White paper

Verizon Wireless Private Network

verizon

Contents

1. Introduction

This white paper provides an overview of Verizon Wireless Private Network as a solution to meet business and government needs in delivering data traffic securely from the customer's Internet Protocol (IP) network (intranet) to devices over the Verizon Wireless network. The information presented within will allow the reader to understand the innovation and promise offered by Verizon Wireless Private Network.

1.1 Audiences

This white paper has been developed for business and government customers, IT administrators, technical decision makers and Verizon sales associates and solution engineers. It is assumed that the reader has an understanding of wireless technologies, as well as of computers and networks.

2. Executive summary

2.1. Wireless standards

The evolution of wireless broadband technology to Long Term Evolution (LTE), with its enhanced capabilities, serves as an enabler to support wireless connectivity to applications and information. The need to ensure that data and communications are secure between the wireless device and the IP network is critical. It's equally critical that only authorized users gain access to that information. To limit risk, organizations need to have control and management capabilities over the wireless network.

Verizon Wireless Private Network extends customers' IP networks to mobile workers and connected devices by segregating the data from the public Internet. This effectively reduces the security risks that result from unprotected public networks with access through public gateways.

Mobile workers, machine-to machine (M2M) solutions and physical sites can now be wirelessly connected, without compromising internal networks, applications or data.

Private Network, enhanced with Verizon 4G LTE technology, enables a fast, direct connection to internal systems and applications without compromising network control and manageability, giving organizations a competitive edge to fuel growth and safely integrate wireless devices into their networks.

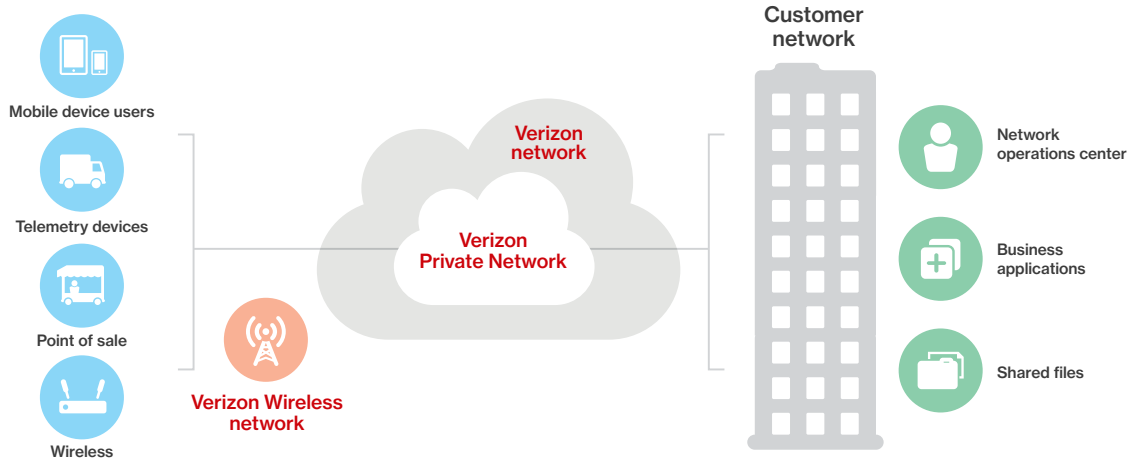


Figure 1: How Verizon Wireless Private Network functions

3. Verizon Wireless Private Network

Verizon Wireless Private Network was created to enable Verizon 3G and 4G LTE wireless devices to send and receive data to and from the customer's IP network, without traversing the public Internet. With Private Network, customers can deliver mission-critical information easily to their 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, providing complete control over device network access to internal applications and resources.

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 the customer-specific IP pools.
- Dedicated Private Network gateways are designated.
- A direct connection is created between Private Network gateways and the customer premises router.

Data travels from wireless devices connected to the radio access network, through the private network to a dedicated connection to the customer's network. Each customer has its own private network whose traffic is kept isolated from the public Internet, avoiding unnecessary risk associated with unsolicited public Internet traffic. Only customer-authorized subscribers may send and receive data.

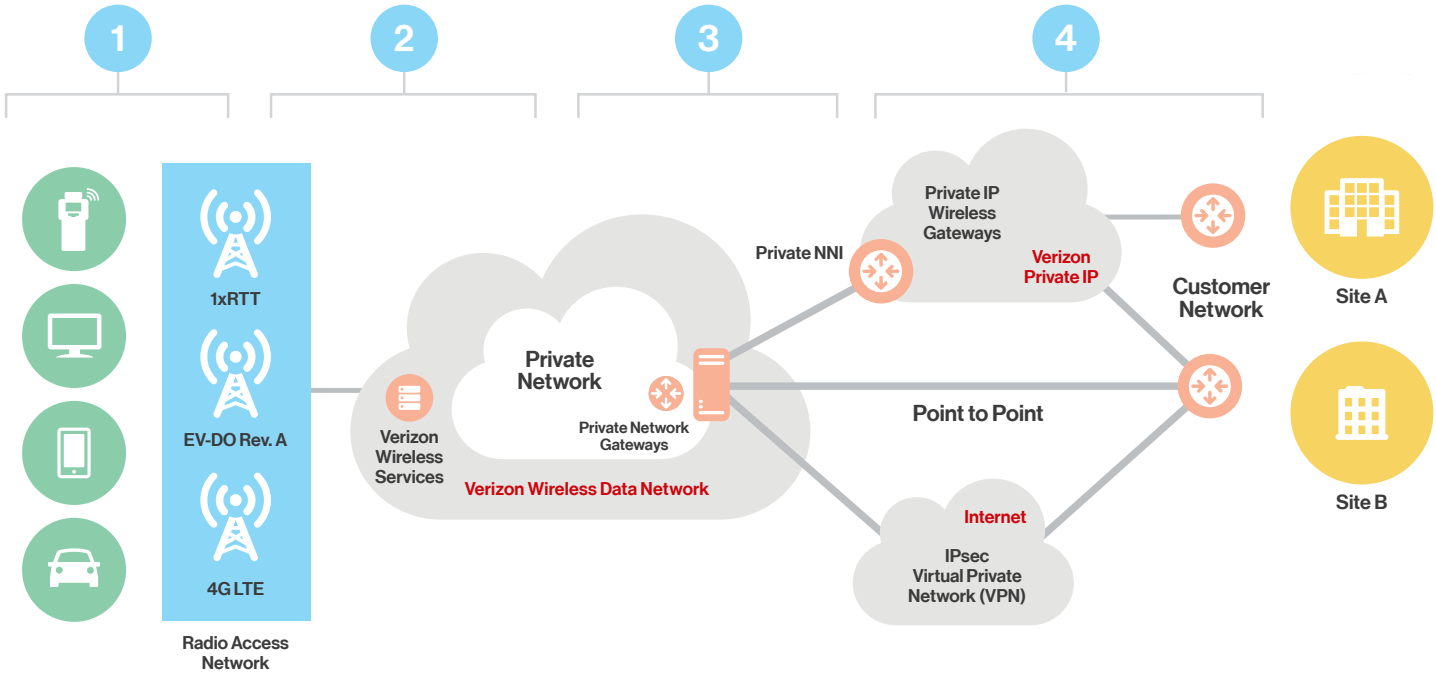


Figure 2: How Verizon Wireless Private Network functions

4. How does Verizon Wireless Private Network work?

Device access to the radio access network
When a wireless device is provisioned on a Private Network, it is authenticated and authorized by Verizon authentication, authorization and accounting (AAA) servers to ensure that it has been conditioned for Private Network access. A device is conditioned with specific feature codes to provide the proper level of authorization onto the Private Network. Those codes provide guidance to the radio access network and wireless data network on how to route data traffic.

