

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2007-135220

(P2007-135220A)

(43) 公開日 平成19年5月31日(2007.5.31)

(51) Int. Cl. F I テーマコード (参考)
 H04L 12/56 (2006.01) H04L 12/56 400B 5K030

審査請求 有 請求項の数 33 O L 外国語出願 (全 58 頁)

(21) 出願番号	特願2006-332586 (P2006-332586)	(71) 出願人	504051087
(22) 出願日	平成18年11月10日 (2006.11.10)		アクセンチュア グローバル サービス
(31) 優先権主張番号	05425795.1		ズ ゲゼルシャフト ミット ベシュレン
(32) 優先日	平成17年11月11日 (2005.11.11)		クテル ハフツング
(33) 優先権主張国	欧州特許庁 (EP)		スイス ツェーハー-8200 シャッフ
(31) 優先権主張番号	MI2005A002166		ハウゼン ヘレナッカー 15 ゲシェフ
(32) 優先日	平成17年11月11日 (2005.11.11)		ツハウス
(33) 優先権主張国	イタリア (IT)	(74) 代理人	100082005
			弁理士 熊倉 禎男
		(74) 代理人	100067013
			弁理士 大塚 文昭
		(74) 代理人	100086771
			弁理士 西島 孝喜
		(74) 代理人	100109070
			弁理士 須田 洋之

最終頁に続く

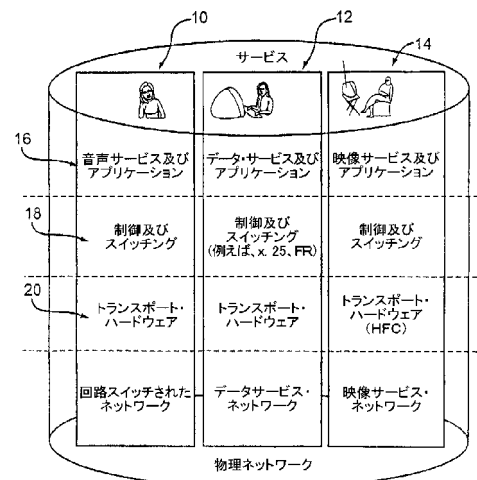
(54) 【発明の名称】 エンド・ツー・エンドのテスト及び診断マネージャ

(57) 【要約】

【課題】 構造化され、エンド・ツー・エンドのアプローチによる、総合的な、エンド・ツー・エンドの、IPトランスポート・レイヤを介して配送されたサービスのテスト及び診断を提供する。

【解決手段】 マルチ・ドメイン、マルチ・サービス・ネットワークにおける、エンド・ツー・エンド・テスト及び診断マネージャが提供される。データベースは、マルチ・ドメイン・ネットワークを介してサービスをカスタムに配送するために必要な、カスタム及びネットワーク・コンポーネントを特定し、説明する、サービス及びネットワーク・インベントリ・データを受信し、記憶する。コンポーネントの構成を確認するための複数のテスト・ツールが存在する。アプリケーション・サーバは、テスト・ツールを呼び出すための命令を実行するように構成される。テストの結果は、インターフェースを介して、オペレータのために表示される。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

マルチ・ドメインのネットワークを介して配送されたサービスのためのサービス配送問題をトラブルシューティングするためのシステムであって、当該マルチ・ドメインのネットワークが、サービスを配送するために必要なネットワーク・コンポーネントを含み、当該ネットワーク・コンポーネントが、作動状態及び構成の少なくとも1つを有し、当該システムが、

サービスをカスタマに配送するために必要な、ネットワーク・コンポーネントの作動状態及び構成の少なくとも1つを学習するための複数のテスト・ツール(318)、

ネットワーク、並びに、カスタマに配送されたサービス、及び、サービスを配送するために必要なネットワーク・コンポーネント、に関連するデータを含むサービス・インベントリ・データ、へのアクセスを有するテスト・マネージャ(300)であって、当該テスト・マネージャは、作動状態をテストするため、及び、指定されたサービスを配送するために必要なネットワーク・コンポーネントの構成を確認するために、特定のサービス配送問題に応じてテスト・ツールを選択的に呼び出すための作業フローを含むものであり、及び、

選択的に呼び出されたテストの結果を表示するためのグラフィカル・ユーザ・インターフェース(GUI)、
を備えるシステム。

【請求項 2】

前記ネットワーク及びサービス・インベントリ・データが、カスタマによって加入されているサービス・プランを含む、請求項1に記載のシステム。

【請求項 3】

前記ネットワーク及びサービス・インベントリ・データが、カスタマの構内において、カスタマの制御下にある、データ記述サービス(data describing service)装置を含む、請求項1に記載のシステム。

【請求項 4】

前記ネットワーク及びサービス・インベントリ・データが、特定のサービスを特定のカスタマに配送するために必要な全てのドメインに対する、必須のネットワーク要素及びコンポーネントの特定を含む、請求項1に記載のシステム。

【請求項 5】

前記テスト・マネージャ(300)が、更に、サービス配送環境内のオペレーション・サポート・システム(304)から情報を引き込む(pull)ようにされたデータベースを含み、当該サービス配送環境が、サービスの配送に関連する全てのネットワーク・ドメインに亘ってサービス配送問題を診断するために必要なテストを実行するための、ネットワーク及びサービス・インベントリ・データを含む、
請求項1に記載のシステム。

【請求項 6】

前記データベースが、フィールド・アクセス・システム(328)からデータを引き込んで(pull)、サービス復旧の最終チェックを実行するようにされ、当該フィールド・アクセス・システム(328)が、カスタマの構内における技術者(technician)の移動端末から前記テスト・マネージャにアクセスする、
請求項5に記載のシステム。

【請求項 7】

前記データベースが、LDAP(軽量(Lightweight)ディレクトリ・アクセス・プロトコル)(330)からデータを引き込んで、ユーザ・アクセスを許可(authorize)するための情報交換を実行するようにされた、請求項5に記載のシステム。

【請求項 8】

前記データベースが、集積オーダーマ・ネジメントシステム(an integrated order management system)(332)からデータを引き込んで、サービス中断に苦情を言っているカスタマに関する作業リクエストの状態についての情報を収集するようにされた、

10

20

30

40

50

請求項 5 に記載のシステム。

【請求項 9】

前記データベースが、ネットワーク・トラブル・マネジメント・システム (334) からデータを引き込んで、ネットワークで配送されたサービスについてのカスタマの苦情を管理し、関連するトラブル・チケットから詳細を獲得するようにされた、請求項 5 に記載のシステム。

【請求項 10】

前記データベースが、故障マネジメント・システム (336) からデータを引き込んで、問題が発見されたときにアラームをオープンし、影響を受けたカスタマについての情報を提供するようにされた、請求項 5 に記載のシステム。

10

【請求項 11】

前記データベースが、サービス配送プラットフォーム (338) からデータを引き込んで、サービス及びユーザ・プロファイル情報を収集するようにされた、請求項 5 に記載のシステム。

【請求項 12】

前記データベースが、パフォーマンス・マネジメント・システム (340) からデータを引き込んで、カスタマへのサービスの配送に関連するネットワーク・コンポーネント内の劣化をチェックするようにされた、請求項 5 に記載のシステム。

【請求項 13】

前記テスト・マネジャが、選択的に呼び出されたテスト・ツールから収集されたデータを、外部オペレーション・サポート・システム (304) に提供して、外部オペレーション・サポート・システムによって管理された特定の工程をサポートするようにされた、請求項 1 に記載のシステム。

20

【請求項 14】

前記複数のテスト・ツールが、特定のネットワーク・ドメイン内のネットワーク要素をテストするようにされたスタンド・アロン・テスト・ツール・パッケージを備える、請求項 1 に記載のシステム。

【請求項 15】

前記複数のテスト・ツールの能力が、特定のネットワーク要素の構成データへのアクセスを有し、特定のネットワーク要素のオペレーション状態をテストする能力を持つネットワーク要素マネジャによって提供される、請求項 1 に記載のシステム。

30

【請求項 16】

前記複数のテスト・ツールの能力が、レイヤ2,3ドメイン・マネジャによって提供される、請求項 1 に記載のシステム。

【請求項 17】

前記複数のテスト・ツールの能力が、テスト及び診断マネジャ内の内部テスト・モジュールとして含まれている、請求項 1 に記載のシステム。

【請求項 18】

前記複数のテスト・ツールが、スタンドアロン・テスト・ツール・パッケージ、ネットワーク要素マネジャ、レイヤ2,3マネジャ、及び、テスト及び診断マネジャ内の内部テスト・モジュール、の組合せを備える、請求項 1 に記載のシステム。

40

【請求項 19】

ユーザ・プロファイル及びアクセス特権 (privileges) を記憶するための、ユーザ・プロファイル・データベース (322) を更に備える、請求項 1 に記載のシステム。

【請求項 20】

前記テスト・ツールを呼び出すための、確立された作業フローを実行するようにされたアプリケーション・サーバ (326) を更に備える、請求項 1 に記載のシステム。

【請求項 21】

GUI ページをユーザにサービスするためのウェブ・サーバを更に備える、請求項 1 に記載のシステム。

50

【請求項 2 2】

前記テスト・マネジャ(300)が、選択的に呼び出されたテスト・ツールからの結果を記憶するための内部データベース(320)を更に含む、請求項1に記載のシステム。

【請求項 2 3】

ネットワーク・コンポーネントをテストし、マルチ・ドメインのネットワークを介して配送されたサービスのためのサービス配送問題を診断するようにされたエンド・ツー・エンドのテスト及び診断マネジャ(300)であって、

ネットワーク、ネットワーク要素、及び、サービス、に関する状態及び診断データを、オペレータに表示し、オペレータからコマンドを受信するためのグラフィカル・ユーザ・インターフェース、及び、

サービス配送問題のレポートを受信すると、アプリケーション・サーバが、カスタマへ配送されたサービス、並びに、サービスをカスタマに配送するために必要なネットワーク及びネットワーク要素を決定し得るように、ネットワーク及びサービス・インベントリ・データへのアクセスを有するアプリケーション・サーバ(326)であって、当該アプリケーション・サーバが、サービス配送問題の原因を決定し、グラフィカル・ユーザ・インターフェースを介して結果を表示するために、作業フローを実行して、1つあるいはそれより多いテスト・ツール(318)を選択的に呼び出し、サービスをカスタマに配送するために必要な、ネットワーク要素のオペレーション状態及び構成データを決定するようにされたものである、

を備える、エンド・ツー・エンドのテスト及び診断マネジャ(300)。

【請求項 2 4】

前記テスト・ツールが、

C P E M S ピング・テスト；シンク・プロファイル；ポート・ベリフィケーション；ポート・ロック/アンロック；ノー・シンク・テスト；ポート・リセット；I P ピング・テスト；テスト・コール；コール・ヒストリ；エンド・ツー・エンド V o N サービス；及び、エンド・ツー・エンド B B サービス；M L T (機械化されたループ・テスト)

を含むリストから採用される複数のツールの何らかの組合せを備える、請求項23に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 2 5】

前記アプリケーション・サーバ(326)が、1つあるいはそれより多いテスト・ツールを直接実行するようにされる、請求項23に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 2 6】

前記アプリケーション・サーバが、ネットワーク・ドメインと関連する外部テスト・ツールを呼び出し、当該外部テスト・ツールが、関連するドメイン内のネットワーク要素をテストするようにされる、請求項23に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 2 7】

前記アプリケーション・サーバが、レイヤ2,3ドメイン・マネジャ(320)を介してテスト・ツールを呼び出す、請求項23に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 2 8】

前記アプリケーション・サーバ(326)が、テストされるべき前記ネットワーク要素に関連する要素マネジャを介してテスト・ツール(318)を呼び出す、請求項23に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 2 9】

ウェブ・サーバ(324)、

オペレータに関連するクライアント端末にサービスするインターフェース・ページを有するウェブ・ベースのグラフィカル・ユーザ・インターフェースを備えるグラフィカル・

10

20

30

40

50

ユーザ・インターフェース、
を更に備える、請求項 2 3 に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 3 0】

エンド・ツー・エンド・テスト及び診断マネジャの使用が許可されたオペレータのアクセス権テスト特権を規定するユーザ・プロファイルを記憶するためのユーザ・プロファイル・データベース (322) を更に備える、請求項 2 9 に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 3 1】

前記データベースが、オペレーショナル・サポート・システム (304) へのアクセスを有することによって、サービスに関連する追加のデータが、受信され得、データベース上に記憶され得、インターフェースを介してオペレータに提示され得る、
請求項 2 3 に記載のエンド・ツー・エンド・テスト及び診断マネジャ。 10

【請求項 3 2】

前記アプリケーション・サーバが、カスタマへのサービスの配送に関連する全てのネットワーク・コンポーネントのオペレーション状態、及び、実際のエンド・ツー・エンドのサービスの配送、をテストするためのテスト・ツールを呼び出すように構成された、請求項 2 3 に記載のエンド・ツー・エンド・テスト及び診断マネジャ。

【請求項 3 3】

レイヤ化された、マルチ・ドメインの、ネットワーク環境を介して配送されたサービスにおけるサービス問題を診断する方法であって、 20

カスタマからサービス問題のレポート (250) を受信し、

サービスをカスタマに配送するために必要な、全てのコンポーネント (ネットワーク要素及びアプリケーション) に関する情報 (252) を収集し、

前記サービス問題の根本原因を特定するために、問題を有することが考えられ得るコンポーネントを遠隔的にテストし (254)、

遠隔的に前記問題を解決し (256)、そして、

サービスが復旧されたことを保証するために、遠隔的なエンド・ツー・エンド・テストを実行する (258)、

ステップを含む方法。

【発明の詳細な説明】 30

【技術分野】

【0001】

本発明は、コンポーネントをテストし、階層化された、マルチ・ドメインのネットワーク環境を介して配送されたサービスのためのサービス問題を診断するための、エンド・ツー・エンドのテスト及び診断マネジャに関連する。

【背景技術】

【0002】

従来、音声通信、データ・サービス、ビデオ・サービス、等のような種々の通信サービスが、スタンドアロンの垂直 (vertical) ネットワークを介して配送 (delivered) されていた。例えば、図 1 は、音声通信サービス及びアプリケーション 10、データ・サービス
及びアプリケーション 12、並びに、ビデオ・サービス及びアプリケーション 14 を配送する
ための、別個の、弁別される (distinct) ネットワークを示す。各別個のネットワークは、
サービス・レイヤ 16、コントロール及びスイッチング・レイヤ 18、トランスポート・ハードウェア・レイヤ 20、及び、物理ネットワーク・レイヤ 22 を含む。それぞれの場合において、サービスは、サービスを分配する (distributing) ために提供される物理ネットワーク及びネットワーク要素に密にカップルされている。例えば、公衆交換電話ネットワーク (PSTN) においては、コントロール及びスイッチング・プロトコル並びに物理的スイッチ自体は、全て、ポイント・ツー・ポイントの音声通信を提供するための、エンド・ツー・エンドの回路 (circuit) を生成することに向けて適合 (geared) される。それら
自身のスイッチング及びコントロール・プロトコル並びに物理的トランスポート・ストラ 50

クチャを有するイーサネット、トークンリング、等のような、類似の専用ネットワークは、データ伝送サービスを提供するために開発された。ブロードキャストか、ブロードバンド・ケーブルを介して配送されるもののいずれかのビデオ・サービスも同様に、それら自身のコントロール及びスイッチング・プロトコルの組、トランスポート・ハードウェア、及びネットワーク、を開発した。それぞれの場合において、種々の統合されたネットワークの全ての面が、ネットワークが配送するように設計された特定のサービスのために特別に構成されていた。

