across the entire network, while host-based IDPS should be used on critical servers and devices to detect system-level threats. Keeping IDPS signatures and rules updated is crucial to protect against the latest threats and vulnerabilities.

7.5. Secure Integration Points

Secure integration points involve protecting interfaces and connections between public and private networks to prevent unauthorized access and data breaches. This approach minimizes vulnerabilities by applying stringent security measures, controls data flow securely, and maintains consistent security policies across all integration points.

To secure integration points, use secure APIs with authentication and encryption for managing data exchange between networks. Data masking techniques should be applied to hide sensitive information during integration processes. Regular security audits of integration points are necessary to identify and address potential vulnerabilities.

7.6. Incident Response and Recovery

Incident response and recovery are critical for preparing for, detecting, and responding to security incidents to minimize their impact and restore normal operations. Effective incident response reduces the damage caused by incidents, ensures faster recovery of affected systems, and improves preparedness for future incidents through lessons learned and continuous improvement.

Implementing incident response involves developing and maintaining a comprehensive incident response plan that outlines procedures for detecting, responding to, and recovering from incidents. Regular drills should be conducted to test the plan's effectiveness and improve readiness. Post-incident analysis is essential to identify root causes, assess impact, and implement improvements to prevent recurrence.

7.7. Compliance and Governance

Compliance and governance involve adhering to legal, regulatory, and industry standards related to data protection and network security. The benefits include ensuring regulatory adherence, managing security risks through best practices and standards, and building trust with customers and stakeholders by demonstrating a commitment to security and compliance.

To ensure compliance and governance, adopt industry standards and frameworks such as ISO/IEC 27001, and NIST. Conduct regular security audits and assessments to ensure regulatory compliance and identify areas for improvement. Additionally, maintain thorough documentation of security policies, procedures, and compliance efforts, and provide regular reports to relevant stakeholders.

8. Conclusion

Leveraging public networks to complement high-performance wireless private networks (HPWPNs) offers an effective strategy for addressing key challenges in today's technological landscape. This hybrid approach enhances connectivity, performance, and reliability by integrating the strengths of both public and private networks, effectively tackling issues related to coverage, scalability, and cost.

- **Coverage and Scalability**: Public networks, such as 5G and advanced Wi-Fi, provide broad coverage and high capacity, bridging gaps in areas where private networks fall short. Private networks offer customized performance and control, and combining these with public networks helps achieve extensive coverage and scalability at a lower cost.
- **Cost Efficiency**: Integrating public networks reduces the capital and operational expenses associated with maintaining a private network. This hybrid model balances the high performance of private networks with the extensive coverage of public networks, optimizing resource use and minimizing costs.
- **Technological Advancements**: Utilizing cutting-edge technologies like 5G, Wi-Fi 6, and edge computing enhances network performance. This approach not only addresses current demands but also prepares enterprises for future innovations, ensuring long-term relevance and competitiveness.
- **Security Measures**: A robust security framework is crucial for protecting data across both public and private networks. Implementing advanced security measures, such as encryption and intrusion detection, ensures network integrity and resilience against potential threats.
- **Meeting Modern Demands**: The hybrid network model supports the connectivity needs of modern applications, including IoT and real-time services. It improves operational efficiency by providing scalable and reliable connectivity solutions.
- **Future Opportunities**: Adopting a hybrid network approach positions enterprises to leverage future technological advancements and maintain a strategic edge in a dynamic market. It supports

growth and adaptability, allowing organizations to meet evolving business needs and navigate future challenges effectively.

In summary, integrating public networks with HPWPNs provides a comprehensive solution to coverage, scalability, and cost challenges. By embracing technological advancements and strengthening security, enterprises can achieve a hybrid network model that enhances performance and reliability, positions them for future success, and ensures they are prepared for the evolving demands of a digital world.

Abbreviations

LTE	Long Term Evolution
IoT	Internet of Things
MNO	Mobile Network Operator
IIOT	Industrial Internet of Things
HPWPNs	High-performance wireless private networks
PTT	Push to talk
UE	User Equipment
SMEs	medium- sized enterprises
OFDMA	Orthogonal Frequency Division Multiple Access
TWT	Target Wake Time
LAN	Local Area Network
SDN	Software-Defined Networking
NFV	Network Functions Virtualization
NGFWs	next-generation firewalls
SIEM	Security Information and Event Management
IDS	intrusion detection systems
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
OTA	Over-the-Air
ITS	Intelligent Transportation Systems
AES	Advanced Encryption Standard
TLS	Transport Layer Security
VLANs	Virtual Local Area Networks
ACLs	Access Control Lists
MFA	Multi-Factor Authentication
RBAC	Role-Based Access Control
IDPS	Intrusion Detection and Prevention Systems
GDPR	General Data Protection Regulation
APIs	Application Programming Interfaces
HIPAA	Health Insurance Portability and Accountability Act
SCTE	Society of Cable Telecommunications Engineers