Private Network roles and responsibilities

Customer guidelines

Introduction

This document presents the roles and responsibilities associated with Verizon Wireless Private Network. The use of Private Network is subject to your service agreement with Verizon Wireless.

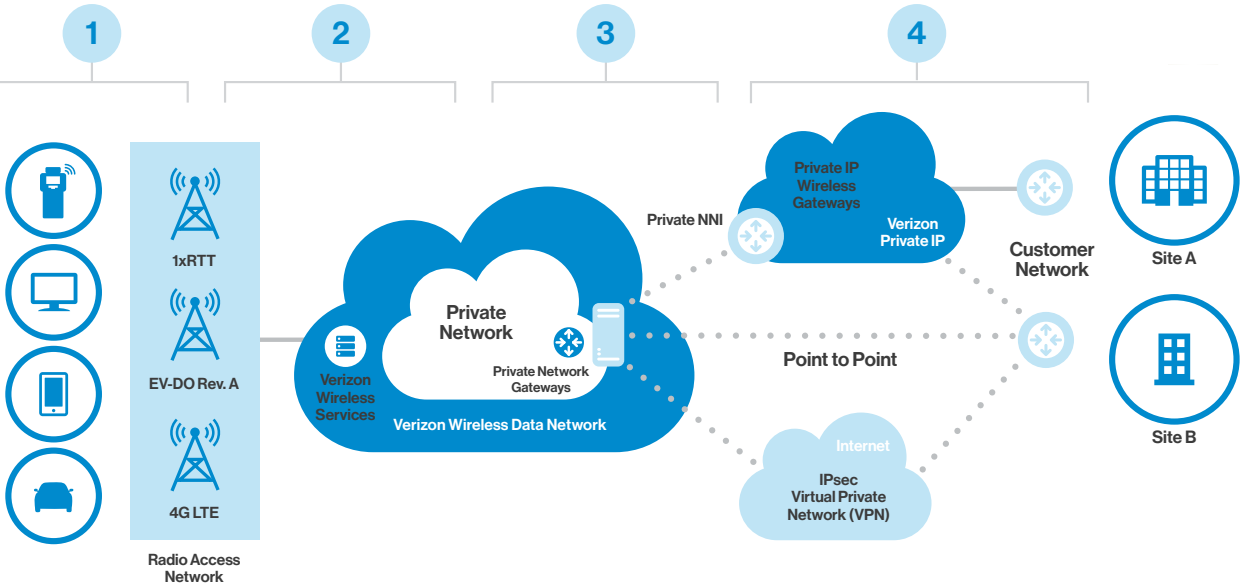
Private Network description – overview

Verizon Wireless Private Network extends your IP networks to mobile workers and wireless connected devices by segregating the data from the public internet. With Private Network, you can deliver mission-critical information easily to your mobile workforces and connected devices on the largest high-speed wireless network in America, while reducing concerns over security and reliability related to the public internet. Having data communications segregated from the public internet blocks unsolicited traffic and reduces security risks associated with malware, viruses, spyware and worms. Private Network offers organizations a reliable and secure wireless extension to IP networks that provides complete control over device network access to internal applications and resources.

Enhanced by Verizon 4G LTE technologies, Private Network enables a fast, direct connection to internal systems and applications without compromising network control and manageability. It gives organizations a competitive edge to fuel growth and safely integrates wireless devices into their networks. It lets mobile workers, machine-to-machine (M2M) solutions and physical sites wirelessly connect without compromising internal networks, applications or data.

With a Private Network:

- Devices are authenticated and authorized for each Private Network (only authorized data can traverse the designated network).
- Data is routed per your IP pools associated with your Private Network.
- Dedicated Private Network Gateways are designated.



Connectivity options

With Private Network, there are multiple methods offered to connect to your corporate configuration. These connectivity options include:

Option 1: Verizon Private IP

If your company is already a Verizon Private IP customer, you can use that Private IP network to connect to the Verizon Wireless network. This approach allows you to implement Private Network without affecting your existing network topology. If your company is not a Private IP customer, Private Network and Verizon Private IP can be implemented together. Either way, you can combine the benefits of wireless with the benefits of a multiprotocol label switching (MPLS) network.

