WHITE PAPER | April 2024

Connectivity

Introduction to cellular networks

Learn more about

- How cellular routers can provide reliable Internet connectivity in remote industrial locations.
- Improving the efficiency of the application by better understanding the basics of cellular networks and key networking concepts.
- Features to consider when selecting a cellular data plan.

Introduction

As industries become more automated, reliable and efficient networking solutions have become essential for seamless operations. Cellular routers provide a versatile and robust solution for remote monitoring and control applications in industrial automation. However, understanding the various networking aspects of using cellular routers can be daunting for those without a background in networking.

This white paper provides an overview of key networking concepts related to cellular routers, including network address translation (NAT), access point names (APNs), virtual private networks (VPNs), port forwarding, and the roles of mobile virtual network operators (MVNOs) and mobile network operators (MNOs). By the end of this white paper, readers will have a better understanding of how to effectively utilize cellular routers in their industrial automation applications, with a focus on ensuring secure and reliable network connectivity.

Network overview

A cellular network is a type of wireless network used for communication between mobile devices, such as smartphones or tablets. Here is an overview of a cellular network considering the major components: user equipment, radio access network (RAN), the carrier network, and the Internet (FIGURE 1).

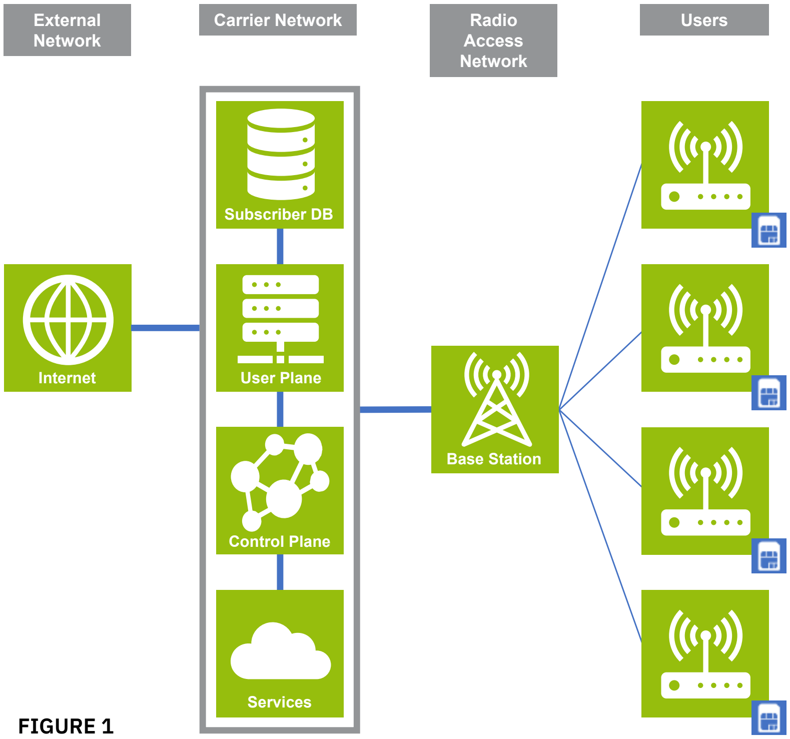


FIGURE 1

continued →

Contents

User equipment (UE): User equipment refers to the mobile devices used to connect to the cellular network. This includes smartphones, tablets, and other mobile devices that use a SIM card to connect to the network.

Radio access network (RAN): The RAN consists of a network of base stations or cell sites that connect user equipment to the carrier network. This network uses radio frequency waves to communicate with the user equipment and transmit data to and from the carrier network.

Carrier network: The carrier network consists of a core network and a backhaul network. The core network provides routing and switching functionality for voice and data traffic, while the backhaul network connects the RAN to the core network.

Note that the major mobile network operators (MNOs) in the U.S. (AT&T Mobility, Verizon Wireless, and T-Mobile/Sprint) each own and operate their own RAN and carrier networks.

Internet: The Internet is a global network of interconnected computers and servers that enables data communication between users and devices. In a cellular network, data from the carrier network is often transmitted to the Internet to allow users to access web-based services and applications.