In addition to specific feature codes, each Private Network built with 4G LTE access is assigned a unique access point name to ensure that only the company's provisioned devices communicate within their Private Network.

See the white paper *Verizon Wireless 4G LTE Network: Transforming Business with Next-Generation Technology* for insight into the market-leading Verizon Wireless network.

Data network
Each Private Network is built with customer-specific IP pools whose IP addresses are assignable only to customer-authorized devices. Private Network isolates the customer's data from the public Internet and routes it to a specific Private Network gateway.

Connectivity to customer network
Each Private Network is built with a dedicated connection between the Verizon network and the company's network. This connection is established between the Private Network gateway and the customer premises equipment (CPE), which allows access into the company's IP network with its hosted applications. By having a dedicated connection, the public Internet's best-effort routing paths are avoided, and concerns over data security are reduced.

Private Network supports multiple connectivity options, which include:

- Verizon Private IP MultiProtocol Label Switching (MPLS) network
- Dedicated physical circuit such as point-to-point T1/DS3
- Dedicated virtual private network (VPN)

The Private Network solution uses IPsec between the Private Network gateway and customer premises to enhance security measures by authenticating and encrypting each IP packet of the data stream, and is compatible with most VPN technologies, as well as with the Verizon Enterprise Solutions Private IP MPLS network.

4.1. Connectivity options

There are a variety of connectivity options for creating the connection between an organization's IP network and the Verizon Wireless Private Network. Organizations can attach to the Verizon Private Network via Verizon Enterprise Solutions Private IP MPLS; VPN over Internet; dedicated point-to-point circuits such as T1; or a mobile-to- mobile Zero Tunnel solution.

Zero Tunnel connectivity
Zero Tunnel connectivity is designed for customers that require only mobile-to-mobile communication, which does not require connectivity from the Private Network gateway to the customer premises (i.e., Private IP, dedicated circuit, VPN). Zero Tunnel configuration has no communication outside of the mobile IP pools and be designed as a hub-and-spoke configuration where the central wireless device at the customer data center provides access to the customer-hosted applications to the field/mobile devices.

Option	Benefit	Consideration
Verizon Enterprise Solutions **Private IP (MPLS)**	• Leveraging existing enterprise network topology, maximizing application flexibility and potential for seamless diversity. • Global network. • Direct, meshed connectivity to all enterprise locations via single Private Network interface for optimized application performance and inherent data-center redundancy. • Extends enterprise WAN infrastructure. • Last-mile diversity. • Private Network redundancy through second Private IP wireless gateway. • Verizon Enterprise Solutions Management. • Secure. Traffic does not traverse the public Internet.	• Border Gateway Protocol (BGP) routing. • Customer AAA proxy server not supported on the same MPLS connections. • Requires separate dedicated physical circuit connection between customer's AAA proxy server and Verizon Wireless proxy server. • Connection port fees. Only the primary connection has fees (secondary port is offered as part of the primary port).
VPN	• Low cost. • Secure. Established direct connection between networks. • Ease of creating redundant connections so if primary VPN fails, sending traffic over secondary can be easily performed.	• BGP routing. • Not supported for enhanced AAA (E-AAA) connectivity. • IPsec Transport Mode/Generic Routing Encapsulation (GRE) or IPsec/Virtual Tunnel Interface (VTI) required • Non-meshed network connection so no site-to-site routing via single Private Network interface.
Dedicated physical circuit	• Secure. Traffic does not traverse the public Internet. • Full routing control. • Private Network redundancy through dual-circuit configuration to Verizon Wireless gateways.	• BGP routing. • Verizon supports only customers that implement access control policies to protect their networks. • IPsec Transport Mode/GRE or IPsec/VTI required • Non-meshed network connection so no site-to-site routing via single Private Network interface. • Connection fees. Circuit fees depend upon customer's local exchange carrier.

Redundancy
Network redundancy provides a backup path when the primary connection experiences a failure and can no longer support data traffic. Each Private Network is built with a primary and secondary gateway where the secondary gateway acts as a hot standby to provide support when the primary gateway has experienced a failure and can no longer operate. Once the primary gateway becomes operational, traffic will be redirected to the primary gateway, and the secondary gateway will go back into hot standby mode.

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. Verizon requires the connectivity redundancy.

Private Network with Verizon Private IP connectivity
For Private Network with Private IP, there is a primary and secondary network-to-network interface (NNI) between the Verizon Wireless data network and the Verizon Private IP network. The primary connection is between the primary Private Network gateway and a Private IP wireless gateway, while the secondary connection is between the secondary Private Network gateway and a secondary Private IP wireless gateway. If the primary connection becomes unavailable, the data traffic will be diverted to the secondary connection.

Private Network with dedicated circuit connectivity
The customer is responsible for ordering dedicated circuits, such as point-to-point T1/DS3, with their local exchange carrier. With dual circuits, the customer will have a backup connection to Private Network when the primary circuit becomes unavailable.

Private Network with VPN connectivity
A redundant VPN structure would require the establishment of a dedicated VPN between the primary Private Network gateway and the CPE, along with a second dedicated VPN between the secondary Private Network gateway and CPE. For more resiliency, it is strongly preferred that the CPE be independent pieces of equipment rather than using the same CPE to support the primary and secondary VPN.

4.2 IP addressing

Private Network offers a variety of IP addressing options that provide several levels of accessibility, protection and manageability. These options include enterprise-owned, private IP address assignment to the devices, essentially making the device a virtual extension of the wired enterprise network. This allows enterprise IT administrators to manage mobile stations and LAN devices using the same tools and techniques. For example, companies can use the same firewall and routing schemes, and the IT administrators define which users get Internet access. This makes it easier for enterprise IT administrators to manage and monitor network usage and enforce company IT policies.

Mobile-to-mobile intra- and inter-pool separation

The ability to control device access within a pool group and between pool groups is supported by Private Network. By default, mobile-to-mobile access is permitted between all mobile devices within a Private Network environment. This includes access between mobiles within a single pool (intra-pool) and between pools (inter-pool) within a single Private Network.

If mobile-to-mobile access is not wanted, it can be blocked within a single pool, and between specified pools. For example, if a Private Network is built with three pools (POOL A, POOL B and POOL C), mobile-to-mobile access can be permitted within POOL

IP addressing type	Description
Dynamic IP	Assign a random address from a pool provided by the customer to the mobile devices. Once the user disconnects from the network, the dynamic IP address goes back into the IP address pool so it can be assigned to another user. Customers can specify any desired range of public or private IP addresses to assign to mobile endpoints (devices). Please note that all dynamic pools will be managed by Verizon Wireless AAA.
Static IP	Assign a permanent address that allows the mobile device to maintain the same IP address every time it connects to the network.