When implemented with Verizon Private IP, all wireless data traffic can be routed directly to any location connected to your Private IP network. This simplifies network routing scenarios and provides redundancy for business continuity. You can also access additional hosted services from Verizon that can help increase your return on investment as well as better position your business for the future.

Option 2: IPsec VPN

You can use virtual private networks (VPNs) to create a secure tunnel between your internal network and the Verizon gateway. This can be a simple and effective solution if your IT staff is already familiar with setting up and managing VPN environments. This option encrypts all traffic from the Verizon Wireless Private Network gateway router and sends it over the tunnel through the public internet to your company location. By layering additional technologies, you could also encrypt the entire path.

Option 3: Dedicated physical circuit

You can also complete the Private Network build-out by installing a dedicated physical circuit at your location to connect to Verizon Wireless. Since the circuit is dedicated, you'll have the entire bandwidth available for use. The use of additional encryption technology becomes optional under this implementation since no data will traverse the public internet.

Option 4: Wireless to wireless

Zero-tunnel configurations are for solutions that require only mobile-to-mobile communications, which use wireless connectivity to your data center instead of a wireline connection. Zero-tunnel configurations have no communication outside of the mobile IP pools and can be designed as a hub-and-spoke configuration in which the central wireless device at the data center provides access between the customer-hosted applications and the devices in the field. With this configuration, you need to consider your data-plan usage because the central wireless device's data traffic is a composite of all data traffic traversing the connection to the data center from all of the field/mobile devices.

Redundancy

Verizon requires connectivity redundancy. Connectivity redundancy provides a backup path when the primary connection between Verizon and the enterprise network experiences a failure that prevents traffic from moving over the connection. To provide connectivity redundancy, each Private Network is built with a primary and secondary gateway. The secondary gateway acts as a hot standby to provide support if the primary gateway experiences a failure and can no longer operate. Once the primary gateway becomes operational again, traffic redirects back to the primary gateway and the secondary gateway returns to hot standby mode.

Customer premises equipment

Customer premises equipment (CPE) used for the connectivity with the Private Network Gateway must meet functionality requirements to provide a secure and acceptable level of performance. Any routers and other CPE that you procure must meet Verizon Wireless requirements for Private Network connectivity. You're responsible for ensuring any CPE meets data capacity and throughput needs. The requirements vary by connectivity type, which are stated in the guidelines below. It is recommended that you contact your Verizon sales representative for the latest CPE guidelines.

Option 1: Verizon Private IP

The connectivity between the Private Network Gateway and Verizon Private IP network has dedicated network-to-network interfaces. These deliver the data traffic between the two networks. For wireline connectivity with Private IP, there are CPE requirements for both Private IP Standard and Enhanced Traffic Management (ETM) solutions.

If you have sites using Private IP Standard, you do not mark any traffic. Instead, traffic is policed at the Private IP provider edge (PE) device. At a minimum, you need to use routers that can support both Internet Protocol (IP) and Internet Engineering Task Force (IETF) frame-relay encapsulation.

If you have sites using Private IP ETM, you control your traffic at the customer edge (CE) or router, and you'll have multiple priority classes to mark your traffic. At a minimum, your routers need to support IP, IETF frame relay, and either Differentiated Service Code Point (DSCP) or IP precedence.

Note: Routers that support a proprietary version of Asynchronous Transfer Mode (ATM)/frame-relay protocol are not supported. And routers that are deemed end-of-life (EOL) status by their manufacturer are not supported.

Option 2: IPsec VPN

Private Network Gateway connectivity to your premises using IPsec VPN requires CPE that meets the following criteria:

- Support Border Gateway Protocol (BGP).
- Support Generic Routing Encapsulation (GRE) tunnel.
- Terminate IPsec tunnel in transport mode.
- Virtual Tunnel Interface (VTI) with IPsec encapsulation:
  - Private Network only supports static VTI. Dynamic VTI is not supported.
  - IPsec transform set must be configured in tunnel mode only (default).
  - The CPE device must be able to terminate BGP, GRE and IPsec.