【 0 0 0 3 】

過去の、垂直に (virtically) 分配されたプロプライエタリ・ネットワークにおけるトラブル・シューティング・サービスの問題は、明らかに直載的な提案 (proposition) であ 10
った。全体のネットワークは、一般的に、エンド・ツー・エンドのサービス配送チェーンの詳細な (intimate) 知識を有する一つのエンティティによって所有され制御されていた。このこと、及び、サービスが、サービスを配送するために提供されるネットワーク要素に非常に密にカップルされているという事実が、特定のカスタマへのサービス配送 (delivery) に影響を及ぼし得る、サービス配送チェーンにおけるコンポーネントを特定することを、かなり単純にしている。可能性のある (likely) サービス問題のソースを知ることが、適切なコンポーネントをテストし、問題のソースを隔離することを、かなり単純にする。

【 0 0 0 4 】

現在では、より多くの通信及びブロードキャスト・サービスの配送は、好ましいトラン 20
スポート・レイヤとしての IP に集中している。IP への集中は、サービスを、下にある (underlying) アクセス及びトランスポート・ネットワークから切り離す。その結果は、サービス自身が、実質的に、物理的トランスポート・レイヤから独立するような、マルチ・サービス、マルチ・ドメイン・ネットワークとなる。図 2 は、好ましいトランスポート・レイヤとしての IP への集中を示す。過去の、プロプライエタリの垂直統合ネットワークとは逆に、この新しいサービス・モデルは、広い水平レイヤを規定する。オープン・プロトコル及び APIs が、明確なアクセス、トランスポート、及び、サービスの分離を伴って、レイヤの間の作動 (operational) インターフェースを提供する。従って、サービス・レイヤ 30 は、ネットワークを介してデジタル的に配送され得る、何らかの、そして全 30
てのサービス (音声 24、データ 26、及びビデオ 28 を含むが、これに限定されない) を表す。トランスポート及び分配レイヤ 32 は、IP レイヤ 30 及び物理的分配レイヤ 36 を包含する。オープン・プロトコル及び APIs の使用を通じて、全てのサービスが、IP を介したトランスポートのためにパッケージ化され得る。IP パッケージされたデータは、仮想的に、何らかの、そして全ての物理的なネットワーク技術に運搬され得る。

【 0 0 0 5 】

マルチブルのサービスをカスタマに配送するための、共通トランスポート・レイヤとしての IP への集中は、サービス配送チェーンに対して、複雑さを大きく追加する。今日、バリュー・アデッド・サービス (VAS) は、複雑なネットワーク・アーキテクチャ、及び、作動プラットフォーム (operational platform) に基礎を置く。サービス配送チェーンの部分は、サービス・プロバイダ自身の制御の外側にあり得、そういう可能性が高い。 40
そのような場合には、サービス・プロバイダは、彼らのサービスを送り届けるために、他者によって提供され、維持されるネットワーク及びハードウェアに依存せねばならない。下にある (underlying) アクセスとトランスポート・システムからのサービスの分断は、診断及び訂正サービス問題を、昔のスタンドアロン・サービス配送プラットフォームであった場合に比して、より大きく困難なタスクにする。

【 0 0 0 6 】

今日のサービス配送プラットフォームの複雑さを説明するために、図 3 に示されるベーシックな DSL サービス・アーキテクチャ 40 を考慮して欲しい。左側において、非対称デジタル・サブスクリバ・ライン (ADSL) 52、又は、対称的高速デジタル・サブスクリバ・ライン (SHDSL) 54 が、カスタマの家又仕事場へのデジタル接続を提供する。 50

D S L 接続は、ネットワーク・アプリケーション・サーバ (N A S) 42を介して、よりブロードな I P ネットワーク又はインターネットへのアクセスを提供する。カスタマの D S L ライン (A D S L 又は S H D L) は、第 1 のローカル D S L アクセス・マルチプレキサ (D S L A M) 50に接続する。ローカル D S L A M 50は、小さな地理的領域内の、限定された数のカスタマにサービスする。ローカル D S L A M 50は、複数のローカル D S L A M S をサービスする遠隔の D S L A M 48に接続する。遠隔の D S L A M 48は、第 1 の B P X スイッチ 46を介して A T M ネットワーク 45に接続する。N A S 42は、A T M ネットワーク 45内のどこかよそにある、第 2 の B P X スイッチ 44に接続する。A T M ネットワーク 45内に、追加の B P X スイッチが存在する可能性が高い。しかし、A D S L ライン 52の端部 (end) におけるカスタマに、N A S 42を介してインターネット・アクセスを配送する観点から、A T M ネットワーク 45へのエントリ及び出口ポイントとして働く B P X スイッチ 44 及び 46、並びに、A T M ネットワーク内の他の B P X スイッチは、サービス配送 (delive ry) チェインには関係無い。D S L 技術は、現在進化していて、G B E (ギガバイト・イーサーネット) 又は M A N s (メトロポリタン・エリア・ネットワーク) ヘイサーネット・インターフェースを通じて接続された I P D S L A M を用いて、異なったインフラストラクチャを通じて、現在の及び新しいサービスを配送する可能性を導入している。

10

20

30

40

50

【 0 0 0 7 】

カスタマ・プレミス装置 (Customer Premise Equipment: CPE) が考慮されるときに、サービス配送チェーンは、より複雑になってくる。図 3 に示される D S L サービスは、最小でも、カスタマの構内 (premise) における D S L モデムを要求する。ローカル・エリア・ネットワーク、W 1 - F 1 ルータ、及び他の C P E は更に、サービス配送の状況を複雑化させる。図 4 は、非定型ではない (not atypical) カスタマ構内アレンジメント 60を示す。A D S L ライン 62は、ネットワーク・インターフェース装置 64を介して、カスタマの構内に入る。スプリッタ 66は音声及び映像を分離し、第 1 のウォール・ジャック 68を介して音声信号を標準電話セット 72に接続し、第 2 のウォール・ジャック 70を介して、データ信号を D S L モデム 74に接続する。ローカル・エリア・ネットワーク・ハブ 76は、複数のコンピュータ 78、80、82を、D S L モデム 74に接続する。従って、各コンピュータは、L A N を介した D S L ラインへのアクセスを持つ。コンピュータ 78、80、82におけるユーザが、D S L ライン 62を介してサービスを受信するために、図 3 を参照して説明されたネットワーク要素に加えて、D S L モデム 74及び L A N H U B 76もまた、適切に作動し、構成されねばならない。従って、もし、これらの要素 (components) が、適切に作動していないならば、或いは、適切に構成されていないならば、C P E ドメインは、他のサービス問題の源を提供することになる。

【 0 0 0 8 】

増大する、配送されたサービスの複雑さに伴って、サービス配送チェーンは更により複雑になる。例えば、図 5 は、ネットワークを介した音声 (V o N) サービスのための一般的なアーキテクチャを示す。この環境における個々のカスタマに対するサービス問題を探し出すことは、非常に複雑なタスクであり得る。これからわかるように、V o N サービスは、マルチプルのネットワーク要素 (elements) 及びサービス・コンポーネントを含むマルチプルのネットワーク・ドメインの相互作用を要求する。更に、異なった位置において、マルチプルのカスタマに提供されたサービスは、異なった接続を持ち、異なった C P E を持つ。

【 0 0 0 9 】

V o N アーキテクチャ 100 は、V o N 又はサービス・レイヤ 102、トランスポート・レイヤ 104、そして、C P E レイヤ 106の間で分割される。C P E レイヤ 106から始まって、いくつかの異なったクライアント構成が示される。異なったクライアント構成は、主に、トランスポート・レイヤへのアクセスのタイプ、利用可能な帯域幅、及び他の特徴に依存する。

【 0 0 1 0 】

クライアント 108は、ローカル・エリア・ネットワーク 114、1つあるいはそれより多い

V o N 電話装置116、及び複数のユーザ・コンピュータ118を含む。カスタマ・エッジ120は、仮想プライベート・ネットワーク (V P N) 140へのアクセスを提供する、トランスポート・レイヤ104内のプロバイダ・エッジとインターフェースをとる。V P N 140は、マルチ・プロトコルのラベル (label) ・スイッチング (M P L S) に基礎を置く。V P N 140は、N A S 154を介して、よりブロード (broader) の I P ネットワークにアクセスする。

【 0 0 1 1 】

クライアント・アレンジメント110は、ローカル・エリア・ネットワーク126、及び、複数の V o N 電話装置122を含む。カスタマ・エッジ124は、I P エッジ・ネットワーク142へのインターフェースを提供する。I P エッジ・ネットワーク142は、より広いネットワーク148へのアクセスを提供する。

10

【 0 0 1 2 】

クライアント112は、複数の伝統的電話装置128、アクセス・ゲートウェイ130、及び、カスタマ・エッジ132を含む。アクセス・ゲートウェイ130とカスタマ・エッジ132は、デジタル・サブスクリバ・ラインを介して D S L A M 158とインターフェースをとる。

【 0 0 1 3 】

ここに示されるように、カスタマ・レイヤ106は、伝統的な P B X 134及び伝統的な電話装置136である。ここに示されるシステムにおいて、P B X 134及び伝統的な電話装置136は、V o N サービスを採用しているカスタマとの電話コールに参加し得る。しかし、P B X 134及び電話装置1365は、伝統的な公衆交換電話ネットワーク146の上で作動し、それら自身は、V o N サービスに修正可能ではない。

20

【 0 0 1 4 】

トランスポート・レイヤ104は、V P N 140、I P エッジ・ネットワーク142、A D S L ネットワーク144、P S T N 146、I P ネットワーク148、及び、伝統的な音声サービスのためのバックボーン・ネットワーク・トランジット・レベル150を含み、それらの間のインターフェース・コンポーネントも含む。例えば、V P N 140は、N A S 154を介して、I P ネットワーク148とインターフェースをとる。A D S L ネットワークは、N A S 156を介してI P ネットワーク148とインターフェースをとる。P S T N は、バックボーン・トランジット・レベル (B B - T L) 150のバックボーン・ネットワークとインターフェースをとる。I P ネットワークは、メディア・ゲートウェイ (M G) 162を介して B B - T L ネットワークとインターフェースをとる。

30

【 0 0 1 5 】

V o N サービス・レイヤ102は、ユーザ・プロファイル・データベース172、サービス・ロジック・アンド・ユーザ・プロファイル・データを含むパケット I N アプリケーション・サーバ174、B B - T L 150を介して P S T N 146とインターフェーシングするための、1つあるいはそれより多い S I P サーバ・アンド・ソフトスイッチ166を含む。

【 0 0 1 6 】

この例では、サービス配送チェーンは、V o N サービスの、エンド・カスタマへの配送に関係するネットワーク要素の全てを含む。例えば、V o N サービスをカスタマ112に配送するために、サービス配送チェーンは、スリップ (slip) ・サーバ・アンド・ソフトスイッチ170、スイッチ166、メディア・ゲートウェイ162、N A S 156、D S L A M 158、及び、アクセス・ゲートウェイ130を含む。A T M スイッチ、I P ルータ等、のような、種々のネットワーク・ドメイン内の追加のコンポーネントもまた、サービス配送チェーンの一部を含み得る。カスタマ112に V o N サービスを提供するために、これらの要素の全ては、適切に作動し、構成されねばならない。勿論、異なったネットワーク及び異なったネットワーク要素は、V o N サービスを他のカスタマに配送しているサービス配送チェーンの一部になる。サービスを特定のカスタマに配送することに関連するネットワーク要素の全てを特定 (identifying) することは、トラブルシューティング・サービス配送問題において重要なタスクである。サービス配送チェーンを含む全ての種々の装置についてテストを実行すること、及び、サービス配送ドメインの全てに亘った構成データをチェックす

40

50

ることは、殆ど不可能であった。

【0017】

今日までに、構造化され、エンド・ツー・エンドのアプローチによる、総合的な、エンド・ツー・エンドの、IPトランスポート・レイヤを介して配送されたサービスのテスト及び診断を提供するためのシステム又は方法は存在しなかった。そのようなシステム及び方法の不存在は、トラブルシューティングサービス配送問題の時間、労力、費用を大きく増大させる。

【発明の開示】

【課題を解決するための手段】

【0018】

本発明は、広範囲の技術プラットフォームに亘る、レイヤ化されたマルチ・ドメイン・サービスの配送ネットワークを介して配送されたサービスのためのサービス問題のトラブルシューティングのための、エンド・ツー・エンドのテスト及び診断マネージャに関連する。特に、本発明の実施例は、共通トランスポート・レイヤとしてインターネット・プロトコル(IP)を用いて配送されたサービスのための、エンド・ツー・エンドのテスト及び診断マネージャを提供する。エンド・ツー・エンドのテスト及び診断マネージャは、IPトランスポート・レイヤを介して配送される(delivered)、VoN、IP-TV、ビデオ・オン・デマンド、統一メッセージング(unified messaging)、等のようなサービスのトラブルシューティングのための総合的なソリューションを提供する。

10

【0019】

実施例によれば、エンド・ツー・エンドのテスト及び診断マネージャは、フロント・エンド・オペレータ(例えば、コール・センタ・カスタマ・サービスの代表)及びバックエンド・オペレータ(例えば、フロントエンド・オペレータによって解決され得ない、より複雑なサービス問題をトラブルシューティングするために利用可能な、より熟練したオペレータ)が、サービス・プロバイダから、マルチプルのネットワーク・ドメインを経由してエンド・カスタマまで広がる全サービス・チェーンをトラブルシュートすることを可能とするソフトウェア・アプリケーションを備える。下にあるトランスポート・メカニズム又はネットワークの管理とは逆に、エンド・ツー・エンドのテスト及び診断マネージャは、カスタマ中心のエンド・ツー・エンドのオペレーショナルなサービスの視点を提供し、サービスの管理に、より焦点を当てる。

20

30

【0020】

本発明の実施例は、マルチ・ドメインのサービス配送ネットワークに亘って配送されたサービスのために、サービス問題をトラブルシューティングするためのシステムを提供する。問題となっている種々のドメインにおける、オペレーションの状態、及び、ネットワーク要素の構成をテストするための複数のテストツールが、提供される。テスト及び診断マネージャは、ネットワーク及びサービス・インベントリ・データへのアクセスを持つ。サービス中断又は他のカスタマの苦情に応じて、どのサービスが、カスタマに配送されたかを知り、サービスをカスタマに配送するために必要なネットワーク要素を特定するために、テスト及び診断マネージャは、ネットワーク及びサービス・インベントリ・データにアクセスする。テスト及び診断マネージャは、選択されたネットワーク要素の作動状態及びの構成を判断するために、次に、選択的に、種々のテスト・ツールを呼び出す。オペレーターが、サービス問題の源を判断し、それを解決するための手を打ち得るように、グラフィカル・ユーザ・インターフェースが、選択的に呼び出されたテストの結果を表示する。

40

【0021】

他の実施例において、エンド・ツー・エンドのテスト及び診断マネージャは、ネットワーク、コンポーネントに関するデータの状態及び構成を表示し、オペレータにサービスし、そこからコマンドを受信するための、グラフィカル・ユーザ・インターフェースを含む。アプリケーション・サーバは、ネットワーク及びサービス・インベントリ・データへのアクセスを持つ。サービス問題のレポートを受信すると、アプリケーション・サーバは、サービスをカスタマに配送するために必要なネットワーク及びネットワーク・コンポーネン

50

トを決定する。アプリケーション・サーバは、サービスの配送において呼び出されたネットワーク要素の作動状態又は構成を決定するために、1つあるいはそれより多いテスト・ツールを選択的に呼び出すために、作業フローを実行するようにされる。オペレータが、問題の源を判断し、それを解決するために手を打ち得るように、結果は、グラフィカル・ユーザ・インターフェースによって表示され得る。

