

VOLUME 1, SECTION 3.2:
NETWORK-BASED IP VPN
SERVICES



3.2 NETWORK-BASED IP VPN SERVICES (NBIP-VPNS) [C.2.7.3, M.2.1.2]

The Level 3 Team Network-Based (NB) Internet Protocol (IP) Virtual Private Network (VPN) Service, together known as NBIP-VPNS, meets or exceeds Government requirements as described in RFP Section C.2.7.3. Section 3.2 of this proposal volume provides a thorough description of the [REDACTED] NBIP-VPNS followed by responses to specific requirements listed in RFP Sections L.34.1.4.1 through L.34.1.4.5.

The (3)Enterprise IP VPN service is built on the Level 3 converged, Multi-Protocol Label Switching (MPLS) backbone. In addition to other benefits, the NBIP-VPNS provides several unique advantages:

- Security equivalent to the Asynchronous Transfer Mode (ATM) and/or Frame Relay
- End-to-end Class of Service (CoS)
- Dedicated edge routers for NBIP-VPNS traffic
- A range of services over a single, converged MPLS network, including Internet access, Voice-over IP (VoIP), and NBIP-VPN
- A single Network Operations Center (NOC) and point of contact for customers

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

encountered in meeting the individual service requirements from the Government.

3.2.1.4 SYNCHRONIZATION

Synchronization of the Level 3 Network architecture occurs the same way for all services we provide. Section 3.1.1.4 of this proposal volume contains a detailed description of synchronization in our network.

3.2.2 Satisfaction of Performance Requirements [C.2.7.3.4]

This section of the proposal addresses requirements in Section L.34.1.4.2 of the RFP. The topics covered are Quality of Service (QoS) with respect to performance metrics; the approach for monitoring and measuring Key Performance Indicators (KPI), and Acceptable Quality Levels (AQL); proposed performance improvements; and benefits, rationale, and measurement of performance improvements.

3.2.2.1 QUALITY OF SERVICE

Level 3 will support the mandatory routine performance metrics shown in Table 3.2-1 for our NBIP-VPNS [REDACTED]

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]


[REDACTED]

3.2.2.2 MONITORING AND MEASURING KPIs AND AQLs

The Level 3 Customer Service Organization (CSO) will monitor all provided (3)Enterprise services using our IP backbone. Section 3.1.2.2 of this proposal volume describes the monitoring tools used by this organization.

Level 3 extends its measurement capabilities to encompass end-to-end Service Enabling Device-to-Service Enabling Device (SED-to-SED) performance as described below.

Level 3 has implemented [REDACTED] architecture to facilitate the collection of NBIP-VPNS network statistics. [REDACTED] is a Level 3 gateway-based probe device that actively tests for KPI/AQL verification. It provides a gateway-to-gateway mesh for backbone measurements. The [REDACTED] server collects and distributes all performance results. [REDACTED] measures latency, jitter, packet loss, out-of-sequence packets, and average ping response time, and has the ability to create Simple Network Management Protocol (SNMP) traps for threshold violations.

Level 3 continuously develops systems to interpret and correlate events collected from the network in real time (see Figure 3.2-1). In this figure, the Level 3 edge routers (Provider Edge or PE routers) that provide Government services are each connected to a monitoring hardware device from  Networks. These probes are all connected in a full mesh over the Level 3 backbone (Provider or P) routers. This mesh of probes provides real time reporting of network trouble in our Network Operations Center as well as providing data for Government required reporting.

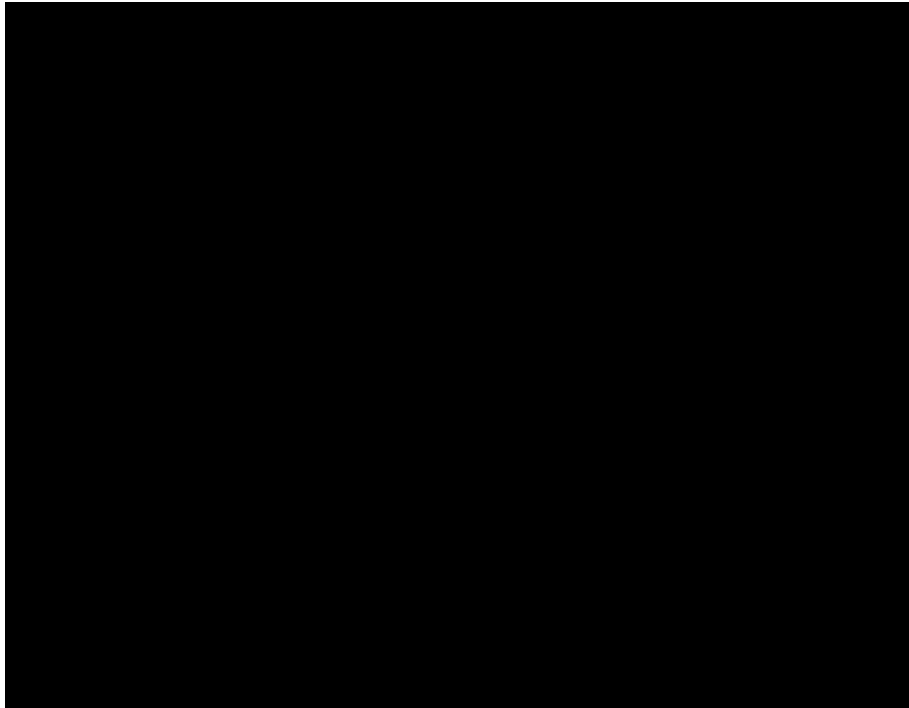


Figure 3.2-1: Level 3's Network performance infrastructure provides a test suite to actively test network performance for NBIP-VPN

Level 3 also provides end-to-end monitoring of Government connections as required by the Government. Our performance monitoring system ensure that KPI/AQLs are maintained end to end. There are five scenarios for monitoring of Government connections depending on how access is ordered. These scenarios are described below.

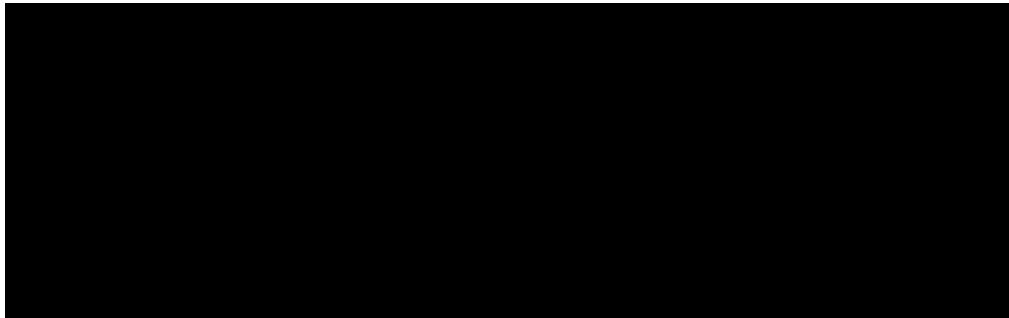


Figure 3.2-1a: Under Scenario 1, Level 3 provides a SED for the NBIP-VPNS to the Government, along with a Dedicated Access Arrangement

Scenario 1, shown in Figure 3.2-1a, is where Level 3 provides a SED for the NBIP-VPN services to the Government, along with a Dedicated Access arrangement. In this case, Level 3 will provide a [REDACTED] SED that supports [REDACTED] IP SLA software based monitoring system at the Government's premises. This software agent will communicate with the [REDACTED] monitoring probe attached to the PE router in the Level 3 gateway facility. Since each [REDACTED] probe also communicates with the other [REDACTED] probes in each facility, we can obtain a complete end to end view of the network by combining the two measures. When combined with the data from other Government sites, this solution will provide end to end monitoring from each Government location across the Level 3 backbone to other Government locations.

There are two options that can be provided in Scenario 1. A [REDACTED] SED can be provided instead of a [REDACTED] SED. The [REDACTED] SED runs [REDACTED] [REDACTED] software, and is also interoperable with our [REDACTED] probe attached to the PE router. For agencies that need high resolution monitoring, a [REDACTED] hardware probe is also available that can be attached to either the [REDACTED] SED or [REDACTED] SED. The [REDACTED] probe provides higher resolution monitoring for the circuit for special applications the require monitoring to the microsecond level. For normal operation, and to meet the

Government's KPI/AQLs the [redacted] or [redacted] software based solution is sufficient.