When a user makes a call or sends a message on a cellular network, the user equipment sends the signal to the nearest base station, which relays the signal to the carrier network. The carrier network uses the core network to route the signal to the recipient's mobile device, or to the Internet if the call or message is intended for a web-based service.

A cellular network is a complex system of hardware and software components that work together to enable wireless communication between mobile devices. The user equipment, RAN, carrier network, and Internet are all essential components of a cellular network that allow users to connect and communicate with each other. ■

APN (private and public)

An access point name (APN) is a unique identifier that mobile network operators use to establish a data connection for a device over their network. In the context of a cellular router for industrial applications, the APN serves as the gateway for the router to connect to the Internet or a private network (FIGURE 2).

When a cellular router is deployed in an industrial environment, it needs to connect to a mobile network to access the Internet or a private network. The router communicates with the mobile network through the APN, which is provided by the network operator. The APN serves as the entry point to the network and provides the necessary information for the router to connect, including the authentication details and the network settings.

Once the router is connected to the network through the APN, it can transmit and receive data over the cellular network. This allows the router to provide Internet connectivity to devices in the industrial environment, such as sensors, cameras, and other equipment. The router can also be configured to provide secure connections to a private network, such as a corporate network, using a virtual private network (VPN) connection.

The function of an APN in the context of a cellular router for industrial applications is to provide a secure and reliable connection between the router and the mobile network. The router can then transmit and receive data over the cellular network and provide Internet connectivity to devices in the industrial environment.

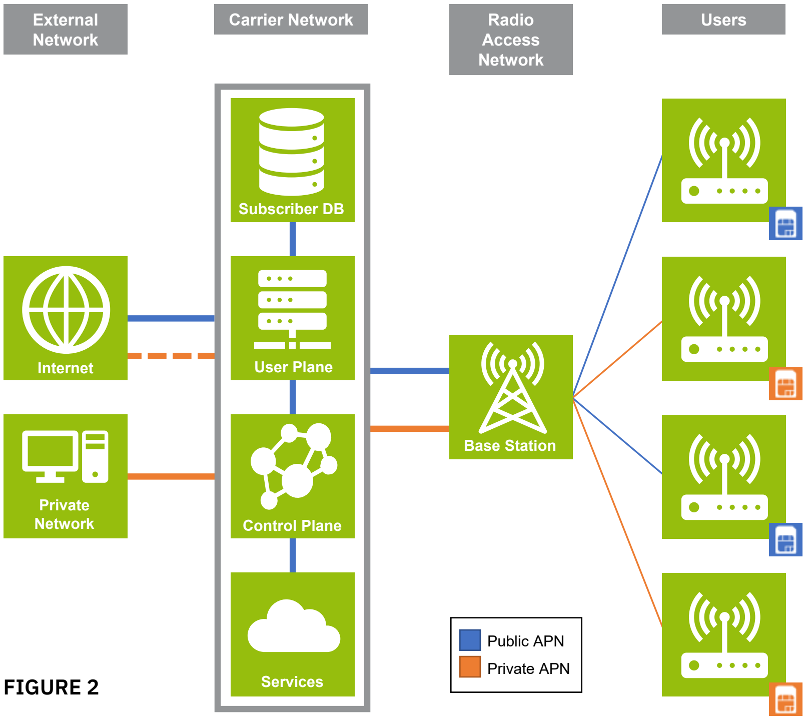


FIGURE 2

continued →

What are the benefits of a private APN?

Enhanced security: A private APN provides a dedicated and secure connection between the business's devices and their private network or cloud resources. Unlike public APNs, which are shared among multiple users and can be vulnerable to attacks, a private APN is dedicated to a specific business and can be configured with additional security measures, such as encryption and firewall rules, to protect against unauthorized access and data breaches.

Customization: A private APN can be customized to meet the organization's specific business needs. For example, the business can configure the APN to prioritize traffic from critical applications or devices, or to limit access to certain network resources based on user roles or device types.

Compliance requirements: Some industries and businesses have strict regulations around data privacy and security. A private APN can help organizations comply with these regulations by providing a secure and controlled network environment.

While a private APN may require additional setup and maintenance costs, it can provide significant benefits for businesses that require a dedicated and secure cellular network connection.