Static IP options

IP addressing type	Description
Static IP – customer hosted	Customer controls device IP assignment by using their own AAA server. Customer supports their own IP addressing management. All customer-hosted AAA servers must be certified to operate on Verizon Wireless network. (See “Customer-hosted AAA.”)
Static IP – Verizon Wireless hosted	Verizon Wireless hosts static IP addressing for customer-provided IP pools. Customer may specify IP assignment by mobile device or allow Verizon Wireless to assign the mobile device to the IP address.
Static IP – Verizon Enterprise Solutions hosted	Static IP address will be assigned to the Verizon Enterprise Solutions–managed router for remote monitoring and management. The Verizon Enterprise Solutions Managed Network Service Organization provides IP addresses that are assigned.

A and between POOL A and POOL C, but blocked between POOL A and POOL B. Alternatively, mobile-to-mobile access can be blocked within POOL B, but permitted between POOL B and POOL C. Intra-pool blocking can be configured on one or multiple pools.

Within a Private Network, the mobile-to-mobile intra- and inter-pool separation allows the creation of any-to-any (mesh) or hub-and-spoke mobile traffic-flow designs.

4.3 Tiered Hierarchy

Tiered Hierarchy design provides separate accounting/billing of data traffic for customers with multiple agencies, business units, departments or organizations whose data traffic transverses over a single private network. Billing can be separated for each agency, business unit, department or organization profile. Tiered Hierarchy is based on a parent/child relationship in which the parent is the entity that manages the data center associated with the connection to Verizon Wireless (e.g., corporate headquarters) and the children would be the business units, departments and agencies that will utilize the network.

Each parent or child entity has its own customer profile ID. To assist in determining if Tiered Hierarchy would be of benefit, the following two questions should be answered:

- Which entity is responsible for the connection to Verizon Wireless Private Network?
- Which entity is responsible for billing on the mobile devices?

If both answers are the same entity (customer profile), then Tiered Hierarchy is not required. If the entity (customer profile) is different—response to question 1 is the parent, while question 2 response is the child—then Tiered Hierarchy should be deployed.

Tiered Hierarchy pool types

A child company can choose to share a dynamic pool of IP addresses with other child accounts or have its own exclusive static or dynamic IP pool assigned. Additionally, the parent account can request an exclusive IP pool for testing, development, etc. Pools can be flagged as Reserved, Exclusive or Shared, and may be dynamic or static.

- Reserved pools are those that are built ahead of time under a parent account but unavailable for use. These will later be assigned to specific child companies as those accounts are built out. A reserved pool becomes exclusive as soon as it is assigned to a child.
- Exclusive pools are those that can only be accessed by one entity: the parent or any child company. Once the pool is assigned exclusively to an account, no other account can have access to the IP addresses within that pool.
- Shared pools are those available to the parent devices as well as all devices belonging to children companies. None of the pools (parent or children) can be overlapping with each other.

4.3.1 Closed User Group

Customers with multiple business units, agencies, departments or organizations may require billing, provisioning and network separation within the same private network. Traditionally, this has required building a stand-alone private network for each agency/department, so for a company with multiple agencies/departments, multiple private networks would be required. Closed User Group (CUG) allows traffic separation per department/agency within the same private network, so data traffic for all of a company's agencies/departments can reside on a single private network.

CUG provides multiple wireless domains within the same private network, which ensures end-to-end separation at the routing and traffic forwarding layers. Each CUG stand-alone wireless domain has the flexibility of controlling Domain Name System (DNS) and routing between the customer's data center and mobile devices.

Benefits of CUG include:

- Full separation of billing, provisioning and network using a single private network
- DNS queries supported at the individual CUG level
- CUG separation on the routing and traffic forwarding layers between the customer's data center and mobile devices.

- Dynamic routing enabled at the customer's data center on a per-CUG basis

4.4 Authentication, authorization and accounting (AAA)

The Verizon AAA server and Enterprise Home Agent (EHA) are used to authenticate, authorize and account for a device's access to the Verizon Wireless radio access network and Private Network. Private Network offers customers a choice to utilize a customer-hosted AAA server that is resident within the enterprise's domain and network.

Customer-hosted AAA

In customer-hosted AAA configuration, Verizon AAA servers act as a proxy to the customer's AAA and require a physical circuit (see 4.1: Connectivity options) to connect the customer-hosted AAA with the Private Network. For a Private Network with Dedicated Physical Circuit connectivity, the same dedicated physical circuit can be used in support of Private Network connectivity and the customer-hosted AAA. When sizing the dedicated physical circuit, one must take into account the traffic associated with data communications and needs of the customer-hosted AAA. If the data-traffic payload exceeds the bandwidth of the circuit, authentication of subscribers could be negatively impacted. It is recommended that a separate dedicated circuit be assigned for customer-hosted AAA traffic.

Customer-hosted AAA configuration will require certification of the customer's AAA proxy servers. A Verizon representative can provide guidance to the certification process.

Customer-hosted AAA solution supports:

IP addressing type	Description
Enterprise authentication of subscribers	Subscriber authentication involves the Mobile IP Home Agent authentication requests to be proxy from the Verizon AAA directly to the customer's AAA or indirectly through either an existing AAA proxy or through an Enterprise Home Agent AAA proxy gateway to the customer's AAA.
Enterprise assignment of device IP	Customer AAA assignment of Framed IP Address and Framed Pool for customer's subscribers. Subscriber Mobile IP Home Agent authentication requests are forwarded to the customer AAA where the Framed IP Address and Framed Pool attribute can be assigned to the subscriber.

4.5 Domain Name System

DNS is a hierarchical distributed naming system that associates information with domain names assigned to participating entities. A DNS resolves queries for these names into IP addresses for the purpose of locating devices and services. The DNS maintains the domain name hierarchy and provides translation services between it and the address spaces.

As part of the data traffic flow, Private Network service passes the data traffic to the CPE, so DNS requests must receive special attention. There are two options supported when building a Verizon Wireless Private Network:

Option 1—DNS Redirect for Enterprise (DRE)
For 3G solutions, this is the preferred solution. Verizon can redirect DNS queries toward customer DNS servers residing within the customer network. This minimizes the need to perform any Network Address Translation (NAT) functionality on the customer side and to advertise routes toward Verizon Wireless. The server assignment can be made as primary/secondary and supports User Datagram Protocol (UDP) or Transmission Control Protocol (TCP)-based DNS. With both options, the wireless device would still display the Verizon Wireless DNS server IP address while in-network and the roaming partners' DNS IP address while roaming.

DRE is not required for 4G LTE solutions since a 4G LTE Private Network build bakes the customer DNS into the access point name associated with the customer's Private Network. This is the functional equivalent of DRE. NAT is a technique to allow a device to act as an agent between a public network and a local or private network by enabling a single, unique IP address to masquerade the IP addresses of an entire network of devices.

Option 2—DNS with NAT by customer
Verizon Wireless forwards all DNS queries to the customer network and, with the use of NAT, customers can direct the queries to their proper DNS servers. This requires that the DNS addresses are advertised back to Verizon Wireless via Border Gateway Protocol (BGP). Symmetric traffic routing is required if dual (primary and secondary) connections to Private Network are used.

NAT is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device. NAT acts as an agent between an external network (e.g., a public network) and a local network (e.g., a company intranet), enabling a single, unique IP address to incorporate the IP addresses of an entire network.

