
## Challenge

Telecom providers are deploying private 5G networks using CBRS at secure locations such as airports, hospitals, and military bases. These networks rely on radio transmitters scattered throughout the facility. After initial deployment, the transmitters are connected to the facility's network, and the telecom provider typically loses direct access.

This lack of access creates significant challenges:

- **Limited Troubleshooting:**
  If updates are needed or network issues arise, the provider must rely on the facility's local IT team or service the devices with a truck roll, potentially delaying resolution times.

- **Security Concerns:**
  Granting the 5G provider full access to the facility's network poses security risks, as the facility network itself could be the source of the 5G network problem.

## The Traditional Fix (and its Drawbacks):

Traditionally, "backdoor" access points are created to allow remote troubleshooting. However, these solutions often involve:

- **Exposed Ports:**
  Opening network ports creates significant attack surfaces for potential security breaches.

- **Uncontrolled Access:**
  Facilities lose control over who can access the backdoor, raising even more security concerns.

## The NoPorts Solution

NoPorts offers a secure and controlled solution for remote access to private 5G network transmitters.

## Here’s how it works:

**Secure Gateway:**
A small device like a Raspberry Pi or firewall equipped with a cellular network modem is installed at each transmitter location. NoPorts software is then installed on this device.

**Policy-Based Access:**
NoPorts utilizes a policy plane that allows the facility to:

- **Maintain Control:** The facility retains ownership of the "backdoor" and can grant or revoke access to the private 5G service provider at any time.
- **Zero Trust Access:** NoPorts employs a zero-trust architecture, ensuring only authorized devices can connect using strong cryptographic authentication.
- **No Exposed Ports:** NoPorts eliminates the need for open network ports, drastically reducing attack surfaces for hackers.

## Benefits

- **Secure Remote Access —** The telecom provider can securely access and troubleshoot 5G network transmitters remotely, even if the facility network is experiencing issues.
- **Enhanced Security —** NoPorts eliminates exposed ports and utilizes zero-trust authentication, significantly improving overall security.
- **Granular Control —** The facility retains complete control over who can access the network, minimizing security risks.
- **Faster Resolution Times —** Remote access capabilities allow for quicker troubleshooting and improved network uptime.

Atsign's **NoPorts** empowers telecom providers to deliver exceptional private 5G network services while ensuring the highest levels of security for both the provider and the facility.

NoPorts.com