Using a public APN can also have several business benefits, including:

Lower costs: Public APNs are often less expensive than private APNs because multiple users share them. This can be a cost-effective solution for businesses that do not require a dedicated cellular network connection or have limited budgets.

Easy setup: Public APNs are typically easier to set up and manage than private APNs. Since the network infrastructure is already in place, businesses can quickly connect their devices to the network without extensive configuration or maintenance.

Scalability: Public APNs can be easily scaled up or down to meet the changing needs of a business. As the number of devices or data usage increases, businesses can simply upgrade their subscription to a higher service tier without investing in additional infrastructure.

While a public APN has its advantages, it might not provide the same level of security or customization as private APNs, making it vulnerable to network congestion or latency issues.

MVNO

A mobile virtual network operator (MVNO) is a company that provides mobile network services without owning its own licensed spectrum or physical network infrastructure (FIGURE 3). Instead, an MVNO leases network capacity from an MNO and resells it under its own brand. Notably, an MVNO can lease and resell network capacity from multiple MNOs. By aggregating data plans from multiple MNOs, the MVNO can offer a major value proposition to users who have cellular devices deployed across the country where coverage from a single carrier may not be available.

The role of an MVNO is to provide mobile network services without the high costs of building and maintaining a physical network infrastructure. By leasing network capacity from an MNO, an MVNO can offer mobile network services at competitive prices while still maintaining its own brand identity and customer base.

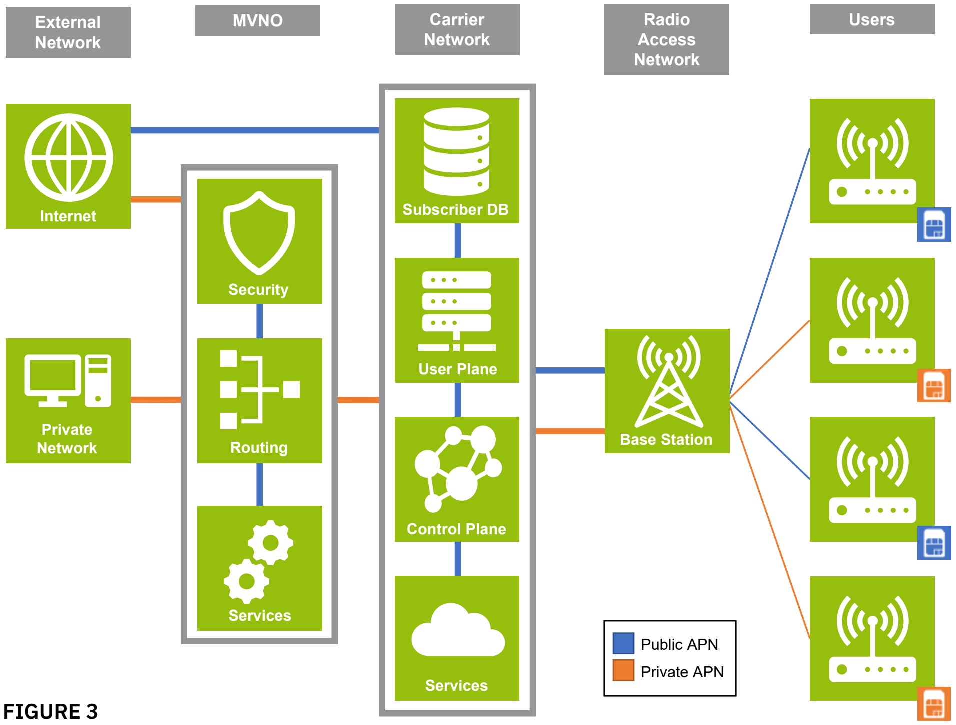


FIGURE 3

continued →

In addition to providing mobile network services, an MVNO may offer additional value-added services such as mobile device sales, customer support, and billing services. An MVNO may also specialize in serving specific customer segments, such as prepaid customers, low-income customers, or international travelers. Some MVNOs even have existing private APNs already built and accessible to their customers. They can facilitate the use of private APNs for improved security with minimal upfront cost or development to the end user.

MVNOs play an important role in the mobile telecommunications industry by increasing competition and providing more choices for consumers. ■

Networking methods

Public static IP

A public static IP address is a unique IP address assigned to a device or network that is reachable from the Internet and remains constant over time. It is called "static" because the address does not change, unlike dynamic IP addresses that are assigned dynamically by the Internet service provider (ISP) each time a device connects to the Internet.