4.6 Mobility

Private Network requires use of Mobile IP (MIP) protocol when on 3G and 1xRTT networks. MIP is designed to support host mobility, which allows mobile device users to move from one network to another without the need to change the device's IP address. Therefore, the device is able to stay connected to the network regardless of its location. This is because Mobile IP is able to track a mobile host without the need to change the mobile host's long-term IP address.

Each mobile device is identified by its home address, regardless its current location within the wireless network. While away from its home network, a mobile device is associated with a care-of address, which identifies the device's current location. The home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile device registers with its home agent and how the home agent routes IP packets to the mobile node through the tunnel. Mobile IP for IPv4 is described in Internet Engineering Task Force (IETF) RFC 5944, and extensions are defined within IETF RFC 4721.

The Verizon 4G LTE network uses General Packet Radio Service Tunneling Protocol (GTP), which allows users to move from one location to another location while maintaining connectivity within the 4G LTE network, and the evolved high-rate packet data (eHRPD) network supports seamless handoffs between the 4G LTE and 3G networks.

5. Private Network enhanced features

Private Network offers features that enhance the overall customer experience. These capabilities include wireless routing and management of devices on the router's local area network, as well as the ability to receive data traffic accounting records and access key reports through a portal.

5.1 Dynamic Mobile Network Routing

Dynamic Mobile Network Routing (DMNR) allows a wireless router to dynamically advertise the subnets it serves (up to eight) to other devices on the customer's network, without the need for Generic Routing Encapsulation (GRE) tunnels or network address and port translation. This delivers the any-site-to-any-site connectivity wireline customers expect when solutions extend the corporate network (e.g., intranet). DMNR is a network-based mobile technology capable of providing dynamic routing and support for mobile or stationary routers in primary wireless access or automatic wireless backup configurations using Mobile IPv4-based Network Mobility (NEMO) protocol.

DMNR simplifies the connection of a wireless router's LAN subnets and devices, such as desktop computers, printers, netbooks or other devices located on those routers, to applications connected to the customer's data centers. This enhances an IT administrator's ability to manage individual subnets behind a wireless router by communicating directly to those nodes. With DMNR, wireless connections are consistent with the customer's wireline network, thereby reducing complexity, scalability, costs and management concerns.

Figure 3: Dynamic Mobile Network Routing

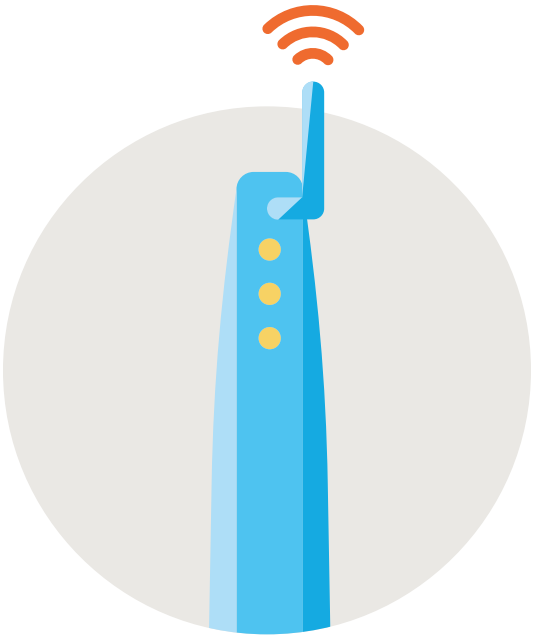
Advantages of Dynamic Mobile Network Routing are:

- DMNR provides the ability to directly communicate and manage devices on the LAN for locations using a wireless router.
  - By having visibility into the LAN, traffic can be easily directed to and from specific LAN devices to a customer's IP network, allowing the management of those LAN devices from a central location.
- DMNR delivers the any-site-to-any-site connectivity expected of a wireline solution that extends beyond the corporate IP network.
  - In the event of dynamic failover, DMNR ensures connectivity directly with LAN devices in providing network and business continuity.
- DMNR allows customers full control over the allocation of LAN and WAN wireless router addresses within their VPN.
- DMNR allows customer to deploy wireless sites and route traffic between the locally attached subnets and their data centers by using routers and the Private Network. This in turn allows customers to:
  - Manage and communicate with devices within a subnet attached to a wireless WAN (WWAN) router.
  - Dynamically register remote subnets with a network-based Enterprise Home Agent.
  - Support bidirectional traffic without having to manage GRE tunnels to each device. Scalability in using GRE may lead to degradation in network performance, since a GRE tunnel must be established with each LAN device, while with DMNR, the device is handled as part of the router connection.

For example, a 100-site deployment with routers would require 200 overlay GRE tunnels (one primary and one secondary per router) along with 200 associated individual routing adjacencies to maintain. With DMNR, those 100 routers would not require overlay tunnels or any special configurations on the data-center routers, since DMNR provides native routing as part of the router's wireless connection. For more information see the Verizon technology white paper *DMNR and Tunnel-less Encryption for Wireless Networks*.

5.2 Account records streaming

Private Network supports the option to have a direct feed of RADIUS accounting records (Start and Stop fields/attributes) sent from the Verizon Data Streaming Server (DSS) to a designated customer accounting server at no additional cost. The customer will receive the RADIUS file in which the raw data (without modification or customization) can be parsed per the customer's reporting needs. The customer's receiving server must be capable of receiving and acknowledging raw accounting information.



5.3 Multiple virtual route forwarding

Private Network with Private IP connectivity allows the ability to support multiple virtual Private IP connections over a single Private Network through the use of virtual routing and forwarding (VRF)-level extranet design. This capability offers secure virtual connections for multiple departments within an organization on a single connection, eliminating the need to purchase multiple physical ports. A single Private Network connection will allow the customer's data traffic to be sent to multiple Private IP sites, which means simplicity in constructing the Private Network/Private IP solution and cost savings as well, since only one connection is needed rather than multiple ones.