【0022】

最後に、マルチ・ドメインのサービス配送ネットワークを介して配送されたサービスにおけるサービス配送問題を診断する方法が提供される。本方法は、カスタマにインタビューすることによるサービス問題の情報の組を収集することを提供する。カスタマ請求番号 (billing number) を用いて問題のレポートを受信すると、サービスをカスタマに配送するために必要な、全てのネットワーク要素に関する情報を収集することが可能である。一旦、サービス配送チェーン内の全てのネットワーク要素が知られると、問題の原因を特定するために、それらが適切に作動しており、正しく構成されているか否かを決定するためにネットワーク要素を遠隔的にテストする。一旦、問題の源が決定されると、それを解決するために手が打たれる。最後に、問題が解決されたときに、サービスが保持されたことを保証するために、遠隔的な、エンド・ツー・エンドのテストを実行する。

10

【0023】

或いは、診断的な工程は、ネットワーク装置問題のレポートによって駆動され得る。ネットワーク問題のレポートを受信すると、特定のネットワーク・リソース (ネットワーク要素又はアプリケーション・コンポーネント) を選択し、それが適切に作動し、正しく構成されているか否かを理解するために、特定のネットワーク・リソースの状態についての情報を集めることが可能となり得る。

20

【0024】

以下の図面及び詳細な説明を検討することによって、本発明の他のシステム、方法、特徴、及び利点が、当業者にとって、明白となるであろうし、或いは、明白であろう。そのような追加のシステム、方法、特徴、及び利点が、本説明の中に、本発明の範囲内に、含まれ、添付の請求項によって保護されることが意図される。

【発明を実施するための最良の形態】

【0025】

マルチ・ドメインのサービス配送環境におけるサービス配送問題を診断することは、広範囲の源からの情報にアクセスし、関連付けし (relating)、サービス配送問題の状態 (nature) 及び原因を迅速に特定し、問題を解決するために、それらに対して、即座の是正アクションがとられることを可能とするために、オペレータがデータをビュー (viewing) することを可能とするように、結果のデータを、構造化され、整理されたやり方で提示することを要求する。

30

【0026】

図6は、サービス配送問題を特定し、解決するために必要なステップの概要を示す。第1に、250において問題がレポートされる。問題についての情報が、252で収集される。収集された情報は、カスタマが加入しているサービス、及び、問題によって影響を受けている1つあるいはそれより多いサービス、カスタマの構内のサービス配送装置、及び、サービスをカスタマに提供するためのサービス配送チェーンを備えるネットワーク及びネットワーク要素のような、問題を被っているカスタマについての情報を含み得る。収集された情報は、問題を被っているサービスについての情報をも含み得る。追加の収集されたデータは、アラーム・レポジトリ、存在する関連トラブル・チケット、計画されたエンジニアリング/メンテナンス・アクティビティ、パフォーマンス・マネジメント・レポート、予測システム・レポート、等を含み得る。

40

【0027】

サービス配送問題の核心の原因が、254で特定される。これは、ネットワーク及びサービス・インベントリを分析し、ネットワーク要素に対して進入性の (intrusive) / 非進入性のテストを実行し、ヒストリカルなテスト結果を分析する、こと等を含み得る。一旦、

50

問題の核心の原因が特定されると、256において、問題を解決するためのステップがとられ得る。これは、カスタマ構内装置、又は、他のハードウェア復旧させるために、サポート人員を急派する(dispatch)こと、ネットワーク要素マネジャ及びテスト・システムにアクセスすること、構成データを修正すること、等を含み得る。最後に、一旦、問題が解決されると、258において、問題はクローズされ得る。問題をクローズすることは、最終のエンド・ツー・エンド確認テストを実行すること、テスト結果を保存(archiving)すること、等を含み得る。

【0028】

エンド・ツー・エンド・テスト及び診断的マネジャ300、及び、当該エンド・ツー・エンド・テスト及び診断的マネジャ300が作動する環境、の単純化された概要(view)が、図7に示される。エンド・ツー・エンド・テスト及び診断マネジャ300は、ネットワーク及びサービス・インベントリ・データ302、及び、他の作動サポート・システム(OSS)304へのアクセスを持つ。エンド・ツー・エンド・テスト及び診断マネジャ300は、特定のサービスを、特定のカスタマに配送するために必要な、ネットワーク・プラットフォーム、システム及びコンポーネントを含む、サービス配送チェーンの理解可能な描写を展開するために、必要に応じて、ネットワーク及びサービス・インベントリ302及びOSS304からデータを引き込み(pull)得る。

10

【0029】

実施例によれば、ネットワーク及びサービス・インベントリ・データは、Oracleのデータベース又は他の商業的に入手可能なデータベース内に格納され、SQLクエリ(queries)を介してアクセスされ得る。情報は、ネットワークとサービス・インベントリの間で交換され、エンド・ツー・エンド・テスト及び診断マネジャは、「商業的情報」及び「技術的情報」を含む。商業的情報は、カスタマ、彼らのサービス・プロバイダ、彼らのサービス・プラン、サービスID、サービス日、等に関連する。ネットワーク及びサービス・インベントリから集められた技術的情報は、回路の正確な表現(representation)を準備し、エンド・ツー・エンド・テスト及び診断マネジャが、関連する(involved)全ての主要装置に問合せする(query)ことを可能とするために、サービスをカスタマに配送するための回路(circuit)を再構築するために必要な情報の全てを含む。技術的情報は、カスタマが加入する全てのサービス、及び、それらのサービスを配送するために必要なコンポーネントの全てについての情報を含まねばならない。

20

30

【0030】

実施例によれば、技術的に関連するデータの全てを得るために、3つの別個のデータベース・テーブルがアクセスされる。主要な入力パラメータは、カスタマID(課金番号: Billing Number)、又は、いくつかの他の信頼できる識別子(identifier)である。アクセスされる第1のテーブルは、特定のサービスを特定のカスタマに配送するための、サービス・プロバイダからカスタマへの回路を構築するために要求される主要コンポーネントの全てを特定するA-Z回路テーブルである。このテーブルにおいて、ポイント「A」は、DSLAMによって表され、ポイント「Z」は、NASによって表される。必要なコンポーネントは、他のもの以外に、ATMドメイン(サービス・プロバイダに直面(facing)しているATMアクセス装置)のポイント「A」、及び、ATMドメイン(カスタマに直面しているATMアクセス装置)のポイント「Z」を含む。サンプルのA-Z回路テーブルが、テーブル1に示される。A-Z回路テーブルは、サービスをカスタマに配送するための回路を構築するために必要なコンポーネントのタイプを定義する複数の属性を含む。対応する値が、それらの役割を充足する(fill)実世界のコンポーネントを特定する。カスタマID値(課金番号)は、カスタマ(そこからサービス配送チェーンが構築される)を特定する。DSLAM名は、特定されたカスタマにサービスするDSLAMを特定する。次のいくつかの属性は、サービスを特定されたカスタマに配送するための、特定されたDSLAM、特定ポート(identifying ports)、加入者ライン(subscriber lines)、等のための接続及び構成データに関連する。NAS名は、サービスを、カスタマにサービスしているATMネットワークを介して、カスタマに提供するネットワーク・アプリケーションズ・サーバ

40

50

を特定する。特定された N A S は、 I P ドメインへのアクセスを提供し、 I P ドメインを介してサービスが配送されることを可能とする。残りの属性は、 N A S に対する接続及び構成データに関連する。

【 0 0 3 1 】

【表 1】

テーブル 1 : (A & Z 回路)

属性名	値
カスタマ I D	0065940342
S L A M 名	MILANUSER/DSL/005
ポート・カスタマ・サイド(A T U - C)	ADSL 2-2-12-19
D S L ライン	2:2:12
ポート・カスタマ・サイド(A T U - C)	ADSL 2-2-12-19
V C I	2-2-12-19:8.35
クロス・コネクション	LT=8.35/NT=34.65
ポート A T M サイド	MRL08C
V C I	34.65
N A S 名	AT-B0256
ポート A T M サイド	ATM4:3:7
V C I	23.65

10

20

【 0 0 3 2 】

テーブル 1 の D S L A M 部分からの「ポート A T M サイド」値は、 A T M ドメイン・ネットワークのポイント「 A 」を決定するために、第 2 のデータベース・テーブル(M U X と A T M ドメインの間の論理的リンクを表す)に問合せする(query)ために使用される。この問合せは、適切な A T M 装置、 A T M 上の適切なポート、等を特定する。これらのデータは、 I P テーブル内で、対応する I P アドレスを特定し、次に、 A T M 装置及び指定されたポートの作動(operational)状態及び構成をチェックするために用いられる。第 2 のデータベース・テーブル(M U X 論理リンク)の例が、テーブル 2 に示される。

【 0 0 3 3 】

【表 2】

テーブル 2 : (M U X 論理リンク)

属性名	値
A T M 装置名	MGX9063
ポート	MGX9063:3:5
V P I	MGX9063:3:5:34

30

40

【 0 0 3 4 】

テーブル 1 の N A S 部分の「ポート A T M サイド」値が、次に用いられて、(サービス配送の検知から) A T M ドメインの反対の端部(opposite end)において、どの装置が、ポイント「 Z 」を表すかを学ぶ(learn)ために、類似の、第 3 のデータベース・テーブルの問合せを実行する。 A T M 装置の作動状態及び構成、並びに、指定されたポートが、確認される(verified)ように、再度、この問合せは、適切な A T M 装置、適切なポート、等を特定する。第 3 のテーブル(N A S 論理リンク)の例が、テーブル 3 に示される。

【 0 0 3 5 】

【表 3】

テーブル 3 : (NAS 論理リンク)

属性名	値
ATM装置名	MGX9064
ポートATMサイド	MGX9064:5:5
VPI	MGX9064:5:5:27

【0036】

最後のステップは、上で特定された装置、即ち、DSLAM、「A」、及び、「Z」の ATM装置、NAS、及び、特定のサービスを特定されたカスタマに配送するために必要であり得る何らかの他の関連する装置、のIPアドレスを決定することである。これは、第4のデータベース・テーブル(IPアドレス装置)の別個の問合せを通じて実現される。IPアドレス装置テーブルの例が、テーブル4に示される。

【0037】

【表 4】

テーブル 4 : IPアドレス・デバイス・テーブル

属性名	値	IPアドレス
DSLAM名	MILANUSER/DSL/005	10.11.134.178
ATM装置名	MGX9063	10.11.156.170
NAS名	AT-B0256	10.11.124.138

【0038】

商業的情報は、更に他のテーブルに問合せすることによって得られる。再度、カスタマID(請求番号: billing number)が、主要キーである。サンプルの商業的情報の計算(tale)が、テーブル5に示される。

【0039】

【表 5】

テーブル 5 : (商業的情報)

属性名	値
カスタマID	0065940342
カスタマ名	Kate Moss
ISP	AOL
PLAN	VoN Fast Access
サービスID	986241585
プラン開始日	07/13/1977

【0040】

技術的情報及び商業的情報は、他の作動サポート・システム304からも引出され得る。例えば、カスタマの構内における装置のIPアドレスは、サービス配送プラットフォーム(SDP)338から得られ得る。例えば、カスタマ構内装置が、単純な「Ping IP」テストを

用いて作動中 (up and running) であるか否かを決定するために、IP アドレスが使用される。他の情報は、SDP 338 から引き出され得る。SDP とエンド・ツー・エンド・テスト及び診断マネージャの間の情報交換は、ウェブ・サービスによって実現され得る。SDP からのパラメータには、

【0041】

- 回路の实在識別子であるテクニカル・キー (TK)。これは、(Name NAS, カード、ポート、VPI、VCI) = (AT-B0256, 3, 7, 23, 65) から構成される。
- マネジメント・セッション :
最初の接続の日、最後の接続の日 = (11/07/2005 22:34; 11/07/2005 23:18)
- データ・セッション :
最初の接続の日、最後の接続の日 = (11/07/2005 22:35; 11/07/2005 23:17)
- マスタ・アカウント :
ユーザ名及び生成日 = (sirio.baldini@aol.us, 08/15/2005)
- データ・サービス :
プラン、商業的提供 = (VoN Fast Access, VoN-3numbers)
- 追加されたサービス :
親制御の状態、キャプティブ・ポータル (Captive Portal) の状態 = (off, off)
- IP アドレス :
マネジメント・セッションの IP アドレス (10.10.148.170)、

が含まれ得る。

【0042】

一旦、サービス配送チェーンのコンポーネント・リンクの全てが特定されると、エンド・ツー・エンド・テスト及び診断マネージャ 300 を採用しているオペレータ 306 は、サービス配送工程 (process) の種々の側面 (aspects) をテストするためのテスト手順 (procedure) を呼び出し得る。例えば、オペレータは、サービス配送問題の根本の原因を特定するために、サービス配送チェーンを作っている (make up) ハードウェア・コンポーネント及びネットワーク要素の状態を分析するテストを開始し得る。

【0043】

実施例によれば、エンド・ツー・エンド・テスト及び診断マネージャ 300 は、カスタマへのサービスの配送に関連している、機能しているドメインの全てをテストするためのテスト・ツールの完全な一式 (full compliment) へのアクセスを持つ。種々の機能している (functional) ドメインには、CPE ドメイン 308、DSL / ATM ドメイン 310、IP ネットワーク・ドメイン 312、及び、VoN (又はサービス) ドメイン 314 が含まれ得る。

【0044】

利用可能であり得る診断ツールの例には、

- CPE MS Ping テスト : これは、全てのカスタマ構内装置 (カスタマの構内における全ての装置) が、エンド・ツー・エンド・テスト及び診断マネージャによって到達され (reached) 得ることを確認するための、単純なテストである。
- シンク・プロファイル : これは、DSLAM 上のカスタマの構成パラメータ (減衰、ノイズマージン、等) を集めるツールである。
- ポート確認 (verification) : このツールは、DSLAM ポート (これに対してカスタマ装置が接続される) の作動状態をチェックする。
- ポート・ロック / アンロック : これは、目標装置 (DSLAM、ATM、IP ルータ) 上のポートをシャット・ダウンさせ、それを再スタートさせる、システム全体の管理コマンドである。
- ノー・シンク・テスト : このテストは、モデム及び DSLAM (シーメンス、アルカテル、等) と、カスタマ装置 (モデム又は CPE) の間の同期についてのブーリアンの結果 (Boolean result) を戻す。
- ポート・リセット : このテストは、DSLAM 上の構成 (クライアント側のポート) をリセットするために用いられる。

10

20

30

40

50

- IP ピング・テスト：このテストは、IP 装置 (N A S、Cisco 10k、Cisco 6004、Juniper ERX、等) の到達可能性を確認するために用いられる。
- テスト・コール：このテストは、スイッチのエレメント・マネージャを介した、カスタマ電話への IP コールをシミュレートするが、カスタマ電話を鳴らせない。
- コール・ヒストリ：これは、カスタマによって為された IP コールについての情報 (最初の、及び、最後のコールの日付、期間、時刻) を提供するツールである。
- エンド・ツー・エンドの VoN サービス：これは、IP コールについての情報 (帯域、通信の品質、インバウンド (inbound) / アウトバウンド (outbound)、等) をチェックし、レポートするツールである。
- エンド・ツー・エンドの BB サービス：これは、特定の N E s に対しての、送られた、失われた、そして、受信されたパケットについての情報を収集するツールである。
- M L T (機械化されたループ・テスト: Mechanized Loop Testing)：これらは、カスタマの P S T N ラインの状態を決定するために用いられるツールの組である；
 - ・ ラインが O K であるというテスト、
 - ・ 欠陥のある電話又は受信器のオフ・フックのような、カスタマの装置に伴う潜在的問題、
 - ・ スピーチ・オン・ザ・ライン (speech on the line)

