This document continues to explore the key trends and capabilities of microwave communication technologies and how they meet the expectations of the telecommunication industry following 5G deployments around the world. There is also continuing interest in using microwave technology in many enterprise applications such as city and industrial scenarios.
Introduction

Data recorded by network service providers across Europe and North America between February and September 2020 (Figure 3) highlighted that many networks experienced a year’s worth of traffic growth (30–50 percent) in just a few weeks, as COVID-19 lockdown measures were implemented. By September, the data indicated that traffic had stabilized at 20–30 percent above pre-pandemic levels. However, the conundrum for service providers is how much capacity they should engineer into their networks to cover similar scenarios in the future.

The COVID-19 pandemic highlighted the crucial role of residential broadband connectivity. Thanks to the agility and immediate actions of service providers and cloud operators, most people in lockdown were able to use their network connections to work, play, socialize and support others. The challenge for service providers today is to find ways to improve the overall network resilience and offer tailored work, play and connect packages.

In this new environment security has never been more important. In situations such as the pandemic where broadband connectivity is an essential service, protecting network infrastructure and services becomes critical. Service providers will need to find better and more cost-effective ways to detect and minimize new forms of denial of service (DDoS) attacks that may go undetected or unmitigated by legacy security tools and approaches.

The network topology evolution

The continuous increase in the capacity of mobile networks is causing a densification of RAN sites and an increase in the usage of higher frequencies. Consequently, the average length of backhaul links is decreasing. For example, across Nokia’s 5G deployments 40 percent of microwave links are shorter than 4 km.

There is an increase of star topologies, with a high number of microwave links terminating at a single fibre point of presence (PoP) and a reduction in the number of links in cascade (typically 2 or 3 hops). In an urban environment, the traffic generated in a RAN site is about 3–4 Gbps, so, the required backhaul capacity is typically 10 Gbps, while in a suburban area, 5 Gbps is sufficient.

In summary, microwave links are evolving towards shorter links, higher capacity and very high density.

To reduce the global microwave mobile backhaul’s Total Cost of Ownership (TCO), site costs optimization is a key factor. Especially in dense areas, it becomes difficult for operators to find new sites. So, one of the major goals for CSP’s is to remove the indoor equipment and deploy Zero Footprint (ZFP) all-outdoor solutions. In outdoor scenarios, costs are mainly dependant on the number and size of the Outdoor Units (ODU) and antennas.

Multiband Carrier Aggregation, e.g. combining traditional bands with E-Band, also in ZFP, is a very attractive solution to cope with the tremendous capacity increase demand. In Figure 1 a ZFP multiband system is shown with a dual band antenna, one outdoor supporting 2 carriers in a traditional frequency band and the other one in E-Band.
Figure 1: 10G 3+0 configuration E-Band + traditional band (XPIC supported)

Compact dual band solutions with dual band antennas are also available in traditional frequency bands, for example one ODU supporting two different frequency bands (e.g. 11 and 13 GHz, see Figure 2)

Figure 2: 11+32 GHz: one ODU, one antenna

Full outdoor solutions are increasingly popular at tail sites, however, the Split Mount system, i.e. mixing IDU and ODU, is still frequently the preferred solution at nodal sites. Additionally, there are several reasons in favour of an IDU, even in 5G last mile backhauling sites.

These include:
- Easy physical access and maintenance operations of the RAN baseband and the Transport equipment
- In the presence of legacy TDM signals (such as E1 or DS1), normally not managed directly by a full outdoor transport node
- Operators may prefer to power the ODU directly from the IDU via Power over Ethernet or via a power cable, relying on EMI/EMC protection directly integrated in the IDU.
- To manage highest scalability of radio directions

In summary, the key features of an indoor unit are:
- Compactness and low cost
- High throughput and high scalability on the number of radio directions and/or in general on the number of ports
- Low maintenance efforts and temperature hardening

The new generation of so-called “pizza box” IDUs are often the preferred choice for operators wanting to match the low cost and reduced maintenance of these fan-less units with the flexibility required in the tail and small nodal applications.
Microwave long haul solutions for a rural environment

The global pandemic has created a challenge for corporations as well as schools to enable work from home and virtual learning. This has had a direct impact on a network’s ability to provide the required bandwidth for teleworking, virtual learning for schools, and telemedicine. This need for bandwidth has meant that operators have had to invest and modernize their rural connections to meet these new demands.