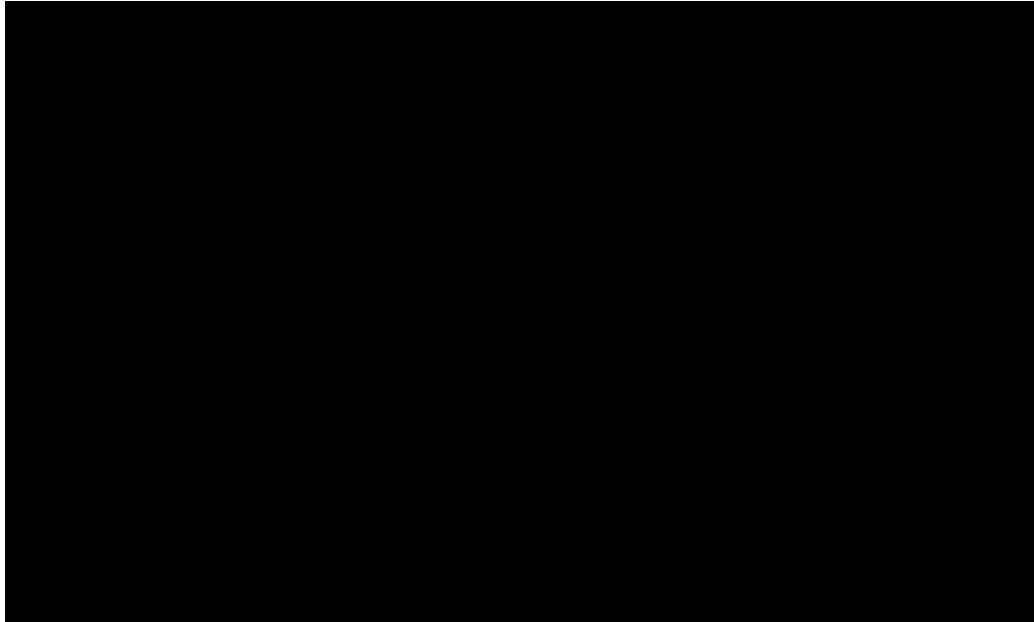


Figure 3.2-1b: Under Scenario 2, Level 3 provides Dedicated Access to the NBIP-VPNS, and the Government provides its own SED.

As illustrated in Figure 3.2-1b, Scenario 2 exists where Level 3 provides Dedicated Access to the NBIP-VPNS, and the Government chooses to provide their own SED router. The Government may have a compatible router from [redacted] or [redacted] that they wish to give Level 3 read only access for monitoring purposes. In this case, Level 3 will utilize the [redacted] Agent or [redacted] software via standard SNMP commands and Internet Control Message Protocol (ICMP) pings to provide monitoring of the solution. If the Government chooses to not provide access to the router, Level 3 will monitor for latency, availability and data delivery via standard circuit monitoring techniques. In this case, our monitoring demarcation point will exist at the end of our dedicated access arrangement.

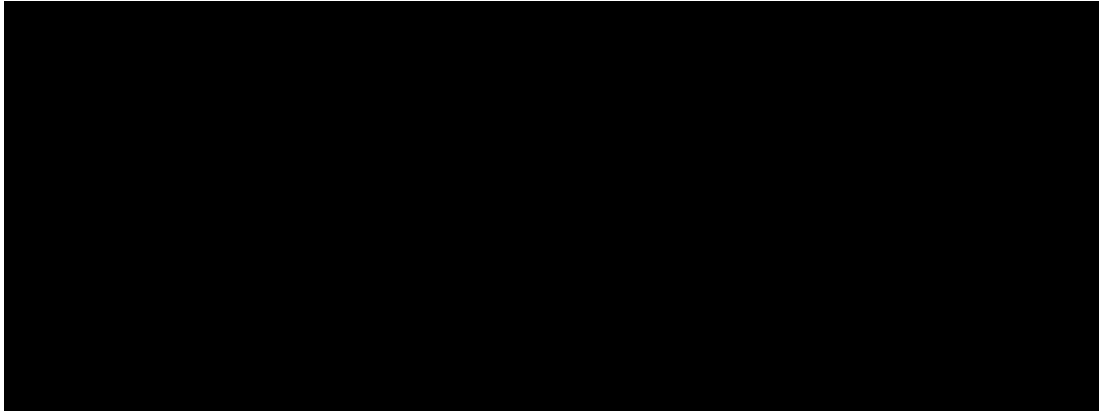




Figure 3.2-1c: Under Scenario 2B, the Government can purchase a Brix 100 Monitoring Probe Device from Level 3.

The Government also has the option to purchase a   monitoring probe device from Level 3 under Scenario 2. We will attach this SED to the Government's router via a 100Mbps Ethernet port, and monitor the circuit through this mechanism. The Government will need to provide IP connectivity through any firewall or filtering devices or software to our SED in this scenario. Figure Scenario 3.2-1c illustrates this configuration.

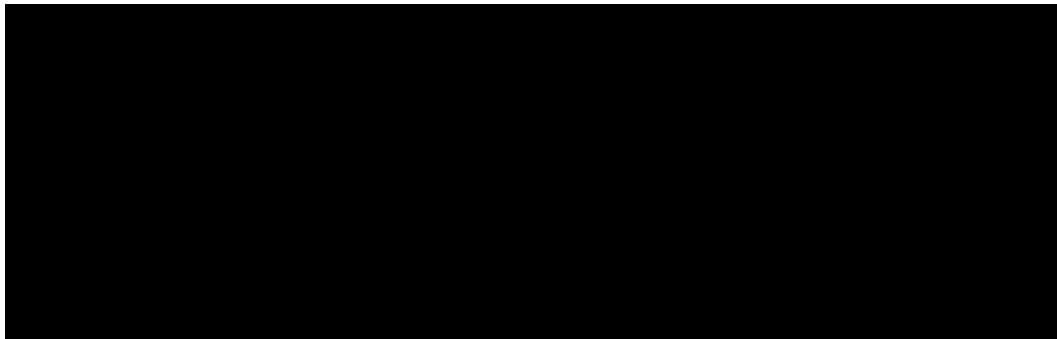


Figure 3.2-1d: Under Scenario 3, Level 3 provides Embedded Access to the Government.

Under a third scenario, Level 3 provides Embedded Access, as illustrated in Figure 3.2-1d. In Embedded Access, the access arrangement, port charge, and Level 3 termination equipment are all included in our CLINs. In this case Level 3 will use on board software in our termination device to

monitor between the device and the [REDACTED] probe in the gateway. In all other respects, this service is identical to Scenario 1.

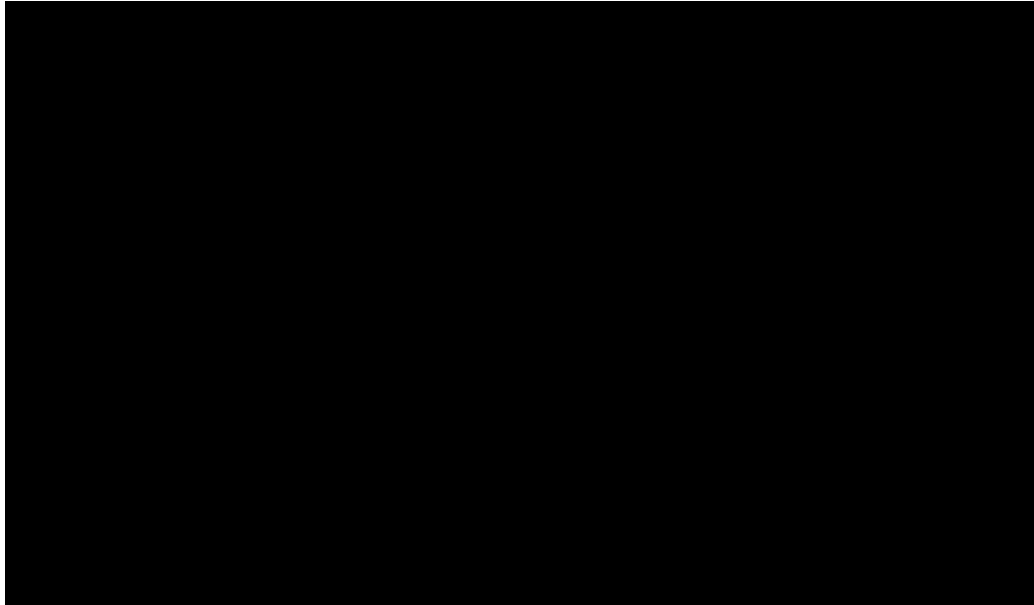


Figure 3.2-1e. Under Scenario 4, the Government uses an Independent Access Arrangement to reach Level 3's NBIP-VPNS and Level 3 provides a SED to terminate the service.

Scenario 4 occurs when the Government uses an Independent Access arrangement to reach Level 3's NBIP-VPN service and Level 3 provides a SED to terminate the service at the Government location. This scenario, illustrated in Figure 3.2-1e, is identical to Scenario 1, and Level 3 will use the [REDACTED] software to monitor to our [REDACTED] probe. Level 3 will not be responsible for correcting issues found on the Independent Access through our monitoring, and will refer these issues back to the Government entity for correction with their vendor. As with Scenario 1, Level 3 can also provide an optional [REDACTED] hardware monitoring device attached to our SED for higher resolution monitoring.

