Virtual Private Network Service (VPNS)

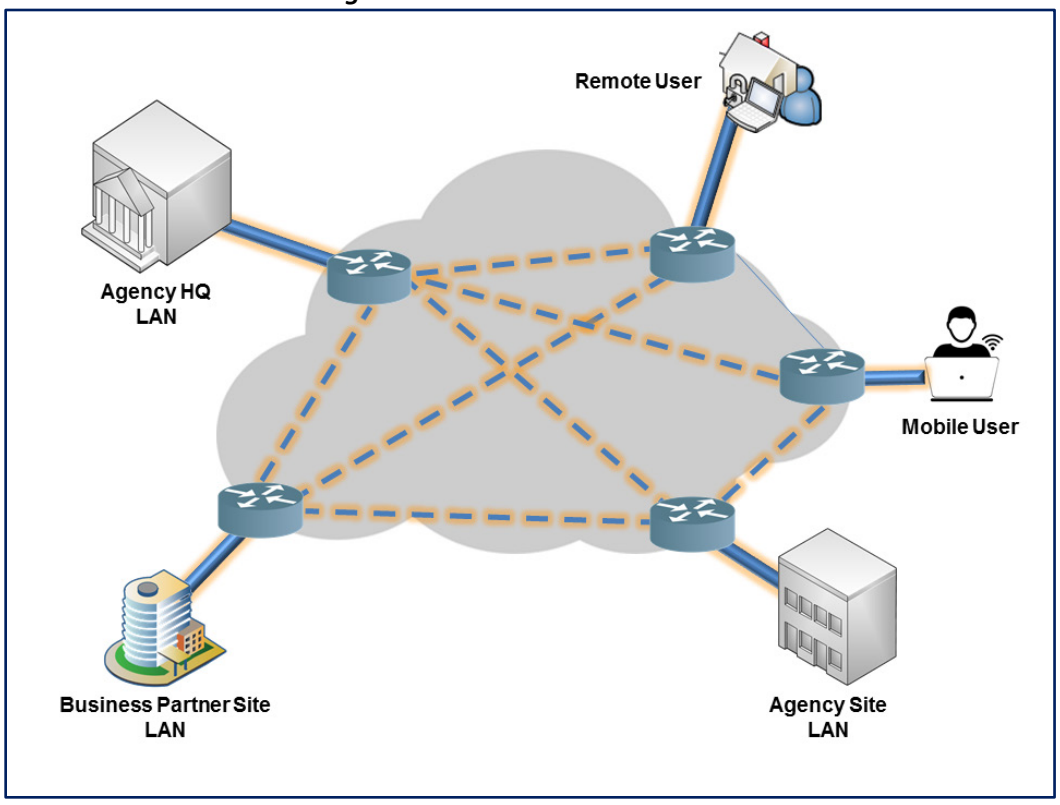
The EIS Virtual Private Network Service (VPNS) provides secure, reliable transport of agency applications across the provider's high-speed, unified, multi-service, IP-enabled backbone infrastructure. The service can provide secure tunnels between remote Intranet sites using broadband or dedicated access, enable authorized users to securely access agency resources via an Extranet, and enable remote users to securely access their files. VPNS is flexible and can accommodate a variety of bandwidths ranging from 64 Kbps to 100 Gbps.

Category: Data Services

Complementary Services Needed: In order to use VPNS, the agency would need EIS Access Arrangements (AAs) or equivalent.

Definitions: Please see EIS contract Section J.12 Glossary of Terms for clarification of technical terms and acronyms.

Figure 1—Virtual Private Network



1. Why an Agency Might Select this Service

- Enables an agency to connect different sites via a secure WAN.
- Available in wide range of interface speeds from 64 Kbps up to 100 Gbps.
- Compatible with a range of data transmission services including Ethernet, Private Line Service, IP over SONET, DSL, High-Speed Internet, and Wireless.
- Advanced Service Level Agreements (SLAs) backed by Quality of Service guarantees. Performance Level Threshold is 99.99% for Critical Service Level.

2. Examples of How VPNS Could be Used

- **Agencies can Provide Secure Connectivity:** The VPN technology is very popular with agencies as a means of securely connecting remote field offices, enabling agency partners and remote users to securely access agency resources.
    - VPNS could be used to enable authorized private and government partners to gain access, via an secured agency extranet, to agency applications and data.
    - An agency could use VPNS to enable remote offices to securely connect to the agency's intranet.
    - An agency with a large number of teleworkers or field agents could use VPNS to enable remote and mobile personnel to securely connect to their Windows accounts over an encrypted connection. This would give workers access to the same information and IT assets that they would have sitting at their desktops.
- **Can be Used to Transmit Different Types of Data:** Agencies can use VPNS to securely and accurately transmit different types of information such as audio, video, email, instant messaging and business transaction data. VPNS ensures the quality of the delivered information by assigning the different types of information the appropriate priority. (Audio for a phone coversation, for example, would be given higher priority than an email message, to ensure a clear phone conversation.)