Figure 3: Networks in 2020 – Key statistics

First weeks of lockdown compared to the previous week:

- **30–50% increase in network traffic**
- **50–100% increase in Netflix traffic**
- **350–700% increase in videoconferencing traffic**
- **100–150% increase in gaming traffic**

One month into lockdown:

- **40% increase in DDoS attacks**
- **100%+ increase in peering traffic as on-net caches reached their capacity**

Six months into the pandemic:

- Traffic levels stabilize at 20–30% above pre-pandemic levels

(Source: Nokia Deepfield 2020 Report)

High Capacity

High-capacity in rural networks can be achieved but is perhaps not as straightforward as for urban or suburban networks where a high bandwidth can be achieved with a high frequency and large channel size microwave link. Spectrum regulators have opened the traditional long-haul bands (i.e. 6, 7, 8, 11 GHz) to larger channels sizes such as 60 MHz and 80 MHz in 6 GHz and 11 GHz respectively. However, there are necessary tradeoffs between large channels and the distance required for rural links. To achieve high-capacity links over longer distances a solution is to “stack” channels and make use of carrier aggregation as previously described. The latest generation of microwave long-haul transceivers can support carrier aggregation with a flexible range of frequencies and channel sizes. This flexibility provides operators with deployment agility when certain channels may not be available.
Reliability

In rural areas, the long-haul microwave system is often a lifeline to these communities and therefore the network must be dependable not only in terms of the hardware reliability but also for path reliability. For this reason, these systems must support hardware protection schemes. However, many customers are opting for N+0 vs traditional 1+1 protection to increase capacity without also increasing costs. In the case of a hardware failure, services will be scaled per the quality-of-service setting, allowing the highest priority services to pass over the remaining hardware transceivers. This can be achieved with a second receiver allowing a combining functionality without the cost of an additional transceiver. This integrated function allows for long paths when diversity is needed and provides up to 3dB more system gain in non-faded conditions.

Figure 4: The most popular applications of long-haul microwave in extreme climate conditions

Focus on RF spectrum: Challenges for 6 GHz

Spectrum Regulators have recently opened the 6 GHz band for unlicensed use. This band is critical for rural long-haul links and some mobile operators have been concerned that the use of this band for Wi-Fi will cause harmful inference to fixed wireless links. Independent studies have shown that a single Wi-Fi router could cause some degradation of a fixed wireless link performance almost 9 kms away. The question is what can be done to combat these frequency issues. One solution is the use of 6+11 GHz in a carrier aggregation configuration. This system coupled with a dual band 6/11 GHz antenna provides an excellent solution to offset any possible interference conditions by using the 11 GHz as both frequency protection and additional capacity. A study performed by Nokia in Las Vegas and Miami has shown that 11 GHz can perform as well with the same capacity as a 6 GHz link.
It is now well known that the 6 GHz band (5925-6425 MHz & 6425-7125 MHz) band known as 6L and 6U and traditionally used mainly for microwave long-haul applications, has been the subject of interest for both Wi-Fi systems and IMT applications. Recently, the whole band has been released for Wi-Fi applications in some countries, provided that incumbent systems are not impacted.

While the IMT ecosystem will discuss these issues at WR23, the Wi-Fi ecosystem has already moved on. Figure 6 highlights the current status. For the sake of simplicity, only two Wi-Fi modes of operation are shown: Indoor and Indoor/Outdoor, without considering other variants with differing power levels and protection methods foreseen or under study.