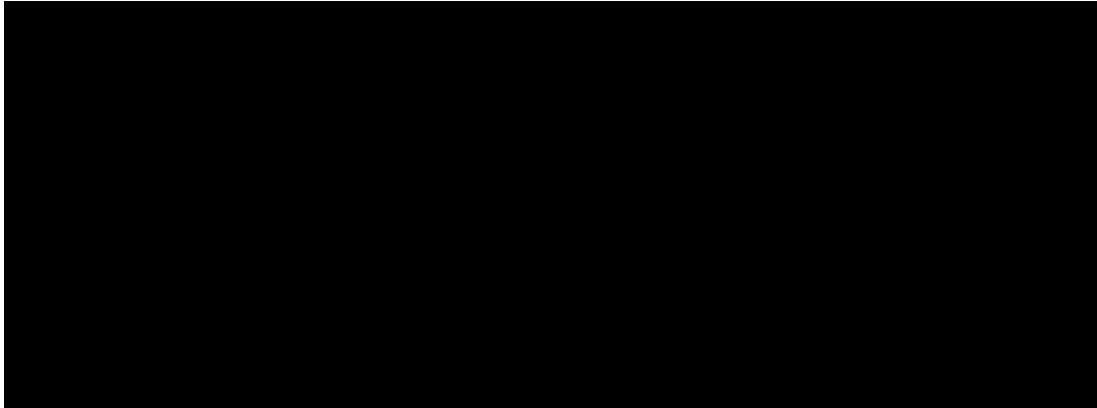



Figure 3.2-1f. Under Scenario 5, the Government purchases an Independent Access Arrangement to reach Level 3's NBIP-VPNS, and provides their own SED.

The last scenario, illustrated in Figure 3.2-1f, occurs when the Government purchases an Independent Access arrangement to Level 3's NBIP-VPN service and chooses to provide their own SED or use a SED from another vendor. In this case, Level 3 will provide performance data from the port of our PE router in our gateway. This configuration is fully supported by the software on the PE router and the  probe attached to the PE router.

These five scenarios explain how Level 3 will provide monitoring to the Government's service location. In addition, Level 3 has a robust system for monitoring performance between our gateway facilities. When this data is combined, we provide the Government with a complete end to end picture of the required KPIs, which can be used to audit compliance with AQLs.

This monitoring system enables the massive amount of performance and fault management data to be used efficiently. It enables faster identification of the source of network problems and ensures that root-trouble source tickets are the immediate focus of trouble resolution, and not corollary tickets, in order to speed restoration for all customers. The KPIs that will be measured for Level 3's NBIP-VPNS are described below.

Latency (CONUS): Latency is an important metric for data services due to the growing bandwidth demand to support converged applications. Applications that used to run over separate networks are now consolidated to one. VoIP and real-time backups for billing can run right next to IP traffic.

Latency measures the delay value based on the average round trip transmissions between agency premises routers for an IPVPN within its CONUS. Sample latency measurements are taken at [REDACTED] intervals, and these samples are then averaged every [REDACTED] minutes. The [REDACTED] samples are again averaged to compute [REDACTED] monthly round-trip delay.

Port Availability: Availability is defined as the percentage of minutes a customer's physical access port is able to send and/or receive traffic in a given month. Availability is determined by the following formula:

$$Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

Unavailability is calculated by the total number of minutes an access port is unable to send and/or receive traffic over the course of a month. Unavailable minutes are determined via Trouble Tickets submitted by the customer.

Time To Restore: Unlike many service providers, Level 3 measures the Time-To-Restore (TTR) in terms of how long a customer must wait until a problem is repaired. Our metric represents the gross internal performance of our Service Management teams. Specifically, the duration of an unexcused outage on an NBIP-VPNS port would be measured from the time a Trouble Ticket is opened to the time that service is restored.

Web tools such as the Federal Web portal, discussed in Section 3.1.2.2 of this proposal volume, will be available for agencies to use when procuring NBIP-VPNS also.

3.2.2.3 PROPOSED PERFORMANCE IMPROVEMENTS

[REDACTED]

[REDACTED]

[REDACTED] Level 3 believes in continuous improvement and will always strive to provide the highest quality services available.

3.2.2.4 PROPOSED PERFORMANCE METRICS

Level 3 recommends that the Government add a KPI for Jitter a performance measure to NBIP-VPNS, as shown in Table 3.2-2.

Jitter is defined as the relative variation in delay between consecutive packets. Jitter is an important factor in the service quality of voice and video data service, and is therefore relevant in converged IP services networks.

To measure jitter, samples are taken every [REDACTED] milliseconds (ms) and

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

Jitter is measured independently among all applicable network IP VPN Level 3 Gateways and reported as a network average that does not include local access loops or CPE.

3.2.3 Satisfaction of Service Specifications

This section addresses the requirements contained in Section L.34.1.4.3 of the RFP. The topics addressed include a technical description of how the service requirements are met, proposed service enhancements, necessary network modifications, and experience providing the service.

3.2.3.1 TECHNICAL DESCRIPTION OF NBIP-VPNS

The Level 3 Team has developed a NBIP-VPNS solution that meets or exceeds all requirements for secure network operations and management specified in RFP Section C.2.7.3. Our solution uses both the Level 3 converged MPLS core network and encrypted NBIP-VPNS to logically separate core network traffic from other customer traffic while taking advantage of the inbuilt economies of scale and reliability. To extend the core network to Government locations requires either dedicated access arrangements or remote access via dialup, DSL or cable. We will optionally deploy CPE dedicated to Government use. An integral part of our service will be to ensure that only Government-authorized personnel have access to, or the ability to view, Government equipment or data.

Government voice, video, and data traffic carried over the Level 3 NBIP-VPN network is logically separated from best effort Internet traffic providing the same level of security as layer 2 VPN technologies such as ATM and Frame Relay.

Government traffic will be further protected as it travels over the Level 3 NBIP VPN service through the use of Internet Protocol Security (IPSec) encryption. Figure 3.2-2 summarizes the flow of an IP packet between the Customer Edge (CE) equipment located at various agency locations.

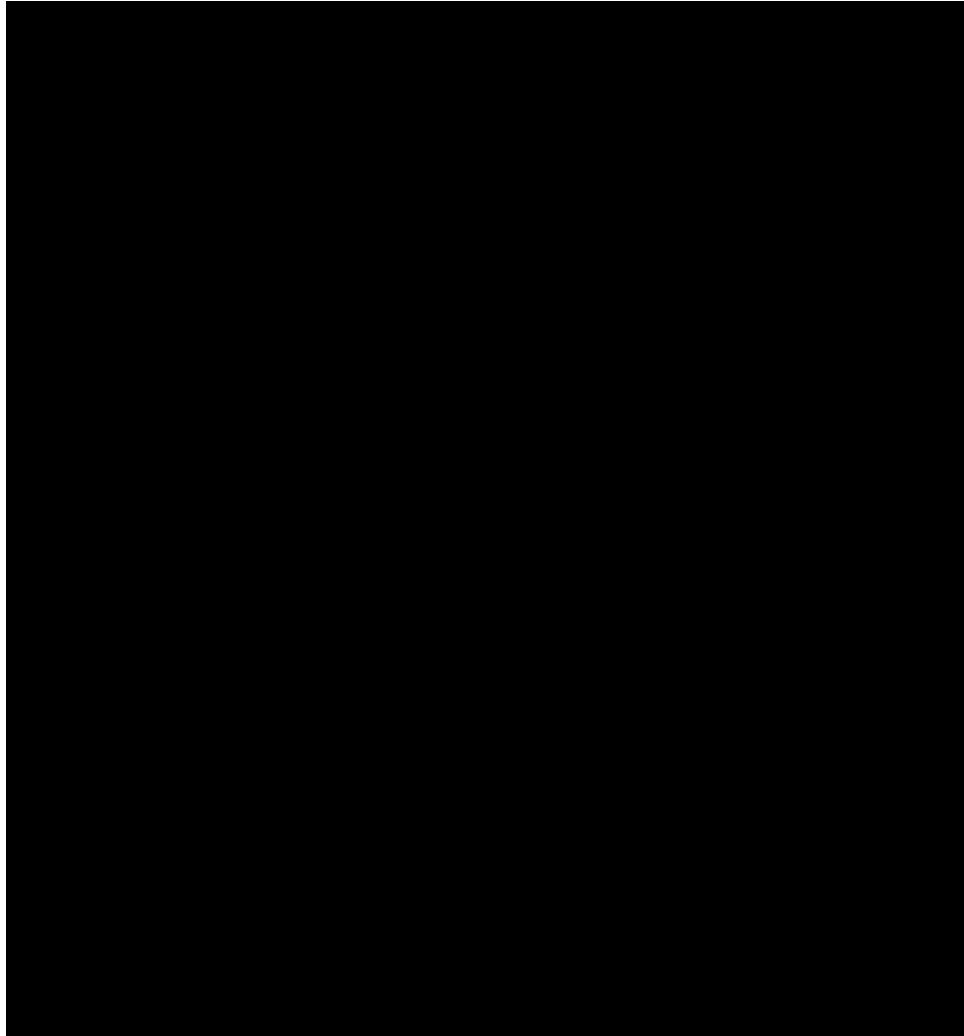

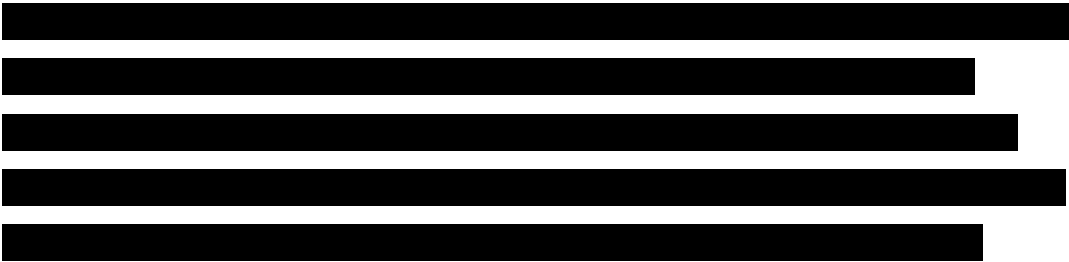


Figure 3.2-2: The Level 3 Team network-based IP VPN solution logically separates Government traffic over our core network to leverage the scale and reliability of the world's largest converged network

Our approach to encryption offers a highly scalable and secure solution for agency traffic. 