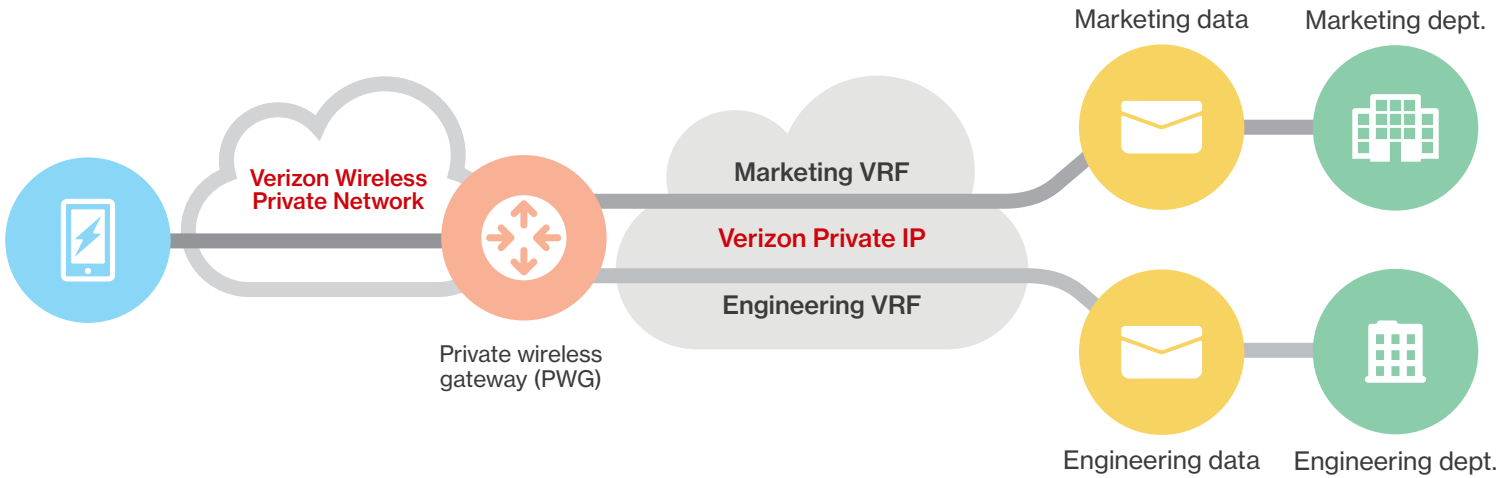


Figure 4: Private Network with Private IP multi-VRF

5.4 Customer account self-management
Customers are able to manage their wireless accounts through either My Business Account or Verizon Enterprise Center, whose portals offer self-service ability in ordering, account maintenance, billing and reporting. The customer experience is enhanced by letting them make changes to their account and devices used within their Private Network, which includes the ability to provision, manage and report IP addresses.

The self-management portal includes the assignment of IP addresses to new or existing lines within the customer private network, as well as the ability to view the organization's IPs, report on IPs and manage changes online.

Ordering	Assign IPs while ordering devices (smartphones, tablets, M2M). This includes dynamic or static IP.
Account maintenance	IP Management Center provides visibility to reserved and assigned IPs through an onboarded dashboard and allows the ability to browse, query and retrieve IPs, along with downloading output to a .csv file. Wireless Number Center: Visibility to a specific device IP address, category and EHA pool. Manage changes to IP addresses.
Reporting	Device, overview of lines and purchase activity reports include IP attributes of IP address, EHA pool, IP category and IP type.

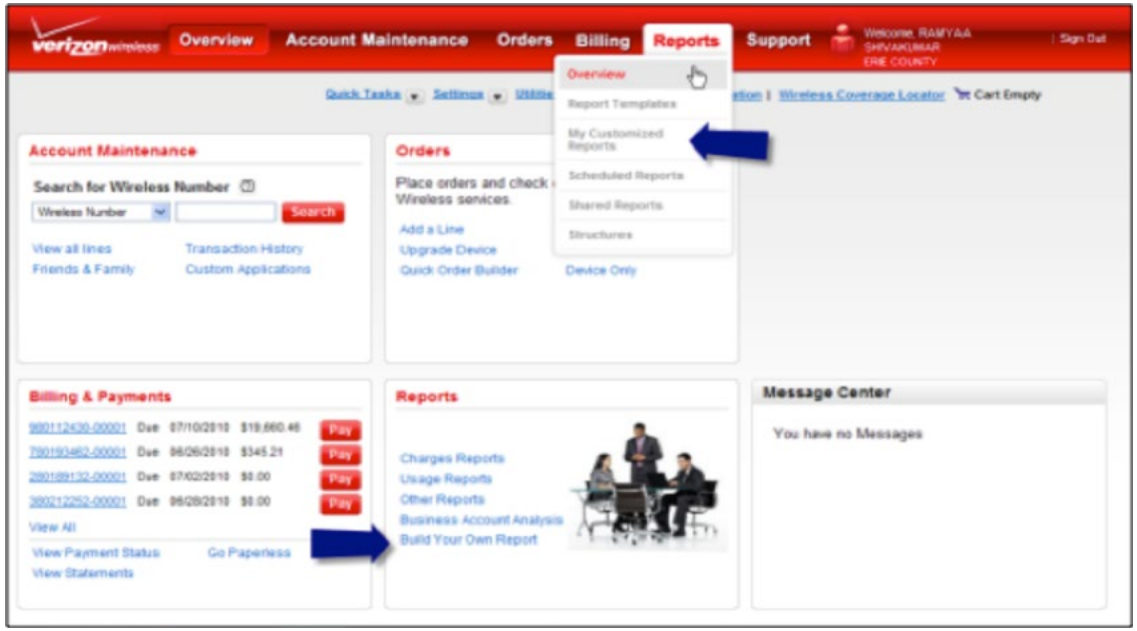


Figure 5: My Business Account screen view

5.5 M2M Management Center

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

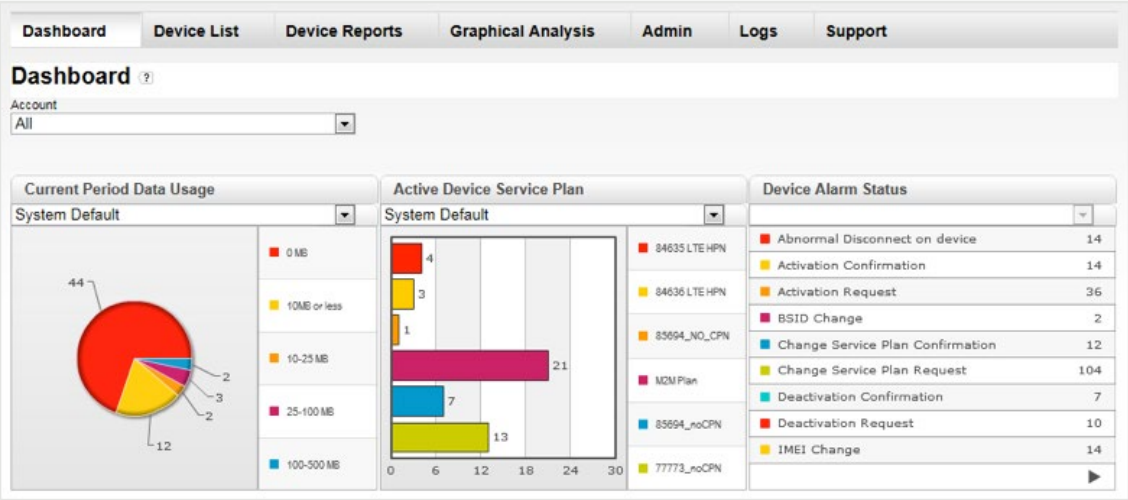


Figure 6: M2M Management Center Dashboard screen view

Monitor devices quickly and easily.

- Graphical dashboard that gives a quick overview of system-wide status.
- Criteria-filtered device lists, plus ability to drill down for usage estimates, connectivity status and history, IP address, provisioning state and history, customer-defined attributes and more.
- Near real-time connectivity status and usage information.
- Customizable reports to facilitate management of devices, usage and costs.
- Custom properties for identifying, searching, sorting and tracking devices.

Manage service efficiently.

Let the Verizon M2M Platform notify you when usage, connectivity or status changes occur outside your definition of normal for individual devices or groups of devices.

- Automatically suspend service for rogue devices or devices that have been relocated without authorization.
- Monitor data usage thresholds.
- Monitor provisioning transactions.

Administer effectively and securely.

- User permissions and account-level security.
- Detailed audit trail of user activities and system events.