が含まれる。

【 0 0 4 5 】

エンド・ツー・エンド・テスト及び診断マネージャ 300 は、いくつかの異なったやり方で、種々のテストをアクセスし、呼び出すように構成され得る。例えば、エンド・ツー・エンド・テスト及び診断マネージャは、異なったドメインにおける種々のコンポーネントの作動状態及び構成をテストするために採られるべきステップを規定する作業フローを含むテスト・リポジトリ 316 を含み得る。テスト・リポジトリで規定された作業フローは、ハードウェア装置及びネットワーク要素に直接応答指令信号を送り (interrogate)、テストするためのステップを含み得る。或いは、作業フローは、種々のドメイン内の特定のコンポーネントをテストするために開発された外部テスト・ツール及びコマースナル・パッケージ 318 を呼び出し得る。更に他の代替例では、エンド・ツー・エンド・テスト及び診断マネージャ 300 は、レイヤ 2、3 ドメイン・マネージャ 320 を呼び出して、1 つあるいはそれより多いドメインの機能 (functionality) をテストし得る。最後に、エンド・ツー・エンド・テスト及び診断マネージャ 300 は、種々のドメイン内の種々のコンポーネントをテストするために構成されたエレメント・マネージャ (E M) 322 を呼び出し得る。テスト・リポジトリ 316 内の作業フローは、かなり複雑であり得る。内部 / 外部テスト・ツールが利用可能か否か、レイヤ 2、3 ドメイン・マネージャが存在するか否か、或いは、いずれかのエレメント・マネージャが利用可能か否か、に依存して、エンド・ツー・エンド・テスト及び診断マネージャは、異なった複数のやり方の組合せで、テスト及びインテロゲート (interrogate) ・コンポーネントを呼び出し得る。例えば、エンド・ツー・エンド・テスト及び診断マネージャは、いくつかのコンポーネントを、エンド・ツー・エンド・テスト及び診断マネージャ内の A P I サーバ上で実行される A P I s を介して、直接テストし得る。外部テスト・ツールを通じて、他のテストが呼び出され得る。また、他のテストが、レイヤ 2、3 ドメイン・マネージャ 320 を通じて呼び出され得る。更に他のテストが、別個のエレメント・マネージャ 322 を通じて呼び出され得る。

【 0 0 4 6 】

エンド・ツー・エンド・テスト及び診断マネージャ 300 は、フロント・エンド及びバック・エンド・オペレータ 306 にグラフィカル・ユーザ・インターフェース (G U I) を提示 (present) する。フロント・エンド・オペレータは、配送問題が、標準的な、容易に実行される手順によって迅速に解決され得るか否かを決定するために、又は、問題を解決するために、より洗練された分析が必要か否かを決定するために、エンド・ツー・エンド・テスト及び診断マネージャを使用して、サービス苦情 (complaints) を評価 (assess) し、単純な初期診断テストを走らせ得る。もし、もし後者ならば、バックエンド・オペレータは、システ

ムを使用して、より洗練されたテストを実行し、より深刻なサービス問題について、より深く探求し得る。フロント・エンド及びバック・エンド・オペレータに利用可能な種々のツールは、ユーザ・プロファイル・データベースにおいて規定され得る。バックエンド・オペレータには、彼らのフロント・エンド・オペレータに比して、より洗練されたテスト及び診断ツールへのアクセスが与えられ得る。例えば、バックエンド・オペレータが、困難なサービス配送問題の原因を決定することを支援するために、インターフェースは、更に、バック・エンド・オペレータに、ヒストリック・テスト結果、アラーム及び故障ログ、メンテナンス及びサービス・スケジュール、パフォーマンス・マネジメント・システム、予測システム、等へのアクセスを提供し得る。エンド・ツー・エンド・テスト及び診断マネージャ・インターフェースは、更に、バックエンド・オペレータに、フロントエンド・オペレータには利用不可能なサービス問題を解決するためのステップ、(例えば適切なサポート・チームの急送(dispatching)、エレメント・マネージャ及び構成マネジメント・システムへのアクセス、等)を採るための手段を提供し得る。一旦問題が解決されると、バックエンド・オペレータは、サービス・テストの確認(verification)を実行でき、種々のテスト結果、及び、問題を解決するために採用されたアクションを保存できる。

10

【0047】

図8は、エンド・ツー・エンド・テスト及び診断マネージャ300、並びに、周辺のマルチ・ドメイン・サービス配送環境の、より詳細な概要を示す。図7に説明されるコンポーネントの多くは、図8に重複されており、類似の記号が与えられている。図示されるように、エンド・ツー・エンド・テスト及び診断マネージャ300は、ネットワーク及びサービス・インベントリ302、及び、他のオペレーションズ・サポート・システム(OSS)304とインターフェースをとる。OSS304は、フィールド・アクセス・システム328、LDAP330、集積オーダーマネジメントシステム(an integrated order management system)332、ネットワーク・トラブルマネジメントシステム334、故障マネジメントシステム336、サービス配送プラットフォーム338、及び、パフォーマンスマネジメントシステム340、を含み得る。

20

【0048】

エンド・ツー・エンド・テスト及び診断マネージャ300は、3つの、あり得る、他のOSSシステム304及びネットワーク・リソースとの相互作用のタイプを持つ。

【0049】

1) エンド・ツー・エンド・テスト及び診断マネージャは、以下から情報を引き出せる：

- 以下に関連するデータを提供するネットワーク及びサービス・インベントリ302；
 - ・ サービス・プロバイダによって提供されるサービス、
 - ・ サービス・プロバイダのカスタマ、
 - ・ 特定のカスタマに提供されるサービス、
 - ・ 特定のサービスの特定のカスタマへの配送において関連するネットワーク・コンポーネント、
- サービス配送プラットフォーム328(サービス及びユーザ・プロファイル情報)
- 特定のツール318、ドメイン・マネージャ320、EM322、及びネットワーク要素
- カスタマに提供されるサービスに関連する装置における劣化についてチェックするための、パフォーマンス・マネジメント340、
- 苦情を言っているカスタマに関する作業リクエストの状態についての情報を収集するための、集積されたオーダー・マネジメント322、

30

40

【0050】

2) エンド・ツー・エンド・テスト及び診断マネージャは、以下に情報を提供する：

- ネットワーク上のサービス問題に関連するカスタマのトラブルを管理し、関連するトラブル・チケット(ticket)を豊富化するためのネットワーク・トラブル・マネジメント334
- 問題が発見されたときにアラームをオープンし、影響を受けたカスタマについての情報を提供するための故障(fault)マネジメント336

50

- カスタマ宅における技術者の移動端末からテスト・マネジャにアクセスしているサービス復旧の最終チェックを実行するためのフィールド・アクセス・システム328

【0051】

3) ユーザ・アクセスを許可するために、エンド・ツー・エンド・テスト及び診断は、LDAP (軽量ディレクトリ・アクセス・プロトコル (Lightweight Directory Access Protocol)) サーバとの情報交換をも実行できる

【0052】

CPEテスト・ツール342、ATMテスト・ツール、DSLテスト・ツール346、IPテスト・ツール348、及び、VoNテスト・ツール350を含む、複数の外部テスト・ツール318が、図8に示される。同様に、複数のエレメント・マネジャ322もまた示される。エレメント・マネジャ322は、CPEエレメント・マネジャ354、ATMエレメント・マネジャ356、IPEエレメント・マネジャ358、及び、VoNエレメント・マネジャ360を含む。各ドメインに対してマルチプルのエレメント・マネジャが示される。なぜなら、各ドメインは、マルチプルのネットワーク・エレメント・タイプを含み得るからである。レイヤ2、3ドメイン・マネジャ320もまた、図8に示される。種々のエンド・ツー・エンド・テスト診断マネジャの実装において、テスト・ツール、エレメント・マネジャ又はレイヤ2、3ドメイン・マネジャの全てが、必ずしも存在する必要は無いことに留意されるべきである。殆どの場合において、テスト・ツール、エレメント・マネジャ、及び、レイヤ2、3ドメイン・マネジャの種々の組合せが、エンド・ツー・エンド・テスト及び診断マネジャ300内の追加の直接アクセス・テスト・プロトコルと一緒に組み合わされる。好ましくは、特定の 20 実施例中に存在する、エンド・ツー・エンド・テスト及び診断マネジャ300、テスト・ツール318、レイヤ2、3ドメイン・マネジャ及びネットワーク・エレメント・マネジャ322が組み合わされて、サービス・プロバイダによって提供される全てのサービスのためのサービス・チェーンの総合的な分析を実行するための診断テストの完全な一式 (full compliance) を提供する。

【0053】

エンド・ツー・エンド・テスト及び診断マネジャ300自身は、内部データベース320、ユーザ・プロファイル・データベース322、ウェブ・サーバ324、及び、アプリケーション・サーバ326を含む。ユーザ・プロファイル・データベース322は、サービス問題のトラブル・シューティングのための、フロントエンド及びバックエンド・オペレータ、並びに、 30 エンド・ツー・エンド・テスト及び診断マネジャ300へのアクセスを有する他の管理要員のユーザ・プロファイルを記憶する。ユーザ・プロファイルは、アクセス権、及び、異なったタイプのユーザに利用可能なテスト及び診断ツール並びに構成データを規定する種々のユーザの特権を含む。

【0054】

内部データベース320は、カスタマ、及び、彼らに配送されたサービスに関連するデータを記憶する。実施例によれば、内部データベース320は、全てのカスタマ、サービス、及び、サービス配送コンポーネントの総合的なデータの組を記憶しない。むしろ、内部データベース320は、特定のサービス配送問題を解決するための必要に応じて、ネットワーク及びサービス・インベントリ302及び他のOSS304から必要なデータを引き込む。データは、次に、内部データベース320内に記憶される。内部データベース320においては、データは、ウェブ・サーバ324によってアクセスされて、種々のデータ・フィールド及びGUIの表示を配置する。或いは、内部データベース320においては、データは、アプリケーション・サーバ326によってアクセスされて、苦情を申し立てた特定のカスタマに配送されたサービスのエンド・ツー・エンド・テストを実行するために必要な種々の作業フローを実行する。 40

【0055】

図9は、エンド・ツー・エンド・テスト及び診断マネジャのグラフィカル・ユーザ・インターフェース (GUI) ページ400の例を示す。GUIページ400は、異なったタイプの情報が表示され、インターフェースと相互作用を行うオペレータによって異なったアクシ 50

ョンが開始され得る、いくつかの明瞭な領域を含む。これらは、カスタマ表示エリア402、診断タイプ領域404、ツール領域406、プロビジョニング (provisioning) 及び構成情報領域408、ネットワーク表示領域410、及び、カスタマ・テスト・ヒストリ領域412を含む。

【 0 0 5 6 】

実施例によれば、カスタマ請求番号 (billing number) は、カスタマIDとしての役割を果たし、エンド・ツー・エンド・テスト及び診断マネージャを動かす。したがって、カスタマが、サービス割込み (interruption) 又は何らかの他のサービス配送問題をレポートするためにコールするとき、オペレータは、カスタマの請求番号を、カスタマ表示領域402内のカスタマIDフィールド414にエンターする。カスタマIDを受信すると、アプリケーション・サーバ326は、ネットワーク及びサービス・インベントリ302並びに他のOSS 304から、カスタマ及びカスタマによって加入されるサービスに関する関連データを引き込む。引き込まれたデータは、内部データベース320に記憶され、ウェブ・サーバ324によってオペレータに提示されるGUIのページを配置するために用いられる。したがって、図9に示された例において、オペレータは、カスタマID 124578909を、カスタマIDフィールド414にエンターしている。カスタマ及びカスタマが加入するサービスに関する情報は、カスタマ表示領域402に表示される。この場合には、カスタマは、Jim Greenである。彼は、VoN Plusサービス、及び、DSL Plusサービスに加入している。カスタマの電話番号、サービスID、プラン開始日、DSL番号、等のような追加のデータもまた、表示され得る。オペレータは、トラブル・ビュー領域402において、カスタマ・トラブル又はネットワーク・トラブル・ビューを選択できる。ネットワーク・トラブル・ビューの選択によって、オペレータが、ネットワーク・リソースの識別子を用いて、又は、特定のアプリケーション・コンポーネントを選択することによって、ネットワーク・リソース (サービスに関連する、ネットワーク要素、又は、アプリケーション・コンポーネント) によって診断を実行することが可能となる。大きな領域の広いサービスの割込みの場合には、これは、問題の源を特定する、最も効率的な方法であり得る。

【 0 0 5 7 】

診断タイプ領域404は、エンド・ツー・エンド・テスト及び診断マネージャが診断するように構成される、サービスのタイプをリストする。診断タイプ領域は、サービス・プロバイダによって提供される全てのサービスをリストし得る。或いは、表示されたリストは、特定されたカスタマが加入している特定のサービスに限定され得る。いずれの場合でも、オペレータは、カスタマの苦情の性質に基づいて、診断タイプ領域404から適切な診断タイプを選択し得る。図示された例においては、オペレータは、カスタマのVoNサービスが診断されるべきであることを選択している。

【 0 0 5 8 】

ツール領域406は、種々のサービスをトラブル・シューティングするために利用可能なテスト及び診断ツールを表示する。ツール領域406に表示されたツールは、診断タイプ領域404で選択されたサービスに適用可能なツールに限定され得る。或いは、利用可能なツールの完全な一式 (full compliment) が表示され得る。いずれの場合でも、オペレータは、コンポーネントをテストし、サービス配送問題を診断するための種々のツールを、ツール領域406から選択する。

【 0 0 5 9 】

ネットワーク表示領域400は、サービス配送チェーンの単純化されたビューを表示する。サービス配送チェーンに関するデータは、ネットワーク及びサービス・インベントリ302から引出され、選択されたサービスの、カスタマへの配送に関連する全てのネットワーク要素を含む。サービス配送ネットワークの単純化されたグラフィカル表現は、フロントエンド・オペレータが、どこに問題が存在するかを容易に理解し、それらの問題を、適切なサービス部門に急送することを助ける。例えば、図5に示される、気の遠くなるような複雑なVoNサービス配送アーキテクチャは、GUIページ400のネットワーク・ディスプレイ領域410に示される、単純化されたネットワークに小さくされる。単純化されてい

10

20

30

40

50

るが、図9に表示されたネットワークは、それにも関わらず、VoNサービスを、特定されたカスタマのJim Greenに配送するために必要な、全ての重要なコンポーネントを含む。

【0060】

プロビジョニング (provisioning) 及び構成情報領域408は、サービス配送チェーンの種々のドメインのための、装置及び装置構成データを表示する。例えば、プロビジョニング (provisioning) 及び構成情報領域408は、CPEドメイン、トランスポート・ドメイン、IPドメイン、及び、VoNドメインのためにプロビジョニング (provisioning) 及び構成データを表示するためのタブを含む。ここに示される例において、CPEタブが選択され、プロビジョニング (provisioning) 及び構成情報領域408は、モデム・タイプ、IPアドレス、及び、MACアドレスを含む、カスタマの家庭内モデムについての情報を表示する。