3. Key Technical Specifications

NOTE: This portion of the service guide has been abridged due to space considerations. Please see EIS contract Section C.2.1.1 Virtual Private Network Service for full technical details on this service.

Table 1-VPNS Technical Capabilities

Capability	*Description*
Compliance with Routing Requirements in EIS contract Section C.1.8.8	Ensures any encrypted tunnels are applied and proxied to allow inspection.
Multiple Tunneling Standards	As required by an agency (i.e., L2TP, GRE, IP-in-IP, MPLS, IPsec, and SSL/TLS)
Various Encryption Levels	As required by an agency (i.e., 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules).
Authentication Services	As required by an agency (i.e., RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates).
IPv4 Support	As both the encapsulating and encapsulated protocol.
QoS Standardized Modes	a) Best effort b) Aggregate Customer Edge (CE) Interface level QoS ("hose" level) c) Site-to-site level QoS ("pipe" level) d) Intserv (RSVP) signaled e) DiffServ marked
QoS Across Subset of Access Networks	a) 802.1p Prioritized Ethernet b) MPLS-based access c) Multilink Multiclass PPP d) QoS-enabled wireless: i. LTE ii. Wireless 802.11.x iii. Cable high-speed access (DOCSIS 1.1) iv. QoS-enabled Digital Subscriber Line (DSL) v. QoS-enabled Satellite Broadband Access
Application Level QoS	One or more of the following application level QoS objectives: a) Intserv model for selected individual flows. b) Diffserv model for aggregated flows.
Isolation of Traffic and Routing Service	Provides isolation of the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN.

Capability	*Description*
Multiple VPN Support	Multiple VPNs are supported by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies.
Secure Routing Services	Provides full routing capability on the VPN platform with a secure policy across the VPN.
Security Management System	Supports the inclusion of encryption, decryption, and key management profiles.
Support of Agency Deployment of Internal Security Mechanisms	Supports an agency in deploying its own internal security mechanisms, in addition to those deployed by the contractor, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.
Alternatives for Authentication	Allows an agency to choose from alternatives for authentication of temporary access users. Authentication server choices include: a) Contractor-provided b) Third party c) Agency-provided

Table 2-VPNS Features

Feature	*Description*
High Availability Options	a) Load sharing b) Fail-over protection c) Diverse access points to service provider's POP(s)
Interworking Services **(NOTE: May not be available from all contractors.)**	Provides the capability for an agency's VPN to transparently access agency locations that use the contractor's Ethernet Transport Service.

4. Pricing Basics for VPNS

Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide to gain an understanding of EIS pricing fundamentals.

4.1 Access Arrangements

Appropriate access arrangements must be selected for each endpoint. Please visit the EIS Resources Listing and locate the Access Arrangements Guide for more detailed information.

4.2 Service Related Equipment (SRE)

- SRE must be chosen based on equipment required at each location. NOTE: SRE is priced using Catalog-based Pricing.
- Request that contractor provide pricing for any SRE that would be required, in addition to the agency's existing infrastructure, to deliver the service.
- Please visit the EIS Resources Listing and locate the Service Related Equipment Service Guide for more detailed information.

4.3 VPNS Price Components

The price structure for VPNS consists of the components shown in *Table 3* below.

Table 3—VPNS Pricing Components

Component	***Charging Unit***
Transport Charges	Port
Transport with Embedded Access Charges	Port
Feature Charges	Port

Figure 2 below shows how the pricing components in *Table 3* are combined to produce the total cost for the service.

Figure 2—This figure shows how the various pricing components in Table 3 would be combined to calculate the total VPNS charges. NOTE: One or more of these components may not be needed to price a particular service package.

The charges for the different components in *Figure 2* are calculated using details provided in the pricing tables in EIS contract Section B.2.1.1 Virtual Private Network Service. (Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide for instructions on using the pricing tables to compute the cost of a service.) The VPNS pricing tables contain CLINs grouped by one of the three main VPNS CLIN categories:

1. Transport Charges (t*able B.2.1.1.3.2—VPNS Port Pricing Instructions Table*)
2. Transport with Embedded Access Charges (*table B.2.1.1.3.3—VPNS Port with Embedded Access Pricing Instructions Table*)
3. Feature Charges (*table B.2.1.1.4.2—VPNS Feature Pricing Instructions Table*)

4.3.1 Auto-Sold and Task Order Unique CLINs

1. Auto-Sold CLINs

   VPNS includes some items that are automatically included with each VPNS port, and are Not Separately Priced (NSP). These items are called “auto-sold CLINs.”

