

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010631 A2

- (51) International Patent Classification⁷: **H04L**
- (21) International Application Number:
PCT/US2003/022654
- (22) International Filing Date: 21 July 2003 (21.07.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/397,109 19 July 2002 (19.07.2002) US
- (71) Applicant: **MASERGY COMMUNICATIONS**
[US/US]; 600 East Las Colinas Boulevard, Suite 134,
Irving, TX 75039 (US).
- (72) Inventors: **FILES, Kirby**; 158 Cameron Station Boule-
vard, Alexandria, VA 22304 (US). **HABERMAN, Ron,**
E.; 10359 Sager Avenue, #303, Fairfax, VA 22030 (US).

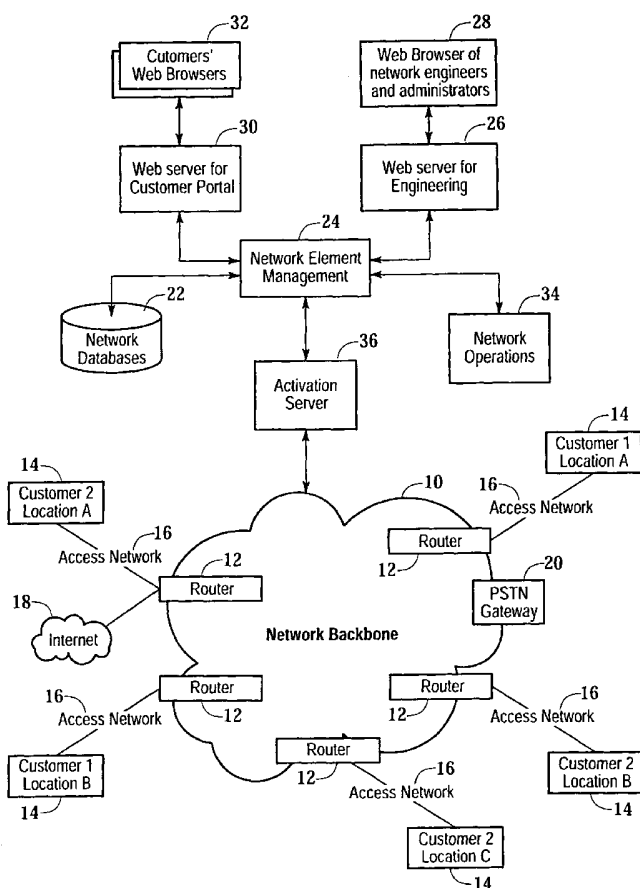
SMITH, Klyne, L.; 8115 Saxony Drive, Annandale, VA 22003 (US). **KRICKUS, Karen, E.**; 1900 East Franklin Street, #210, Richmond, VA 23223 (US). **ROUILLER, Guy, J.**; 310 Hillmoor Drive, Silver Spring, MD 20901 (US). **STEELE, David J.**; 4473 Shady Point Place, Chantilly, VA 20151 (US). **COLLINS, Jason, H.**; 5524 Callander Drive, Springfield, VA 22151 (US).

(74) Agents: **HUBBARD, Marc, A.** et al.; Munsch Hardt Kopf & Harr, P.C., 4000 Fountain Place, 1445 Ross Avenue, Dallas, TX 75202-2790 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: AUTOMATED CONFIGURATION OF PACKET ROUTED NETWORK



(57) Abstract: Detailed configurations for specific network elements are automatically generated and, if desired, automatically activated in response to an addition, modification and/or deletion of a network service or topology specified at high level. Network configuration information is stored in a database. Metadata, including descriptions of network elements, properties of network elements and relationships between network elements, is used to describe network elements, is used to describe network topologies. Data fields described the metadata store current configuration data for each network element.



(84) **Designated States (regional):** ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AUTOMATED CONFIGURATION OF PACKET ROUTED NETWORK**TECHNICAL FIELD OF THE INVENTION**

The invention pertains generally to provisioning of packet routed networks.

BACKGROUND OF THE INVENTION

With the availability of various types of network engineering and quality of service (QoS) mechanisms, packet routed networks, in particular those using the Internet Protocol, are increasingly being used to implement wide area networks that provide differentiated, end-to-end transport services. Such networks have several advantages. As compared to other types of networks, such networks can handle differentiated traffic relatively efficiently. They are also relatively inexpensive to build and can be run over heterogeneous infrastructures.

SUMMARY OF THE INVENTION

Configuring network elements in a packet routed network can however be a relatively complex task, especially when a network is comprised of heterogeneous types of equipment from different vendors.

The invention has as a general objective reducing the complexity of changing configurations in individual network elements in packet routed networks for purposes of adding or changing logical links or topologies, specifying bandwidths, and adding, changing or deleting the types of service run over links. Reduced complexity not only reduces burdens on network engineers, administrators and operators in making changes, but also enables, if desired, customers or users of services on such networks to undertake at least a certain level of provisioning, with little to no intervention by those who operate the network.

Various aspects and features of the invention, in their preferred embodiments, are described below with reference to an exemplary network element management system implementing them. Some of these aspects are briefly summarized below, with the understanding that the summary is not intended to limit the scope of the invention as claimed.

According to one aspect, detailed configurations for specific network elements are automatically generated and, if desired, automatically activated in response to an addition, modification and/or deletion of a network service or topology specified at high level. Examples include, but are not limited to, a new or changed point-to-point link and/or bandwidths and service treatments (e.g. a specified quality of service) on those links.

A customer or other user of a network may thus be permitted to add, drop and modify their own network topology and services relatively frequently, as conditions or its needs change, without the

customer having direct access to the network elements. In other words, they may be permitted to take care of at least some of the network provisioning. A customer could, for example, specify a new link between two sites, having a certain bandwidth for voice traffic and a certain bandwidth for priority data traffic. The link could be implemented by establishing, for example, a label switched path through the network using MPLS, and configuring QoS mechanisms in affected routers treat traffic according to the selected service levels.

According to another aspect, the service changes could be specified interactively through, for example, a web portal, with the configurations being automatically generated and activated on affected network elements. For customers, a Web portal may also include lists of current services, traffic statistics for those services, and other information (e.g. account and billing). A customer is thus able to monitor traffic in addition to relatively easily changing network topology and services to meet its requirements.

According to another aspect, network configuration information or data is stored in a database using a vendor-independent schema, and actual configurations generated and transferred to network elements using this information. The network configuration information is not the specific data stored on the network elements or devices. Rather, information necessary for configuring specific network elements or devices is stored. Preferably, each type of network element is modeled or defined using a metadata language that defines each type of network element in terms of configuration data fields, properties, and/or relationships to other elements. The metadata thus specify what configuration data or other information is stored for each specific type of element.

According to yet another aspect, logic specific for each type of network element and service to be implemented on the device populates the actual configurations with data from the database. A generic configuration template, containing fixed or unchanging text, forms a basis for the configuration prior to populating it with data. Instructions implementing this logic are preferably specified at a relatively high level using an interpreted script language that can be easily learned and used by non-programmers. Changes in the logic can thus be easily implemented without changing the programming code of a software engine that executes the logic by reading the script. The logic preferably also indicates how to activate the configuration.

The invention is described below, with reference to the accompanying drawings, with respect to an exemplary network element management system implementing various aspects and features of the invention in its preferred embodiment. The invention is not, however, limited to this specific example.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a packet routed network and a network element management system for generating configurations for elements in the network.

FIG. 2 is a flow diagram of steps in a process for adding, modifying or canceling services on a packet routed network.

FIG. 3 is a flow diagram of steps for a process of auditing configurations of network elements.

FIG. 4 is a schematic representation of the database schema for databases used in the network element management system of FIG. 1

FIG. 5 is a flow diagram of a process for generating a device-specific configuration in response to a request to add, modify or delete a specific service, using activation scripts and templates

5 FIG. 6 is a flow diagram of the basic steps of defining an activation script for a new type of service for a network.

FIGS. 7-13 are screen shots of an example of a customer portal for specifying additions, modification and deletions to network services and links.