Public static IP addresses are typically used by servers, web hosts, and other network devices that require constant accessibility from the Internet. With a public static IP address, devices can be easily accessed from anywhere on the Internet without the need for dynamic DNS services, which can be unreliable or require additional configuration.

Some benefits of having a public static IP address include:

Remote access: A public static IP address allows remote access to devices on the network, such as servers, cameras, or other network devices, from anywhere on the Internet.

Hosting services: Public static IP addresses often host services, such as websites or email servers, that need to be accessible from the Internet.

Network identification: A public static IP address can be used to identify a specific device or network on the Internet, making it easier to manage and monitor network traffic.

Stable network configuration: A public static IP address allows network administrators to set up more stable network configurations, such as firewall rules and port forwarding, that can be relied on over time.

However, a public static IP address can also expose the network to more security risks, as attackers can more easily target specific devices or services. It is important to properly secure the network and use appropriate security measures, such as firewalls and intrusion detection systems, to mitigate these risks. Finally, a public static IP address can add cost, so it is important to consider the tradeoffs when opting for a public static IP address. ■

continued →

NAT routing

NAT (network address translation) routing is a technique that allows devices on a private network to share a single public IP address for communication with the Internet. NAT works by translating private IP addresses into a public IP address and vice versa.

In the context of cellular routers, NAT routing allows devices connected to the router to have private local IP addresses (192.168.1.XX, for example), while the cellular router has a public IP address (FIGURE 4).

Private IP addresses: Devices on a private network are assigned private IP addresses, which are not directly routable on the Internet. Private IP addresses are used to create a separate address space for devices on the private network, which can be reused across different networks.

Public IP address: The network gateway, such as a router, is assigned a public IP address that is routable on the Internet. The gateway acts as a mediator between the devices on the private network and the Internet.

Translation: When a device on the private network initiates communication with the Internet, the NAT device translates the private IP address of the device into the public IP address of the gateway. The NAT device maintains a table of active translations, which allows it to route incoming traffic back to the appropriate device on the private network.

Reverse translation: When a device on the Internet initiates communication with a device on the private network, the NAT device translates the gateway's public IP address into the private IP address of the device. This routes incoming traffic to the correct device on the private network.

NAT allows multiple devices on a private network to share a single public IP address, which conserves the limited supply of public IP addresses. It also provides a degree of security by hiding the private IP addresses of devices on the private network from the Internet, preventing unauthorized access to the network. However, NAT can introduce latency, so it might not work well with applications that rely on direct communication between devices on different networks.

