White paper: mission-critical networks

A new approach to network management gives defence forces secure, dependable connectivity for voice and data, with improved bandwidth utilisation

In the defence domain, communication networks are under increasing pressure. Defence forces must fulfil a wider set of roles and functions, so the number and scope of applications they use is constantly expanding. Equally, the applications themselves have a growing appetite for bandwidth, and the volume of users and end-points continues to rise. Growth in cyber-security threats means that more communications must be encrypted, putting further pressure on costly bandwidth resources and coordination efforts. In the background, defence organisations are struggling to reconcile growing requirements with shrinking budgets, while the high cost of managing legacy equipment reduces the ability to invest in new technologies.

To help ensure the ongoing security and reliability of voice and data communications, defence organisations can now take advantage of a new approach to network management. By deploying an application-aware, software-defined network integration layer, defence organisations can automatically prioritise network traffic, mitigate against multiple simultaneous network failures, and scale the network to meet evolving operational requirements. With greater flexibility to support both existing and future technologies and standards, a software-defined approach offers greater scalability of networks, improved shared situational awareness, and intelligent routing for true quality of service.

Defence Networks

FREQUENTIS

Growing needs, shrinking budgets

There are rising expectations today for defence forces to meet broader requirements, including responding to terrorist attacks, supporting civilian authorities during natural disasters, and deploying to international locations for crisis response or peace-keeping missions. To meet these new demands, defence forces seek significantly greater flexibility, scalability, versatility and intelligence in communication networks.

As requirements evolve, defence organisations must ensure that there is sufficient bandwidth for voice and data, and that the bandwidth can be shared and reallocated flexibly and dynamically. If budgets were unlimited, organisations could overprovision networks to ensure capacity at all times, but in the real world they need to stretch scarce resources to meet requirements. The challenge is magnified by high ongoing costs for maintaining multiple new and legacy networks across what is typically a poorly integrated patchwork of systems.

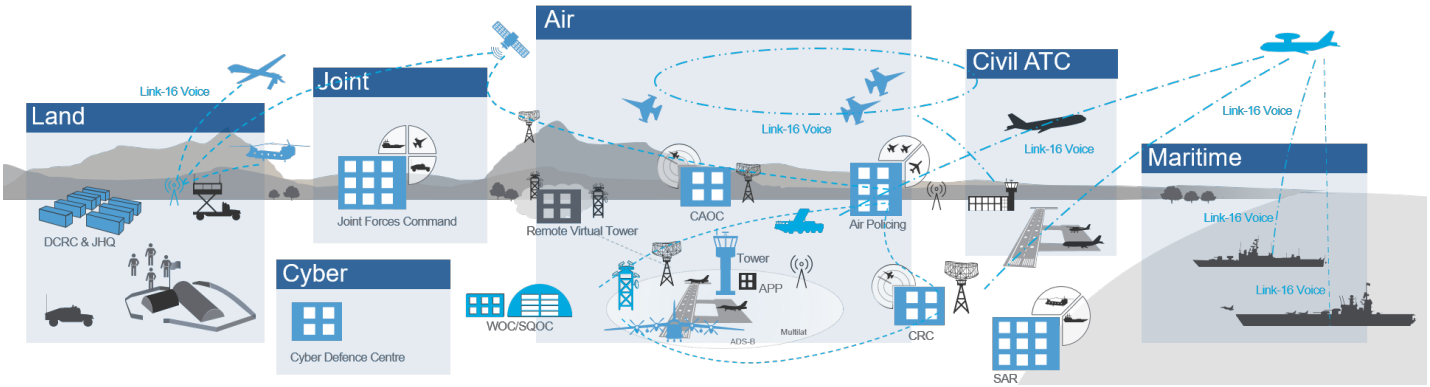
Reliability and bandwidth challenges

Secure and reliable communication has always been a critical component in assuring effective operations for defence forces. Modern defence forces rely on a growing set of channels and applications, yet bandwidth remains limited and expensive—particularly when operations take personnel to remote locations that lack fixed infrastructure. Where mobile units are deployed in harsh environments, maintaining tactical data links that offer both reliability and sufficient bandwidth is a major challenge. Emerging requirements, not least the rapid uptake in the use of unmanned vehicles, are putting further strain on bandwidth.

To enable more sophisticated functionality and greater interoperability between joint forces, defence organisations are converging to Internet Protocol (IP)-based networks. However, they must often continue to maintain legacy networks and capabilities, particularly given limited budgets.