DETAILED DESCRIPTION OF THE DRAWINGS

10 In the following description, like numbers refer to like elements.

Referring to FIG. 1, network 10 is a representative example of a backbone network 10 in which packets are routed. The network includes a plurality of edge routers 12, in addition to core routers, which are not shown. The routers are intended to be representative generally of elements in the network. Other network elements might include switches, network interfaces, and other equipment depending on the types of link layer networks used. Although multiple different types of link layers can be used, the backbone network can also be comprised of a homogeneous infrastructure. As an example only, a plurality of customer sites 14 are shown connected to backbone network 10. Although the invention contemplates a service provider operating the network and selling services to third parties, the invention could be deployed in a wide area network operated by an enterprise, with various constituencies within the enterprise being, in effect, customers of the network. Thus, "customers" will refer to any type of consumer of network services, unless the context indicates otherwise. The sites connect to edge routers 12 on backbone network 10 through access networks 16. The access networks may be, for example, a single TI or frame relay line, or an Ethernet connection. Customers may use backbone network 10 to create a wide area network connecting multiple sites, as shown, to connect to Internet 18, the public telephone switched networks (PSTN) through gateway 20, and/or to other networks, and/or for other purposes. These are just examples of network elements that may be present in such a packet routed network.

For example, the network may allow for private links to be set up or changed between customer sites, thus permitting a logical network topology to be established for a customer and changed. Various types of transport services may be offered or implemented by backbone network 10. It may also have predefined tiered service planes, with different quality of service. Examples of such service planes are normal or best effort for lowest priority traffic; priority data for data applications, with traffic being classified low, medium or high; reserved bandwidth for critical data applications that require assured bandwidth; video, with reserved bandwidth with videoconferencing-quality latency, jitter packet delivery; and voice, with reserved bandwidth with voice-quality latency, jitter and packet delivery. For each of these services a customer may specify parameters, such as a bandwidth for those services with reserved bandwidth and the customer's sites between which the service will be offered. These are just examples

that will be referenced in the following description. A network operator may define fewer or more service tiers. Additional services may also be offered.

Information, including configuration data, for one or more of the network elements in backbone network 10 and/or access networks 16 is stored in network databases 22 of network element management system 24. In a preferred embodiment, configuration data does not consist of the complete configuration files stored in each of the network elements. Rather, it is data that is defined to be stored on each network element in the network. Database 22 is representative of one or more databases, which may be distributed and which may also exist in multiple instances. Preferably, and in the example given below, the network databases store information on the entire network. However, they could just store information on subnets or parts of the network, depending on the purpose for which they are used.

The network element management system 24 represents one or more software controlled processes on one or more programmable computers. In the preferred embodiment, it represents several different software controlled processes for implementing different functions, tied together with core logic. However, the software controlled processes may be implemented in different processing entities. It is therefore not limited to any particular implementation, and any reference to the network element management system should not necessarily be construed to be a reference to a system implementing all of these functions.

One of these functions is creating, accessing and modifying information on the network stored in the network databases 22, including configuration data for network elements. The logical structure for implementing this function may be referred to as a database engine, and be implemented separately from the core logic of the system as software controlled processes.

Another function, which is described in greater detail below, is generation of specific configurations for network elements based on relatively high level information specifying a service or other network function, which high level information is provided by a user. The logic for this function, preferably implemented using software executing on a computer, may be referred to herein specifically as a configuration generator.

Personnel may have access to network element management system for purposes of generating configurations, as well as for updating the network databases 22 or other logic contained in the system. This may be done, for example, through web server 26 and a web browser 28, though other access methods can be used, giving direct access to the network element management system, or modules or components thereof, with access to network databases 22. Multiple instances of the network element management system can also be run. Similarly, network operations 34, which may be individuals or programs used in network operations, may have access to the network configuration information for purposes of obtaining information on current network topology, as well as automatically generating configurations in network elements for traffic monitoring or other purposes. Although not shown, network operations personnel may have access to the network element management system 24 through a web portal or other user interface, preferably a graphical one for simplicity of use.

In the preferred embodiment shown, customers or users of network services may indirectly access the network element management system through an interactive portal available on web server 30 using web browsers 32 executing on the customers computers. Though this portal is a preferred method for providing access, other methods can be used, including client applications executing on the customers computers or even instances of the network element management system or one or more of its components. The portal allows customers to add, modify or delete services. Services are specified at a high level, preferably in reference to predefined services. For example, a customer may add a link between two of its sites by specifying the two sites and a service plane. Examples of predefined service planes include the examples given above: normal, priority, reserved bandwidth, voice or video. One or more parameters can be specified, such as bandwidth, whether the link is shared or reserved, and priority levels. Access speed or bandwidth tiers could also be specified for the customer's access network or line. Enhancements for the services could also be specified. The portal could also be used to provide a summary of the customer's services and usage statistics and billing and account information. For purposes of the example described herein, the software controlled processes for interacting with the web server is included in the network element management system 36, though it could be separated.

A single instance of the network element management system could be used for interacting with both network engineering and the customer and executing the activation function. However, it is preferred that a separate instance, referred to as the activation server, execute activation of new configurations in network elements in order to provide much stricter access and tighter security, and additional logging and auditing. Other instances of the network element management system can be provided for use by network engineering, administration and operations. Activation server 36 is, in the preferred embodiment, a second instance of the network element management system, or at least certain processes of the network element management system, that permit it to generate configurations using data or information supplied by a customer, or network engineering or operations, which then activates on network elements. The logical and physical elements for this activation function may be referred to herein as an activation engine or mechanism and are implemented preferably as software controlled computing processes executing, for example, on a computer.

Once generated by the activation server, configurations are then communicated to network elements using any available communication mechanism for that network element. Examples of such mechanisms include FTP, Telnet, and SNMP. The exact method of communication and update or changing configurations depends at least in part on the specific network element involved. The activation engine enables all changes to be made consistently across the network, preferably with comprehensive logging. The configurations may relate not only to service activation, but also application of security policies and network maintenance, including collecting performance monitoring information to give to a customer or network operations. The activation server may thus be used by those who run the network for tracking and configuring network elements

Referring now also to FIG. 2, an exemplary process flow 38 for a service addition, modification or cancellation starts with receiving a request for service addition, modification or deletion at step 40. If the request comes in through an interactive portal, such as web server 30 for customer portal 30 or the web server for engineering 26, or directly from an instance of the network element management system 24, it is handled by logic that specifies how each type of service request is to be handled. The logic may be implemented as instruction scripts and stored as part of the network databases 22. For purposes of this description, the logic will be treated as part of network element management system 24 or activation server 36. In the illustrated example, service requests are passed to the activation server 36. The location of execution of the logic depends on the particular implementation and is not critical. Indeed, it may take place in multiple places. The logic determines at step 42 which network elements are affected by the change, relying on information in network databases 22 for making this determination. Some service requests may only affect devices on the edge of a network and others may affect core devices.

At step 46, the logic generates configurations for each affected network element. The term "configuration" does not necessarily refer to the entire configuration of a network device. Rather, it may also refer to a configuration of a particular feature or set of features, or incremental changes to the configurations such as a new logical interface or access list of a router. The entire configuration of the element need not be regenerated, unless required by that particular element.

In a preferred embodiment, a configuration is built from predefined template fragments and populated using configuration data taken from the network database 22. This data may include specific configuration data for each element, including data provided by the party requesting the service addition, modification or deletion (e.g. bandwidth and other service parameters).

It is also preferred to use a script to, at least in part, define the logic or process by which a configuration is generated and/or activated on the network element. Use of a script and predefined templates fragments permits new services and equipment to be added without requiring software to be modified and recompiled. Scripts can be created by non-programming network engineers administrators to define steps at relatively high level. Use of configuration data and script permits the network element management system to be neutral or independent of the particular requirements of a piece of equipment, as those requirements can be handled in the scripts and/or template fragments. For an operator of a network, this permits vendor-independence. Equipment from different vendors can therefore be supported by the network. Furthermore, the scripts may make use of abstract network topology or connectivity data stored in the database, which enables creation of logic for generating a configuration that is independent of specific network topology. New types of equipment can be added, or equipment changed, relatively quickly.

If desired, the activation can be queued for later execution. All outstanding configuration activations could be run at the same time, such that a networks configuration only changes once a day, for example. However, the service activation could also be executed quickly, appearing in effect in "real time" once the request is made.

Before a configuration is activated on a network element, it is checked at step 48 to make sure that it is generally consistent with the configuration of the network. This verification step relies on network configuration data in network databases 22, and reduces the risk that the new configuration inadvertently is inconsistent with the configuration of the network. Once verification is made, step 50 involves updating the network databases with data on the new configurations. The activation server then downloads or communicates the new configurations to the affected network elements at step 52, and then checks the configurations of the network elements to determine that they have correctly loaded at step 56.

With the process shown in FIG. 2, a person with no or little knowledge can implement service requests, with little or no intervention by a network engineer or administrator. For a customer of transport services, service additions, modifications and cancellations can be made relatively quickly, perhaps even in real time, without direct access to the network elements. The customer requests service modification, addition or deletion, a new configuration is automatically generated for the affected network elements and then automatically activated in the network elements.