   The VPNS services listed below are auto-sold. These services are defined in EIS contract Section C.2.1.1.1.4 Technical Capabilities under the indicated paragraph #:

   - All network security services as defined under paragraph #2, #3 and #4.
   - All Quality of Service (QoS) configurations as defined under paragraph #7, #8 and #9.

   Contractors may also include other auto-sold CLINs for the services offered on their contracts. All auto-sold CLINs for a particular contract are listed in EIS contract table *B.1.2.11.1 Auto-Sold CLINs Table*.

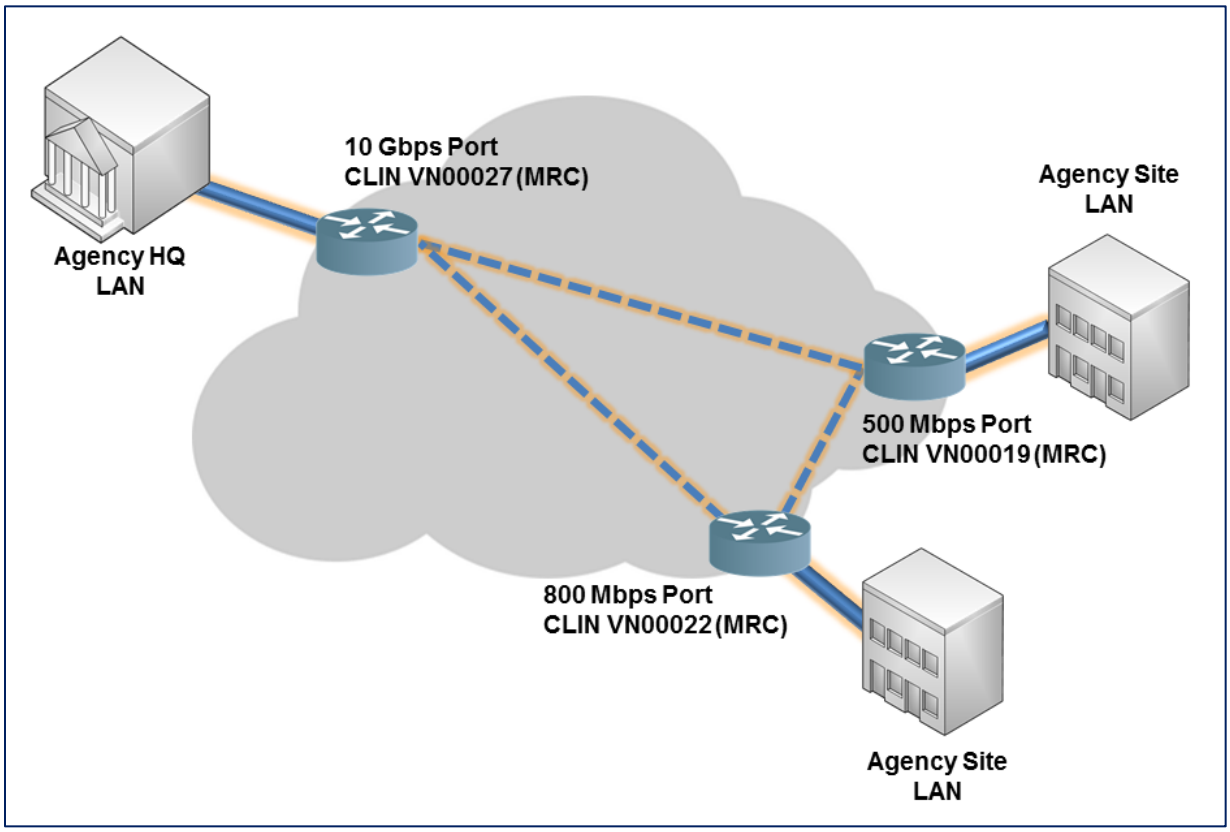
2. Task Order Unique CLINs

   A contractor may offer a custom variation of VPNS to meet an agency’s unique requirements. Such a customization would be identified with a Task Order Unique CLIN (TUC), and would include charges that would have to be added to the components in *Figure 2* to determine the total cost of the service.

4.4 VPNS Pricing Examples

Example 1: Agency VPN Serving Three Sites with Varying Data Rates (500 Mbps, 800 Mbps, and 10 Gbps), Ethernet Ports