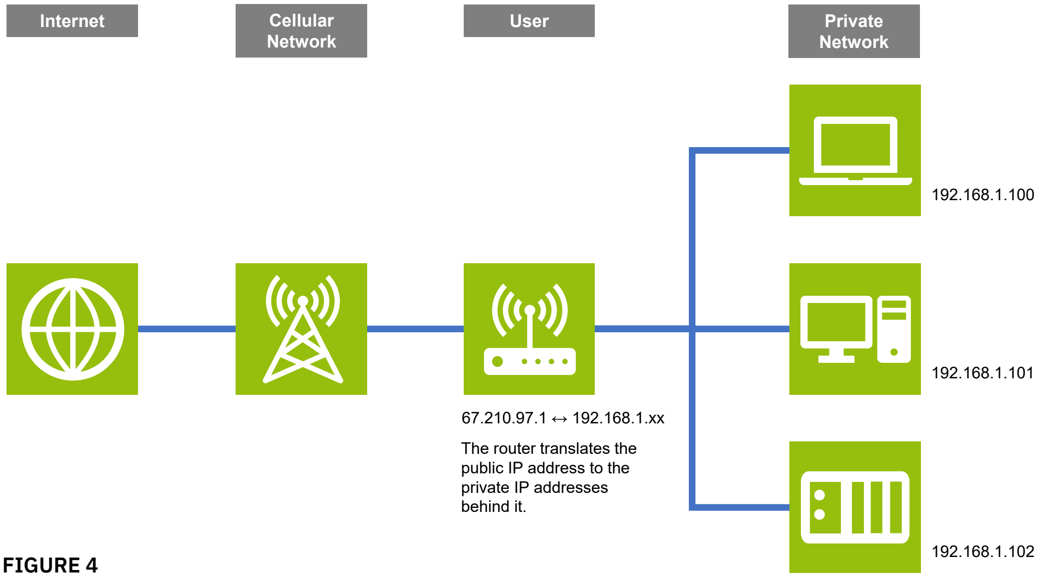

Internet
Cellular Network
User
Private Network
192.168.1.100
192.168.1.101
192.168.1.102
67.210.97.1 ↔ 192.168.1.xx
The router translates the public IP address to the private IP addresses behind it.

FIGURE 4

continued →

Port forwarding

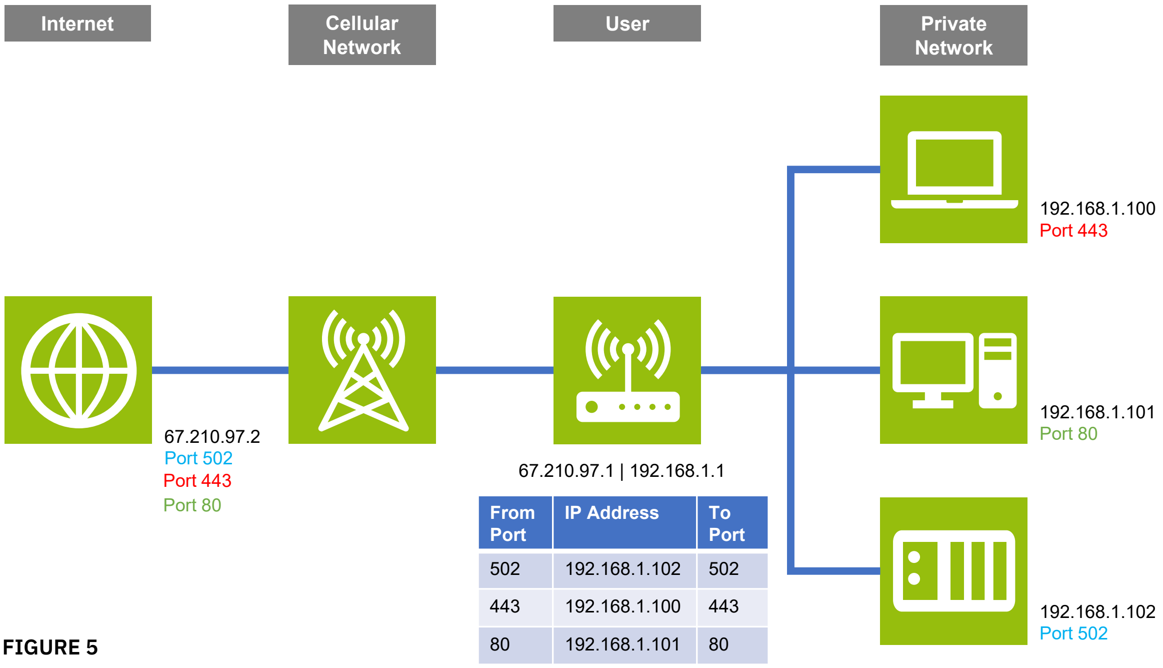
Port forwarding allows incoming traffic initiated by a device on the Internet to be directed to a specific device or service on a private network. Port forwarding maps a specific port on the public IP address of a network to a port on a device or service on the private network (FIGURE 5).

Public IP address: A device on the Internet initiates communication with the cellular router that has a public IP address. The router acts as the mediator between the device on the Internet and the devices on the private network.

Port number: Each service or application running on a device or server has a specific port number associated with it. For example, HTTP traffic typically uses port 80, while HTTPS traffic typically uses port 443.

Inbound traffic: When incoming traffic arrives at the gateway on the specified port, the gateway forwards the traffic to the mapped port on the private network. This allows the incoming traffic to reach the specific device or service on the private network.