10

【0061】

最後に、カスタマ・テスト・ヒストリ領域412は、より初期の問題をトラブルシューティングするために、選択されたカスタマのために実行された、以前のテストに関連するデータを表示する。オペレータは、「から (From)」及び「まで (To)」フィールド416、418に日付け範囲をエンターし得、カスタマ・テスト・ヒストリ領域412は、指定された期間中に、そのカスタマのために実行された全てのテストに関する情報を表示する。情報は、テスト日、テストID、テスト・タイプ、テストに関連するトラブル・チケット番号、及び、当該テストを始めたオペレータ、を含む。テスト・ヒストリは、現在のサービス配送問題への洞察 (insight) を提供し得る。

20

【0062】

GUIページ400上に表示された情報は、種々のサービスをカスタマに配送するための、サービス配送チェーンの、完全なエンド・ツー・エンドのビューを提供する。GUIは更に、サービス配送問題のトラブルシューティングのために、オペレータに利用可能な、種々のテスト及び診断ツールを表示する。

【0063】

図8を参照して、アプリケーション・サーバ326は、いくつかのテスト及び診断ツールが呼び出されるときに実行される作業フローを含む。例えば、特定のテストが、特定のネットワーク要素上で実行されるときに、アプリケーション・サーバは、テストが、ネットワーク・エレメント・マネージャ、別個のスタンドアロン・テスト・ツール、レイヤ2、3ドメイン・マネージャ、又は、アプリケーション・サーバ自身によって実行されるか否かを決定する。テストが、アプリケーション・サーバ326自身によって実行されねばならない場合には、アプリケーション・サーバは、適切な装置に直接アクセスし、選択されたテストを実行するために必要なコマンドを実行する。アプリケーション・サーバは、テスト結果を受信し、それらを、データベース320内に記憶する。このデータベースにおいて、テスト結果は、GUIを介してオペレータに提示されるべきウェブ・サーバによってアクセスされる。さもなければ、アプリケーション・サーバは、作業フローによって、命令を、適切なテスト・ツール、レイヤ2、3ドメイン・マネージャ、又は、適切なネットワーク・エレメント・マネージャに送り、所望のテストを呼び出す。テスト・ツール、レイヤ2、3ドメイン・マネージャ、又は、ネットワーク・エレメント・マネージャは、適切なネットワーク要素にアクセスし、要求されたテストを実行する (という場合が多いであろう)。いずれの場合でも、テスト結果は、アプリケーション・サーバに戻され、ウェブ・サーバ324を介してオペレータにサービスされているGUIページに取り込まれる。アプリケーション・サーバは、サービス配送チェーン内の全てのネットワーク要素へのアクセスを持つので、直接、或いは、仲介テスト・ツールズ・レイヤ2、3ドメイン・マネージャ又はネットワーク要素マネージャを介して、エンド・ツー・エンド・テスト及び診断マネージャは、完全なエンド・ツー・エンドの、サービス配送チェーンのカバレッジを提供できる。作業フローは、より複雑な診断を実行するために、基本のテスト・ツールが実行されるべき順序 (sequence) をも規定できる。テスト・マネージャによって、特定の作業フローに従うためのトリガと

30

40

50

して、単一のテスト結果が用いられる。

【0064】

本発明の種々の実施例が説明された一方、当業者にとって、本発明の範囲内において、更に多くの実施例及び具現方法が可能であることが明白である。したがって、本発明は、添付の請求項及びそれらの均等物によって限定される場合を除いて、限定されない。

【図面の簡単な説明】

【0065】

【図1】専用の垂直に統合されたサービス配送ネットワークを示す説明である。

【図2】好ましいサービス配送トランスポート・レイヤとしてのIPへの収束を示す説明である。

10

【図3】DSLネットワークのブロック図である。

【図4】一般的なカスタム構内装置を示すブロック図である。

【図5】一般的なボイス・オーバー・ネットワーク(VoN)アーキテクチャを示す図面である。

【図6】サービス配送問題のトラブルシューティングで呼び出されたステップを示すフローチャートである。

【図7】エンド・ツー・エンドのテスト及び診断マネージャの単純化されたブロック図である。

【図8】より詳細な、エンド・ツー・エンドのテスト及び診断マネージャ及びサービス配送環境のブロック図である。

20

【図9】エンド・ツー・エンドのテスト及び診断マネージャGUIページの説明である。

【符号の説明】

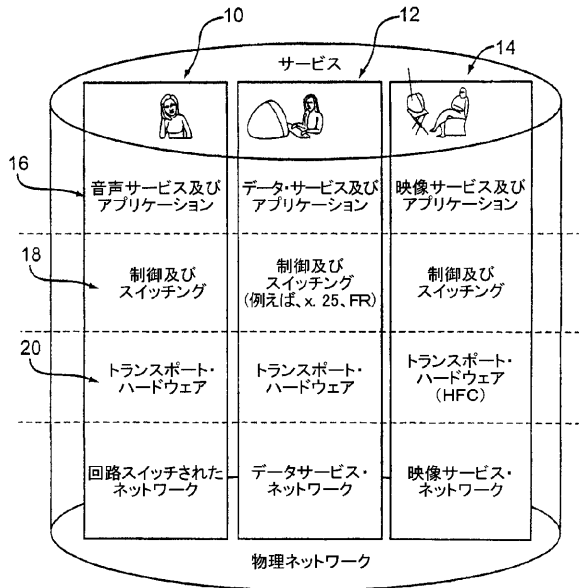
【0066】

- 40 DSLサービス・アーキテクチャ
- 60 非定型ではない(not atypical)カスタム構内アレンジメント
- 62 ADSLライン
- 64 ネットワーク・インターフェース装置
- 66 スプリッタ
- 68 第1のウォール・ジャック
- 72 標準電話セット
- 74 DSLモデム
- 78 コンピュータ
- 80 コンピュータ
- 82 コンピュータ
- 104 トランスポート・レイヤ
- 106 CPEレイヤ
- 114 ローカル・エリア・ネットワーク
- 116 VoN電話装置
- 118 ユーザ・コンピュータ
- 120 カスタム・エッジ
- 124 カスタム・エッジ
- 126 ローカル・エリア・ネットワーク
- 130 アクセス・ゲートウェイ
- 132 カスタム・エッジ
- 136 伝統的な電話装置
- 148 より広いネットワーク
- 162 メディア・ゲートウェイ(MG)
- 166 SIPサーバ・アンド・ソフトスイッチ
- 170 スリップ(slip)・サーバ・アンド・ソフトスイッチ

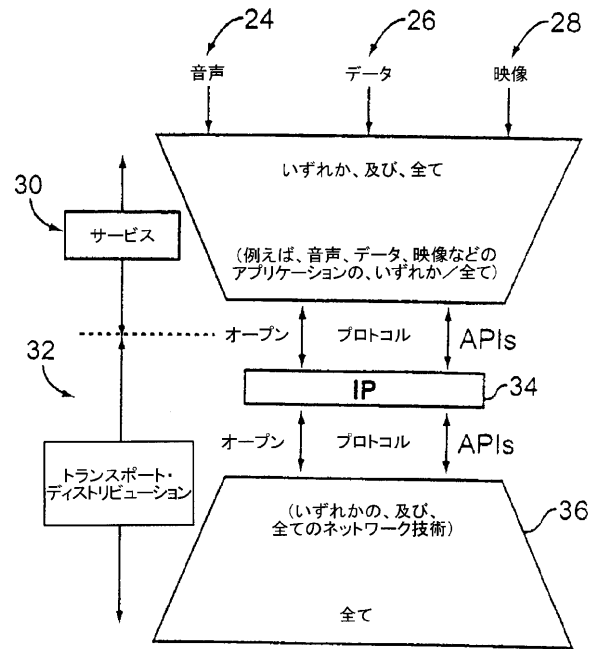
30

40

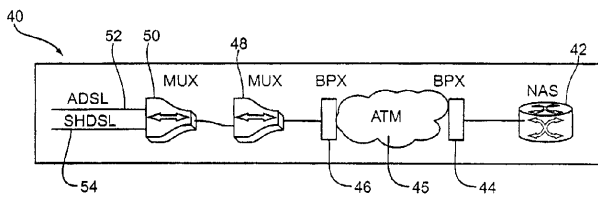
【 図 1 】



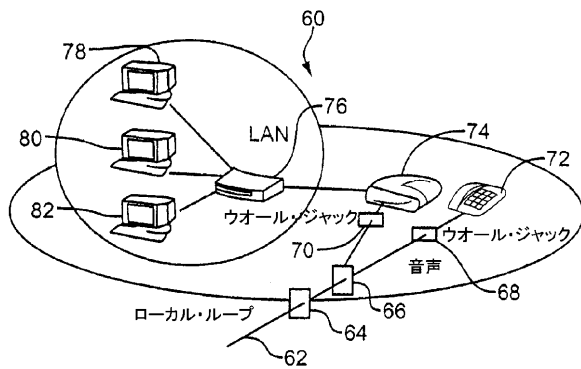
【 図 2 】



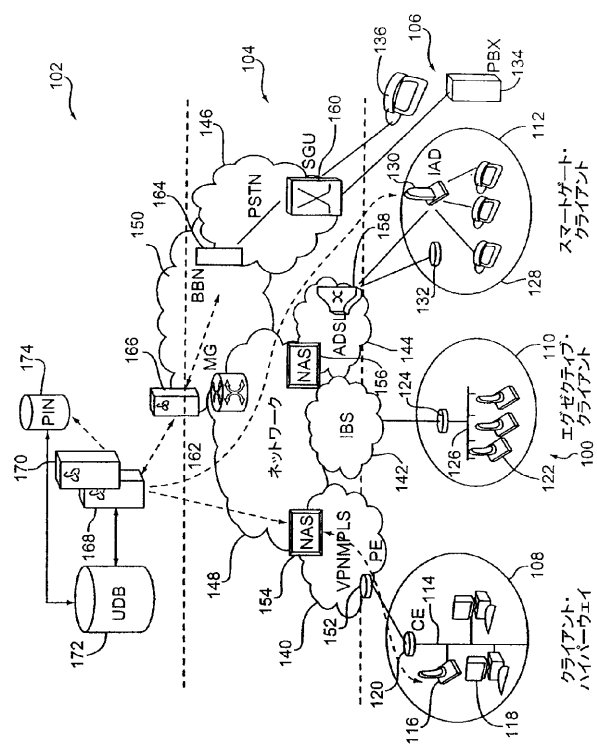
【 図 3 】



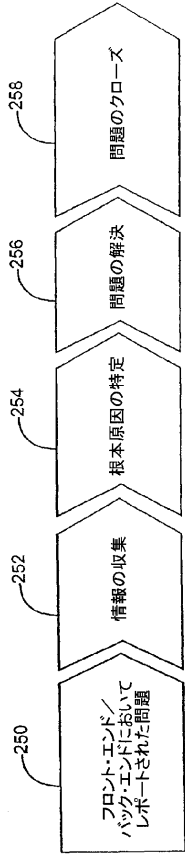
【 図 4 】



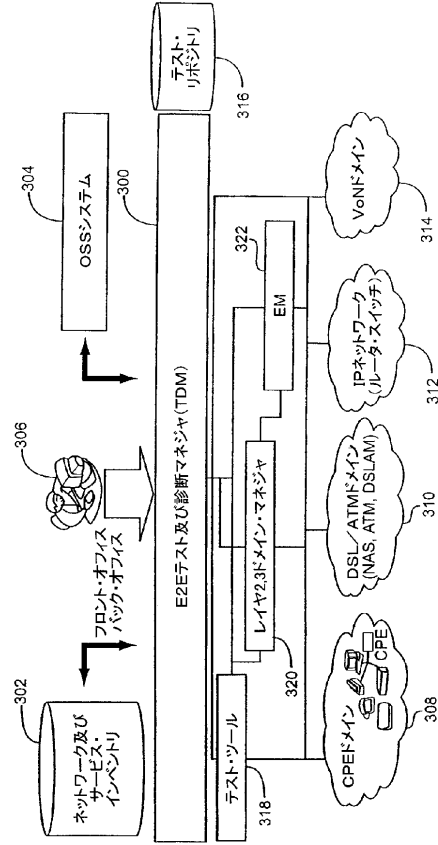
【 図 5 】



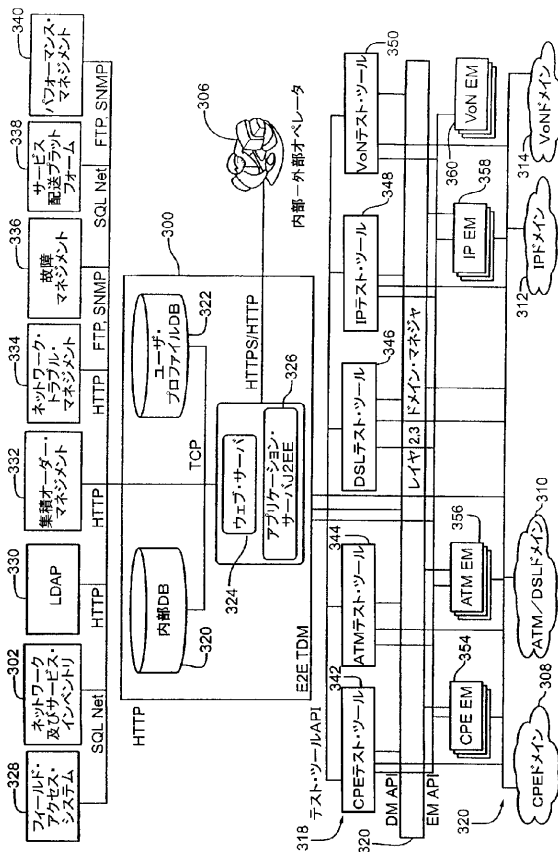
【図6】



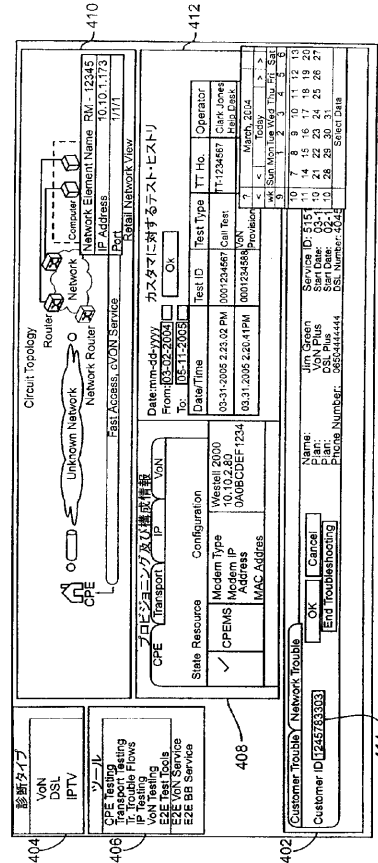
【図7】



【図8】



【図9】



フロントページの続き

(72)発明者 アントニオ サマーレ

イタリア 00136 ローマ ヴィア ジョルジョ スカリア 27

(72)発明者 ガブリエレ ルボ

イタリア 00131 ローマ ヴィア コラヤンニ 4

(72)発明者 シリオ プロイエッティ

イタリア チアピ 00145 ローマ ヴィア グロッタ ペルフェッタ 337

Fターム(参考) 5K030 GA12 HA08 HD03 KA04 LB05 LE11 MC03 MC08

【 外国語明細書 】

END-TO-END TEST AND DIAGNOSTIC MANAGER

BACKGROUND

The present invention relates to an end-to-end test and diagnostic manager for testing components and diagnosing service problems for services delivered via layered, multi-domain network environments.