As networks grow and become more diverse, it is becoming harder for defence organisations to ensure adequate performance and quality of service. This is especially the case when multi-security-domains and encrypted communications are involved: these can raise bandwidth demands by as much as 400 percent, in addition to increasing the complexity of managing the network. For defence organisations, which face targeted kinetic or cyber attacks, there is a heightened threat of network degradation—and it is precisely during incidents of electronic warfare that maintaining communication is most critical. At such times, defence forces need to ensure quick incident handling to minimise disruptions in the communication of mission-critical data.

Figure 1: interconnected forces on air defence networks



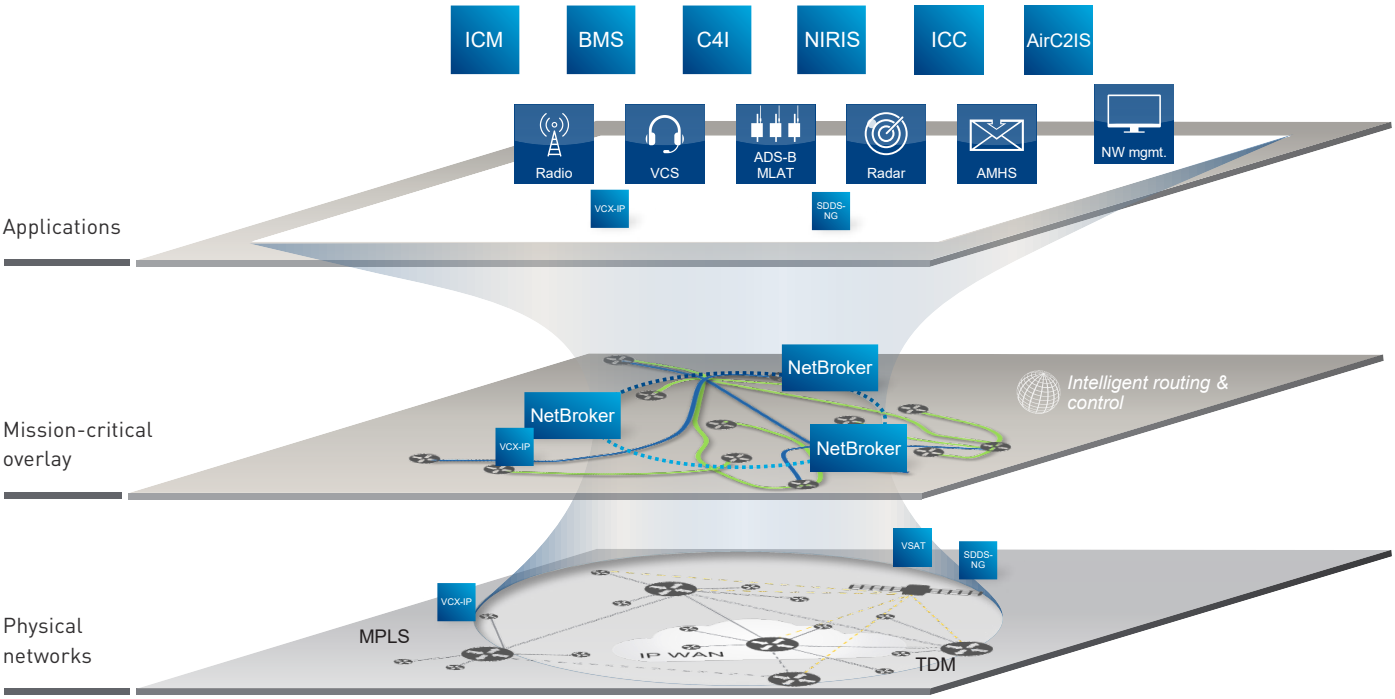


Figure 2: application-aware network

New approach to defence networks

Defence organisations should adopt an application-aware network that can intelligently prioritise and dynamically re-route traffic to ensure "evergreen" performance levels for applications. By introducing a flexible integration layer on top of existing communication equipment, defence organisations can continue to use legacy systems more cost-effectively while introducing newer technologies as required and as budget becomes available. In addition to improving the speed and ease of scaling the network to meet new requirements, this approach makes it possible to unite the capacity inherent in multiple underlying network routes and manage it as a single, highly flexible resource. This opens up the possibility to monitor end-to-end network performance and quality of service in real-time, and to automatically switch traffic between network routes as conditions change.

With capacity virtualised into a shared resource, defence organisations can eliminate single points of failure and ensure resilience of critical communications even if part of the network fails. They can also monitor and control all network traffic centrally regardless of the carrier, enabling deterministic performance. Multiple standards, both new and legacy, can be supported more easily, simplifying interoperability with external partners, and the use of a flexible integration layer enables faster deployment of new fixed and mobile network sites.