**Figure 6: The Wi-Fi ecosystem**

<table>
<thead>
<tr>
<th></th>
<th>Indoor</th>
<th>Indoor/Outdoor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Implemented</td>
<td>Planned</td>
</tr>
<tr>
<td>Entire band 5925-7125 MHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qatar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Costa Rica</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Korea</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peru</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lower portion 5925-6425 MHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Morocco</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In the U.S., the entire band will be released to “Wi-Fi like” systems with power limitations in some portions of the band with an obligation to implement the Automatic Frequency Control (AFC) system for outdoor AP systems to protect primary services such as microwave links. In Europe, only the lower part of the band will be released to Wi-Fi. It is still under discussion whether the upper portion of the band will be assigned to IMT and under which conditions.

Microwave transport vendors are carefully monitoring the situation as their ultimate scope will be to properly protect their systems. One method currently under discussion is the AFC system that guarantees good protection to microwave links, but unfortunately AFC is only applied to outdoor systems. CSPs, especially in the U.S., are already challenging their microwave suppliers to provide monitoring systems able to detect interference from Wi-Fi systems.

Spectrum above 100 GHz

Frequency bands above 100 GHz have gained considerable interest due to their ability to meet the growing demand for high-capacity and low-latency wireless backhauling systems.

W-Band (92-114 GHz) and D-Band (130-175 GHz) were considered in recent regulatory activities:
- ECC published the two recommendations on frequency arrangement: ECC Rec(18)02 and ECC Rec(18)01;
- ITU is currently discussing the two versions of the frequency arrangements for these two bands.

Looking at the Radio Regulation (RR), the two bands (or rather the portions of the spectrum that today we call the W-Band and D-Band) are allocated for the fixed service. The following figure gives an overview of the two bands including the limitations of use. The figure also shows the E-Band (71-86 GHz) for comparison.
It is worth highlighting that the portions of bands adjacent to EESS services require particular care from an interference perspective. The stringent level of allowed emissions imposes some restrictions on the usage of the FS channels close to these bands making them difficult to use. This is particularly evident for the W-band which includes 4 portions for EESS.

A special characteristic of these two bands is that they are composed of 4 different blocks, separated by portions of spectrum that cannot be used. E-Band is also composed of two separate portions of bandwidth, in two equal parts. The classical FDD approach is possible by using a ‘go’ and a ‘return’ portion divided by a guard band. In the two ECC recommendations, FDD and TDD usage plans for W-Band and D-Band are defined.

Nokia and the other main microwave vendors are carefully evaluating the possible added value provided by these 2 bands concerning the existing solution in E-Band. There is a common interest in developing new products by exploring new approaches to bring additional benefits.
W-Band can be considered an extension of the E-Band, however, the need to manage 4 portions of spectrum would make a commercial solution more complex. In addition, the solution would not offer added value to the E-Band already available today. For these reasons, almost the entire microwave ecosystem (vendors and operators) is not considering such a band as a priority.

In contrast, recent studies and projects on D-Band (i.e. H2020 DREAM and H2020 DRAGON) have highlighted that this high frequency can enable a possible evolution of the radio architecture that allows more functional use of the four portions exploiting the flexible FDD (fFDD) concept (two separate antennas for TX and RX). The main challenge for the development of a product in this band is related to the implementation of flat antennas (possibly active) based on SiGe components with benefits also in terms of costs.

Major microwave vendors believe that the D-band could be exploited for future high capacity fronthaul/backhaul systems in urban environments thanks to the reduced weight and volume that are key success factors for street level applications. The following figure shows the actual availability of channels in the two bands (plus E-Band for comparison) in FDD, TDD and fFDD modes.

**Figure 9: E-Band, W-Band and D-Band - Available channels**

The first picture shows the results for the three duplex methods in 250, 1000 and 2000 MHz channels, while in the second one, only FDD cases are shown. As we can see, the W-Band as conceived today, provides a very modest contribution while the introduction of the D-Band will instead offer an effective and considerable availability of bandwidth, even wider if the fFDD solution is exploited. Moreover, a large number of wider channel spacings (i.e. 1,000 and 2,000 MHz) will be made available for multiple Gbps backhauling connections.