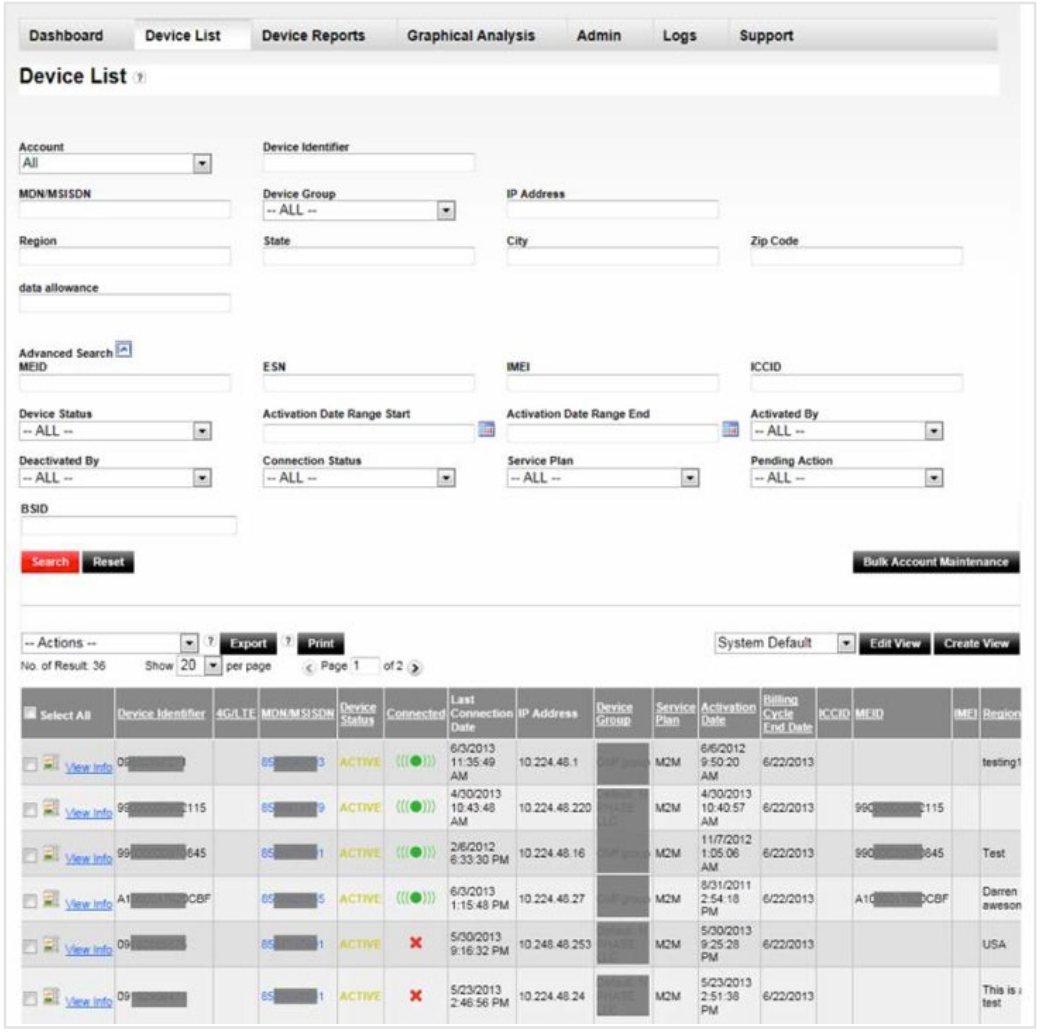
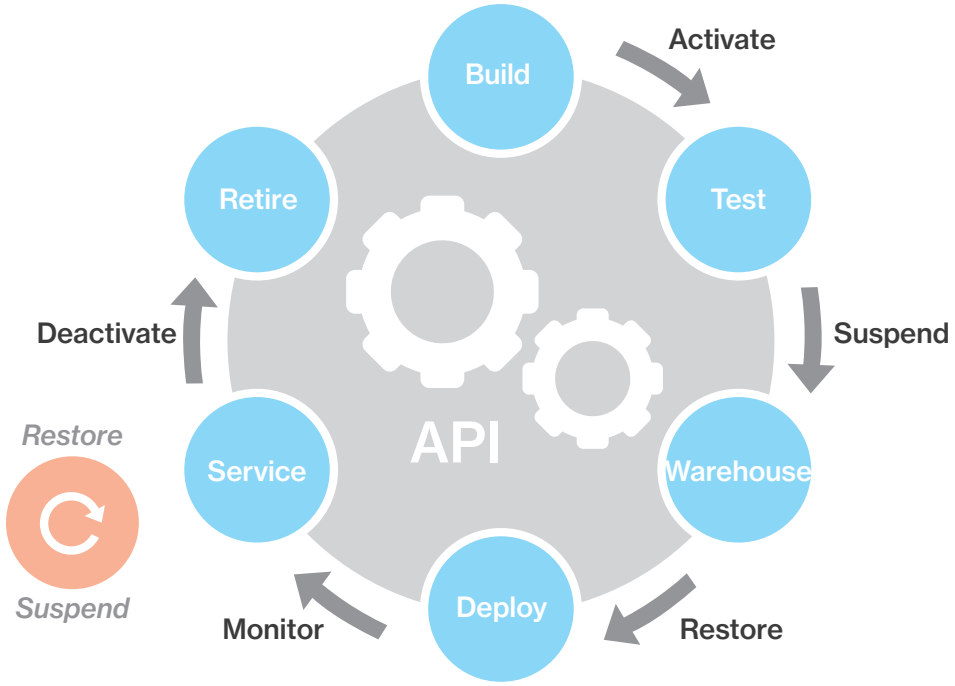


Figure 7: Sample M2M Management Center device list

Automate connectivity management tasks. Many M2M application managers must provision, monitor and control numerous devices. To manage device volumes effectively, you need the ability to execute connectivity management tasks automatically, without human intervention, from within other enterprise systems.

Use the M2M Platform application programming interface (API) to automate connectivity tasks throughout a device's life cycle. For example, you might activate service when testing units during manufacturing, suspend service when assigning units to warehouse inventory locations and then resume service when selling or fielding a unit. The M2M Platform connectivity management solution provides easy-to-use, standards-based SOAP/XML web service APIs that enable you to integrate connectivity management tasks with your enterprise applications, improving operational efficiency through automation.

See the Verizon M2M Platform tech brief for more insight into what the M2M Management Center can do for enterprises.



5.6 Access to Verizon services

Service Based Access (SBA)* is an optional configuration that enables customers to access Visual Voice Mail (VVM), Multimedia Messaging Services (MMS) and location-based services Assisted Global Positioning System (aGPS).

Visual Voice Mail

VVM is an application that allows subscribers to manage voice mail directly from a device instead of dialing into the traditional voicemail system. Customers can view, listen to, delete and manage all voice messages on the device. Premium service includes voicemail to text, personalized greetings for call groups and the ability to receive fax messages (PDF format) to the device. These services are supported on both Verizon Wireless 3G and 4G LTE devices that are compatible with VVM.

Multimedia Messaging Services

MMS include picture and video messaging services that provides the ability to send and receive picture and video messages from a camera-enabled phone to other mobile phones. These services also provide the ability to send and receive video or picture between email and the MMS-enabled device. Service Based Access configuration is required for Verizon Wireless 3G-compatible MMS products on Private Network, while Verizon Wireless 4G LTE–compatible products can have access to MMS functionality without needing SBA configured within their private network.

