

1.0 VOLUME 2, SECTION 2.13 (CONTINUED): Network Operational Support Systems






1.1

2.13.1.4.5 Respond to technical support.


The (3)Enterprise portal will provide a link to respond to technical support questions as well as a point of contact list for questions. As with our commercial customers, we will provide a method of escalation upon award. Our technical support help desk is staffed 24 X 7 with Technical Customer Account Managers .

1.1.1.1 2.13.1.5 Service Management

Level 3's existing integrated network management and element management systems (NMS and EMS) are robust and scalable. The Level 3 Team will provide real-time visibility into network management statistics and network configuration information for the managed services delivered to the Government. As a result of our experience with a comprehensive set of telecommunications services, we maintain an unparalleled set of tools and capabilities that are required to make a converged network function. The following sections describe the infrastructure for network information reporting.




 depicts the demarcation between   of our managed services. This integrated infrastructure provides common fault and performance management statistics .





Transport Management Infrastructure: The 





 comprise a transport element management system enabling for provisioning, alarming, and inventorying all Level 3 transport network elements.  detects device component interface failures and environmental conditions using 

 feeds all events to the network topology viewer. All transport events are viewable by the network topology viewer, enabling operation-centric parsing, filtering, and sorting. All critical events provide automatic notification and automatic ticket notification. 





IP Management Infrastructure: The [REDACTED]

[REDACTED]
[REDACTED] Additional details, specific to the IP NMS and EMS infrastructure, [REDACTED]
[REDACTED]

We use [REDACTED], together with event interpretation and processing, to support subject-based organization of multicast events over the Information [REDACTED] detects device component and interface failures, significant control and protocol events, environmental conditions, and configuration changes via parsing through [REDACTED], simple network management protocol [REDACTED]

[REDACTED]
[REDACTED]

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

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

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

[REDACTED]
[REDACTED]

[REDACTED]

Level 3 also provides end-to-end monitoring of Government connections as required by the Government. [REDACTED]

[REDACTED] There are several scenarios for monitoring of Government connections depending on how access is ordered, each of which is described below.

[REDACTED]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

The last scenario occurs when the Government purchases an Independent Access Arrangement to Level 3's IPS 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

[REDACTED]

router in our gateway. This configuration is fully supported by the software on the PE router and the Brix probe attached to the PE router.

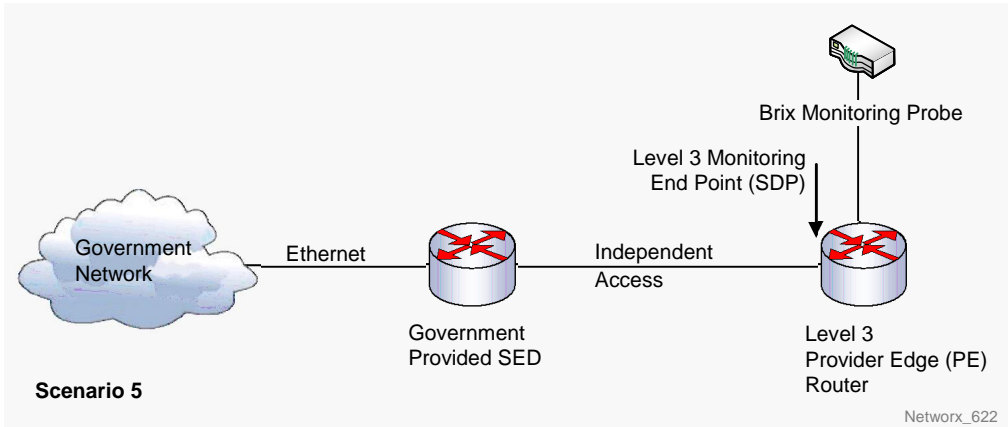


Figure 2.13-9f: Under Scenario 5, the Government purchases an Independent Access Arrangement to reach Level 3’s IPS and provides its own SED.

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.

Level 3 will leverage its NMS and EMS infrastructure, together with its (3)Scape™ provisioning system, to provide network management statistics on and network configuration information as part of fault management for the Governments networks.

1.1.1.2 2.13.1.6 Network Inventory Operational Support Systems

The Level 3 cross domain management solution uses the Network Inventory Management (NIM), centralized inventory management platform , [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[Redacted text block]

1.1.1.3 2.13.1.7 Integration Approach [L.34.2.3.13]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Transaction Capabilities: [Redacted]

[Redacted text block]

[Redacted text block containing multiple lines of blacked-out information]

Level 3 Administration: Our Networkx Program architecture provides for secure administration of Level 3 CPO functions that will be the primary point of contact between our Networkx Program team and the PMO and agency users interested in the (3)Enterprise portal. These administrative functions include requests for user ID's and passwords, maintenance of the agency hierarchy list, and updates to content, as required.

Networkx User: The (3)Enterprise portal supports the Networkx Program requirement for both public and secured areas. A secured user will be able to access authorized data, make queries, obtain reports, and perform on-demand downloads for audit, billing verifications, and other Government program management purposes. Access to specific data will be based on the user's association in the agency hierarchy. Only Authorized personnel can access data in the secured area, meeting the roles and responsibilities in Section G.1, Authorization of Orders, in Section C.3.5 of the RFP.

Login and User Hierarchy: Level 3 believes that good security is a good business practice. For that reason we established an enterprise security program and the appropriate network infrastructure to deliver world-class security for our Government and commercial clients. We provide that world-class security in a manner consistent with industry best practices and regulatory requirements.

© 2007 Level 3 Communications, Inc. All rights reserved. Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this proposal.

The foundation for Level 3's risk-based security model is a Security Policy that already incorporates most of the policies and principles found in NIST 800-14. For the databases, OSS, and information processing systems that are critical for the continuous operation of the Network Program, we will use the results of the initial risk assessment performed for this RFP to identify [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.1.2 2.13.2 OSS Approach to Verification Testing [C.3.9.2.2, L.34.2.3.13.1]
[REDACTED]



[Redacted text block]

1.1.2.1 2.13.2.1 Level 3 Delivers a Fully Compliant OSS Verification Test Plan

[Redacted text block]

[Redacted text block]

1.1.2.2 2.13.2.2 Testing Approach Description

[Redacted text block]

1.1.2.3 2.13.2.3 Effective and Timely testing for New Functionality or Services

[Redacted text block]



[Redacted text block]

1.1.2.4 2.13.2.4 Complete description of data and interfaces

[Redacted text block]

[Redacted text block containing multiple lines of blacked-out content]