**Microwave KPI definition**

In recent years we’ve seen examples of deployed links utilizing higher modulation schemes to achieve extra capacity while still guaranteeing availability for high priority traffic at a lower modulation. Mixing low and high modulation schemes in adaptive modulation enables the transmission of a multitude of different services that have different requirements in terms of quality. However, this brings some new challenges that operators must face.
The system gain difference is very high (at approximately 35dB) at the minimum modulation, which is reserved to transmit the high priority traffic in case of link degradation and the maximum modulation which is used by the best-effort traffic. The link is commonly dimensioned considering a single-point check, e.g. 99.999% or 99.995%, for the modulation required to guarantee the transmission of the high-priority traffic. This leads to a non-optimum solution.

The radio link design should be tailored to satisfy the different traffic requirements. This can be achieved by exploiting additional check points in the design phase. According to Nokia, the link dimensioning could be based on the following points:

- Point 1: Committed high priority traffic (XX Mbps @ 99.99X%)
- Point 2: Normal average/busy hour traffic (YY Mbps @ 99.9x%)
- Point 3: Peaks of best-effort traffic (ZZ Mbps @ stable conditions)

With reference to the Figure 10:

- Committed traffic is for example any mix of voice and video conferences, business-to-business (B2B) connections with stringent Service Level Agreement (SLA), mission-critical services for public and private networks, and other high-priority services based on 5G technology. In the case of 5G, the capacity is in the range of tens to hundreds of Mbps and availability required usually exceeding 99.995%
- Normal average/busy hour traffic is the typical traffic generated daily by a radio Base Station. It contains a mix of committed traffic and best-effort traffic. A multitude of applications used today are built to operate under a best-effort transport network, so the availability target for this mix of traffic should be set to avoid degrading the user experience during normal daily operating conditions. In this case, the capacity may vary as it is highly dependent on the type of services offered by the CSP and site position (i.e. urban/suburban/rural). The required availability is usually in the 99.95% to 99.99% range.
- Peak traffic refers to any instantaneous burst of traffic reaching the maximum capacity allowed by the RAN. As it is impossible to identify a correlation between these traffic peaks
and the propagation impairments that can impact a microwave link, we need to ensure that the microwave link provides that maximum capacity under a stable operating condition. Based on Nokia’s experience, this stable operational condition can be associated with a minimum fade margin guaranteed for maximum modulation. This value depends on the frequency band, distance, region, and the Customer Operation and Maintenance acceptance procedures may also influence this value. According to the feedback from the field, we consider 10dB a good reference across all frequency bands.

Security

Today’s environment requires all operators to take security in networks very seriously. All products from suppliers must be designed with security in mind. A dedicated team of security professionals, independent of the business groups must ensure security. This is of paramount importance within their company. Microwave products are no exception. Rigid standards must be in place to confirm the designs meet security robustness and an independent team must review all third-party software applications for security vulnerabilities. Products that are to meet acceptable security standards in today’s networks must be submitted to the utmost scrutiny during security standards compliance and vulnerability testing.

Recent high profile security breaches have exposed the need for all types of network operators to place a laser focus on security within their corporate environments. Today, service providers are faced with a significant and rapid evolution in three key areas that are evolving in parallel: threats, technologies and compliance. Security practices must therefore evolve also and should be updated proactively to stay ahead of the rapid changes in these three areas.

Figure 11: Security key areas

Technology is changing rapidly. Today, there is much more intertwining of access with day-to-day operations from employees, customers and suppliers all accessing the network. The advent of the cloud has made the concept of just “firewalling out the bad guys” impractical. New technologies and methods are needed to identify and ward off cyber criminals.