FIG. 3 is a flow diagram of an auditing process 58 that confirms that the configurations of the network elements are consistent with the configuration data stored in network databases 22 (FIG. 1). This process is, in the example, executed by the activation server 36 (FIG. 1), but it could be implemented as a separate process. Unlike other auditing processes, which simply read configurations out of each network element and compare them line by line to a stored configuration to detect any changes or corruption, audit process 58 compares the configurations in the network elements to data on the configuration stored in network database for that network element. That data stored in the network database is stored in multiple fields. Logic is used to extract from the configurations the values that correspond to the data values stored in the network database. Thus, at steps 60 and 62, which can be executed in any order, the audit process reads the configuration from the network element and looks up device-specific audit logic in the database. This audit logic is, in the example, stored in the network databases 22 as a template or script. Step 64 involves identifying the fields or data values in the configuration that map to fields in the network databases that store configuration data for the particular device. The data values are then compared at step 66. Exceptions can then be generated for investigation.

Referring now to FIG. 4, in the preferred embodiment, metadata is used to describe or model network elements and the topology of a network, such as network 10 of FIG. 1, at an abstract level. This metadata is then used to define the schema with which actual data, including, but not limited to, what is referred to above as configuration data, for actual elements in the network is stored. This data on the elements actually present in the network may also be referred to herein as network element inventory data or network inventory data. The metadata is preferably written using a language that is easily understood or learned by network engineers and administrators. Metadata model 68 is a very simple example intended only to illustrate and explain the concept and relationship between the metadata description or model of the network and data records, such as configuration data records 70. Both the metadata description or model and the configuration data records would be, in the preferred embodiment of FIG. 1,

stored in network databases 22. The network element management system 24 would rely on the metadata in generating and activating configurations. Thus, changes to a network in terms of new types of services or elements can be relatively easily added without having to change any software. Fields of configuration data required are specified using the metadata and simple scripts can be written with reference to the metadata to specify how the configurations are generated and activated. No changes to the programming code are required.

Metadata includes entities designated as "meta_elements", three of which are identified by reference numbers 72, 74 and 76 in the example. Associated with each of the meta elements are "meta_properties" and/or "meta_fields". In the illustrated example, meta_element 72 has associated with it meta_properties 78, and meta_element 76 has associated with it meta_fields 80. The meta elements may be related to each other using "meta_element_relation" objects. These specify a relationship between elements. Meta_element_relation 82 relates meta_element 72 to meta_element 74. Similarly, meta_element_relation 84 relates meta_elements 74 and 76. Preferably, meta_element_relations may not only specify the existence of a relationship, but also its nature. For example, it is preferable to be able to define a relationship as being a parent-child, a sibling or a peer relationship.

Thus, for example, the metadata describes how to define a network element, such as a router. Furthermore, it provides an abstract description of a network's topology, with relationships between the different types of network elements. As an example, a particular type of router from a particular vendor may be defined as a meta_element. This type of router may be able to accept different types of physical network interfaces. Each network interface could be a separate meta_element with a parent-child relationship with the router meta_element. The meta_element for the router might then be a child to a meta_element defining a network, or a subnet.

Examples of meta_properties include, but are not limited to, captions or information shown in user interfaces, help strings that would be displayed in user interfaces, whether or not meta element has a template, whether or not it is a connectable type of element, whether or not the element has been accepted by operations, whether the device is activated, and which version of the metadata the device is operating off of. Examples of meta_fields include, but are not limited to, framing, encryption settings, the name of a logical interface, a name of device, its serial number, routing information, information for QoS mechanisms, and whether it is under maintenance contract. Thus, any type of data could be specified to be stored, including not only data need for generating configurations, but also data for use in operations.

Configuration data records 70 include data for actual network elements. The data schema for these records map to the metadata definitions for the type of network element. Thus, records 86, 88 and 90 have structures that map, in the given example, to meta_elements 72, 74 and 76, and have relationships 92 and 94 specified by meta_element_relations 82 and 84. The configuration data records are used in generating actual device configurations.

Multiple, different instances of metadata models of the network and network elements and instances configuration data can be stored if desired, with one model and instance of configuration data being active.

FIG. 5 illustrates a process 96 by which new or modified service request is activated by the network element management system 24 or 36 using a script. The scripts, which in a preferred embodiment will be called activation scripts herein, specify the logic for translating service requirements into configurations and deployment. Scripts further permit modularization of the service activation logic. Such modules may be referred to as script objects.

At step 98, after a service request is received, objects and fields for the requested service are added and/or updated in the network inventory stored in the network database 22 (FIG. 1). Information on each specific service provided to a user or customer of network is preferably stored prior to the service being activated. The network equipment affected by the change is determined at step 100 and, as indicated by steps 102 and 110, steps 104, 106, and 108 are repeated for each device.

At step 104, script objects are retrieved from a library of such objects based on the type of device, its vendor and its role. Script objects are device and vendor specific scripts that may be used by a new service script. Abstract network topology information, or more generally, abstract connectivity/relationship information, for the affected network device or element is obtained at step 106. This information is preferably from a metadata model of the network. This data specifies how network elements are, at an abstract level, connected and work together. The scripts can therefore be written without knowing the specific network topology, and changes to network topology made without having to rewrite scripts.

Step 108 involves building a device-specific configuration from a library of template fragments, the abstract connectivity/relationship information and the network inventory data for the specific device and service. The configuration may be a partial or full configuration. The necessary template fragments, which are predefined configuration text stored in a database such as network database 22 (FIG. 1), are selected by the script, assembled into a template and populated with the device and service specific network inventory data. The fragments preferably include tokens that act as place holders for the specific data to be inserted. The population of the templates may be performed in two steps, with the second step involving populating the template with global network inventory data common to all configurations using a standard script objects. After the configuration for an affected device is generated, it is communicated at step 112 to the device. After communication, the new configuration is validated. It is preferable that configurations for all affected devices be generated prior to communicating them to any of the devices.

In sum, the templates and activation process are preferably data-driven. That is to say, none of the configurations, network configuration data, script logic is inherent in the software for the network element management system. It is stored in and retrieved from a database, such as network database 22, using metadata. Software for the network element management system can thus be made vendor-neutral, with

scripts specifying the vendor- and product-dependent configuration logic. The addition of a new service thus requires no changes to the management system software.

FIG. 6 illustrates basic steps of a process 114 for adding a new type of service to a network managed by the network element management system using activation scripts. At step 116 logic for selecting equipment affected by an addition, modification or deletion of the service for a specific customer is specified. Processes for storing and retrieving data on the connectivity/relationships of network elements is specified at step 118. This data is, as previously mentioned, the metadata used to create an abstract definition of the network. Step 120 involves defining logic for translating abstract network connectivity/relationship information or data and network inventory data into a vendor-dependent configuration for each affected device. The final basic step 122 includes defining how the configurations are to be communicated to the affected network devices and validated.

FIGS. 7-13 are examples of interface screens 124 for a customer web portal, through which a customer may provision for itself services on a network, such as network 10 of FIG. 1. Generally, these screens are self-explanatory and are intended to be merely examples. Provided below are brief descriptions of them.

FIG. 7 is a "home" screen. It includes a list form which a customer may select other screens to modify its services, analyze its own network activity, or view billing information, among other things.

FIG. 8 is a screen shown summarizing the services of a particular customer. The customer in this example has three sites. Under each site are listed is a basic service for the sites access circuit, including the type of access circuit and the type of service offered over that circuit. For example, the first two sites have a T3 line and the third has a OC3 line. The types of services that are listed include basic IP service, labeled "inControl IP", priority service (labeled "inControl Link"), voice and video (labeled "inControl Voice" and "inControl Video", respectively). These are examples only. Many other predefined services could be made available to a customer to chose from.

FIG. 9A is a screen that is displayed following selection of service 126 in FIG. 8, which has a service ID of "MS000020". FIG. 9A allows a customer to select a different tier or bandwidth for the access circuit, enable/disable priority bursting (i.e. allowing the bandwidth to be exceeded for priority traffic) on the access circuit, select whether the circuit is shared or dedicated, and add QoS services for priority, voice or video. As an example of how a service is added, FIG. 9B is the first screen of a process for adding the priority service for the customer site. It allows another of the customer's sites to be specified using a drop down menu. Once a second site is selected, a new screen, shown in FIG. 9C, is presented. WAN IP addresses for the two sites are specified, as well as the CSIR, service plane, and a billing option. Billing options may include, for example, metered and flat rate billing options. FIG. 9D is a summary page for the change.