In the past, various telecommunications services such as voice communication, data services, video services, and the like were delivered via stand-alone vertical networks. For example, Figure 1 shows separate distinct networks for delivering voice communication services and applications 10, data services and applications 12, and video services and applications 14. Each separate network includes a service layer 16, control and switching layer 18, transport hardware layer 20, and a physical network layer 22. In each case the services are tightly coupled to the physical networks and network elements provided for distributing the services. For example, in a public switched telephone network (PSTN) the control and switching protocols and the physical switches themselves are all geared toward creating end-to-end circuits for providing point-to-point voice communication. Similar dedicated networks such as Ethernet, token ring, and the like having their own switching and control protocols and physical transport structures were developed for providing data transmission services. Video services, either broadcast or delivered via broadband cable, likewise developed their own set of control and switching protocols, transport hardware and networks. In each case, all aspects of the various integrated networks were configured specifically for the particular service the networks were designed to deliver.

Troubleshooting service problems in the vertically distributed proprietary networks of the past was a fairly straightforward proposition. The entire network was typically owned and controlled by a single entity having intimate knowledge of the end-to-end service delivery chain. This and the fact that the services were so tightly coupled to the network elements provided for delivering the services made it fairly simple to identify the components in the service delivery chain that might affect service delivery to a particular customer. Knowing the likely sources of service problems made it fairly simple to test the appropriate components and isolate the source of a problem.

Today the delivery of more and more telecommunications and broadcast services is converging on IP as the preferred transport layer. The convergence on IP decouples the services from the underlying access and transport networks. The result is a multi-service, multi-domain network where the services themselves are substantially independent of the physical transport layer. FIGURE 2 illustrates the convergence on IP as the preferred transport layer. As opposed to the proprietary vertically integrated networks of the past, the new service model defines broad horizontal layers. Open protocols and APIs provide the operational interfaces between layers, with clear separation of access, transport, and services. Thus, the services layer 30 represents any and all services that can be delivered digitally over a network, including, but not limited to voice 24, data 26, and video 28. The transport and distribution layer 32 encompasses the IP layer 30 and the physical distribution layer 36. Through the use of open protocols and APIs all services can be packaged for transport via IP. The IP packaged data may be carried by virtually any and all physical network technologies.

The convergence on IP as the common transport layer for delivering multiple services to customers adds significant complexity to the service delivery chain. Today value added services (VAS) are based on complex network architectures and operational platforms. Portions of the service delivery chain may be, and likely are, outside the control of the service providers themselves. In these cases service providers must rely on networks and hardware provided and maintained by others to deliver their services. The decoupling of the services from the underlying access and transport system makes diagnosing and correcting service problems a much more difficult task than it was in the standalone service delivery platforms of the past.

To illustrate the complexity of today's service delivery platforms, consider the basic DSL service architecture 40 shown in Figure 3. On the left, an Asymmetric Digital Subscriber Line (ADSL) 52, or a Symmetrical High-Speed Digital Subscriber Line (SHDL) 54 provides a digital connection to a customer's home or business. The DSL connection provides access to the broader IP network or internet via a Network Application Server (NAS) 42. The customer's DSL line (ADSL or SHDL) connects to a first, local DSL access multiplexer (DSLAM) 50. The local DSLAM 50 serves a limited number of customers in a small geographical region. The local DSLAM 50 connects to a remote DSLAM 48 which serves a plurality of local DSLAMS. The remote DSLAM 48 connects to an ATM network 45 via a first BPX switch 46. The NAS 42 connects to a second BPX switch 44 elsewhere in the ATM network 45. There are likely additional BPX switches in the ATM network 45. However, from the point of view of delivering internet access to the customer at the end of the ADSL line 52 via NAS 42, BPX switches 44 and 46

serve as the entry and exit points to the ATM network 45 and any other BPX switches within the ATM network are not relevant to the service delivery chain. The DSL technology is currently evolving introducing the possibility to deliver current and new services through different infrastructures using IP DSLAMs connected through Ethernet interface to GBE (Gigabit Ethernet) or MANs (Metropolitan Area Network).

The service delivery chain becomes more complicated when the Customer Premises Equipment (CPE) is taken into account. The DSL service depicted in Figure 3 requires at minimum a DSL modem at the customer's premises. Local area networks, WI-FI Routers, and other CPE can further complicate the service delivery picture. Figure 4 shows a not atypical customer premises arrangement 60. ADSL Line 62 enters the customer's premises via a network interface device 64. A splitter 66 separates voice and data, connecting the voice signal to a standard telephone set 72 via a first wall jack 68 and connecting data signal to a DSL modem 74 via a second wall jack 70. A local area network hub 76 connects a plurality of computers 78, 80, 82 to the DSL modem 74. Thus each computer has access to the DSL line via the LAN. In addition to the network components described with regard to Figure 3, the DSL modem 74 and the LAN HUB 76 must also be operating and configured properly in order for users at computers 78, 80, 82 to received services over the DSL line 62. Thus, if these components are not operating properly or are not configured properly, the CPE domain can provide another source of service problems.

The service delivery chain becomes even more complicated with the increased complexity of the services delivered. For example, Figure 5 shows a typical architecture for voice over network (VoN) service. Tracking down a service problem for an individual customer in this environment can be a very complicated task. As

can be seen, the VoN service requires the interaction of multiple network domains, including multiple network elements and service components. Furthermore, the service is provided to multiple customers, at different location, having different connections and having different CPE.

The VoN architecture 100 is divided between the VoN or service layer 102, the transport layer 104, and the CPE layer 106. Starting with the CPE layer 106, a number of different client configurations are shown. The different client configurations will depend mainly on the type of access to the transport layer, the available bandwidth, and other factors.

Client 108 includes a local area network 114, one or more VoN telephone devices 116, and a plurality of user computers 118. A Customer Edge 120 interfaces with a Provider Edge in the transport layer 104, providing access to a virtual private network (VPN) 140. VPN 140 is based on multi-protocol label switching (MPLS). The VPN 140 accesses the broader IP network via NAS 154.

The Client arrangement 110 includes a local area network 126 and a plurality of VoN telephone devices 122. A Customer Edge 124 provides the interface to an IP Edge Network 142. The IP Edge Network 142 provides access to the broader IP network 148.

Client 112 includes a plurality of traditional telephone devices 128, an Access Gateway 130, and a Customer Edge 132. The Access Gateway 130 and the Customer Edge 132 interface with DSLAM 158 via a digital subscriber line.

Also shown in the customer layer 106 are a traditional PBX 134 and a traditional telephone device 136. In the system shown, the PBX 134 and the traditional telephone device 136 may participate in telephone calls with customers

employing the VoN service. However, the PBX 134 and telephone device 136 operate on a traditional public switched telephone network 146 and are not themselves amenable to VoN service.

The transport layer 104 includes the VPN 140, the IP Edge network 142, the ADSL network 144, the PSTN 146, the IP network 148, and a backbone network transit level 150 for traditional voice service, as well as the interface components therebetween. For example, the VPN 140 interfaces with the IP network 148 via NAS, 154. The ADSL network interfaces with the IP network 148 via NAS 156. The PSTN interfaces with the backbone network of backbone transit level (BB-TL) 150. The IP network interfaces with the BB-TL network via a media gateway (MG) 162.

The VoN service layer 102 includes a user profile database 172, Packet IN application server 174 that includes service logic and user profile data, one or more SIP Servers and Softswitches 166 for interfacing with the PSTN 146 via the BB-TL 150.

In this example, the service delivery chain includes all of the network elements involved in delivering VoN service to the end customer. For example, to deliver VoN service to customer 112 the service delivery chain includes the Sip Server and Softswitch 170, the switch 166, the media gateway 162, the NAS 156, DSLAM 158, and the Access Gateway 130. Additional components within the various network domains such as ATM switches, IP routers, and the like may also comprise part of the service delivery chain. All of these elements must be operating and configured properly to provide VoN service to the customer 112. Of course different networks and different network elements will be part of the service delivery

chain delivering VoN service to other customers. Identifying all of the network elements involved in delivering service to a particular customer is a significant task in troubleshooting service delivery problems. Performing tests on all the various equipment comprising service delivery chain and checking configuration data across all of the service delivery domains has been well nigh impossible.

To date there has been no system or procedure for providing comprehensive end-to-end test and diagnostics of services delivered via the IP transport layer with a structured, end-to-end approach. The lack of such systems and procedures adds significantly to the time, effort and expense of troubleshooting service delivery problems.

BRIEF SUMMARY OF THE INVENTION

The present invention relates to an end-to-end test and diagnostic manager for troubleshooting service problems for services delivered via layered multi-domain service delivery networks across diverse technology platforms. In particular, an embodiment of the invention provides an end-to-end test and diagnostic manager for services delivered using Internet Protocol (IP) as the common transport layer. The end-to-end test and diagnostic manager provides a comprehensive solution for troubleshooting services, such as VoN, IP-TV, video on demand, unified messaging, and the like delivered via the IP transport layer.

According to an embodiment, an end-to-end test and diagnostic manager comprises a software application that allows front-end operators (e.g., call center customer service representatives) and back-end operators (e.g., more skilled operators available to troubleshoot more complex service problems that cannot be resolved by front-end operators) to troubleshoot the entire service chain extending

from the service provider, across multiple network domains, to the end customer. The end-to-end test and diagnostic manager provides a customer-centric end-to-end operational view of services, focusing more on managing services as opposed to managing the underlying transport mechanisms or networks.

An embodiment of the invention provides a system for troubleshooting service problems for services delivered over multi-domain service delivery networks. A plurality of test tools for testing operational status and configuration of network elements in the various domains involved is provided. A test and diagnostic manager has access to network and service inventory data. In response to a service interruption or other customer complaint, the test and diagnostic manager accesses the network and service inventory data to learn which services are delivered to the customer and identify the network elements necessary to deliver the services to the customer. The test and diagnostic manager then selectively invokes the various test tools to determine the operational status and configuration of selected network elements. A graphical user interface displays the results of the selectively invoked tests so that an operator may determine the source of a service problem and take steps to resolve it.

In another embodiment an end-to-end test and diagnostic manager includes a graphical user interface for displaying status and configuration data regarding networks, network components, and services to, and receiving commands from an operator. An application server has access to network and service inventory data. Upon receiving a report of a service problem, the application server determines the networks and network components necessary to deliver the service to the customer. The application server is adapted to execute workflows to selectively invoke one or more test tools to determine the operational status or configuration of

the network elements involved in delivering the service. The results may be displayed by the graphical user interface so that an operator may determine the source of the problem and take steps to resolve it.

Finally, a method of diagnosing service delivery problems in services delivered over multi-domain service delivery networks is provided. The method includes gathering a set of information of a service problem interviewing a customer. Upon receiving the report of a problem using a customer billing number, it is possible to gather information regarding all network elements necessary to deliver the service to the customer. Once all of the network elements in the service delivery chain are known, remotely testing the network elements to determine if they are operating properly and are configured correctly to identify the cause of the problem. Once the source of the problem is determined, taking steps to resolve it. Finally, when the problem is resolved, performing a remote end-to-end test to ensure the service has been restored.

Alternatively, the diagnostic process may be driven by report of network device problem. Upon receiving the report of a network problem it may be possible to select a specific network resource (network element or application component), and gather information about the status of the specific network resource in order to understand if it is operating properly and configured correctly.

Other systems, methods, features and advantages of the invention will be, or will become, apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the following claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration showing dedicating vertically integrated service delivery networks.

Figure 2 is an illustration showing the convergence on IP as the preferred service delivery transport layer;

Figure 3 is a block diagram of a DSL network;

Figure 4 is a block diagram showing typical customer premises equipment.

Figure 5 is a diagram showing a typical voice over network (VoN) architecture.

Figure 6 is a flow chart showing the steps involved in trouble shouting a service delivery problem.

Figure 7 is a simplified block diagram of an end-to-end test and diagnostic manager.

Figure 8 is a more detailed block diagram of an end-to-end test and diagnostic manager and the service delivery environment.

Figure 9 is an illustration of an end-to-end test and diagnostic manager GUI page.

DETAILED DESCRIPTION OF THE DRAWINGS AND THE PRESENTLY PREFERRED EMBODIMENTS

Diagnosing service delivery problems in a multi-domain service delivery environment requires accessing and relating information from diverse sources and presenting the resulting data in a structured and consolidated manner to allow operators viewing the data to quickly identify the nature and cause of service

delivery problems and allow them to take immediate corrective actions to resolve the problems.

Figure 6 shows an overview of the steps necessary to identify and resolve service delivery problems. First, a problem is reported at 250. Information about the problem is collected at 252. The collected information may include information about the customer experiencing the problem, such as the services the customer subscribes to, and the service or services affected by the problem, the service delivery equipment on the customer's premises, and the networks and network elements that comprise the service delivery chain for providing the service to the customer. The collected information may also include information about the service that is experiencing a problem. Additional collected data may include alarm repositories, existing related trouble tickets, planned engineering/maintenance activities, performance management reports, predictive systems reports and the like.

The root cause of the service delivery problem is identified at 254. This may involve analyzing the network and service inventory, performing intrusive/non-intrusive tests on network elements, analyzing historical test results, and the like. Once the root cause of the problem has been identified steps may be taken to resolve the problem at 256. This may involve dispatching support personnel to repair customer premises equipment or other hardware, accessing network element managers and test systems, modifying configuration data, and the like. Finally once the problem has been resolved the problem may be closed at 258. Closing the problem may include performing a final end-to-end verification test, archiving test results, and so forth.

A simplified view of an end-to-end test and diagnostic manager 300 and the environment in which it operates is shown in Figure 7. The end-to-end test and diagnostic manager 300 has access to network and service inventory data 302 and other operating support systems (OSS) 304. The end-to-end test and diagnostic manager 300 may pull data from the network and service inventory 302 and OSS 304 as needed in order to develop a comprehensive picture of the service delivery chain including the network platforms, systems and components necessary to deliver a particular service to a specific customer.

According to an embodiment, the network and service inventory data are stored in an Oracle database or some other commercially available database, and may be accessed via SQL queries. The information exchanges between the network and service inventory and the end-to-end test and diagnostic manager includes “commercial information” and “technical information.” The commercial information relates to customers, their service provider, their service plan, service ID, service dates, and the like. The technical information gathered from the network and service inventory includes all of the information necessary to rebuild the circuit for delivering services to a customer in order prepare an accurate representation of the circuit, and to allow the end-to-end test and diagnostic manager to query all the major devices involved. The technical information must include information on all services that a customer subscribes to and all of the components necessary to deliver those services.

According to an embodiment, three separate database tables are accessed to obtain all of the technical relevant data. The key input parameter is the customer ID (Billing Number) or some other reliable identifier. The first table accessed is the A-Z Circuit Table which identifies all of the major components

required to build the circuit from the service provider to the customer for delivering a particular service to a particular customer. In this table the point "A" is represented by the DSLAM and the point "Z" is represented by the NAS. The necessary components include, among others, the point "A" of the ATM domain (the ATM access device facing the service provider) and the point "Z" of the ATM domain (the ATM access device facing the customer). A sample A-Z circuit table is shown in Table 1. The A-Z circuit table includes a plurality of attributes that define the types of components necessary to build the circuit for delivering a service to a customer. Corresponding values identify the real world components that fill these roles. The customer ID value (Billing Number) identifies the customer for whom the service delivery chain is being constructed. The DSLAM name identifies the DSLAM that serves the identified customer. The next several attributes relate to connection and configuration data for the identified DSLAM, identifying ports, subscriber lines, etc. for delivering services to the identified customer. The NAS name identifies a network applications server that provides the service to the customer via the ATM network serving the customer. The identified NAS provides access to and allows services to be delivered through the IP domain. The remaining attributes relate to connection and configuration data for the NAS.