Option 3: Dedicated physical circuit

Private Network Gateway connectivity to your premises using dedicated physical circuit requires CPE that meets the following criteria:

- Support BGP.
- Support GRE tunnel.
- Terminate IPsec tunnel in transport mode.
- Virtual Tunnel Interface (VTI) with IPsec encapsulation:
  - Private Network only supports static VTI. Dynamic VTI is not supported.
  - IPsec transform set must be configured in tunnel mode only (default).
  - The CPE device must be able to terminate BGP, GRE and IPsec.

Option 4: Wireless to wireless

Only Verizon Wireless devices approved for Private Network activations may be used.

Customer responsibilities

Implementation of Private Network

You are responsible for providing the resources to work with the Verizon solution engineer (SE) through the Private Network implementation process. This includes the following activities:

1. **Private Network connectivity form**
   Provide the required information to complete the form, such as contacts, IP pools and CPE. This information is used to build the connection between the Private Network Gateway and your premises, along with how IP addressing will be assigned to the wireless devices. Completing the Private Network connectivity form with accurate information is crucial to timely building a Private Network. Any missing or incorrect information will result in delays in building out the Private Network.
   a. You are responsible for procuring private IP addresses, which must be communicated to Verizon Wireless during implementation. Private Network supports static and dynamic addressing for 1X service and/or EV-DO service, 4G LTE service and internet addressing system Internet Protocol version 4.
2. **Turn-UP call**
   a. You are responsible for having the CPE prepared to support the Private Network connection. Readiness involves configuring your CPE. This might include activities such as Phase I exchange of pre-shared keys and/or Phase II setup of the IPsec tunnel.
   b. You need to provide resources to participate in the Turn-UP, which validates the connectivity from Private Network Gateway to your premises. Personnel supporting the Turn-UP call must have the CPE knowledge of the configuration being used and have the authority and capability to make configuration changes as necessary. This includes expertise on the configuration of the IPsec tunnel, Domain Naming System (DNS), Network Address Translation (NAT) and firewall. It also includes the ability to monitor, trace and troubleshoot to confirm that the connection is operational.
   c. The Verizon sales team will communicate to you the proposed Turn-UP call dates. It is expected that you will be able to provide the necessary personnel for the selected Turn-UP call date.
3. **Customer test**

Upon successful Turn-UP call, Verizon will release up to 10 IP addresses associated with your Private Network. You are responsible for activating a limited number of devices to validate their connectivity to your applications. If successful, you will use those devices to provide the Verizon solution engineer with trace routes and ping tests.

4. **Wireless Enterprise Help Desk**

Upon completion of the Turn-UP call, you will receive a welcome packet that provides details on

engaging Wireless Enterprise Help Desk (WEHD) for Private Network support. This information should only be shared with those personnel on your help desk that have been designated to support your Private Network implementation.

a. Enterprise Customer Management System (ECMS). You will have a profile established within ECMS in order to receive support from WEHD. Once the ECMS profile has been approved and customer testing was successful, Verizon will make available the remaining IP addresses within your Private Network build.

Other customer responsibilities

Network Event Notification

Network Event Notifications (NENs) provide alerts to scheduled network maintenance or network outages that may impact your Private Network performance. You have the option of receiving NENs via email to designated personnel for the following events:

- Planned and/or unplanned work or outages
- Low and/or high priority—what are the chances this event would affect your network and/or devices?
- Technology affected (i.e., 1xRTT, EV-DO, LTE and push to talk)
- Enterprise Wireless Gateway (primary or backup data center where your private network is based)
- Geographic location (region, state or city)

The Verizon Wireless solution engineer and WEHD personnel will work with you in completing the NEN profile.

Customer premises equipment

It is your responsibility to select CPE that meets the requirement for connectivity. You should consult with your equipment vendors to determine if their routers support the minimum requirements.

Device guidelines

Only Verizon Wireless–approved devices may be activated. 4G devices must be verified for Private Network usage. It is recommended that you contact your Verizon sales representative for the latest approved devices.