FIGS. 10A is an example of a screen by which a customer may add voice service at a particular site. The customer specifies a bandwidth cap, a contract term and a billing option in the example. FIG. 10B summarizes the new service before it is submitted. The screen in FIG. 11A allows modification of

the added voice service. Modification of the bandwidth cap and the billing option previously specified are available, as well as an option to cancel the services. Phone numbers may also be added, modified, or deleted. A private dialing plan may also be available for management. This allows private telephone numbers to be used between the customer sites. FIG. 11B shows the screen for modifying the bandwidth cap. FIG. 11C shows the screen for adding telephone numbers.

FIG. 12 is a screen for modifying a previously added priority service between two sites. A drop down lists for type of priority (e.g. low, medium, high or reserved) and CSIR are available for a customer to select from. A billing option may also be specified using a drop down list.

FIG. 13 is a screen for generating a report on traffic for each of the services on a particular access circuit, allowing a customer to determine whether any of the settings for any of the services should be modified, whether any should be dropped, or whether any should be added.

Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware and application logic. If desired, the different functions discussed herein may be performed in any order and/or concurrently with each other. Furthermore, if desired, one or more of the above-described functions may be optional or may be combined without departing from the scope of the present invention.

WHAT IS CLAIMED IS:

1. A method, comprising:

receiving a service request for adding, modifying or canceling a packet transport service having defined service levels of one or more packet networks; and

5 automatically generating configuration data for one or more of a plurality of network elements of said one or more packet networks necessary for implementing the service request.

2. The method of claim 1, further comprising automatically determining which of the plurality of network elements will be affected by the service request.

10

3. The method of claim 1, wherein automatically generating configuration data includes generating confirmation data based at least in part on data from a network database storing current configuration data for said one or more network elements.

15

4. The method of claim 1, wherein automatically generating configuration data further comprises automatically generating said configuration data based at least in part on a predefined script.

5. The method of claim 1 wherein generating configuration data includes populating predefined templates with data from a network database storing configuration data on the one or more
20 network elements and new configuration data based on the service request.

6. The method of claim 5, further comprising running one or more automated routines for automatically populating the templates with data from the network database and the new data.

25 7. The method of claim 1, further comprising verifying that said configuration data is consistent with a configuration of said one or more packet networks.

8. The method of claim 1, further comprising updating a network database, storing configuration data for said one or more network elements with said generated configuration data.

30

9. The method of claim 1, further comprising automatically updating a configuration of said one or more network elements based with generated configuration data.

10. The method of claim 9, further comprising verifying that said updated configuration of
35 said one or more network elements is consistent with configuration data, for said one or more network elements, stored in a network database.

11. The method of claim 10, wherein said verifying step comprises:
retrieving said configuration data regarding said one or more network elements from said network
database;

identifying one or more fields in said updated configuration of said one or more network
5 elements; and

comparing values of said one or more identified fields with values of corresponding fields in said
retrieved configuration data.

12. The method of claim 11, further comprising generating an exception in response to said
10 values of said one or more identified fields not matching said values of corresponding fields in said
retrieved configuration data.

13. A method for generating a network element specific configuration, comprising:
receiving a request for adding, modifying or canceling a service on one or more packet networks;
15 updating, upon receiving said request, one or more corresponding objects for said service in a
network database comprising of network element inventory data for a plurality of network elements of
said one or more packet networks;

determining which ones of said plurality of network elements are affected by said request; and
automatically generating configuration data, for each of said one or more affected network
20 elements, from at least said network element inventory data and one or more of a plurality of template
fragments comprising predefined configuration text.

14. The method of claim 13, further comprising retrieving one or more selected script objects
from a plurality of script objects, each of said selected script objects specifying a network element
25 specific script for a corresponding one of said one or more affected network elements.

15. The method of claim 14, further comprising obtaining abstract connectivity information
for each of said one or more affected network elements from said network database.

30 16. The method of claim 15, wherein said abstract connectivity information specifies a
manner of connection between said one or more affected network elements.

17. The method of claim 16, wherein said automatically generating configuration data further
comprises:

35 selecting said one or more of said plurality of template fragments; and
assembling said selected template fragments into a template.

18. The method of claim 17, further comprising populating said assembled template with said network element inventory data.

19. The method of claim 13, further comprising communicating said configuration data to
5 each of said one or more affected network elements.

20. The method of claim 19, wherein said automatically generating step is performed prior to said communicating step.

10 21. Computer readable media storing instructions that when read a computer enable the computer to undertake a method comprising:

receiving a service request for adding, modifying or canceling a packet transport service having defined service levels of one or more packet networks; and

15 automatically generating configuration data for one or more of a plurality of network elements of said one or more packet networks necessary for implementing the service request.

22. The computer readable media of claim 21, wherein the method further comprises automatically determining which of the plurality of network elements will be affected by the service request.

20

23. The computer readable media of claim 21, wherein automatically generating configuration data includes generating confirmation data based at least in part on data from a network database storing current configuration data for said one or more network elements.

25

24. The computer readable media of claim 21, wherein automatically generating configuration data further comprises automatically generating said configuration data based at least in part on a predefined script.

30

25. The computer readable media of claim 21, wherein generating configuration data includes populating predefined templates with data from a network database storing configuration data on the one or more network elements and new configuration data based on the service request.

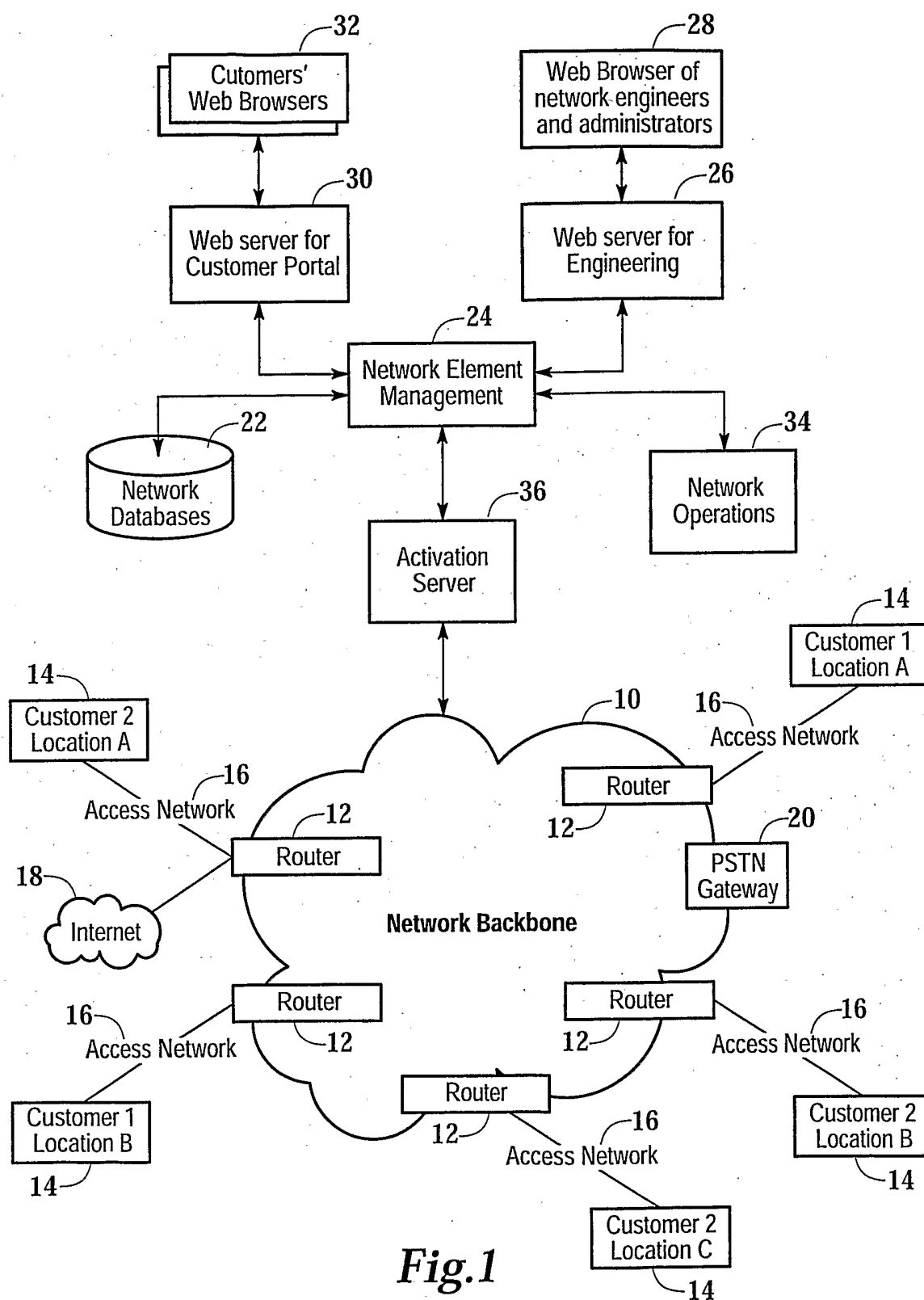
35

26. The computer readable media of claim 25, wherein the method further comprises comprising running one or more automated routines for automatically populating the templates with data from the network database and the new data.