The network of the future

Based on IP and other open standards, the converged software-defined network of the future will empower defence organisations to maintain reliability, use expensive redundancy effectively, improve performance and enhance security for critical data services and voice communication. These improved capabilities strengthen shared situational awareness, particularly in joint-forces scenarios. Real-time statistics on performance and quality of service will be automatically assessed against application requirements, enabling intelligent traffic prioritisation and network admission.

Adopting a software-defined approach will enable defence organisations to embed an understanding of the business logic behind each application's changing bandwidth requirements, permitting the system to dynamically allocate adequate capacity based on organisational priorities.

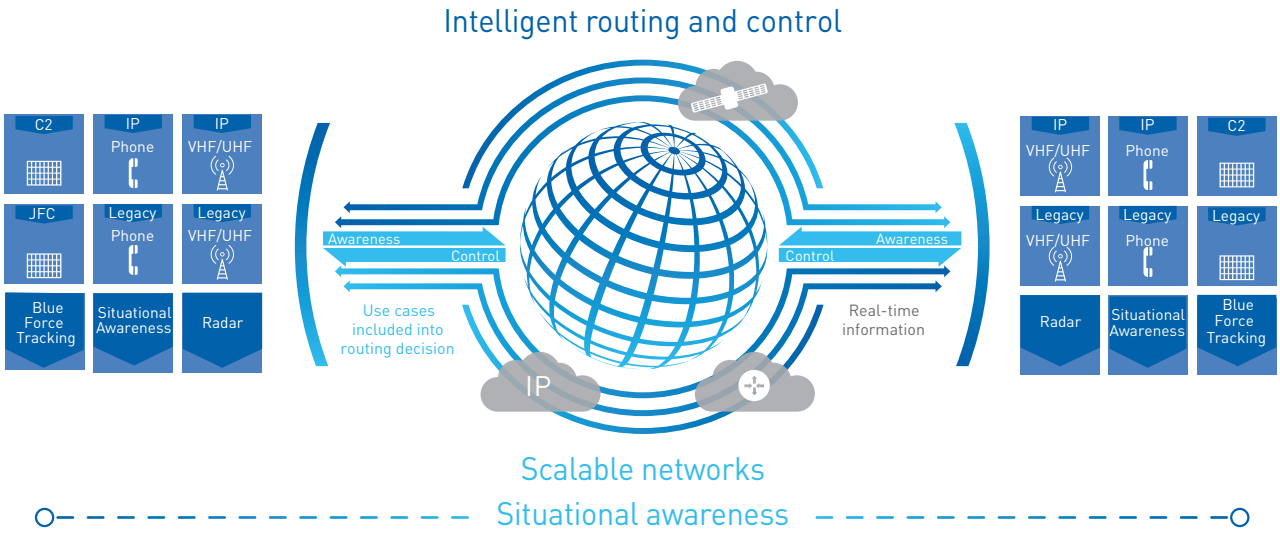


Figure 3: Networks for highest end-to-end performance for every application

Using software-defined secure networks also provides valuable new opportunities in predictive management of requirements. When the network detects degradation in a particular link, it can proactively prevent failure by re-routing high-priority traffic to ease load on that link. Equally, the network can monitor transmission parameters and estimate the expected future changes in bandwidth capacities across every network layer, providing vital intelligence to assist in the prioritisation of traffic. In defence scenarios, where both static deployed and mobile sites may face targeted electronic warfare attacks, the ability of the network to proactively route communication around bottlenecks and points of failure is extremely valuable.

Secure and dependable connectivity

With a software-defined network, defence organisations will be able to balance performance with efficiency to maximise the value of limited network bandwidth, all while ensuring sufficient capacity to support the additional demands of secure encrypted communication in multi-security-domains.

By choosing to work with Frequentis as an experienced provider of software-defined defence communication solutions, defence organisations can resolve the growing challenges of maintaining performance, security and quality of service as demands grow and budgets shrink. With network virtualisation reducing the overall complexity, organisations can lower their costs while improving reliability and simplifying the introduction of new technologies.

With decades of experience in providing reliable and secure communication technology to the defence sector, Frequentis is well positioned to help defence organisations set up highly scalable networks. These feature intelligent routing that ensures ongoing situational awareness across joint forces even when networks are under electronic and/or physical attack. They also offer an open approach that maximises compatibility with past, present and future networking equipment and standards. Over time, organisations will be able to phase out older technologies to reduce their costs, and scale up more efficiently to meet future requirements.

For more information on how a software-defined approach can help defence organisations to achieve secure, reliable, high-performance communication at low total cost, please contact Frequentis.

FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
Tel: +43-1-811 50-0
www.frequentis.com