The Level 3 NBIP-VPNS supports the three basic solutions required by the Government.

Intranet: NBIP-VPNS offers dedicated site-to-site connectivity. In this scenario, geographically separated sites can establish secure communication channels through the Level 3 NBIP-VPNS Network via the VPN gateways deployed at the Level 3 Points-of-Presence (POPs).

Extranet: The Level 3 NBIP-VPNS supports extranets that enable trusted business partners to connect securely to an agency intranet via encrypted tunnels and utilizing broadband or dedicated access. The Level 3 NBIP-VPNS can be combined with our Managed Firewall Service (MFS) to create agency extranets.

Remote Access: In the remote-access scenario, the remote-access users establish secure communication tunnels from remote computers to the Government network using the VPN software installed on user computers or CPE devices via dial up, broadband, or dedicated access. This software creates an IPsec or SSL tunnel to a remote-access aggregation device located at a Level 3 facility. The remote-access aggregation device connects to both the Internet and an agency intranet to allow access to remote users from anywhere in the world. Secure token-based or smartcard-based authentication is used to ensure that only authorized users can create an encrypted tunnel into an agency network. Since all communications are encrypted, Government data is protected against unwanted disclosure.

3.2.3.1.1 Standards [C.2.7.3.1.2]

The Level 3 NBIP-VPNS product complies with the required standards as delineated in RFP Section C.2.7.3.1.2. Level 3 architects were heavily involved in the development of RFC2547bis for BGP-VPNs. We continue to be involved with IETF standards, particularly around the issues associated with inter-provider VPNs. Level 3 is committed to implementing future standards as technologies are developed and as new standards are defined and become commercially available.

3.2.3.1.2 Connectivity [C.2.7.3.1.3]

The Level 3 NBIP-VPNS service supports a dedicated site-to-site access via leased lines. The Level 3 Team NBIP-VPNS service supports secure remote access via either dialup, DSL or Cable. The NBIP-VPNS service provides for full meshing among VPN end-locations as a default configuration. [REDACTED]

3.2.3.1.3 Technical Capabilities [C.2.7.3.1.4]

The mandatory capabilities included in the RFP Section C.2.7.3.1.4 show that maintaining the integrity of the network with flexible interfaces is a significant concern. This discussion provides a detailed description of the Level 3 Team recommended NBIP-VPNS solution focusing on network integrity and access options. A summary of the other RFP capability requirements follows, identifying additional details if necessary.

Tunneling Standards: The Level 3 Team proposes to provide security for Government traffic by implementing a Layer 3 IPSec encryption solution for all agency traffic as it traverses the managed NBIP-VPNS environment.

[REDACTED]

[REDACTED]

[REDACTED]

The IPsec solution that the Level 3 Team proposes is based on a robust solution that will enable IPsec to support the required CoS through Encapsulating Security Payload (ESP) via transport mode to enable payload encryption. The CoS bits are automatically copied into the IPsec IP header to preserve CoS across the network without compromising any of the payload content. The IPsec solution will support the automatic, scalable, hierarchical design and the reestablishment of encrypted circuits in the event of an interruption in service. The solution proposed by the Level 3 Team will not

inhibit the use of resilient or redundant hardware, routing, or firewall configurations

Encryption Standards: The IPSec solution deployed for the NBIP-VPNS will support both industry standards and Government specifications, such as Federal Information Processing Standards (FIPS), to meet requirements for both authentication and encryption, such as Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Figure 3.2-3 shows the conceptual design:

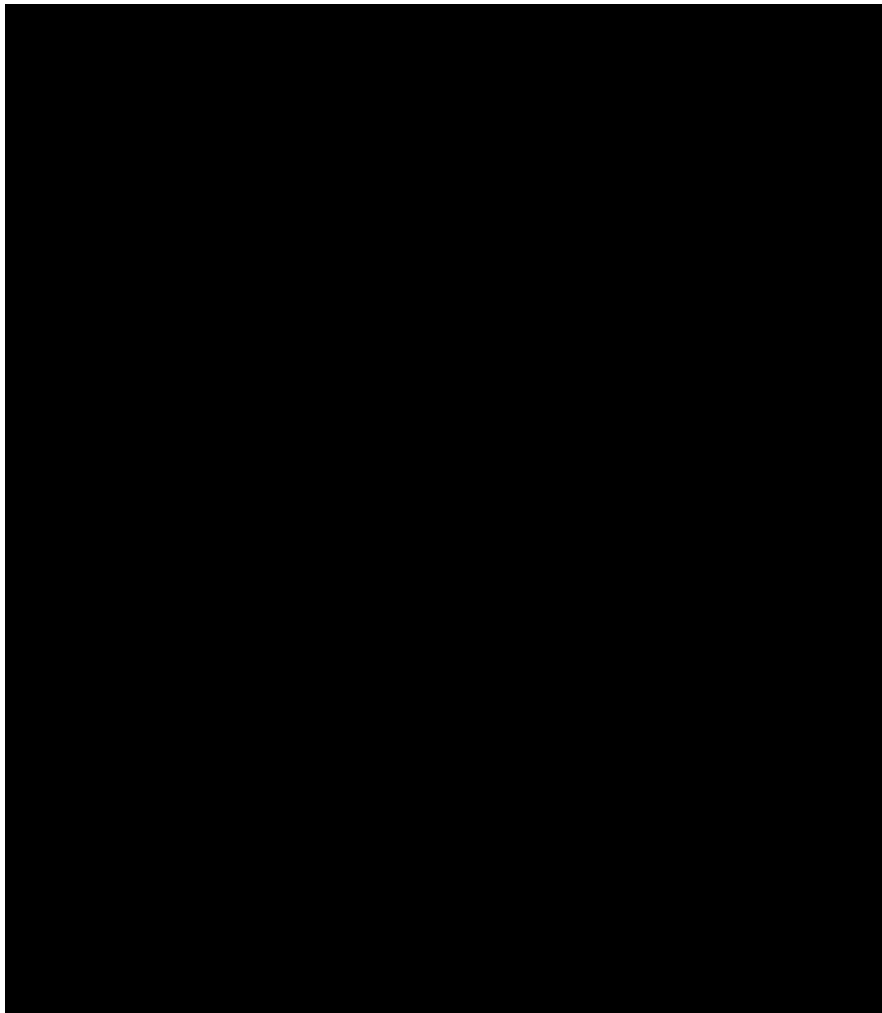


Figure 3.2-3: Conceptual design for IPSec solution deployed for Level 3 NBIP-VPNS

[Redacted text block]