M2M configuration guidelines

Devices classified as Internet of Things (IoT)/M2M must conform to the "Application, Device, Network Usage Guidelines for IoT and M2M." Your sales team can provide a copy of these guidelines.

Support enterprise-class APN

Each Private Network built will have a unique access point name (APN). The typical structure for Private Network enterprise-class APN is: [COMPANY].GW [XX].VZWENTP

Field values:

- [Company] is the derived company abbreviation.
- GW[XX] is the Gateway number associated with your Private Network.
- VZWENTP is the enterprise indicator.

4G-capable devices must support enterprise-class APN. Verizon 4G LTE device requirements contain specific requirements that the device vendor must conform to in order to support enterprise-class APN. This conformance is verified as part of Verizon Wireless device certification.

3G CDMA devices

Private Network requires use of mobile IP (MIP) protocol when on 3G and 2G networks for non-4G-capable devices.[1] MIP is designed to support host mobility. This allows mobile device users to move from one network to another without the need to change the device's IP address. As a result, devices can stay connected to the network regardless of their location. This is made possible by the ability of MIP to track a mobile host without the need to change the mobile host's long-term IP address.

Roaming

Private Network supports device connectivity when leaving the Verizon Wireless network footprint (aka outbound roaming) with approved Verizon roaming providers whose wireless technologies may include GSM, UMTS, HSPA or 4G LTE.

In order for a device to roam with Private Network, you must take the following into consideration:

1. The device must be Verizon Wireless certified and have the proper modem to connect to the roaming provider's network.
2. The SIM profile used within the device must contain plans that support roaming within the desired geographic area.
3. Devices must initially be activated on the Verizon Wireless U.S. network to allow the enterprise APN to be correctly configured per over-the-air delivery.
4. Guidelines associated with international IoT and M2M roaming requirements will apply.
5. Only the Verizon IMSI is supported.
6. 3G-only (non 4G LTE-capable) devices are not supported.

When roaming off the Verizon Wireless network, the data connection with Verizon Wireless will be dropped and a new data connection will be established with the roaming provider's network. This new connection will send the data traffic to Verizon Wireless, which will be routed to the EXGW associated with your Private Network.

Private Network options

Private Network offers features that enhance your overall experience. These are optional Private Network build capabilities. You have the following responsibilities associated with these options. In order to include these options as part of your Private Network solution, you will be required to meet the guidelines described below.

Machine to Machine Management Center

The M2M Management Center is a self-service portal with specialized features for managing the connectivity of M2M devices. This lets you monitor near real-time device usage and connection status, and set up notifications to alert you when a specific event occurs or when a predefined threshold is exceeded. It also lets you generate current and historical reports on device usage, provisioning and connected data sessions. You can easily access the M2M Management Center from the My Business Account or Verizon Enterprise Center portals.

You are responsible for the following to enable M2M Management Center:

1. Establish a My Business Account or Verizon Enterprise Center profile.
2. Provide resources to work with the Verizon Solution Engineer through the M2M Management Center implementation process, which includes these activities:
   a. Provide at least 10 device IDs.
   b. Meet any Verizon legal requirements per National Account Agreement (NAA); Major Account Agreement (MAA); state and local government agreement; or other Verizon customer agreements.
   c. Supply contact information to those authorized to access the M2M Management Center.

Customer account self-management

You can manage your wireless accounts through either My Business Account or Verizon Enterprise Center. These portals offer self-service ability in ordering, account maintenance, billing and reporting. To enhance your experience we let you make changes to your account an d devices used within your Private Network. This includes the ability to provision, manage and report IP addresses.

You are responsible to work with your Verizon account team to establish a profile to access these portals.

Service-based access

Service-based access (SBA) enables access to Verizon's Visual Voice Mail, multimedia messaging services and 3G location-based assisted-GPS services. Only devices approved by Verizon will be allowed for access with solutions that use 3G assisted-GPS service. This requires meeting the following criteria:

1. Open Development device certification
2. Location-based services interoperability testing

Private Network regression testing

You are responsible for any charges associated with the customization of your CPE to support SBA.