Location-based services

aGPS service provides the ability to obtain a device's location by using data from within the Verizon Wireless network as a complement to satellite GPS. There are areas where satellite signals have poor performance, which hinders the ability for the device to receive GPS coordinates. By leveraging aGPS, the device can send information to the cellular network, which will calculate the device's location (latitude and longitude) and send t he location data back to the device for communications to the applications the device uses. The device must be GPS-compatible and Verizon Wireless–approved.

5.7 Group Encrypted Transport (GET) VPN

Private Network support of Group Encrypted Transport (GET) VPN provides a scalable solution to protect data traffic between the wireless router and the enterprise IP network, which can simplify the provisioning and management of a VPN across multiple sites. GET VPN enables encrypted IP packets to be routed directly to remote sites based on routing protocol decisions, along with the concept of a trusted group to eliminate point-to-point tunnels and their associated overlay routing. All group members share a common security association, which enables the group members to decrypt traffic that was encrypted by any other group member. In GET VPN networks, there is no need to negotiate point-to-point IPsec tunnels between the members of a group, because GET VPN is tunnel-less. GET VPN uses the Group Domain of Interpretation (GDOI) group key-management protocol (RFC 3547) developed by the IETF. GET VPN integrates easily with DMNR to provide tunnel-less encryption with any-to-any encrypted data traffic routing and centralized router authentication and ciphering policy management.

* Service Based Access is not supported for customers utilizing Hosted Private Network, Closed User Group or Zero Tunnel Private Network features.

5.8 Private Network Traffic Management

Traffic Management is a Private Network feature, available only for Verizon 4G LTE devices, that provides a premium and differentiated network experience. It enables application differentiation and quality of service (QoS) over the LTE Private Network using standards-based IP packet marking to create IP traffic preferences for business-critical applications and to achieve more predictable application performance during times of peak network demand.

IP packets can be prioritized in the 4G LTE Private Network using standards-based QoS markings between wireless user equipment (UE) and the Private Network gateway. It is also implemented on the IP core network (e.g., Verizon Private IP's MPLS service) connecting to the customer IP network. There is a set of bearers between the UE and the Private Network gateway that carries user-data IP flows and receives specific IP traffic treatment.

Traffic Management relies on the customer's applications IP marking to place the prioritized IP packets within the respective bearer.

- **Default bearer.** When the UE attaches to the 4G LTE Private Network, it will be assigned a default bearer, which remains as long as the UE is attached. The default bearer transports IP traffic that does not require any specific QoS treatment, such as best-effort IP flows (e.g., email, Web, etc.). The default bearer IP flows are carried on the Best Effort class over the 4G LTE Private Network.
- **Dedicated bearer.** When the UE attaches to the 4G LTE Private Network, an additional bearer on the top of the default bearer remains as long as the UE is attached. The dedicated bearer transports more specific IP flows that need the specific QoS treatment (e.g., enterprise Voice over IP [VoIP]). Business-critical applications are mapped to the dedicated bearer utilizing applications IP marking.

With Private Network Traffic Management, businesses can realize an improved user experience during peak network demand through:

- **More control.** When the wireless 4G LTE Private Network becomes congested, Private Network Traffic Management 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.** Private Network Traffic Management lets you map your applications into the Business Critical Class of Service (CoS) based on the applications' requirements.
- **New potential.** Private Network Traffic Management extends QoS policies traditionally provided on fixed WAN to the 4G LTE Private Network, giving you expanded 4G LTE Private Network control.

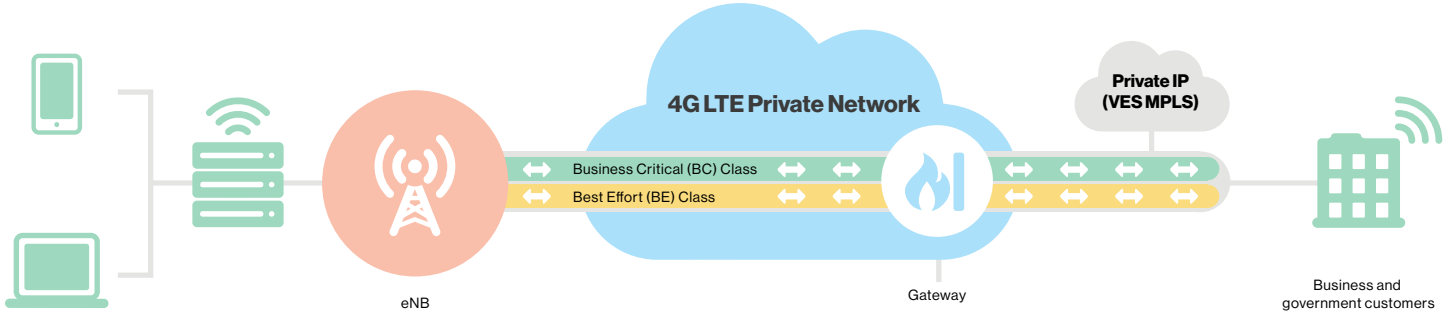


Figure 8: Private Network Traffic Management bearers

Private Network Traffic Management can be added to an LTE Private Network device for a monthly charge and is available on configurations using Verizon Private IP, dedicated physical connection and Zero Tunnel connectivity.

Private Network Traffic Management has three subscription options: Enhanced, Premium and Public Safety. The Enhanced and Premium subscriptions are available to enterprise and government accounts; Public Safety is only available to eligible first-responder accounts (e.g., police departments, fire departments, etc).

See the Private Network Traffic Management white paper for more insight.

5.9 International roaming

Private Network devices are able to have connectivity when leaving the Verizon Wireless network footprint (aka outbound roaming) with approved Verizon roaming providers whose wireless technologies include GSM, UMTS, HSPA or 4G LTE. This allows solutions involving devices such as smartphones, tablets, laptops and Internet of Things (IoT) roaming flexibility to expand beyond the Verizon U.S. network to other countries where Verizon supports international roaming. International IoT and M2M roaming offers:

- The ability to send and receive data to and from Verizon-certified, international-capable devices, modules or chipsets (LTE with GSM/UMTS) deployed outside of the U.S.
- Support for occasional (incidental) roaming as well as devices that will be used exclusively in another country (limited permanent roaming) as part of an international deployment that includes the U.S.
- Streamlines the ability for customers to deploy IoT and M2M solutions in multiple countries by enabling them to leverage Verizon roaming capabilities for international IoT and M2M connectivity.

5.10 Cloud access

There is a transition occurring where businesses are moving applications that have historically been residing within their corporate IT network to residing with a cloud service provider. Private Network customers are seeking solutions where they can use the value of Private Network and have access to their business applications/data that reside within a cloud service provider. This can include the ability to have applications continue to reside within their corporate IT network, as well as with the cloud service provider.

Private Network can be constructed with connectivity to cloud service providers using Verizon's Secure Cloud Interconnect (SCI) or direct connect from Private Network Gateway to Amazon Web Services (AWS).