Port forwarding allows devices or services on a private network to be accessed from the Internet, which can be useful for hosting a website, remote access to a server or application, or online gaming. However, port forwarding can also introduce security risks by exposing specific devices or services on the private network to the Internet. It is important to properly configure port forwarding and use appropriate security measures to mitigate these risks. ■



From Port	IP Address	To Port
502	192.168.1.102	502
443	192.168.1.100	443
80	192.168.1.101	80

FIGURE 5

continued →

VPN

A VPN (virtual private network) allows users to securely connect to a private network over the public Internet. VPNs create a secure and encrypted connection between a user's device and a remote server, enabling users to access resources on the private network as if they were directly connected to it.

The main features of a VPN include:

Encryption: VPNs use encryption to secure the connection between the user's device and the VPN server, protecting the data from being intercepted or viewed by unauthorized users.

Authentication: VPNs require users to authenticate themselves with a username and password or other credentials to establish a secure connection.

Tunneling: VPNs create a virtual tunnel between the user's device and the VPN server, which ensures that all data transmitted between them is encapsulated and encrypted.

Privacy: VPNs provide users with privacy and anonymity by masking their IP address and location, which helps prevent tracking by advertisers and other third parties.

Most industrial applications for VPN over a cellular network are in a "hub-and-spoke" configuration. Typically, the spokes (remote sites) initiate the VPN connection to the hub (central site).

Having the spokes initiate the VPN can improve network security, scalability, and availability. When the spokes initiate the connection, the hub has no knowledge of the network topology of the spokes, which provides an additional layer of security. It also ensures that only authorized spokes can access the central site.

As the number of spokes increases, it is easier to manage the VPN configuration if each spoke is responsible for initiating its own connection. And if a network fails, this type of VPN can provide a higher level of availability, since each spoke can establish its own connection. This ensures that the network can continue to function even if one or more spokes experience connectivity issues.

Finally, it also simplifies network configuration: The hub only needs to be configured to accept incoming VPN connections from the spokes, which is simpler than establishing multiple outgoing VPN connections to each spoke. ■

Use cases

Cellular routers are used in a variety of industrial applications where Internet connectivity is required in remote or hard-to-reach locations. Some of the primary applications for cellular routers in industrial settings are:

Legacy SCADA (remote monitoring and control)

Cellular routers can monitor and control remote industrial equipment, such as pumps, valves, and sensors. This can help reduce downtime and maintenance costs by allowing operators to quickly detect and respond to issues. In many SCADA applications, the host system periodically requests data from the remote sites, so the IP addresses of those sites must be fixed and known.

In applications that have fewer than 10 remote devices, the simplest and most cost-effective method is to obtain public static IP addresses for each cellular router in the field and use NAT routing or port forwarding to connect to controllers or other devices behind the router.

However, having a public static IP address can also expose the network to more security risks, as attackers can more easily target specific devices or services. Establishing a VPN connection between the cellular router and the SCADA host will help protect the data. If the router supports additional firewall rules, this can further increase protection.

Larger SCADA systems may need to use both a private APN and a secure VPN connection from the SCADA host to the carrier network or MVNO. Establishing a private APN includes a range of private IP addresses that reduce networking complexity. ■

continued →

Internet access/IIoT

Cellular routers can provide Internet connectivity to mobile offices, field service vehicles, skids, or other equipment. This can help improve productivity and communication by allowing workers to access the Internet and company resources from remote locations. It can also be used to bypass IT infrastructure in some cases.

In IIoT applications, the cellular device may establish a network connection on a periodic or event-driven basis to publish data to a cloud platform or other system.

In both cases, since the cellular router or device is establishing the connection and the destination is fixed, a dynamic public IP address can be used. This can be achieved using a standard “IoT” SIM card and data plan. Cellular routers can be configured to route traffic to and from devices below it using NAT routing or exposed host functionality. ■

Remote access

Remote access applications differ slightly from data acquisition (SCADA or IIoT) using cellular routers. In remote access applications, routers are used to allow access to connected devices for maintenance purposes such as firmware updates, configuration changes, or troubleshooting. This may be in parallel with data acquisition. Remote access is achieved through the use of a VPN connection. The way in which the VPN connection is established dictates the requirements of the SIM card, data plan, and services. Using a web-based VPN allows users to use a standard IOT SIM card, as static IP addresses are not necessary. ■