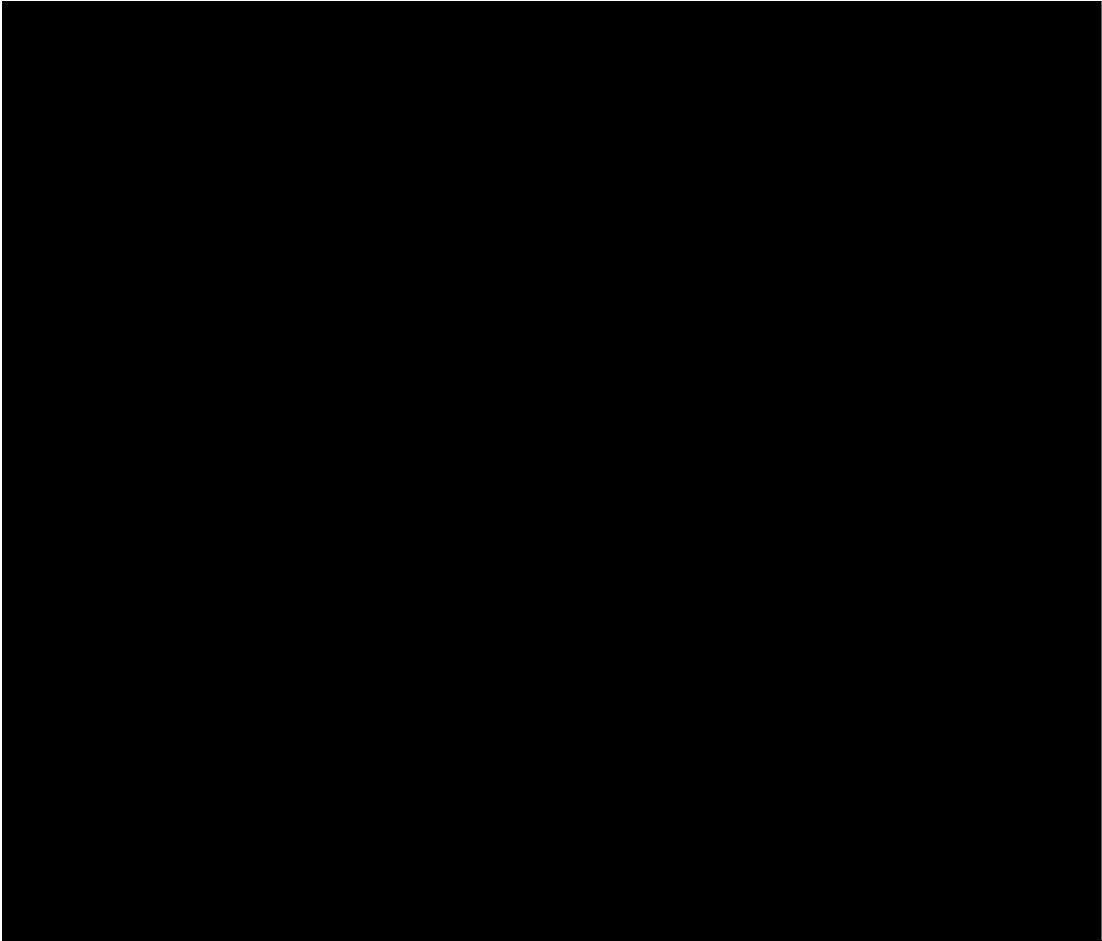
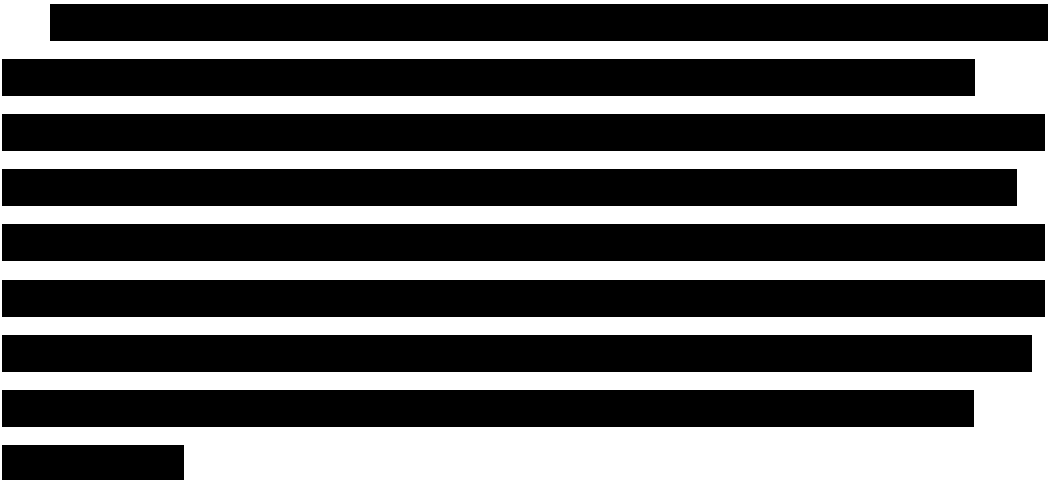
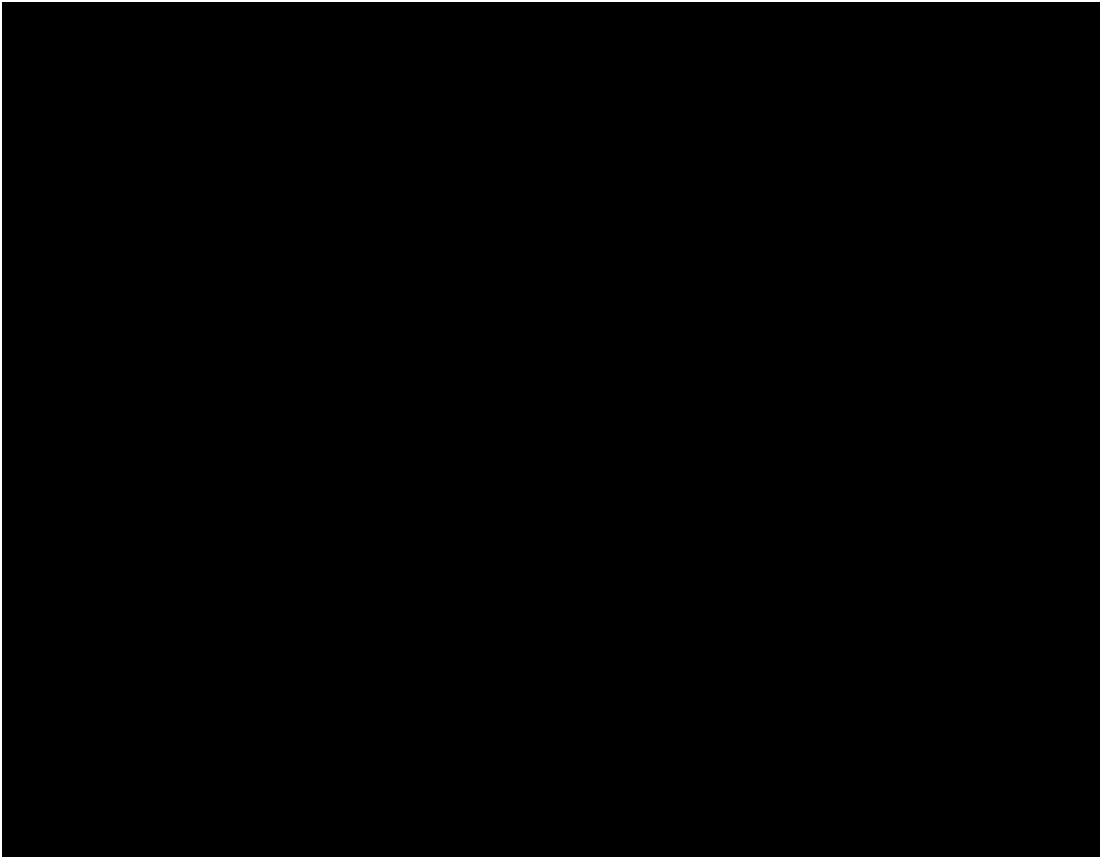


Figure 3.2-4: IPSec aggregators will maintain IPSec connections to all other IPSec aggregators in a full-mesh topology





[Redacted line of text]

[Redacted line of text]

[Redacted line of text]

[Redacted line of text]

[Redacted line of text]

[Redacted line of text]

[Redacted line of text]