The techniques of attackers have become much more sophisticated and organized. The days of a single rogue hacker impacting the microwave network are less pronounced and now the attackers are much more focused in particular on high-value target organizations. The advent of
Ransomware as a Service (RaaS), where a shadow company sells its ransomware infrastructure to various small dark web enterprises, has become a troubling concern over the past 12-18 months for companies and governmental organizations.

To meet shifting customer expectations, networking companies must provide communications infrastructure with highly secure solutions that are embedded into the products they deploy. Suppliers of radio systems must continually evolve and update the solutions provided to their clients to thwart the cyber criminals that are pervasive in today’s changing world.

Who are these attackers that we must be so vigilant to guard against? Some are criminals trying to steal the end customer information or other corporate secrets. Sometimes they are insiders such as an employee determined to damage their employer’s reputation or steal corporate information for personal gain. Increasingly, terrorists are trying to take over networks either for political purposes or economic gain. Finally, state terrorists want to disrupt a country’s infrastructure or attack government facilities to gain compromising, private information.

Figure 12: Attackers

Criminals can penetrate the networks at several points and in a number of ways. Independent of the entry point, the most common method to gain access is to secure official credentials through various phishing methods (i.e. email, text, phone, etc.). Many phishing methods are quite effective and difficult to recognize. All organizations must train their employees to recognize these techniques and have frequent “refresher” sessions on how to spot nefarious actors.

To successfully secure network infrastructure, an operator must focus on four key areas:

1. Harden – Best practices must be implemented to harden all operating systems, platforms and applications with updates that ensure enhanced security compliance.
2. Protect – Physical access to sites must be monitored. All traffic planes (RF, Layer 2, Layer 3), Control and OAM should deploy leading edge encryption algorithms. High-value hardware and software assets must be closely guarded.
3. Control – Proper firewall management and user management (AAA) techniques will ensure control to the software and corresponding infrastructure assets.
4. Detect – If an unauthorized criminal has managed to circumvent safeguards and gain access to your network, proper monitoring of logs and alarms must be embedded in your company’s operational process to limit any potential damage to infrastructure, loss of critical data assets, and/or total loss or partial impairment of your network’s viability to service your customers.

There are six security domains critical to any organization to ensure adequate securing of the corporate network infrastructure (Figure 13).
Figure 13: The security domains

- **User Account Management**
  - Prevention of unauthorised access, local and remote accounts, Nokia Service Accounts, granular roles and policies.

- **Public Key Infrastructure**
  - X.509 certificates, Automated Life Cycle Management, Revocation list management

- **Secure Transport**
  - TLS, HTTPS, SSH, secure LDAP

- **Personal Secure Environment**
  - Signed SW, Data confidentiality and integrity, Sensitive data encrypted at rest

- **Cybersecurity Regulations & Compliance**
  - DfSEC, Cybersecurity Regulations Compliance & testing

- **Interfaces and internal hardening**
  - Hardening and reducing surface of vulnerability, Firewalls, Overload, DoS and brute force protection

With reference to the Figure 14, the outer edges must be properly maintained with Firewalls and Rate limiters as well as operator access (AAA). Service access is a joint domain between the external suppliers, subcontractors and the internal personnel. Signed software that guarantees a legitimate and untainted copy of the software being deployed is a necessity. Trusted Boot and a hardened OS sourced and tested by a licensed third-party provider is also a must have and every vendor needs to provide this level of security assurance.

Figure 14: Security practices
Following these security practices will give confidence to avoid network intrusions or data compromises which would seriously impact the company’s reputation and ability to operate.

Microwave real-time analytics

Why is data so important for our networks, in general, and for wireless transmission specifically? There are two main reasons:

- Networks are becoming more and more complex, growing in size due to coverage extensions or densification. Additionally, new technologies like E-Band and Carrier Aggregation, have been deployed to enrich the use cases based on the traditional frequency bands.
- The other driver comes from users that are raising their expectations in terms of network performance: mobile subscribers and also Enterprises are keen to use new applications and exploit new use cases enabled by 5G.