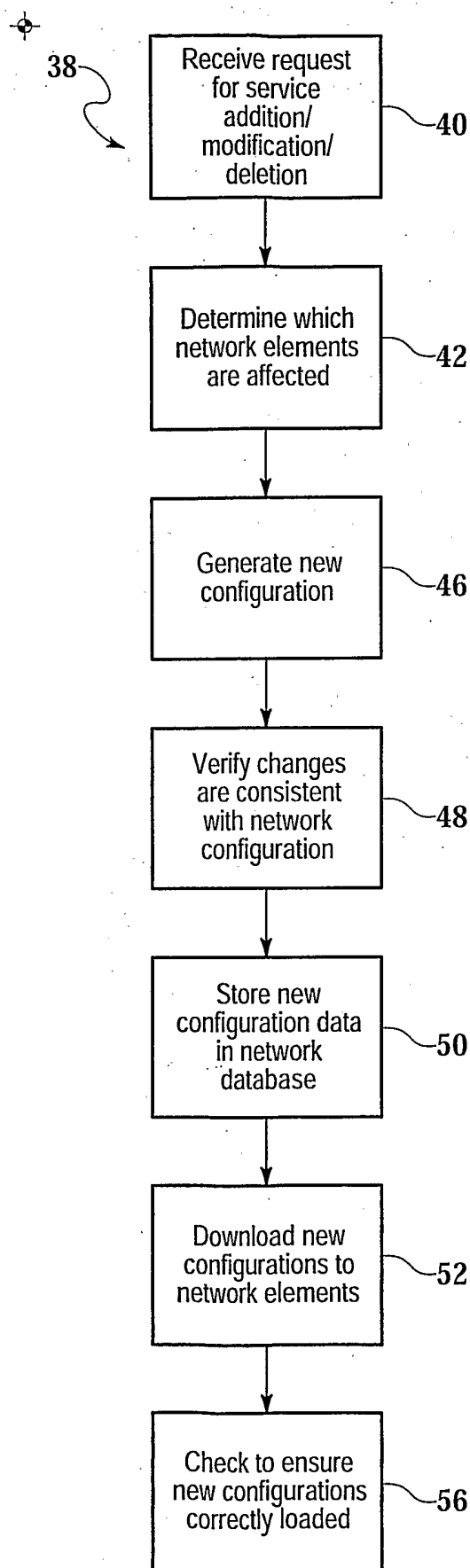
27. A computer readable storage medium comprising:

stored metadata for describing elements of a pocket network, relationships between the elements of the packet network, and types of properties to be stored with respect to each element of the packet network; and fields defined by the metadata for storing configuration data.