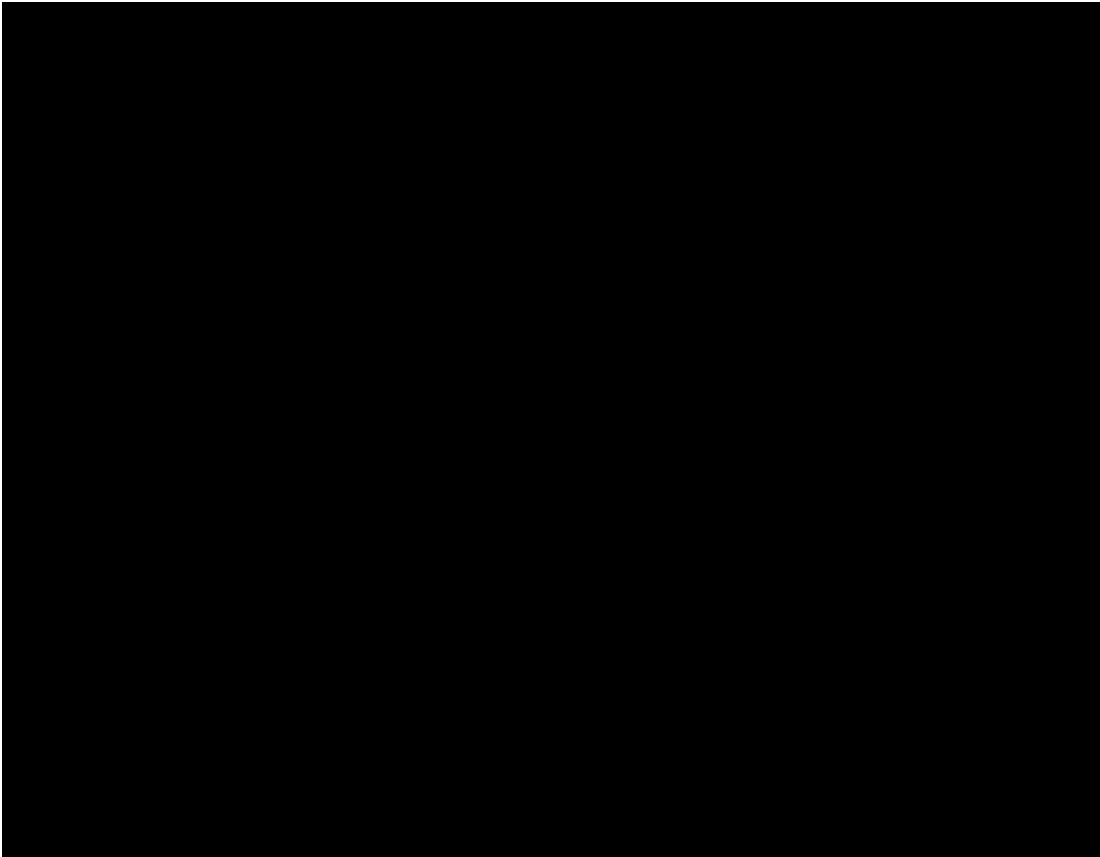
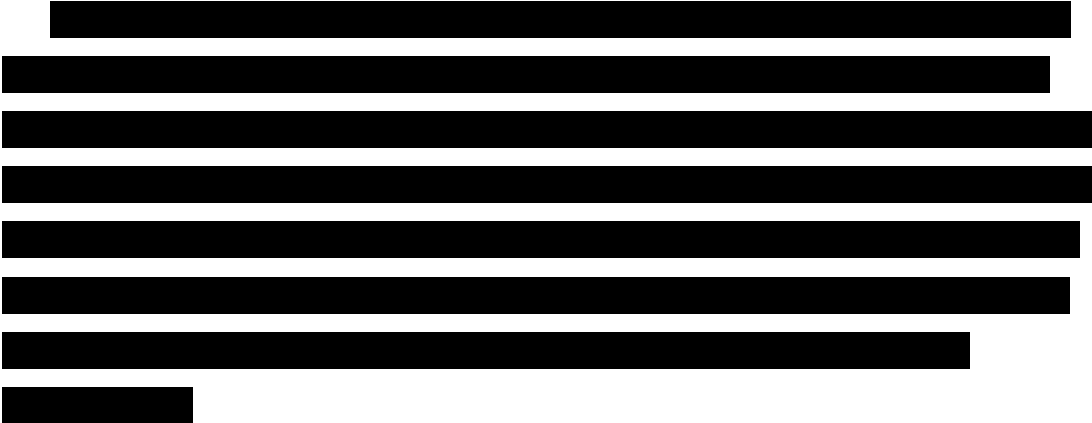
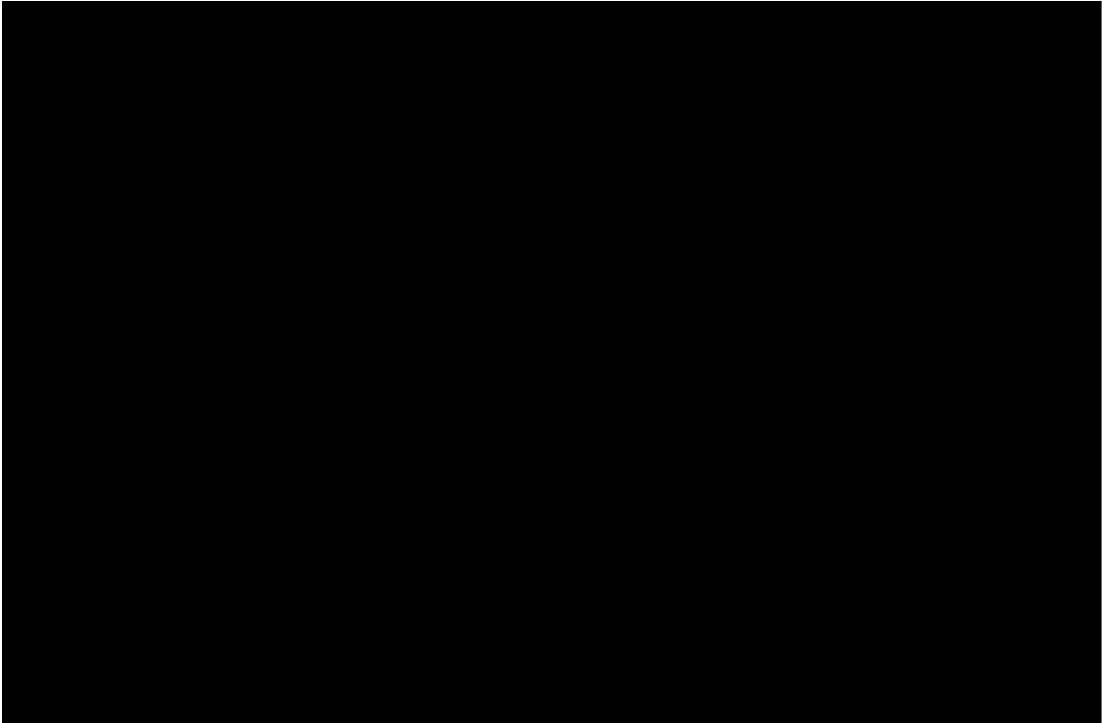


Figure 3.2-6: The CPE to IPSec aggregator tunnel provides a new label for the packet before it reaches its destination end point





[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text] encrypted IP-VPN. It might also be an



In Figure 3.2-8, network firewalls are used to link the two agencies or business partners together. In this design, agency A maintains its own encryption key space up to the link connecting it to the firewall. A shared key, jointly maintained between the two partners, is then used to create a connection between the two intranets. Agency B, the business partner, also maintains its own key space internally. The agency does not have to use a network-based firewall. A premises-based firewall may also be used at a larger Government location, which might make sense in a building that several agencies share. Level 3 can provide the firewall services to the

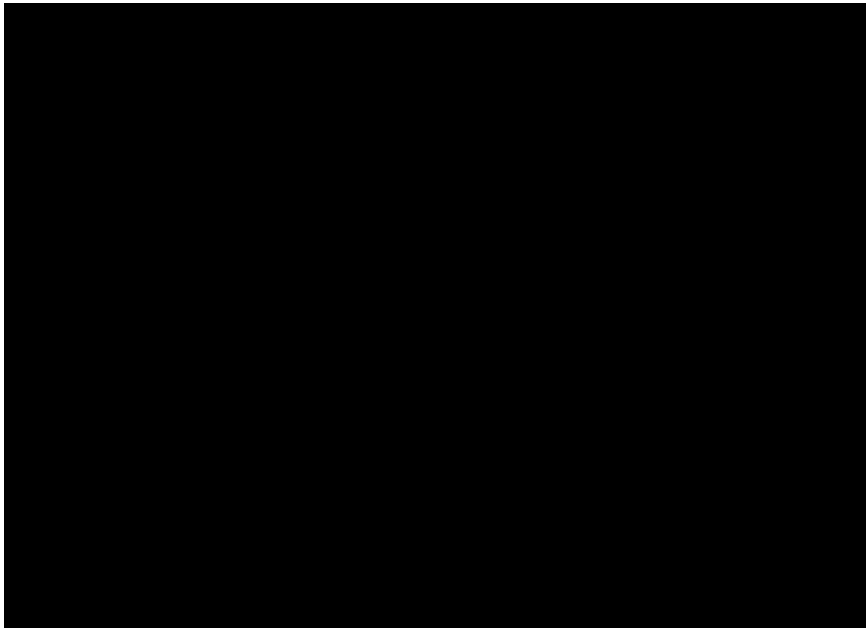


Figure 3.2-8: Our IPSec aggregation solution will enable any-to-any-type connectivity and lower latency, which is a key benefit of the NBIP-VPNS

Government, or the agency might choose to manage this portion of the network design themselves. The Level 3 NBIP-VPNS gives Government the flexibility to build extranet designs as required to meet its business requirements.

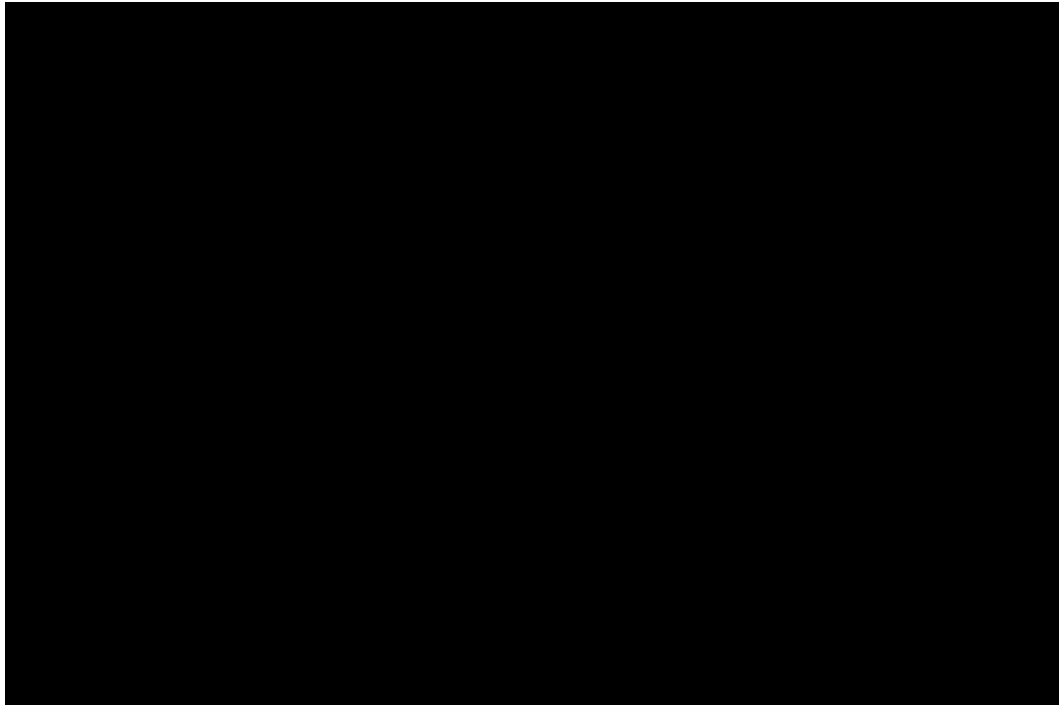
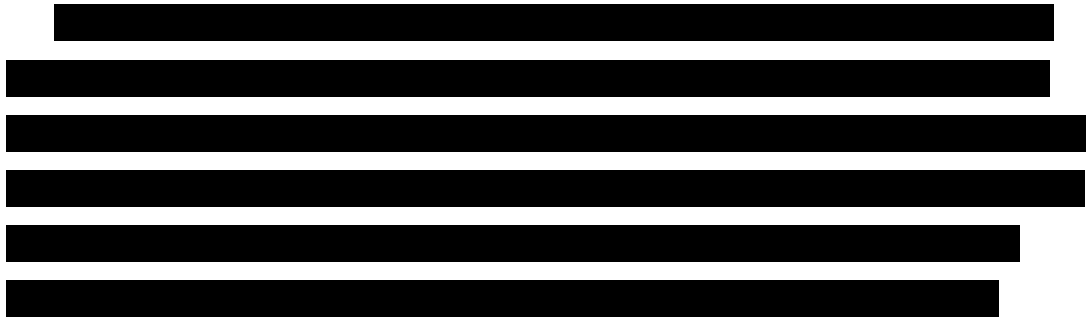