Conclusion

As cellular coverage continues to expand around the globe, the use of cellular routers can provide a flexible and reliable solution for Internet connectivity in remote or hard-to-reach industrial locations. This technology will improve efficiency, safety, and productivity across a wide range of applications. ■

About Phoenix Contact

Phoenix Contact is a global market leader based in Germany. Phoenix Contact produces future-oriented components, systems, and solutions for electrical controls, networking, and automation. With a worldwide network reaching across more than 100 countries, and with over 20,300 employees, Phoenix Contact maintains close relationships with its customers, which is essential for shared success. The company’s wide variety of products makes it easy for engineers to implement the latest technology in various applications and industries. Phoenix Contact focuses on the fields of energy, infrastructure, process, and factory automation.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com**, call technical service at **800-322-3225**, or email **us-info@phoenixcontact.com**.

References

This paper was written with assistance from artificial intelligence. Microsoft CoPilot cites the following sources used to create the original draft.

https://en.wikipedia.org/wiki/Cellular_network

https://cellularnews.com/device-reviews-and-comparisons/mobile/what-are-mobile-networks/

https://www.samsung.com/in/support/mobile-devices/what-is-a-cellular-network-or-mobile-network/

https://www.khoury.northeastern.edu/home/rraj/Courses/6710/S10/Lectures/CellularNetworks.pdf

https://www.techopedia.com/definition/24962/cellular-network

https://pangea-group.net/2022/09/01/everything-you-need-to-know-about-public-and-private-apns/

https://novotech.com/learn/m2m-blog/blog/2023/02/21/9187what-the-heck-is-an-apn-plus-where-to-find-it-and-how-to-change-it/

https://thingsdata.com/miniblog/public-apn-versus-private-apn/

https://1ot.com/resources/blog/vpn-apn-fixed-ip

https://www.hologram.io/blog/whats-an-apn/

https://en.wikipedia.org/wiki/Mobile_virtual_network_operator

https://www.gartner.com/en/information-technology/glossary/mvno-mobile-virtual-network-operator

https://www.tomsguide.com/reference/mvnos-what-are-they-and-what-are-the-best-options

https://www.itu.int/hub/2020/04/the-benefits-of-mobile-virtual-network-operator-mvno-partnerships/

https://www.androidauthority.com/what-is-an-mvno-1140159/

https://www.lifewire.com/what-is-a-static-ip-address-2626012

https://www.pcmag.com/encyclopedia/term/public-ip-address

https://phoenixnap.com/glossary/static-ip-address

https://www.techguide.com.au/news/internet-news/advantages-disadvantages-static-ip-explained/

https://www.hitechwhizz.com/2021/09/advantages-and-disadvantages-drawbacks-benefits-of-static-ip-address.html.html.html

https://www.comptia.org/content/guides/what-is-network-address-translation

https://en.wikipedia.org/wiki/Network_address_translation

https://csrc.nist.gov/glossary/term/Network_Address_Translation

https://blog.davidvarghese.dev/posts/nat-explained/

https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-network-address-translation-nat/cisco-ccna-nat-advantages-a-disadvantages/

https://www.geeksforgeeks.org/advantages-and-disadvantages-of-nat/

https://en.wikipedia.org/wiki/Port_forwarding

https://www.makeuseof.com/important-vpn-features-explained/

https://www.tomsguide.com/features/how-does-a-vpn-work

https://us.norton.com/blog/privacy/what-is-a-vpn

https://www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke

https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/hub-spoke-network-topology

https://www.aveva.com/en/perspectives/blog/going-cellular-for-remote-scada-data/

https://usatcorp.com/advantages-limitations-cellular-communication-scada/

https://www.isa.org/intech-home/2017/january-february/features/using-cellular-data-for-scada-data

https://lte.callmc.com/advantages-limitations-cellular-communication-scada/

https://novotech.com/learn/m2m-blog/blog/2022/02/08/cellular-router-lte-routers/

https://www.oliviawireless.com/public-fixed-ip-routes

https://www.soracom.io/blog/remotely-access-iot-devices-behind-cellular-routers/

https://help.ui.com/hc/en-us/articles/115012240067-UniFi-Remote-Management-Requirements

https://www.pusr.com/blog/OpenVPN-Application-Scenario-of-Best-Cellular-Router