Additionally, there will be new use cases tailored for special applications like network slicing and high-performance and demanding applications such as Ultra Reliable Low Latency Communications. In this changing environment, there are some operational tasks that require proper data management.

- Network inventory: to keep all the elements of the network under control: configurations, hardware and software variants, frequencies and licenses.
- Resource optimization: to adapt the network resources to the real needs of the transported applications and save money.
- Service Level Agreement: to check whether the committed performance is fulfilled – services being more and more demanding and posing new requirements, for example in terms of latency constraints.
- Detect performance degradation ahead of a service impact or an outage: this is a particularly precious task for the wireless transport whose physical layer is conditioned by several external conditions.

In all these cases, and many others, for the owner of the network data the possibility to extract their real value has a great business relevance. If we analyze the possible approaches to address a degraded condition, we can group them into three models (see Figure 15).
A reactive model is usually based on on-demand troubleshooting activities taking place once the KPI degradation is already happening. The consequent user experience impact, in magnitude and persistence, increases if assurance and monitoring tools are limited in the network.

In some cases, the performance degradation might not be detected for months or years until it becomes visible due to the combination of the degradation with other extraordinary events (e.g., a bad quality-of-service (QoS) configuration might last for years until the moment congestion or physical layer changes severely impact the high priority traffic).

With analytics and monitoring tool enhancements, a proactive model can be adopted with reduced levels of human involvement in the analysis execution (Figure 16).

Analytics reporting capabilities allow the operator to periodically assess the performance trends: reports can be triggered by the user periodically or generated on demand. An efficient ranking and filtering of the resources places the user in a better position to address the most impacting cases first.

**Figure 16: The proactive model**
The analytics system can enhance the proactive model even more via the introduction of baselining capabilities and anomaly detection. This happens when the user selects a reference period where KPIs behave in the expected manner, storing this observation as a reference called a baseline. Then autonomously and continuously, the system is set to run anomaly detection ML/AI algorithms against the baselined measurement. The user is alerted as soon as an anomaly is detected. Thanks to the capabilities of the baseline, the operator is not required to periodically screen the analytics report. The system itself is in charge of observing the network and requesting user intervention if needed (Figure 17).

Figure 17: The proactive model - baseline and anomaly detection

![Figure 17: The proactive model - baseline and anomaly detection](image)

Analytics and automation boundaries are becoming more and more similar and overlapping. This technology evolution may allow an anomaly detection to be used as a trigger condition for an automated procedure to collect further troubleshooting information or even fix the root cause issue.

An additional approach in the analytics landscape is the predictive model. In this model, the monitoring system implements a ML/AI predictive algorithm to infer the future trend of a KPI based on the present and past observation. Thanks to this model, a future degradation can be detected even before it has any effect on the network performance (Figure 18).

Figure 18: The predictive model

![Figure 18: The predictive model](image)

A proactive model can be applied to a microwave interference detection use case. Radio KPIs are baselined typically at the time of link commissioning and can be used as a reference to detect divergences concerning the expected behavior. The moment when an anomaly is revealed triggers a set of additional monitoring steps to further narrow down the observed event and confirm an interference condition.
Predictive models find their best applicability in throughput trend analysis. Here it has a great advantage allowing the tool to plan in advance any network upgrade whenever the network utilization exceeds a certain level. The lifecycle of such an upgrade is long and it could bring additional costs and user dissatisfaction if not addressed promptly. Via the prediction of the utilization trend information, the network upgrade can be planned with a structured operation and delivery chain.

From an architectural perspective, the analytics functions are enabled via a set of domains that are part of a modular infrastructure.

- The data collection domains include network and analytics system capabilities to monitor the network KPIs and collect them in a centralized location for further processing.
- The data is stored and framed by the data storage domain which guarantees high availability and long data retention. The latter aspect is important for any proactive/predictive post-processing function.
- The data processing domain is the layer in charge of analyzing the collected data to:
  - Identify and aggregate the most critical events (reporting-based proactive model)
  - Process baselines and anomalies (baseline-based proactive model)
  - Infer future KPI trends (predictive model)
- The result of these processes is then reported via the reporting domain to the user.