Figure 3—Agency VPN Serving Multiple Sites with Varying Data Rates

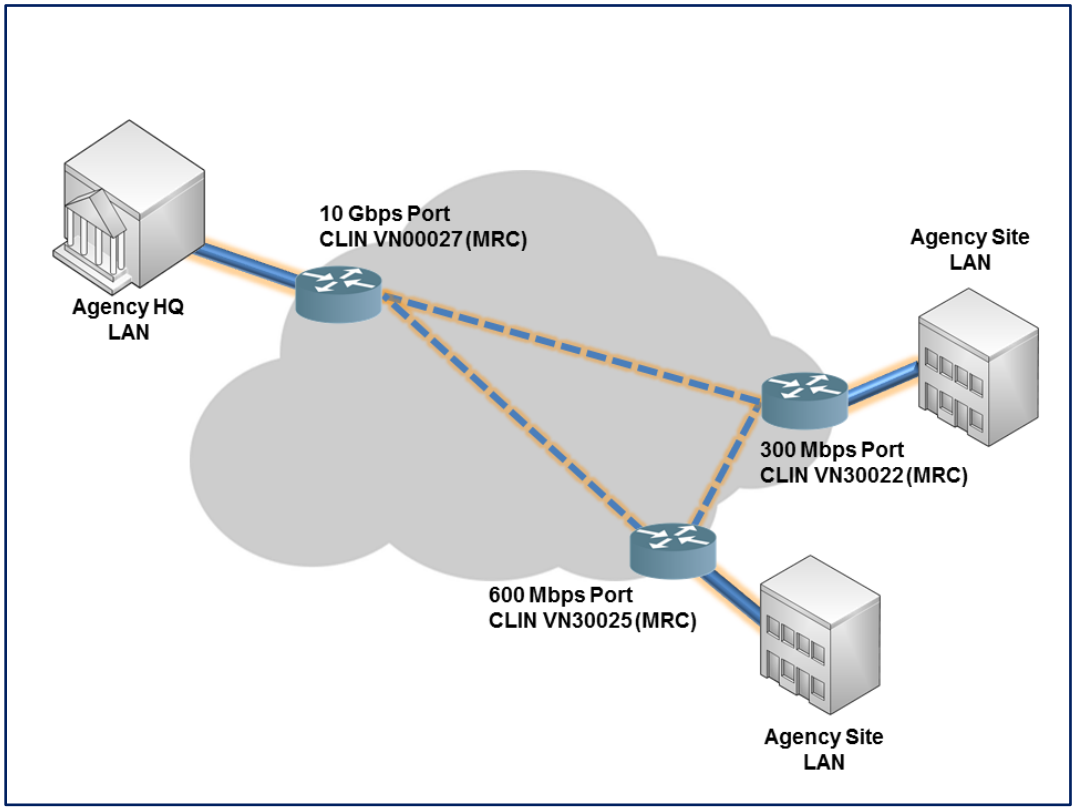


CLIN Selection

- Choose CLIN VN00019 "Ethernet – 500 Mbps" (see EIS contract table *B.2.1.1.3.2 – VPNS Port Pricing Instructions Table*)
- Choose CLIN VN00022 "Ethernet – 800 Mbps" (see EIS contract table *B.2.1.1.3.2 – VPNS Port Pricing Instructions Table*)
- Choose CLIN VN00027 "Ethernet – 10 Gbps" (see EIS contract table *B.2.1.1.3.2 – VPNS Port Pricing Instructions Table*)

Example 2: Agency HQ VPN with 10 Gbps Port, Serving Two Sites with Varying Data Rates (300 Mbps and 600 Mbps), both of which are Burstable to 1 Gbps

Figure 4—Agency VPN with Varying and Burstable Data Rates



CLIN Selection

- Choose CLIN VN30022, "Ethernet – 300 Mbps committed, burstable to 1 Gbps" (see EIS contract table *B.2.1.1.3.2 – VPNS Port Pricing Instructions Table*).

  CLIN VN31300, "Ethernet burstable overage for 300 Mbps committed port burstable to 1 Gbps" is auto-sold with the above CLIN.

- Choose CLIN VN30025 "Ethernet – 600 Mbps committed, burstable to 1 Gbps" (see EIS contract table *B.2.1.1.3.2 – VPNS Port Pricing Instructions Table*).

  CLIN VN31600, "Ethernet burstable overage for 600 Mbps committed port burstable to 1 Gbps" will be auto-sold with the above CLIN.

- Choose CLIN VN00027 "Ethernet – 10 Gbps" (see EIS contract table *B.2.1.1.3.2 – VPNS Port Pricing Instructions Table*)

NOTE: The two auto-sold CLINs listed above (VN31300 and VN31600) are used to bill the agency for usage exceeding the committed data rate.

5. References and Other Sources of Information

- For more technical details and information on VPNS, please refer to EIS contract Section C.2.1.1; for pricing details, Section B.2.1.1.
- For more information on service-related items, please see:
    - EIS contract Section B.2.10 Service Related Equipment
    - EIS contract Section B.2.11 Service Related Labor
- Please refer to a contractor's individual EIS contract for specifics on the contractor's VPNS offerings.
- For additional EIS information and tools, visit the EIS Resources Listing.
- For guidance on transitioning to EIS, please visit EIS Transition Training where you'll find several brief video training modules.