Figure 3.2-9: Our team will manage a remote-access IPSec aggregator that will collect encrypted tunnels from analog modems, DSL, and cable users



 This design provides maximum flexibility to the Government in enabling remote users at home and on the road to connect for agency business. It also allows the Government to use inexpensive DSL and cable

services to connect small remote and branch offices that do not warrant the expense of a dedicated NBIP-VPNS circuit.

The Level 3 remote-access solution is flexible and enables the Government to achieve its goals of seamless access to teleworkers, small offices, and remote users. It maintains the security of a NBIP VPN and, at the same time, provides for flexible access to the network.

For Government agencies that do not wish to use the (3)Enterprise fully managed solution, the hub-and-spoke, partial-mesh, and full-mesh architectures are fully supported. The agency may chose to implement its own CPE or encryption where its security requirements are beyond what Level 3 can provide. These designs might also be used by agencies with legacy network support requirements.

[REDACTED]

[Redacted]

The Level 3 Team NBIP-VPNS offering provides the capabilities, required in the RFP. The security-related capabilities such as tunneling and encryption were discussed above. How the Level 3 Team provides the remaining capabilities is described below.

Authentication Services Support for IPv4 and IPv6: The Level 3 NBIP-VPNS supports IPv4 as both as the encapsulating and encapsulated protocol and will support IPv6 when it becomes commercially available. Section 2.3.6 of this proposal volume discusses our approach for converting to IPv6.

Multiple QoS Options: NBIP-VPNS offered by Level 3 supports [Redacted] QoS levels, each designed to ideally accommodate different traffic types with different performance parameters.

One element differentiating Level 3 from other providers is that we are able to offer true end-to-end CoS, as opposed to CoS simply from the Customer Edge (CE) to the Provider Edge (PE). NBIP-VPNS supports end-to-end class of service, including access and backbone prioritization. An agency may designate its VPN to support either Port Mode (PM) or Type of Service (ToS)-based Class of Service. However, these two CoS options may not be mixed within a single VPN.

Port Mode: Using PM, Level 3 will map all traffic in a particular virtual connection to a customer-specified class of service queue on Level 3's backbone. All traffic in the virtual connection will be placed in the same CoS queue [Redacted]. On the outbound PE-CE link, all traffic is

treated the same and placed in a single, First-in, First-out (FIFO) queue. There is no per-packet differentiation.

Type-of-Service Mode: This mode allows customers to use ToS fields in the IP header to enable more granular management of bandwidth on access (ingress and egress) circuits. In ToS mode, the customer may set the bandwidth allocation level for each ToS value, allowing very granular control and effective bandwidth management. Level 3 will also map each of the ToS values into one [REDACTED] pre-defined backbone queues: [REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

The NBIP-VPNS QoS model supports Weighted Random Early Detection (WRED) where appropriate, specifically in the “Silver” category.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

To achieve the necessary treatment for differentiated traffic classes, the agency must mark its VPN traffic flows according to requirements of the application. Accordingly, the CE or other site routers will classify and mark the IP packet with the appropriate DSCP value and send it to the PE. The PE will assign a forwarding treatment to the packets according to their DSCP values by mapping to various backbone queues shown in Table 3.2-4. Level 3 can provide managed CE routers, and can assist the Government with marking of DSCP values as required through our Managed Network Services (MNSs) offering.

The NBIP-VPNS Diffserv feature allows the Government to mark and prioritize packets at the edge of the network to ensure that time sensitive traffic is prioritized across the Level 3 backbone. The Government can also choose to use a simpler ToS model where only eight values are supported, or a PM where an entire port assumes one CoS class. Through these three modes, any number of CoS models can be supported for maximum agency flexibility. See Section 2.2.2 of this proposal volume for more information about how the Level 3 Network protects time sensitive traffic.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

before our customers even know of an issue. The NOC performs regular network connectivity performance reviews. If an irregularity is detected, the organization follows documented procedures to restore service.

The Level 3 Team concept of operations integrates network surveillance performed by the NOC with our Customer Support Organization (CSO) to provide seamless coverage and end-to-end management of all critical network elements. The CSO will serve as liaison between the Level 3 NOC and the subscribing agency. The CSO staff will gather performance data on the systems supported and use these data to optimize network efficiency, helping Government agencies to avoid unnecessary costs.

The CSO will be available 24x7 to the agency via the dedicated agency help desk, which is described in Section 5.1.3.1.3.4 of this proposal volume.

An extension of the agency-dedicated Help Desk, the [REDACTED] portal will provide users with access to an entire host of business performance metrics that empower an agency to manage its network. The [REDACTED] portal will provide these capabilities:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Access Technologies: Level 3 enables customers to use a single port for multiple VPNs. Level 3 supports multiple Layer 2 interfaces in our NBIP VPN ports. Some interfaces such as Frame Relay or ATM have logical Layer 2

identifiers, such as Data Link Connection Identifiers (DLCIs) or Virtual Channels (VCs), respectively, to assign to different customer traffic flows from their routers. Level 3 can map those logical Layer 2 identifiers to VPN groups to separate customer traffic into separate logical communications. In addition, those flows can be mapped into specified QoS levels to ensure the necessary service level for customer applications.

Design and Engineering Service: Level 3 will provide pre-sales design and engineering services, as part of the standard NBIP-VPNS, that includes bandwidth determination and CPE design. Engineering above and beyond these services would be offered as part of the Customer Specific Design and Engineering Services (CSDES) or the Design and Engineering Services (DES) portion of our MNSs, as appropriate.

Secure Routing: NBIP-VPNS service supports a centralized routing policy with our routing registry. Routing is secure in that no other customer can inject routes into another customer's VPN.

Encryption, Decryption, and Key Management: The NBIP-VPNS service supports the encryption, decryption, and key management profiles for an agency. Agencies are able to determine the level of security that they want to provide for themselves or have Level 3 provide. An example of such a division of responsibility would be that Level 3 provides the NBIP-VPNS for the transport of secure communications but that the agency provides the VPN gateways for encryption, tunneling, and other security features.

Authentication of Temporary Remote Users: The Level 3 Team offering allows alternate methods of authenticating temporary remote users. The authentication server can be operated and managed by either Level 3, an agency, or a third party, as required.

3.2.3.1.4 Features [C.2.7.3.2]

RFP Section C.2.7.3.2 contains six mandatory features for NBIP-VPNS. How Level 3 will accomplish offering each of these features is discussed below:

1. **Class of Service:** Level 3 is different from other providers because we are able to offer true end-to-end CoS, as opposed to CoS simply from the CE to the PE. NBIP-VPNS service supports end-to-end CoS, including access and backbone prioritization. A customer may designate its VPN to support either PM or ToS-based CoS. However, the two CoS options can not be mixed within a single VPN.

a) **Port Mode:** Using PM, Level 3 will map all traffic in a particular virtual connection to a customer-specified class of service queue on the Level 3 backbone. All traffic in the virtual connection will be placed in the same CoS queue: [REDACTED]. On the outbound PE-CE link, all traffic is treated the same and placed in a single, First-in, First-out (FIFO) queue. There is no per-packet differentiation.

b) **Type of Service Mode:** ToS mode allows the customer to use the ToS fields in the IP header to enable more granular management of bandwidth on access (ingress and egress) circuits. In ToS mode, the customer may set bandwidth allocation level for each ToS value, allowing very granular control and effective bandwidth management. Level 3 will also map each of the ToS values into either a [REDACTED] backbone queue.

2. **High Availability:** Level 3 offers two different redundancy options for the routers on which the customer's NBIP-VPNS service is terminated, router redundancy and gateway redundancy.

If the customer agency would like to connect from its site via two

distinct access lines, they may choose each access to terminate to a different Level 3 router within the gateway to ensure a connection in the unlikely event one of the Level 3 PE routers should encounter an outage.

Customers may elect to have multiple connections from their sites to more than one Level 3 Gateway. In this way, customers request redundant connections to ensure against the unlikely event an outage will occur that affects an entire Level 3 Gateway or metropolitan area.