An analytics architecture conceived in this way allows the toolset to move from one model to the next one protecting the prior investments.

**Wavence dual-band system in heavy rain-rate region**

Nokia has recently demonstrated and deployed its Wavence dual-band system supporting high capacity. The deployment in carrier aggregation demonstrated stable multi-gigabit capacity and high-performing microwave links in an area with high rainfall like Panama City. The use of the Wavence dual-band solution will give Liberty Latin America additional deployment options when building out their 5G backhaul and broadband connectivity.

With this deployment, Nokia together with Liberty Latin America have demonstrated that even with the most challenging environmental conditions the Nokia Wavence dual-band system outperformed the calculated system performance. In Figures 19 and 20, the details of the deployment and the performance of the 0.6 km E-Band link performance are shown.

**Figure 19: The deployment**
Figure 20: E-Band Received Signal Level, Modulation and Availability
This example demonstrates that dual-band Carrier Aggregation is technically feasible and it can achieve a very high capacity by employing E-Band high bandwidth and benefit from the high availability of the lower microwave bands links. Furthermore, the same system can be even further stretched to longer hops. In fact, the E-band performance is not significantly degraded and the system can rely on the traditional microwave band (e.g. 15-18-23 GHz) which keeps the link fully active in a hitless manner during transients when E-Band is disturbed by heavy rain.

The hitless QoS of Wavence dual-band system preserved the committed traffic unaffected as per the SLA while E-Band served the remaining huge data amount for the rest of the time. In terms of investment, a dual-band system provides a cost-effective solution even in challenging conditions confirming it as an alternative to fiber.

At the time of this paper publication, the cooperation with Liberty Latin America is one of a series of activities where Nokia helped different CSPs in assessing E-Band technology in Latin America and Central Africa. Nokia in-field experience is not finished with additional results to come in the near future.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>AFC</td>
<td>Automatic Frequency Control</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>CSP</td>
<td>Communication Service Providers</td>
</tr>
<tr>
<td>DDoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DfSEC</td>
<td>Design for Security</td>
</tr>
<tr>
<td>DRAGON</td>
<td>D-band RAdio 5G netwOrk techNology</td>
</tr>
<tr>
<td>DREAM</td>
<td>D-band Radio Enabling up to 100 Gbps reconfigurable Approach for Meshed</td>
</tr>
<tr>
<td>DS1</td>
<td>Digital Signal 1</td>
</tr>
<tr>
<td>ECC</td>
<td>Electronic Communications Committee</td>
</tr>
<tr>
<td>EESS</td>
<td>Earth Exploration Satellite Service</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>FDD</td>
<td>Frequency Division Duplex</td>
</tr>
<tr>
<td>fFDD</td>
<td>Flexible Frequency Division Duplex</td>
</tr>
<tr>
<td>FS</td>
<td>Fixed Service</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext transfer protocol secure</td>
</tr>
<tr>
<td>IDU</td>
<td>Indoor Unit</td>
</tr>
<tr>
<td>IMT</td>
<td>International Mobile Telecommunications</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>ML</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, Administration and Management</td>
</tr>
<tr>
<td>ODU</td>
<td>Outdoor Unit</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PoP</td>
<td>Point of Presence</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RR</td>
<td>Radio Regulation</td>
</tr>
<tr>
<td>RSL</td>
<td>Received Signal Level</td>
</tr>
<tr>
<td>SDN</td>
<td>Software Defined Networking</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>TDD</td>
<td>Time Division Duplex</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>XPIC</td>
<td>Cross Polarization Interference Cancellation</td>
</tr>
<tr>
<td>ZFP</td>
<td>Zero Footprint</td>
</tr>
</tbody>
</table>
References


About Nokia

At Nokia, we create technology that helps the world act together.

As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2021 Nokia
Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

Document code: CID210908