Table 1: (A&Z Circuit)

Attribute Name	Value
Customer ID	0065940342
DSLAM Name	MILANUSER/DSL/005
Port Customer side (ATU-C)	ADSL 2-2-12-19
DSL Line	2:2:12
Port Customer side (ATU-C)	ADSL 2-2-12-19
VCI	2-2-12-19:8.35
Cross Connection	LT = 8.35 / NT = 34.65

Port ATM Side	MRL08C
VCI	34.65
NAS Name	AT-BO256
Port ATM Side	ATM4:3:7
VCI	23.65

The “Port ATM Side” value from the DSLAM portion of Table 1 is used to query a second database table (that represent the logical link between the MUX and the ATM domain) in order to determine the point “A” of the ATM domain network. This query identifies the appropriate ATM device, the proper port on the ATM and so forth. These data are used to identify, in the IP table, the corresponding IP address and then check the operational status and configuration of the ATM device and the designated port. An example of the second database table (MUX Logical Link) is shown in Table 2.

Table 2: (MUX Logical Link)

Attribute Name	Value
ATM Device Name	MGX9063
Port	MGX 9063:3:5
VPI	MGX 9063:3:5:34

The “Port ATM Side” value of the NAS portion of Table 1 is then used to perform a similar query of a third database table to learn which device represents the point “Z” at the opposite end (from the service deliver standpoint) of the ATM domain. Again, this query identifies the appropriate ATM device, the proper port, and so forth, so that the operational status and configuration of the ATM device and the designated port can be verified. An example of the third table (NAS Logical Link) is shown in Table 3.

Table 3: (NAS Logical Link)

Attribute Name	Value
ATM Device Name	MGX9064
Port ATM Side	MGX 9064:5:5
VPI	MGX 9064:5:5:27

The last step is to determine the IP addresses of the devices identified above, namely the DSLAM, the “A” and “Z” ATM devices, the NAS, and any other relevant devices that may be necessary to deliver a particular service to the identified customer. This is accomplished through a separate query of a fourth database table (IP Address Device). An example of an IP Address Device Table is show in Table 4.

Table 4: IP Address Device Table

Attribute Name	Value	IP Address
DSLAM Name	MILANUSER/DSL/005	10.11.134.178
ATM Device Name	MGX9063	10.11.156.170
NAS Name	AT-BO256	10.11.124.138

Commercial information is obtained by querying yet another table. Again, the customer ID (billing number) is the primary key. A sample commercial information tale is shown in Fig. 5.

Table 5: (Commercial Information)

Attribute Name	Value
Customer ID	0065940342
Customer Name	Kate Moss
ISP	AOL
PLAN	VoN Fast Access
Service ID	986241585
Plan Start Date	07/13/1977

Technical information and commercial information may also be pulled from the other operational support systems 304. For example, the IP address of the device at the customer’s premises may be obtained from the service delivery platform

(SDP) 338. The IP address may be used, for example, to determine whether the customer premises equipment is up and running using a simple “Ping IP” test. Other information may also be pulled from the SDP 338. The information exchange between the SDP and the end-to-end test and diagnostic manager may be accomplished by web services. Parameters from the SDP may include:

Technical Key (TK) that is the real identifier of the circuit; it's composed by:
(Name NAS, card, port, VPI, VCI) = (AT-BO256, 3, 7, 23, 65)

Management Session:
date of first connection, last connection = (11/07/2005 22:34;
11/07/2005 23:18)

Data Session:
date of first connection, last connection = (11/07/2005 22:35;
11/07/2005 23:17)

Master Account:
user name and date of creation = (sirio.baldini@aol.us, 08/15/2005)

Data Service:
Plan, Commercial offering = (VoN Fast Access, VoN-3numbers)

Added Services:
State of Parental Control, State of Captive Portal = (off, off).

IP Address:
IP Address of the management session (10.10.148.170)

Once all of the component links of the service delivery chain have been identified, an operator 306 employing the end-to-end test and diagnostic manager 300 may invoke test procedures for testing various aspects of the service delivery process. For example, the operator may initiate tests analyzing the status of hardware components and network elements that make up the service delivery chain in order to identify the root causes of service delivery problems.

According to an embodiment, the end-to-end test and diagnostic manager 300 has access to a full compliment of test tools for testing all of the functional domains involved in delivering the service to the customer. The various functional domains may include the CPE domain 308, the DSL/ATM domain 310, the IP network domain 312 and the VoN (or service) domain 314.

Examples of the diagnostic tools that may be available include:

- CPEMS Ping Test: this is a simple ping test to verify that all of the Customer Premises Equipment (all the devices at the customer premises) may be reached by the end to end test and diagnostic manager.
- Sync Profile: this is a tool that gathers the configuration parameters (attenuation, noise margin, etc.) of the customer on the DSLAM.
- Port verification: this tool checks the operational status of the DSLAM port to which the customer device is connected).
- Port Lock/Unlock: this is a system wide administrative command that shuts down the port on a targeted device (DSLAM, ATM, IP router,...) and restart it.
- No Sync Test: this test returns a Boolean result about the synchronization between the modem and the DSLAM (Siemens, Alcatel, etc.) and the customer device (Modem or CPE).
- Port Reset: this test is used to reset the configuration on the DSLAM (Client side port).
- IP Ping Testing: this test is used to verify the reachability of the IP devices (NAS: Cisco 10k, Cisco 6004, Juniper ERX, etc.).
- Test Call: this test simulates an IP call through the element manager of a switch to customer telephone but does not cause the customer phone to ring.
- Call History: this is a tool that provides information (date of first and last call, the duration, the time, etc.) about IP calls made by the customer.
- End-To-End VoN Service: this is a tool that checks and reports information about the IP calls (band, quality of communication, inbound/outbound etc.).
- End-To-End BB Service: this is a tool that gathers information about packets sent, lost, and received for specific NEs.
- MLT (Mechanized Loop Testing) these are a set of tools used to determine the condition of a customer's PSTN line:
 - testing that the line is OK;
 - a potential problem with customer's equipment, such as defective telephone or receiver off hook;
 - speech on the line.

The end-to-end test and diagnostic manager 300 may be configured to access and invoke the various tests in a number of different ways. For example, the

end-to-end test and diagnostic manager may include a test repository 316 that includes workflows that define the steps to be taken to test the operational status and configuration of the various components in different domains. The workflows defined in the test repository may include steps for interrogating and testing hardware devices and network elements directly. Alternatively, the workflows may invoke external test tools and commercial packages 318 developed to test specific components in the various domains. In yet another alternative, the end-to-end test and diagnostic manager 300 may invoke a Layer 2, 3 Domain Manager 320 to test the functionality of one or more domains. Finally, the end-to-end test and diagnostic manager 300 may invoke Element Managers (EM) 322 configured to test various components within the various domains. The workflows within the test repository 316 may be fairly complex. Depending on whether internal/external test tools available, whether or not a Layer 2, 3 Domain Manager is present or if any Element Managers are available, the end-to-end test and diagnostic manager may invoke tests and interrogate components in a combination of different ways. For example, the end-to-end test and diagnostic manager may test some components directly via APIs executed on an API server within the end-to-end test and diagnostic manager. Other tests may be invoked through external test tools, others through the Layer, 2, 3 Domain Manager 320, and still others through separate Element Managers 322.

The end-to-end test and diagnostic manager 300 presents a graphical user interface (GUI) to front-end and back-end operators 306. Front-end operators may use the end-to-end test and diagnostic manager to assess service complaints and run simple initial diagnostic tests in order to determine whether a service delivery problem may be resolved quickly by standard, easily performed procedures, or

whether more sophisticated analysis is necessary to resolve the problem. If so, back-end operators may use the system to perform more sophisticated tests and delve deeper into more trouble some service problems. The various tools that are available to front-end and back-end operators may be defined in a user profile database. Back-end operators may be given access to more sophisticated tests and diagnostic tools than their front-end counterparts. For example, the interface may further provide back-end operators access to historic test results, alarm and fault logs, maintenance and service schedules, performance management systems, predictive systems, and the like, in order to assist back-end operators in determining the cause of difficult service delivery problems. The end-to-end test and diagnostic manager interface may further provide back-end operators with means for taking steps to resolve service problems that are not available to front-end operators, such as dispatching appropriate support teams, accessing Element Managers and configuration management systems, and the like. Once problems are resolved back-end operators can perform verification of service tests and archive the various test results and the actions taken to resolve the problems.

Figure 8 shows a more detailed view of an end-to-end test and diagnostic manager 300 and the surrounding multi-domain service delivery environment. Many of the components described in Figure 7 have been repeated in Figure 8 and have been given like reference numbers. As shown, the end-to-end test and diagnostic system 300 interfaces with network and service inventory 302, and other operations support systems (OSS) 304. The OSS 304 may include a field access system 328, an LDAP 330, an integrated order management system 332, a network

trouble management system 334, a fault management system 336, a service delivery platform 338, and a performance management system 340.

The end-to-end test and diagnostic manager 300 has three possible types of interaction with other OSS systems 304 and network resources.

1) The end-to-end test and diagnostic manager can pull information from:

- Network and service inventory 302 that provide data related to:
 - services offered by the service provider;
 - service provider's customers;
 - services provided to specific customers;
 - network components involved in delivering particular services to particular customers.
- Service delivery platform 338 (service and user profile information).
- Specific tools 318, Domain Manager 320, EM 322 and network elements.
- Performance management 340 in order to check about a degradation in the devices involved in the service provided to the customer.
- The integrated order management 332 to gather information about the status of the work request concerning the claiming customer.

2) The end-to-end test and diagnostic manager provides information to:

- Network trouble management 334 in order to manage the customer trouble related to service problems on the network and to gain an enrichment of the related trouble ticket.
- Fault management 336 in order to open an alarm when a problem is found and to provide information about impacted customers.

- The field access system 328 to perform a final check of the service restoration accessing the test manager from the mobile terminal of the technicians at the customer house.
- 3) The end-to-end test and diagnostic can also perform an information exchange with LDAP (Lightweight Directory Access Protocol) server in order to authorize user accesses.

A plurality of external test tools 318 is shown in Figure 8, including a CPE test tool 342, an ATM test tool 344, a DSL test tool 346, an IP test tool 348, and a VoN test tool 350. Similarly, a plurality of element managers 322 is also shown. The element managers 322 include CPE element managers 354, ATM element managers 356, IP element manager 358, and VoN element managers 360. Multiple element managers are shown for each domain since each domain may include multiple network elements types. The Layer 2, 3 Domain Manager 320 is also shown in Figure 8. It should be noted that in various end-to-end test diagnostic manager implementations not all of the test tools, Element Managers or the layer 2, 3 Domain Manager will necessarily be present. In most cases various combinations of the test tools, element managers and the Layer 2, 3 Domain Manager will be combined together with additional direct access test protocols within the end-to-end test and diagnostic manager 300. Preferably, the end-to-end test and diagnostic manager 300 the test tools 318, the Layer 2, 3 Domain Manager and the Network Element managers 322 that are present in a particular embodiment will combine to provide a full compliment of diagnostic tests for performing a comprehensive analysis of the service chain for of all services offered by a service provider.

The end-to-end test and diagnostic manager 300 itself includes an internal database 320, a user profile database 322, a web server 324, and an application server 326. The user profile database 322 stores the user profiles of the front-end and back-end operators and other administrative personnel having access to the end-to-end test and diagnostic manager 300 for troubleshooting service problems. The user profiles will include the access rights and privileges of the various users, defining the test and diagnostic tools and configuration data available to the different types of users.

The internal database 320 stores data relating to customers and the services delivered to them. According to an embodiment, the internal database 320 does not store a comprehensive data set of all customers, services and service delivery components. Rather, the internal database 320 pulls the necessary data from the network and service inventory 302 and other OSS 304 as needed to resolve specific service delivery problems. The data are then stored in the internal database 320 where they are accessed by the web server 324 to populate the various data fields and displays of the GUI, or by the application server 326 to execute the various workflows necessary to perform an end-to-end test of the services delivered to the particular customer who lodged the complaint.

Figure 9 shows an example of an end-to-end test and diagnostic manager graphical user interface (GUI) page 400. The GUI page 400 includes a number of distinct areas where different types of information are displayed, and where different actions may be initiated by an operator interacting with the interface. These include a customer display area 402; a diagnostic type area 404; a tools area

406; a provisioning and configuration information area 408; a network display area 410; and a customer test history area 412.

According to an embodiment, the customer billing number serves as the customer ID and drives the end-to-end test and diagnostic manager. Accordingly, when a customer calls to report a service interruption or some other service delivery problem, an operator enters the customer's billing number into the customer ID field 414 in the customer display area 402. Upon receiving the customer ID, the application server 326, pulls the relevant data relating to the customer and the services subscribed to by the customer from the network and service inventory 302 and other OSS 304. The pulled data are stored in the internal database 320, and are used to populate the pages of the GUI served to the operator by web server 324. Thus, in the example shown in Figure 9, the operator has entered a customer ID 124578909 in the customer ID field 414. Information regarding the customer and the services the customer subscribes to are displayed in the customer display area 402. In this case, the customer is Jim Green. He subscribes to VoN Plus service, and DSL Plus service. Additional data such as the customer's phone number; service ID number, plan start dates, DSL ID number; and the like may also be displayed. The operator can select a customer trouble or network trouble view in the trouble view area 402. The selection of the network trouble view allows the operator to perform a diagnosis by network resources (network elements or application components involved in the service) using the identifier of network resource or selecting the specific application component. In cases of a large area wide service interruption, this may be the most efficient method of locating the source of a problem.

The diagnostic type area 404 lists the types of services that the end-to-end test and diagnostic manager is configured to diagnose. The diagnostic type area may list all of the services offered by the service provider, or the displayed list may be limited to the particular services the identified customer subscribes to. In either case, the operator may select the appropriate diagnostic type from the diagnostic type area 404 based on the nature of the customer's complaint. In the example shown, the operator has selected the customer's VoN service to be diagnosed.

The tools area 406 displays the test and diagnostic tools available to troubleshoot the various services. The tools displayed in the tools area 406 may be limited to the tools applicable to the service selected in the diagnostic type area 404, or the full compliment of available tools may be displayed. In either case, the operator selects the various tools for testing components and diagnosing service delivery problems from the tools area 406.

The network display area 400 shows a simplified view of the service delivery chain. The data regarding the service deliver chain are pulled from the network and service inventory 302, and include all the network elements involved in delivering the selected service to the customer. The simplifies graphical representation of the service delivery network helps the front-end operator to easily understand where problems lie, and to dispatch them to the appropriate service departments. For example, the numbingly complex VoN service delivery architecture show in Figure 5 is reduced down to the simplified network shown in the network display area 410 of GUI page 400. Although simplified, the network displayed in Figure 9 nonetheless includes all critical components necessary for delivering VoN service to the identified customer Jim Green.

The provisioning and configuration area 408 displays equipment and equipment configuration data for various domains of the service deliver chain. For example, the provisioning and configuration information area 408 includes tabs for displaying provisioning and configuration data for the CPE domain, the transport domain, the IP domain and the VoN domain. In the example shown the CPE tab is selected, and the provisioning and configuration information area 408 displays information about the customers in-home modem including the modem type, IP address and MAC address.

Finally, the customer test history area 412 displays data relating to previous tests that have been performed for the selected customer to troubleshoot earlier problems. The operator may enter a date range in the “From” and “To” fields 416, 418 and the customer test history area 412 will display information regarding all tests performed for that customer during the designated period. The information includes the test date, the test ID, the test type, a trouble ticket number associated with the test, and the operator who instituted the test. The test history may provide insight into current service delivery problems.

The information displayed on the GUI page 400 provides a complete end-to-end view of the service delivery chain for delivering the various services to the customer. The GUI further displays the various tests and diagnostic tools that are available to the operator for troubleshooting service delivery problems.