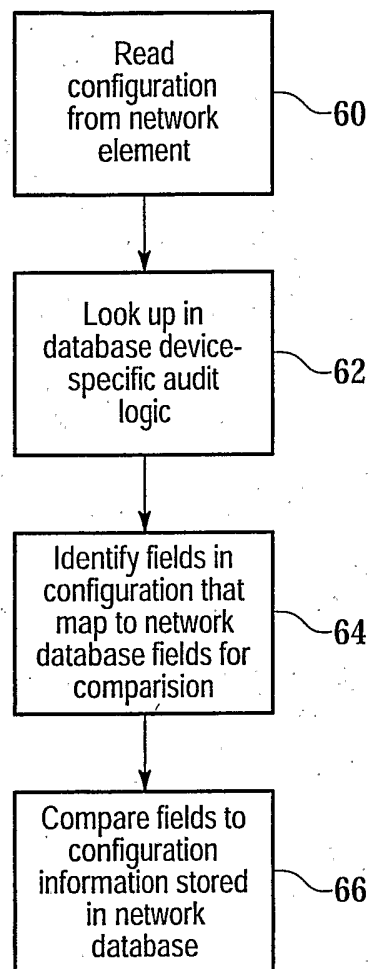
1/14



2/14



58



3/4

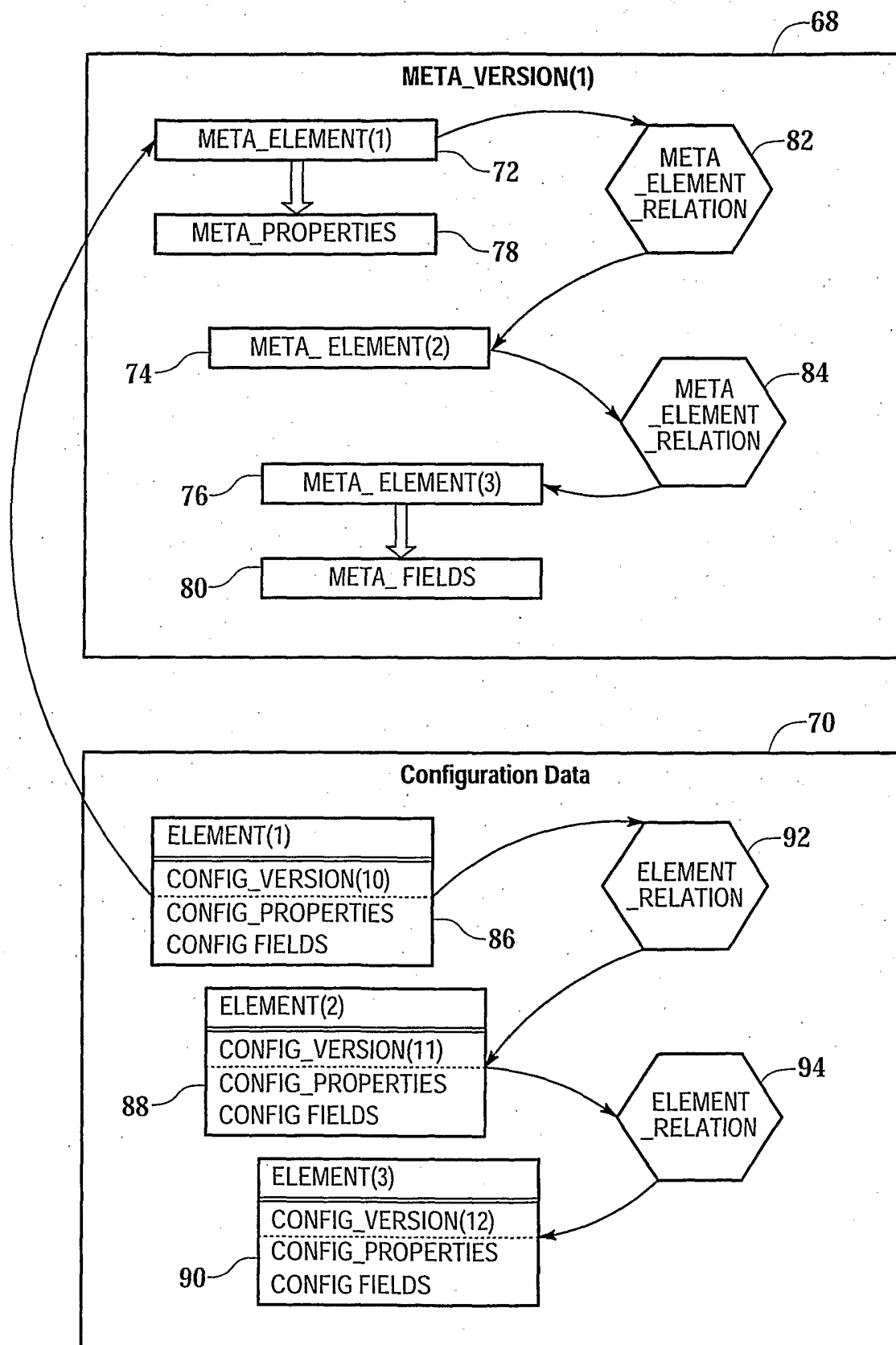
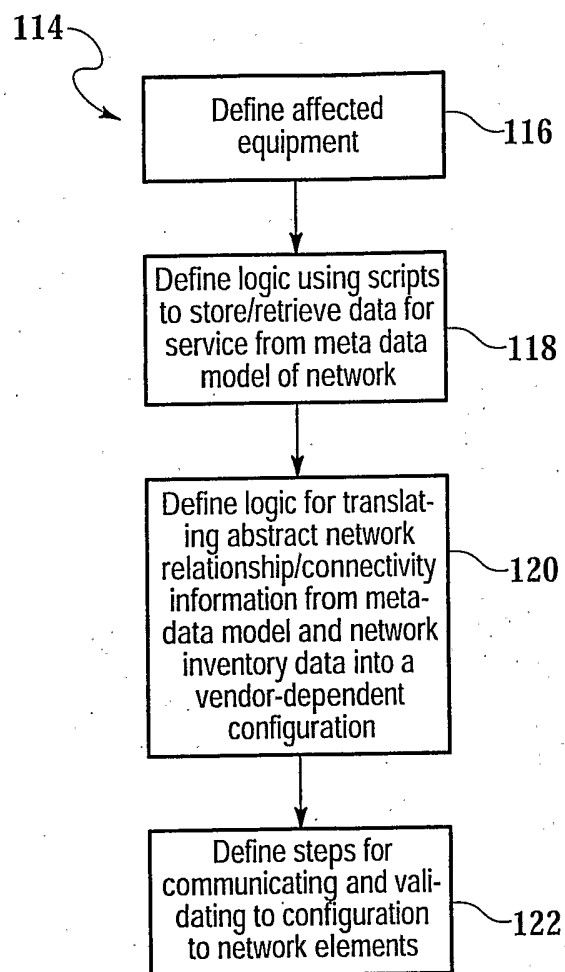
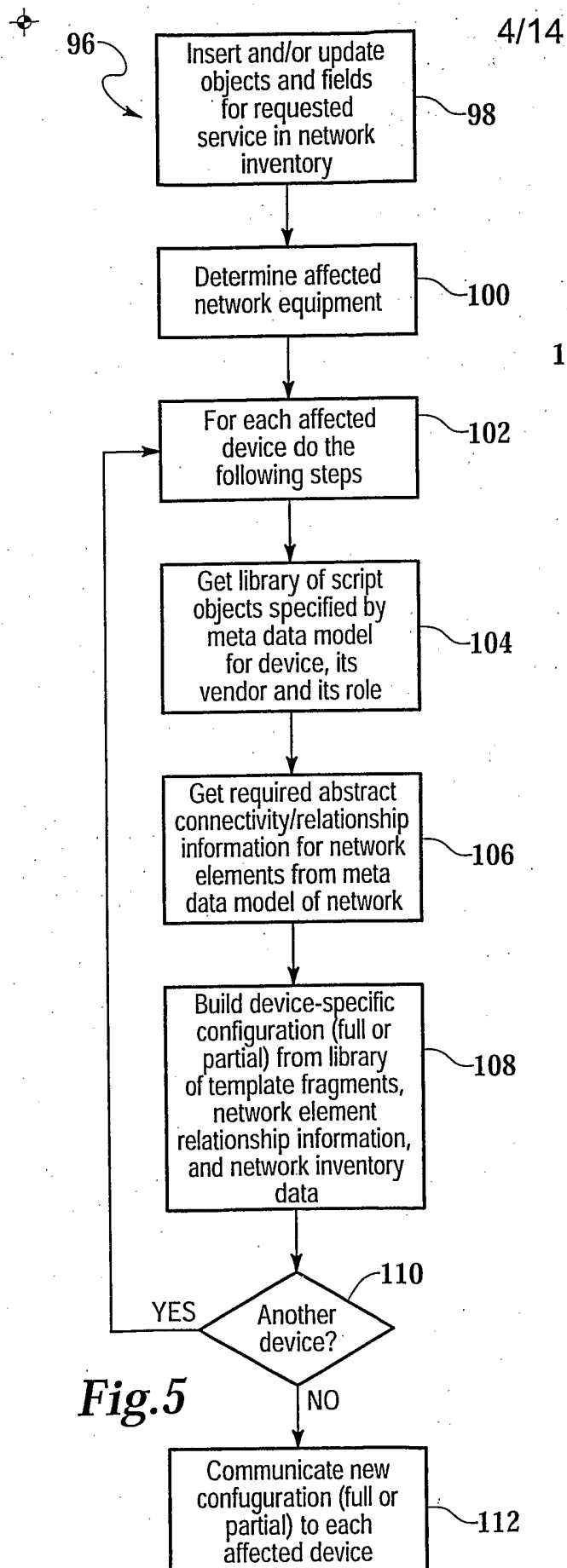


Fig.4



5/14

124

MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

Home [Log Out]

Welcome Customer ABC...
to Masergy's Service Control Center. Here you can:

- [Upgrade/modify network services](#)
- [Analyze network activity](#)
- [View SLA reporting](#)
- [Check the status of current orders](#)
- [View billing information](#)
- [Submit trouble tickets](#)
- [View and modify account information](#)

CUSTOMER MESSAGES

Masergy is proud to announce our inCONTROL Voice VPN service! This service will provide significant cost savings over current voice solutions. Features include:

- Toll quality IP Voice Transport
- Customer controlled private voice functionality across the WAN
- Off-net termination at competitive rates

Please contact your MASERGY account executive (1-866-MASERGY) for further details and special introductory promotional pricing.

Scheduled network maintenance tonight from 2am—4am.
[Click here for details.](#)

Fig.7

6/14

124

MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS [Log Out]

My Services

Services Summary

SERVICES SUMMARY

Search

Modify Services

Manage Network
View Usage
View CDRs
Service Levels
Maintenance

Home

7978 CAMDEN DRIVE—DALLAS, TX

Service ID	Service	Details	Bandwidth	
MS000020	InCONTROL IP	Type: T3 Encapsulation: PPP Ded. Option: Shared	9 Mbps	MODIFY
▶ MS000022	InCONTROL Link <i>From Service ID: MS000020 To Service ID: MS000030</i>	Plane: Reserved DLCI: Billing Method: Metered	128 Kbps	MODIFY
▶ MS000024	InCONTROL Voice	Bandwidth Cap: 512 Kbps Billing Method: Metered	512 Kbps	MODIFY
▶ MS000025	InCONTROL Video	Bandwidth Cap: 6 Mbps Billing Method: Flat Rate	6 Mbps	MODIFY

1512 LOCUST HIGHWAY—DALLAS, TX

Service ID	Service	Details	Bandwidth	
MS000030	Access Circuit	Type: T3 Encapsulation: Frame Ded. Option: Shared	45 Mbps	MODIFY
▶ MS000032	InCONTROL Link <i>From Service ID: MS000030 To Service ID: MS000040</i>	Plane: Normal DLCI: Billing Method: Flat Rate	0 Kbps	MODIFY

6018 REED ROAD—DALLAS, TX

Service ID	Service	Details	Bandwidth	
MS000040	InCONTROL IP	Type: OC3 Encapsulation: PPP Ded. Option: Dedicated	60 Mbps	MODIFY
▶ MS000043	InCONTROL Voice	Bandwidth Cap: 1.5 Mbps Billing Method: Metered	1.5 Mbps	MODIFY

Fig.8

7/14

124


SERVICE CONTROL CENTER
Customer Controlled Intelligent Networks

[HOME](#)
[MY ACCOUNT](#)
[MY SERVICES](#)
[MY SUPPORT CENTER](#)
[MY BILLING](#)
[MY ORDERS](#)

[My Services](#)
[\[Log Out \]](#)

[Services Summary](#)
[MODIFY SERVICES](#)

[Search](#)

T3 For InCONTROL IP / Service ID: MS000020

[Modify Services](#)
[Modify Tier](#)

[Manage Network](#)
[Enable/Disable Priority Bursting](#)

[View Usage](#)
[Modify Dedication Option](#)

[View CDRs](#)

[Service Levels](#)

[Maintenance](#)

[Home](#)

[Add inCONTROL Link](#)

[Add inCONTROL Voice](#)

[Add inCONTROL Video](#)

Fig.9A

124


SERVICE CONTROL CENTER
Customer Controlled Intelligent Networks

[HOME](#)
[MY ACCOUNT](#)
[MY SERVICES](#)
[MY SUPPORT CENTER](#)
[MY BILLING](#)
[MY ORDERS](#)

[My Services](#)
[\[Log Out \]](#)

[Services Summary](#)
[ADD inCONTROL Link](#)

[Search](#)

[Modify Services](#)