Private Network Traffic Management

Private Network Traffic Management (PNTM) provides a premium and differentiated network experience. It enables application differentiation and quality of service (QoS) over the 4G LTE Private Network using standards-based IP packet marking (IP DSCP) to create IP traffic preferences for business-critical applications and to achieve more predictable application performance during times of peak network demand. With PNTM, your business can improve your users' experience during peak network demand through:

- **More control.** When the wireless 4G LTE Private Network becomes congested, PNTM gives you the ability to prioritize your applications for optimal performance.
- **Higher productivity.** With more predictable application performance during high-traffic periods, you can use business-critical applications when and where you need them.
- **Increased flexibility.** PNTM lets you map your applications into the Business Critical Class of Service (CoS) based on the applications' requirements.
- **New potential.** PNTM extends QoS policies traditionally provided on fixed WAN to the 4G LTE Private Network, giving you expanded 4G LTE Private Network control.

Only user SIM profiles that contain the PNTM feature will be supported with CoS capability. You are responsible for selecting the appropriate CoS

to be associated with the SIM profile, as well as any associated charges with the service and any charges associated with the customization of its CPE to support PNTM. 4G LTE Private Network subscribers with unlimited data plans are ineligible for PNTM.

PNTM capability will not be in service when roaming off Verizon Wireless network since the roaming provider's network can't establish the dedicated bearer used for PNTM.

PNTM for Public Safety

Eligible public safety accounts can take advantage of priority access to a data channel over the wireless service for its data traffic during times of heavy network demand. While PNTM for Public Safety enables a dedicated data channel, Verizon Wireless makes no guarantee of wireless service availability, which is subject to the limitations of wireless service availability as detailed in the agreement. PNTM for Public Safety is only available to customers approved by Verizon Wireless that qualify as Public Safety Entities classified by the following NAICS codes:

- 621910 Ambulance Services
- 922110 Courts
- 22120 Police Protection
- 922160 Fire Protection
- 922190 Other Justice, Public Order, and Safety Activities

Dynamic Mobile Network Routing

Dynamic Mobile Network Routing (DMNR) allows configuration of Private Network for dynamic routing support of mobile or stationary routers to the subnets it serves (up to eight) to other devices on your network. DMNR is based off Mobile IPv4-based Network Mobility protocol and requires the router to be configured to support this capability. You are responsible for the configuration and any charges associated with the customization of your CPE to support DMNR.

Customer-hosted E-AAA

In a customer-hosted enhanced authentication, authorization and accounting (E-AAA) configuration, the Verizon authentication, authorization and accounting (AAA) server acts as a proxy to your E-AAA and requires a physical circuit to connect the customer-hosted E-AAA with the Private Network AAA. You must provide geographically diverse primary and failover servers and associated dedicated connections. Connectivity to customer-owned E-AAA servers over VPN connection is not supported. Customer-hosted E-AAA configuration will require certification of your E-AAA proxy servers.

For solutions involving customer-hosted E-AAA, you are responsible to:

1. Provide the information required within the Private Network connectivity form.
2. Provide the physical circuit to be terminated at a Verizon Wireless fixed-end system (FES) location. You are responsible for charges associated with the circuit.
3. Submit your E-AAA server for certification and pay associated certification costs.
4. Only Bridgewater or Bridgewater-certified equipment is supported today for authentication and authorization E-AAA functionality. This certification is conducted by Bridgewater/AMDOCS, which charges a fee for the testing. You will be responsible to pay to Bridgewater/AMDOCS for the testing. A Verizon representative can provide guidance to the certification process.
5. Provide geographically diverse primary and failover E-AAA servers and the associated dedicated connections.

Data records streaming

Private Network supports the option to have a direct feed of Remote Authentication Dial-In User Service (RADIUS) accounting records (start and stop fields/attributes) sent from the Verizon Data Streaming Server (DSS) to an accounting server you designate. You will receive the RADIUS file with the raw data (without modification or customization) that you can parse according to your reporting needs. Your receiving server must be capable of receiving and acknowledging raw accounting information. A physical circuit is required for sending the accounting records from Verizon Wireless to your accounting server. You are responsible for charges associated with the circuit.