Returning to Figure 8, the application server 326 includes workflows that are executed when some tests and diagnostic tools are invoked. For example, when a specific test is to be performed on a specific network element, the application server determines whether the test is to be performed by a network Element Manager,

27]

a separate stand along test tool, a Layer 2, 3 Domain Manager, or by the application server itself. In cases where the test must be performed by the application server 326 itself, the application server accesses the appropriate device directly and executes the commands necessary to perform the selected test. The application server receives the test results and stores them in the database 320 where they may be accessed by the web server to be presented to the operator via the GUI. Otherwise, the application server sends instructions to the appropriate test tool, the Layer 2, 3 Domain Manager, or the appropriate network Element Manager, according to the workflows, and invokes the desired test. The test tool, Layer 2, 3 Domain Manager or the network Element Manager, as the case may be, accesses the appropriate network element and performs the required test. In either case, the test results are returned to the application server, and incorporated into the GUI pages served to the operator via the web server 324. Since the application server has access to all network elements in the service delivery chain, either directly or through the intermediary test tools layer 2, 3 domain manager or network element managers, the end-to-end test and diagnostic manager can provide complete end to end coverage of the service delivery chain. A workflow can also define the sequence of elementary test tools to be executed in order to perform a more complex diagnosis. The single test results are used by the test manager as a trigger to follow a specific workflow.

While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible within the scope of the invention. Accordingly, the invention is not to be restricted except in light of the attached claims and their equivalents.

CLAIMS

1. A system for troubleshooting service delivery problems for services delivered over multi-domain networks wherein the multi-domain networks include network components necessary to deliver a service, the network components having at least one of an operational status and a configuration, the system comprising:

a plurality of test tools (318) for learning at least one of the operational status and configuration of network components necessary to deliver a service to a customer;

a test manager (300) having access to network and service inventory data including data relating to services delivered to customers and the network components necessary to deliver the services, the test manager including workflows for selectively invoking test tools in response to specific service delivery problems to test the operational status and verify the configuration of network components necessary to deliver a specified service; and

a graphical user interface (GUI) for displaying results of the selectively invoked tests.

2. The system of Claim 1 wherein the network and service inventory data include service plans subscribed to by customers.

3. The system of Claim 1 wherein the network and service inventory data include data describing service equipment at a customer's premises and under the customer's control.

4. The system of Claim 1 wherein the network and service inventory data include identification of essential network elements and components for all domains necessary to deliver a particular service to a particular customer.

5. The system of Claim 1 wherein the test manager (300) further includes a database adapted to pull information from operations support systems (304) in the service delivery environment, including the network and service inventory data in order to perform the necessary tests to diagnose a service delivery problem across all network domains involved in delivering the service.

2

6. The system of Claim 5 wherein the database is adapted to pull data from a field access system (328) to perform a final check of service restoration, the field access system (328) accessing the test manager from a technician's mobile terminal at a customer's premises.

7. The system of Claim 5 wherein the database is adapted to pull data from an LDAP (Lightweight Directory Access Protocol) (330) to perform an information exchange to authorize user accesses.

8. The system of Claim 5 wherein the database is adapted to pull data from an integrated order management system (332) to gather information about the status of a work request concerning a customer claiming a service interruption.

9. The system of Claim 5 wherein the database is adapted to pull data from a network trouble management system (334) to manage customer complaints on a network delivered service and to gain details from a related trouble ticket.

10. The system of Claim 5 wherein the database is adapted to pull data from a fault management system (336) to open an alarm when a problem is found and to provide information about impacted customers

11. The system of Claim 5 wherein the database is adapted to pull data from a service delivery platform (338) to gather service and user profile information.

12. The system of Claim 5 wherein the database is adapted to pull data from a performance management system (340) to check for degradation in the network components involved in delivering a service to a customer.

13. The system of Claim 1 wherein the test manager is adapted to provide data gathered from the selectively invoked test tools to external operations support

3

systems (304) to support the specific processes managed by the external operations support systems.

14. The system of Claim 1 wherein said plurality of test tools comprise stand alone test tool packages adapted to test network elements in specific network domains.

15. The system of Claim 1 wherein the capabilities of said plurality of test tools are provided by network element managers having access to specific network elements' configuration data and which are capable of testing the specific network elements' operational status.

16. The system of Claim 1 wherein the capabilities of said plurality of test tools are provided by a layer 2, 3, domain manager.

17. The system of Claim 1 wherein the capabilities of said plurality of test tools are included as internal test modules within the test and diagnostic manager.

18. The system of Claim 1 wherein said plurality of test tools comprise a combination of stand alone test tool packages, network element managers, a layer 2, 3 manager, and internal test modules within the test and diagnostic manager.

19. The system of Claim 1 further comprising a user profile database (322) for storing user profiles and access privileges.

20. The system of Claim 1 further comprising an application server (326) adapted to execute established workflows for invoking said test tools.

21. The system of Claim 1 further comprising a web server for serving GUI pages to a user.

22. The system of claim 1 wherein the test manager (300) further includes an internal database (320) for storing results from the selectively invoked test tools.

4

23. An end-to-end test and diagnostic manager (300) adapted to test network components and diagnose service delivery problems for services delivered over multi-domain networks, the test and diagnostic manager comprising:

a graphical user interface for displaying status and diagnostic data regarding networks, network components, and services to an operator and for receiving commands from an operator; and

an application server (326) having access to network and service inventory data such that upon receiving a report of a service delivery problem the application server may determine the services delivered to a customer and the networks and network elements necessary to deliver the services to the customer, the application server being adapted to execute workflows to selectively invoke one or more test tools (318) to determine operational status and configuration data of the network elements necessary to deliver a service to a customer to determine the cause of the service delivery problem and display the results via the graphical user interface.

24. The end-to-end test and diagnostic manager of claim 23 wherein the test tools comprise any combination of tools taken from the list comprising: CPOMS Ping Test; Sync Profile; Port verification; Port Lock/Unlock; No Sync Test; Port Reset; IP Ping Testing; Test Call; Call History; End-To-End VoN Service; and End-To-End BB Service; MLT (Mechanized Loop Testing).

25. The end-to-end test and diagnostic manager of claim 23 wherein the application server (326) is adapted execute one or more test tools directly.

26. The end-to-end test and diagnostic manager of claim 23 wherein the application server invokes an external test tool associated with a network domain and the external test tool is adapted to test the network elements within the associated domain.

27. The end-to-end test and diagnostic manager of claim 23 wherein the application server invokes test tools via a layer 2,3 domain manager (320).

5

28. The end-to-end test and diagnostic manager of claim 23 wherein the application server (326) invokes test tools (318) via element managers associated with the network elements to be tested.

29. The end-to-end test and diagnostic manager of claim 23 further comprising a web server (324), the graphical user interface comprising a web based graphical user interface having interface pages served to a client terminal associated with an operator.

30. The end-to-end test and diagnostic manager of claim 29 further comprising a user profile database (322) for storing user profiles defining access rights test privileges of operators permitted to use the end-to-end test and diagnostic manager.

31. The end-to-end test and diagnostic manager of claim 23 wherein the database has access to operational support system (304) whereby additional data relevant to service may be received and stored on the database and presented to an operator via the interface.

32. The end-to-end test and diagnostic manager of claim 23 wherein the application server is configured to invoke test tools for testing the operational status of every network component involved in delivering a service to a customer and the actual end-to end delivery of the service.

33. A method of diagnosing service problems in services delivered via layered, multi-domain network environments, comprising,
receiving a report (250) of a service problem from a customer;
gathering information (252) regarding all components (network elements and applications) necessary to deliver the service to the customer;
remotely testing (254) the possible components having problems in order to identify the root cause of the service problem;
resolving remotely the problem (256) ; and
performing a remote end-to-end test (258) to ensure the service has been restored.

ABSTRACT

An end-to-end test and diagnostic manager and a method of diagnosing service problems in a multi-domain, multi-service network are provided. A database receives and stores service and network inventory data identifying and describing the customer and the network components necessary to deliver a service to the customer over a multi-domain network. An interface for displaying service information to an operator and for receiving commands from an operator is also provided. A plurality of test tools for testing operational status and verifying the configuration of components necessary to deliver the service to the customer. An application server is configured to execute instructions for invoking the test tools. The results of the test are displayed for the operator via the interface.

FIG. 1

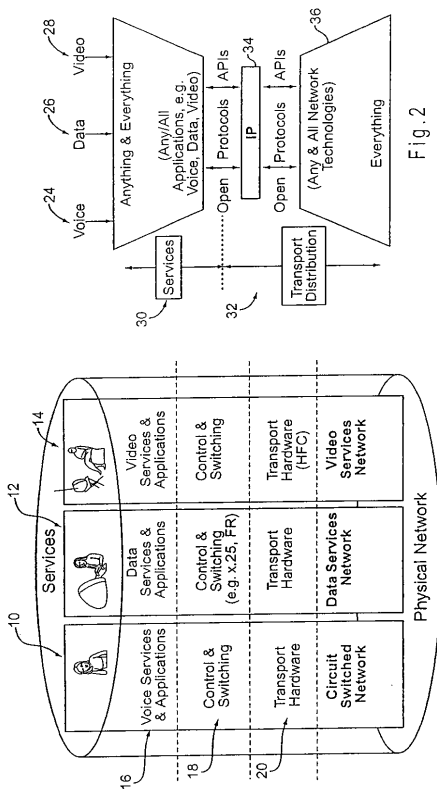


Fig. 1

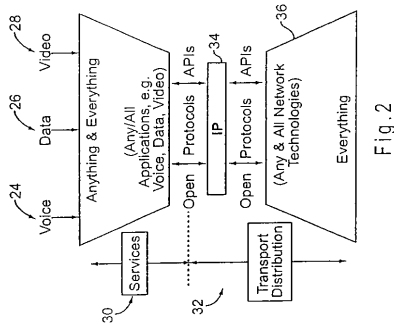


Fig. 2

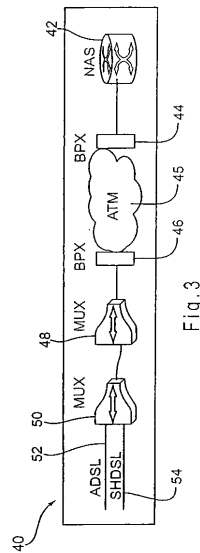


Fig. 3

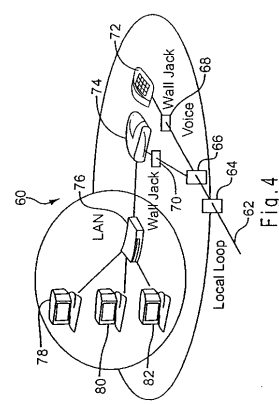


Fig. 4

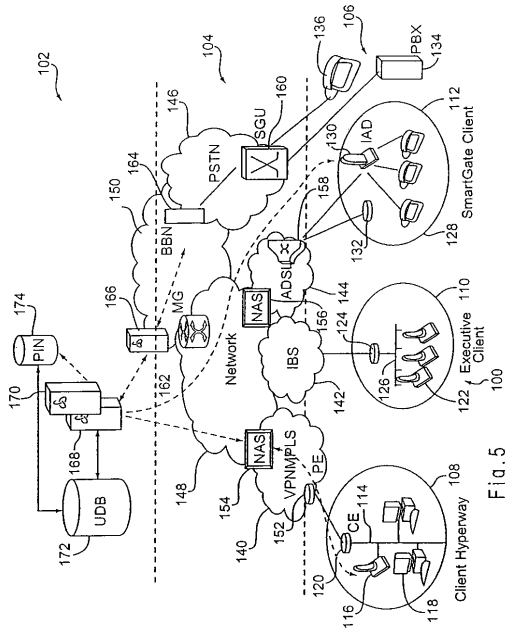


Fig. 5

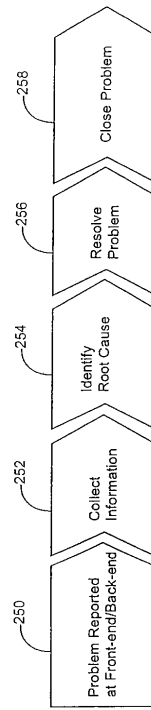


Fig. 6

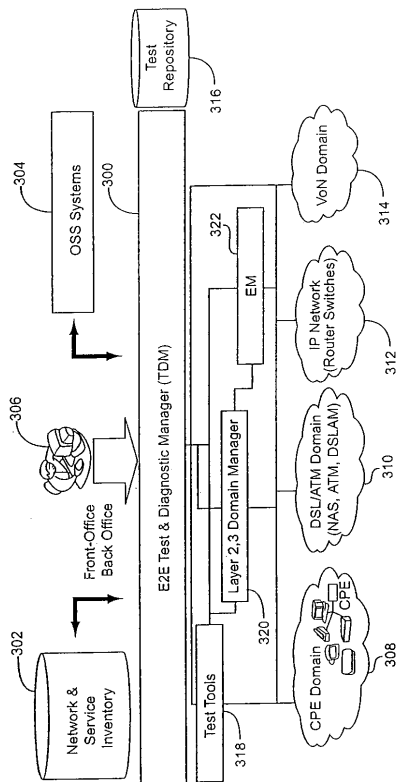


Fig. 7

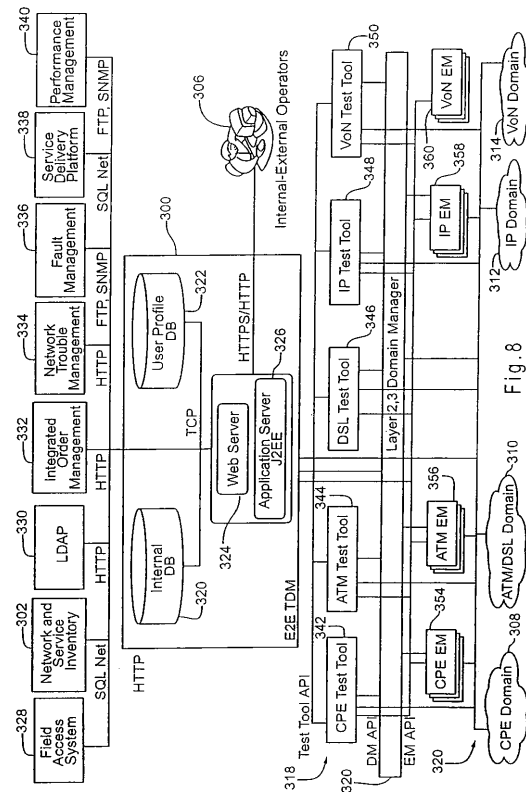


Fig. 8

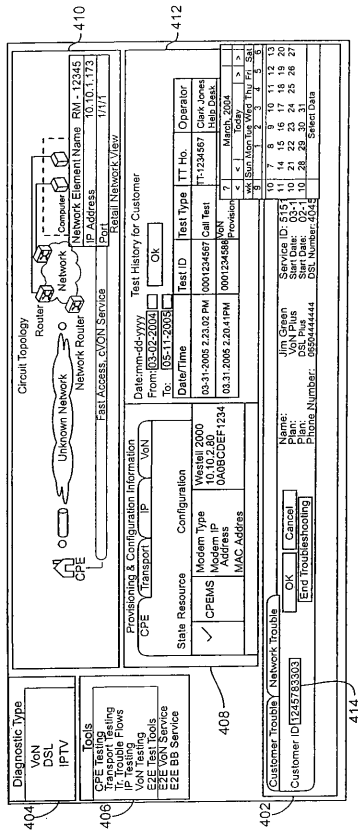


Fig. 9