3. **Internet Gateway Service:** Level 3, in combination with our MFS and our Internet Protocol Service (IPS), can provide an Internet gateway option for the NBIP VPN. This solution allows an agency to access the Internet using the same physical circuit and NBIP-VPNS port that is used for the VPN.

Figure 3.2-10 illustrates all agency locations accessing the Internet through a central hub site PBIP-VPNS port. IPsec-encrypted VPN traffic remains unchanged, and all Internet traffic (ingress and egress) must traverse the VPN and exit via the hub site PBIP-VPNS port:

4. **Interworking with NBIP-VPNS:** NBIP-VPNS is designed to interoperate with our Internet Protocol Service and Ethernet Service. Remote access (Dial, DSL, and Cable) for NBIP-VPNS is delivered via the same network as the NBIP-VPNS. Additionally, the NBIP-VPNS has an Internet gateway feature that allows for internetworking with NBIP-VPNS.
5. **Key Management:** The NBIP-VPNS service provides the management of encryption keys to include the generation, distribution, storage and security of said keys.

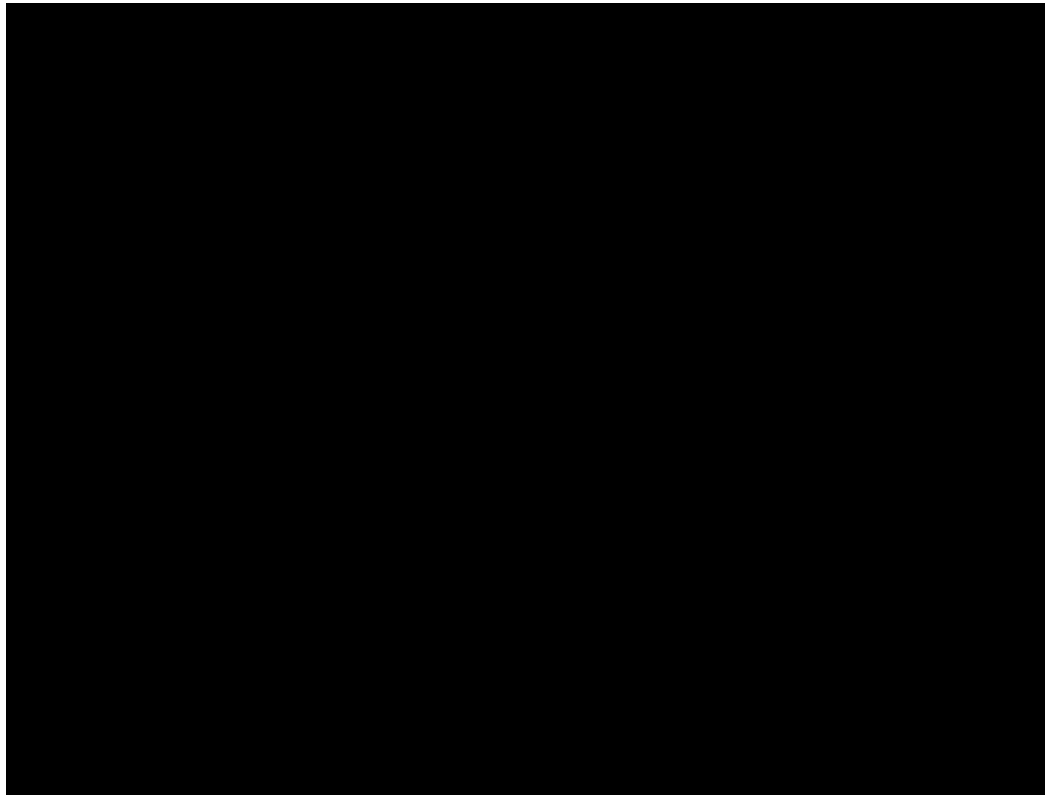


Figure 3.2-10: Networx NBIP VPN internet gateway

6. **Security Services:** Managed Security Services are offered as add-on features to the NBIP-VPNS service, to include the following capabilities as required by the Government:
- a) Firewall Services
 - b) Network Scanning
 - c) Managed IDS
 - d) DOS Protection
 - e) Network Address Translation
 - f) Port Address Translation
 - g) Edge-to-Edge Encryption

h) Replay Attack Protection

3.2.3.1.5 Interfaces [C.2.7.3.3]

The Level 3 NBIP-VPNS supports the following, commercially available, User-to-Network Interfaces (UNIs):

Intranet and Extranet NBIP-VPNS (C.2.7.3.3.1)

- Ethernet Interface
 - 1 Megabits-per-second (Mbps) up to 1 Gigabit Ethernet (GbE)
 - 10 GbE
- Private Line Service
 - DSO
 - Fractional T1
 - T1
 - T3
 - Fractional T3
 - OC-3c
 - OC-12c
 - OC-48c
 - OC-192c
- IP over SONET Service
 - OC-3c
 - OC-12c
 - OC-48c
 - OC-192c

Remote-Access, NBIP-VPNS (C.2.7.3.3.2)


- Voice Service: Analog Dial-up at 56 Kbps
- DSL Service: xDSL Access at 1.5 to 6 Mbps
- Cable High-Speed Access: 320 Kbps up to 10 Mbps

- Satellite Access
- Circuit-Switched Data Service: ISDN at 64 and 128 Kbps

3.2.3.2 PROPOSED SERVICE ENHANCEMENTS



3.2.3.3 NETWORK MODIFICATIONS

The NBIP-VPNS provides a foundation for the network convergence trend currently underway in the telecommunications industry.  provides this service over the Level 3 state-of-the-art, converged MPLS backbone. The Government can achieve this convergence without sacrificing the QoS or security levels of traditional ATM and Frame Relay offerings. NBIP-VPNS solutions are designed to support:

- Converged Data, Video, and Voice Traffic on a Single Platform
- Both Existing and Emerging IP Applications
- Disaster Recovery Initiatives Based on Rapid Transfer and Redundancy
- Interconnections with Legacy Network Equipment

Minimal modifications will need to be made to the Level 3 Network in order to deliver the NBIP-VPNS to the Government. All service enhancements are rigorously tested in the Level 3 engineering lab and are fully certified prior to deployment on the live network. Minor modifications that need to be made, such as Multi-Link point-to-point Protocol MLPPP support, can be achieved with today's hardware and software and represent little or no risk.

3.2.3.4 NBIP-VPNS EXPERIENCE

The Level 3 Team has extensive experience managing NBIP-VPNSs. Through experienced people, mature processes, and specialized tools,

Level 3 has over [REDACTED] IP VPN Ports under its management. Additionally, Level 3 uses the IP VPN architecture and managed services as the foundation for its own Management Operations Support Systems (MOSS) network, which monitors and manages every backbone and customer service offered by Level 3.

3.2.4 Robust Delivery of Service

This section addresses the requirements of RFP Section L.34.1.4.4. The topics addressed are the ability of the Level 3 Team to support additional traffic from (3)Enterprise customers on our network, our congestion and flow control strategies, and our approach to providing robust access while ensuring resiliency and planning for growth.

3.2.4.1 TRAFFIC CAPACITY

The Level 3 proposed NBIP-VPNS is delivered over the same primary network as the proposed IPS. The details of traffic modeling provided in Section 3.1.4.1 are applicable to the NBIP-VPNS as well.

3.2.4.2 CONGESTION AND FLOW CONTROL STRATEGIES

The Level 3 proposed NBIP-VPNS is delivered over the same primary network as our IPS. Our strategies for congestion and flow control are similar for all IP-based services proposed under this solicitation. See Section 3.1.4.2 for details regarding Level 3 strategies for congestion and flow control.

3.2.4.3 ACCESS, RESILIENCY, AND GROWTH

Level 3 designed the IP backbone, enabling the proposed NBIP-VPNS to be robust and physically strong, resilient and able to recover from inevitable problems, and positioned for continued growth as traffic increases and technology evolves.

Section 3.1.4.3 of this proposal volume discusses the robustness of the access and backbone, the resiliency, and the plans for network growth.

3.2.5 Optimization and Interoperability

This section addresses the requirements of RFP Section L.34.1.4.5. The topics covered include our approach for optimizing engineering, methods to optimize the network architecture, how to handle large concentrations of diverse customer applications, and network interoperability.

3.2.5.1 OPTIMIZING ENGINEERING

Level 3 services are provided over a common network. Therefore, optimization of the network architecture for one service effectively optimizes the network for all services delivered. See Section 3.1.5.1 of this proposal volume for a discussion of the methods we use for optimization.

3.2.5.2 OPTIMIZING NETWORK ARCHITECTURE

Section 3.1.5.2 of this proposal volume describes the Level 3 Network architectures optimization in detail. Since NBIP-VPNS is provided using the same network backbone as IPS, the methods and approaches for optimizing for IPS are applicable to NBIP-VPNS as well.

3.2.5.3 ACCESS WITH DIVERSE CUSTOMER APPLICATIONS

Level 3 uses a common network for delivery of all proposed services. The details regarding our optimization of access in a diverse service environment are contained in Section 3.1.5.3 of this proposal volume.

3.2.5.4 INTERNETWORKING OVER A COMMON INFRASTRUCTURE

The discussion contained in Section 3.1.5.4 of this proposal volume is applicable to NBIP-VPNS as well.