Split Data Routing

Dual Access Point Name (APN) provides simultaneous data sessions to a Private Network and the internet from an enterprise-owned device. The functionality is device driven where the Class 3 APN value data traffic is associated with internet destination and the Class 6 APN value data traffic is assigned to the Private Network connection. Verizon provides the ability to route the data traffic to the gateway within its network based on the Class APN value the device has chosen to route the data. Mobile-originated data into Verizon's network will be based on the Class APN the device has chosen to route the data. For example, Class 3 APN data will be routed within Verizon's network to a public gateway that connects to the

public internet, while Class 6 APN data will be routed to the Private Network gateway that contains the customer's build.

The wireless device selected must have the ability to:

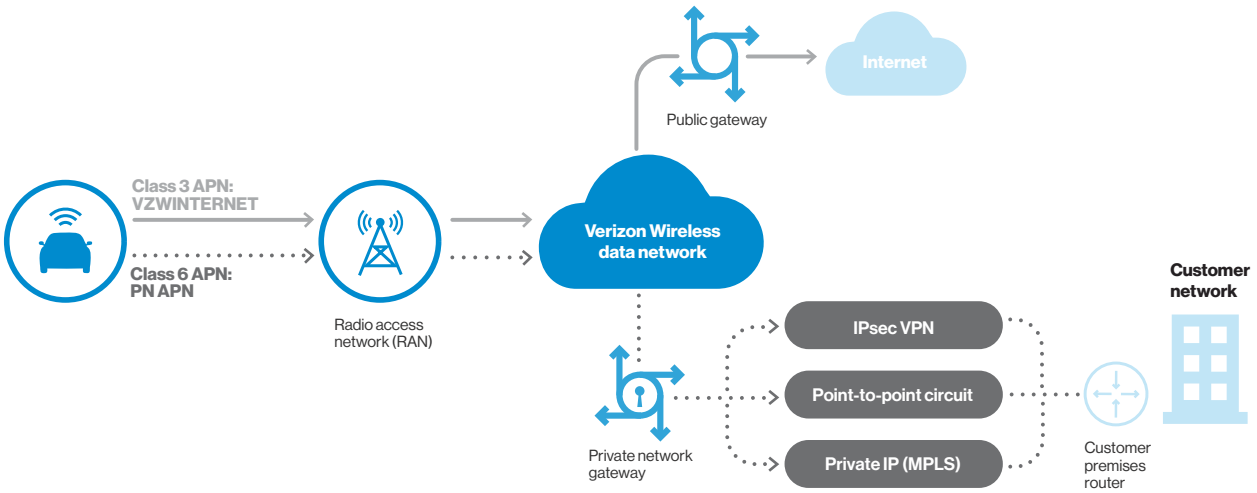
- Support multiple APNs based on the *LTE Data (LTEDATA) Device Requirements* issue April 2016 or later.
- Route internet-designated data traffic using the Class 3 APN and data traffic categorized for the customer's Private Network using Class 6 APN.
- Separate internet and private data traffic to ensure internet data uses Class 3 APN only and private data uses Class 6 APN only.

For solutions involving Dual APN, it's your responsibility to:

- Confirm with your Verizon account team that your billing profile contains the Dual APN special feature offerings.
- Select devices that support Dual APN.
- Accept that the device has the capabilities required by you to protect your private data traffic from internet data traffic. The device must provide protection in keeping private data private by not allowing internet data traffic to mix with private data associated with your Private Network. Data within the device is managed by the device or its applications, Verizon is not responsible for device data management and how the device protects data associated with Private Network from data associated with the internet.
- Select one of the billing options:
  - **Single-party billing.** You will be billed for both the internet and Private Network data traffic as part of your data price plan.
  - **Multi-party billing.** You can have internet data traffic billed to an entity other than your Private Network account.

Learn more.

To learn more about Verizon Wireless Private Network, contact your Verizon Wireless business specialist or visit us at **verizonwireless.com/contactrep**



1 Mobile IP capability only applies to Verizon Wireless 3G and 2G devices.
Network details & coverage maps at **vzw.com**. © 2017 Verizon. UG02640317