Secure Cloud Interconnect

Secure end-to-end mobile/4G LTE connectivity is available by using Private IP wireless access with SCI, allowing secure and efficient connectivity of mobile cloud applications. It allows organizations to simplify the provisioning and access to cloud services that previously was only available over the public Internet, where there is the potential for data security breaches, unreliable performance and a complete lack of control over the user experience. SCI offers:

- **Security.** Private connections are used that are completely separated from public Internet traffic. Therefore, the traffic doesn't touch the public Internet.
- **Reliability.** Global interconnectivity to cloud providers ensures that cloud applications use the most optimal, reliable paths with built-in redundancy.
- **Interconnectivity.** Pre-engineered secure and diverse interconnections to leading cloud service providers allow customers to select best-of-breed cloud services and/or use multiple cloud service providers for redundancy.
- **Customer enablement.** Within the Verizon Enterprise Center portal, customers have the ability to directly manage their SCI ports and value-added services from the cloud to their end users. Use the SCI Dynamic Network Manager ports on a map, to manage connectivity, or to view usage per connection.

5.11 Verizon Mobile Device Management

Verizon Mobile Device Management (MDM) is a Verizon-branded solution that integrates enterprise Firmware over the Air (FOTA), device diagnostics and broadband hotspot management into a single, unified and intuitive customer experience. Verizon MDM is a portal for differentiated Verizon management services and integrates with multiple mobility services. Verizon MDM features:

Enterprise FOTA management	• Assess customer/corporate applications on new device firmware. • Scheduled firmware update deployment after successful assessment. • Track firmware update deployment on all devices.
Device Diagnostics	• Obtain technical data from devices. • Streamline troubleshooting of device-related issues. • Monitor devices to ensure virus/malware protection is enabled and rooting detection.
Broadband Hotspot Management	• Manage corporate-liable (CL) devices over the air. • Set security policies (Service Set Identifier [SSID], Passphrase, Encryption, Administrator password). • Prevent users from viewing or changing settings. • Currently supports selected Jetpack® and USB devices.
Verizon Software Management	• Host firmware images and software updates for wireless devices. • Create and schedule campaigns for devices • Deliver software and firmware updates to enterprise devices. • Monitor status of campaigns to devices. Note: This is not a service to manage software on retail devices. Customer's device must meet Verizon's Open Development standards and use certified modules. Customers register at opennetwork.verizonwireless.com.

Check with your Verizon representative for latest on MDM information and what devices are supported.

6. What differentiates Verizon from other providers

Verizon Wireless Private Network is superior to other providers' offerings due to its:

- Industry-leading 4G LTE network.
- Ability to serve as a single provider for end-to-end connectivity.
- Enterprise-class features.
- Complementary offerings portfolio.

4G LTE network

Verizon Wireless offers America's largest 4G LTE network. With the largest coverage area, lightning-fast upload and download speeds and low latency, enterprises can effectively utilize mobile devices and connected devices.

Verizon as end-to-end provider

Private Network with Verizon Private IP provides the wireless and wireline capabilities required for a true end-to-end solution. Having Verizon delivering wireless and wireline needs means fewer contacts to manage, going to a single source for support and the comfort of knowing that data traffic will be delivered quickly and securely.

The extensive portfolio of Verizon services means that enterprises can outsource activities outside of core competencies, so they can remain focused on what they do best.

Managed Network Services

Managed Network Services is a suite of services that range from simple monitoring and reporting to complete outsourcing of corporate network and data management. Enterprises can control their network by simply submitting requests through an online portal.

Professional Services

Verizon Professional Services delivers technology solutions spanning IT, security, networking, communications and mobility, delivered by experts located around the globe who are dedicated to helping businesses evaluate and adopt new technologies securely and effectively.

Verizon Professional Services reaches across every phase of the solution's life cycle, and includes:

- **Planning.** Verizon provides a detailed analysis of current state and options, enabling improved decision making and a foundation for change.
- **Designing.** Verizon leverages its expertise in a wide range of technologies and extensive vendor relationships to maximize current customer investments and control the cost of new technologies.
- **Implementing.** Verizon professionals, certified across a wide range of technologies and vendor ecosystems, manage customer implementation, while addressing the physical and human factors involved in each solution installation.
- **Operating and managing.** From completely managed to do-it-yourself solutions, Verizon Professional Services experts keep enterprise technologies performing efficiently and reliably.

Enterprise-class features

Private Network Traffic Management, Dynamic Mobile Network Routing, AAA options and Reporting functionality help remove the barriers for business acceptance of setting up a Private Network.

Private Network Traffic Management extends wireline QoS policies over Verizon LTE network.

- Allows prioritization of mission-critical applications over best-effort applications during congested/non-congested environments.
- Delivers more predictable application performance for subscribers using mission-critical applications during network congestion.
- Delivers end-to-end QoS with Verizon Wireless Private IP and other wireline solutions.

Dynamic Mobile Network Routing

Verizon is the only provider of DMNR, which simplifies the management of devices behind routers connected to the 3G or 4G LTE network. That means there's no need to establish multiple overlay tunnels for each remote router. The benefits of DMNR include:

- Simplify the connection process between remote LAN subnets and the enterprise's data center.
- Allow organizations to manage the LAN from a central location.
- Provide network and business continuity by ensuring connectivity directly with enterprise LAN devices in the event of dynamic failover.
- Avoid the degradation in network performance typically associated with GRE solutions.

Customer-hosted AAA
Customer-hosted AAA delivers control of subscriber authentication and assignment of device IP.

Reporting
Easy-to-use, easy-to-access portals provide rich data needed to manage accounts and devices.
- M2M Management Center empowers management of M2M devices through a user-friendly portal.
- My Business Account and Verizon Enterprise Center offer online account and IP addressing.
- Account Streaming provides the data and details to meet customized reporting need

7. Conclusion

Verizon Wireless Private Network with 4G LTE provides a secure and reliable foundation to enable mobile workforces and connected devices to communicate with IP networks.

Private Network features include:

Protection
- Segregated data traffic keeps information confidential and secure.
- With data isolated from the public Internet, inherent risks and unsolicited traffic are avoided.
- Only customer-authorized subscribers may send and receive traffic.
- Enterprises have complete control over device access to the Internet and applications.

Performance
- Provide access to temporary or new locations without the need for lengthy wireline installation.
- 4G LTE speeds enable even media-rich business apps and customer and corporate data.
- 4G LTE devices work with our 3G network, so costly upgrades are not necessary.

Productivity
- Maintain business continuity with wireless routers as primary or backup for sites such as ATMs, kiosks, tradeshows and conventions.
- Increase efficiency with capabilities such as automated meter reading, monitoring, digital signage, vehicle management and smart vending.
- Get new locations up and running within days instead of waiting weeks for wireline installation.

Value
- Simple device management is cost-effective—no need for costly onsite technical expertise.
- Reduce costs by eliminating the need for a VPN client, as well as licensing and management.

8. Contact information

For more information, visit the Verizon Wireless Private Network Web site and view the overview video: **business.verizonwireless.com/content/b2b/en/wireless-products-services/private-network.html**

For more information about Verizon Wireless, speak with a Verizon Wireless business specialist. Call **1.800.VZW.4BIZ** or visit Business Solutions: **business.verizonwireless.com/content/b2b/en/wireless-products-services.html**

Verizon Wireless business home page: **verizonwireless.com/wcms/business.html**

SB02710416

Learn more.

VerizonEnterprise.com/contact-us