[Manage Network](#)

[View Usage](#)

[View CDRs](#)

[Service Levels](#)

[Maintenance](#)

[Home](#)

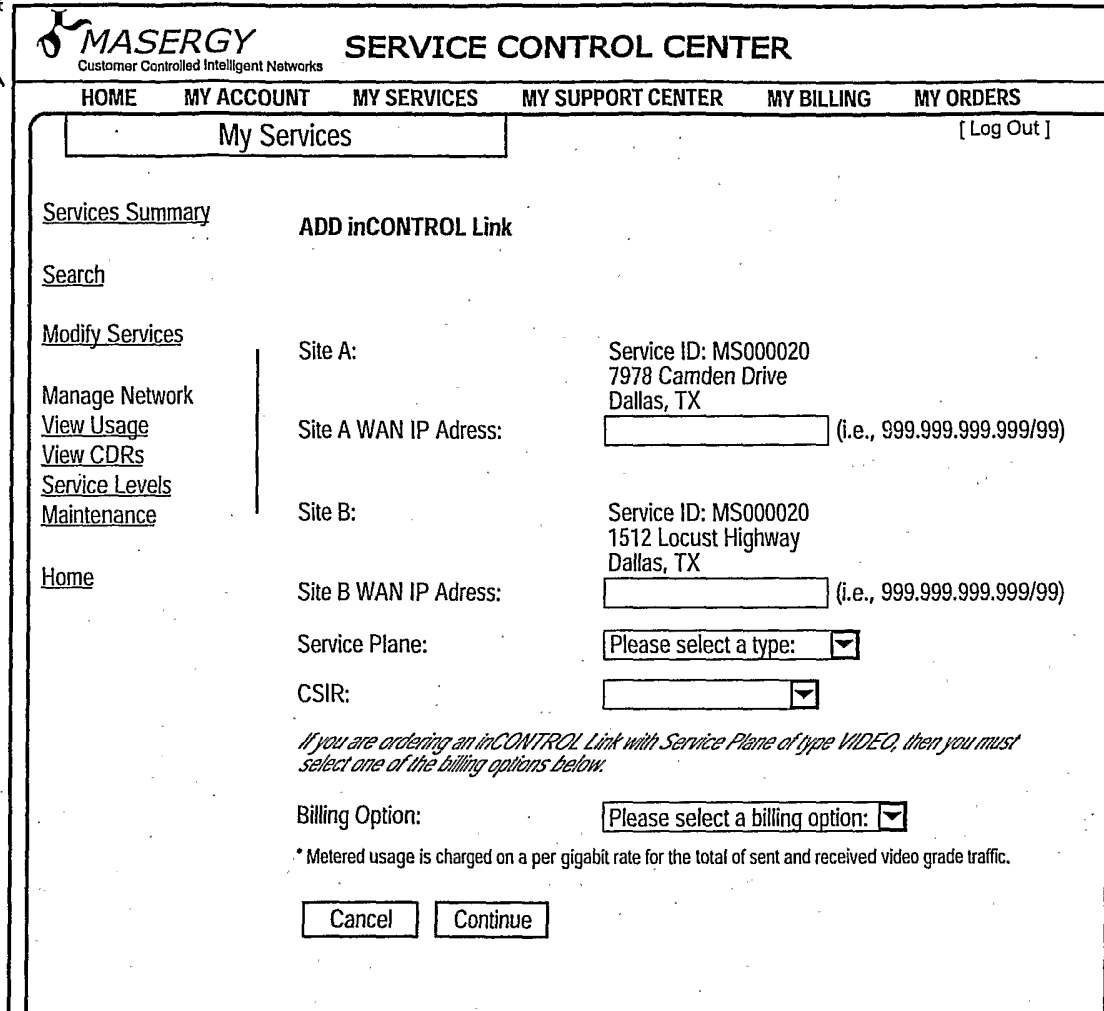
Site A Location: Service ID: MS000020
7978 Camden Drive
Dallas, TX

Site B Location:

Fig.9B

8/14

124



The image shows a web browser window displaying the MASERGY SERVICE CONTROL CENTER. The browser's address bar shows the number 124. The page has a header with the MASERGY logo and the text 'Customer Controlled Intelligent Networks'. Below the header is a navigation bar with links: HOME, MY ACCOUNT, MY SERVICES, MY SUPPORT CENTER, MY BILLING, and MY ORDERS. The 'MY SERVICES' link is highlighted, and a 'My Services' tab is visible. In the top right corner, there is a '[Log Out]' link. The main content area is divided into two columns. The left column contains a 'Services Summary' section with links: Search, Modify Services, Manage Network, View Usage, View CDRs, Service Levels, and Maintenance. The right column is titled 'ADD inCONTROL Link' and contains a form for adding a new service. The form has two sections for Site A and Site B. Site A information includes Service ID: MS000020, 7978 Camden Drive, Dallas, TX, and a WAN IP Address field. Site B information includes Service ID: MS000020, 1512 Locust Highway, Dallas, TX, and a WAN IP Address field. Below the site information, there are dropdown menus for 'Service Plane' (with the text 'Please select a type:') and 'CSIR'. A note states: 'If you are ordering an inCONTROL Link with Service Plane of type VIDEO, then you must select one of the billing options below.' Below this note is a 'Billing Option' dropdown menu (with the text 'Please select a billing option:'). At the bottom of the form are 'Cancel' and 'Continue' buttons. A footnote at the bottom reads: '* Metered usage is charged on a per gigabit rate for the total of sent and received video grade traffic.'

MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary

Search

Modify Services

Manage Network

View Usage

View CDRs

Service Levels

Maintenance

Home

ADD inCONTROL Link

Site A: Service ID: MS000020
7978 Camden Drive
Dallas, TX

Site A WAN IP Address: (i.e., 999.999.999.999/99)

Site B: Service ID: MS000020
1512 Locust Highway
Dallas, TX

Site B WAN IP Address: (i.e., 999.999.999.999/99)

Service Plane: Please select a type: ▼

CSIR: ▼

If you are ordering an inCONTROL Link with Service Plane of type VIDEO, then you must select one of the billing options below.

Billing Option: Please select a billing option: ▼

* Metered usage is charged on a per gigabit rate for the total of sent and received video grade traffic.

Cancel Continue

Fig.9C

9/14

124

MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary

Search

Modify Services

Manage Network

View Usage

View CDRs

Service Levels

Maintenance

Home

ADD inCONTROL Link

In order to complete your request to add an inCONTROL Link, we need to verify the following information:

Order information for inCONTROL Link:

Service: inCONTROL Link

Site A: Service ID: MS000020
7978 Camden Drive
Dallas, TX

Site B: Service ID: MS000020
1512 Locust Highway
Dallas, TX

Service Plane: Reserved

CSIR: 128 Kbps

Billing Option: Metered

New Charges

Site A Location	
Final inCONTROL Link Monthly Fee	\$250.00
Site B Location	
Final inCONTROL Link Monthly Fee	\$250.00
Total Monthly Fee for inCONTROL Link	\$500.00

Please note: By submitting this form, you will be changing your service with Masergy. Once you submit this change, you will have to wait 24 hours until you can make any additional modifications that change the billing for this service. The monthly fee(s) listed above will be applied and reflected in your next invoice.

If all of the information above is correct, then submit your order.

Submit Cancel

Fig.9D

10/14

124

The screenshot displays the MASERGY SERVICE CONTROL CENTER interface. At the top, the MASERGY logo is followed by the text 'Customer Controlled Intelligent Networks' and the title 'SERVICE CONTROL CENTER'. Below this is a navigation bar with links: HOME, MY ACCOUNT, MY SERVICES, MY SUPPORT CENTER, MY BILLING, and MY ORDERS. The 'MY SERVICES' link is highlighted, and a 'My Services' tab is visible. A '[Log Out]' link is located in the top right corner. On the left side, there is a sidebar with links: Services Summary, Search, Modify Services, Manage Network, View Usage, View CDRs, Service Levels, Maintenance, and Home. The main content area is titled 'ADD inCONTROL Voice'. It contains the following fields and options: 'Service Location:' with the address '7978 Camden Drive, Dallas, TX'; 'Service ID:' with the value 'MS000020'; 'Add to inCONTROL IP:' with the value 'Service ID: MS000020' and 'Service Type: Access Circuit with inCONTROL IP'; 'Bandwidth Cap:' with a dropdown menu showing 'Please select a bandwidth:'; 'Contract Term:' with a dropdown menu showing '12 months'; and 'Billing Option:' with two radio buttons: 'Metered' (selected) and 'Flat Rate'. A footnote states: '* Metered usage is charged on a per gigabit rate for the total of sent and received video grade traffic.' At the bottom, there are 'Next' and 'Cancel' buttons.

MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary **ADD inCONTROL Voice**

Search Service Location: Service ID: MS000020
7978 Camden Drive
Dallas, TX

Modify Services Add to inCONTROL IP: Service ID: MS000020
Service Type: Access Circuit with inCONTROL IP

Manage Network Bandwidth Cap: Please select a bandwidth: ▼

View Usage Contract Term: 12 months ▼

View CDRs Billing Option: ☒ Metered ☐ Flat Rate

Service Levels * Metered usage is charged on a per gigabit rate for the total of sent and received video grade traffic.

Maintenance

Home

Next Cancel

Fig.10A

11/14

124

**MASERGY**
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOMEMY ACCOUNTMY SERVICESMY SUPPORT CENTERMY BILLINGMY ORDERS

My Services[Log Out]

Services Summary
Search
Modify Services
Manage Network
View Usage
View CDRs
Service Levels
Maintenance
Home

ADD inCONTROL Voice
In order to complete your request to add an inCONTROL Voice, we need to verify the following information:
Order information for inCONTROL Voice:
Service: inCONTROL Voice
Location: 7978 Camden Drive
Dallas, TX
inCONTROL IP Information: Service ID: MS000020
Service Type: Access Circuit with inCONTROL IP
Bandwidth Cap: 512 Kbps
Contract Term: 24 months
Billing Option: Metered

New Charges
inCONTROL Voice
Monthly Fee \$1,000.00
Discount 25%
Final Monthly Fee \$750.00

Please note: By submitting this form, you will be adding inCONTROL Voice to your services with Masergy. Once you add inCONTROL Voice, you will have to wait 24 hours before you can modify or delete this service. The monthly fee(s) listed above will be applied and reflected in your next invoice.

If all of the information above is correct, then submit your order.

SubmitCancel

Fig.10B

12/14

124

MASERGY SERVICE CONTROL CENTER
Customer Controlled Intelligent Networks

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary

Search

Modify Services

Manage Network

View Usage

View CDRs

Service Levels

Maintenance

Home

MODIFY SERVICES

Service ID: MS000024

Service: inCONTROL Voice

Modify Voice Bandwidth Cap

Modify Billing Option

Delete inCONTROL Voice

Add Phone Numbers

Modify Phone Numbers

Delete Phone Numbers

Manage Private Dialing Plan
This function is only supported when logged directly into the Masergy network.
Contact Customer Service at 1-877-4MASERGY if you have any questions.

Fig.11A

124

MASERGY SERVICE CONTROL CENTER
Customer Controlled Intelligent Networks

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary

Search

Modify Services

Manage Network

View Usage

View CDRs

Service Levels

Maintenance

Home

MODIFY inCONTROL Voice IP

Service ID: MS000024

Service: inCONTROL Voice

Site Location: 7978 Camden Drive
Dallas, TX

inCONTROL IP Information: Service ID: MS000020
Service Type: Access Circuit with inCONTROL IP

Contract Term: 24 months

Bandwidth Cap: 512 Kbps

Update Cancel

Fig.11B

13/14

124



MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary **ADD PHONE NUMBERS**

Search Site ID: MS000020

Modify Services Address: 7879 Camden Drive
Dallas, TX

Manage Network
View Usage
View CDRs
Service Levels
Maintenance

To add additional phone numbers, you can:

1. Submit a file with a block of phone numbers in ??? format:

OR

2. Submit a range of phone numbers:

NPA	NXX	Starting Number	Ending Number	International	National
				☐ Yes ☐ No	☐ Yes ☐ No

OR

3. Submit a single phone number:

NPA	NXX	Number	International	National
			☐ Yes ☐ No	☐ Yes ☐ No

Fig.11C

124



MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary **MODIFY inCONTROL Link**

Search Service ID: MS000022

Modify Services Service: inCONTROL Link

Site A Location	Site B Location	Type	Type
Service ID: MS000020 7978 Camden Drive Dallas, TX	Service ID: MS000020 7978 Camden Drive Dallas, TX	Reserved	128 Kbps

If you are changing the Service Plane to VIDEO, then you must select one of the billing options below.

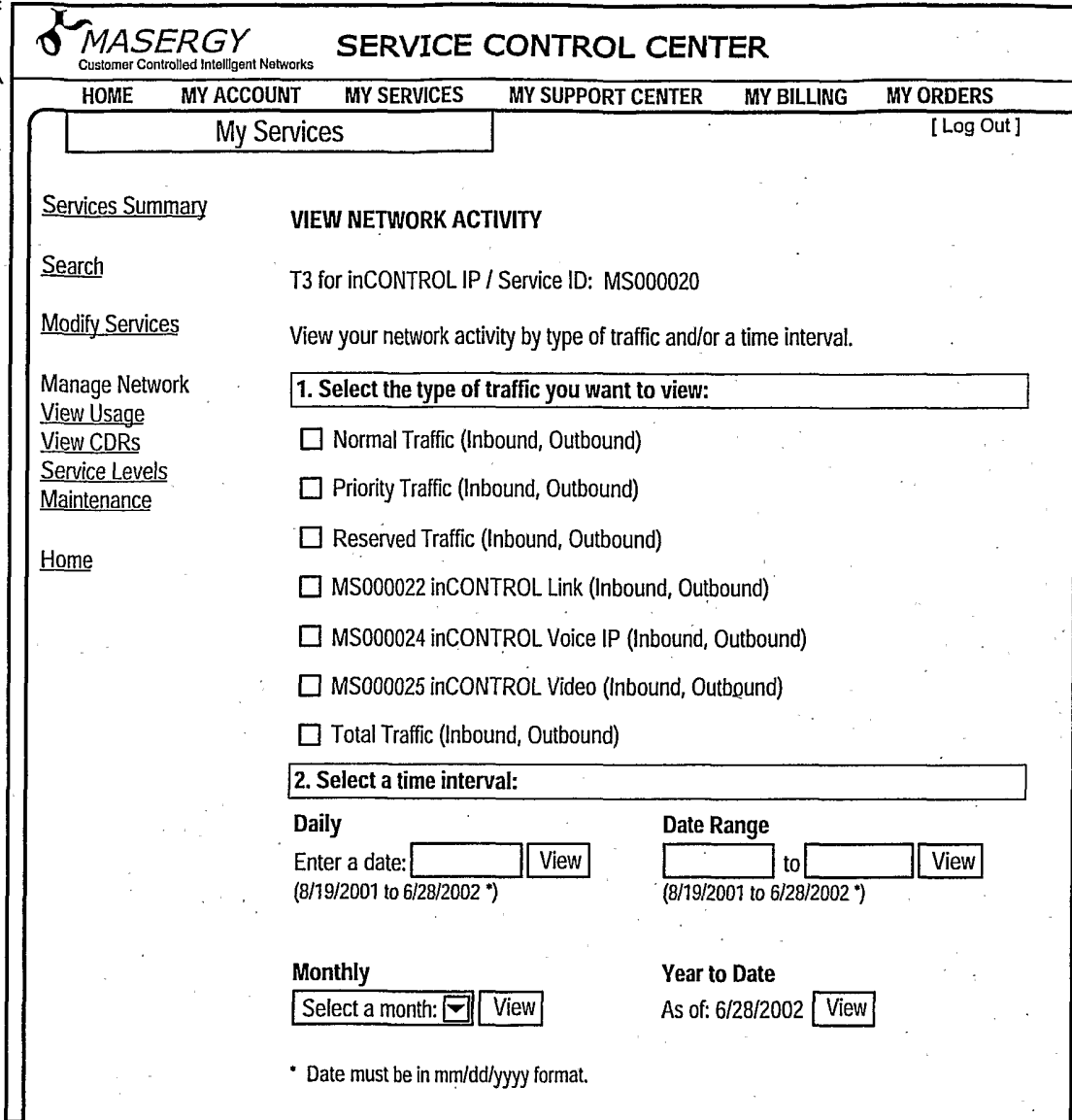
Billing Option:

* Metered usage is charged on a per gigabit rate for the total of sent and received video grade traffic.

Fig.12

14/14

124



The figure shows a web browser window displaying the MASERGY SERVICE CONTROL CENTER. The browser's address bar shows '124'. The page has a header with the MASERGY logo and 'Customer Controlled Intelligent Networks'. Below the logo is a navigation bar with links: HOME, MY ACCOUNT, MY SERVICES, MY SUPPORT CENTER, MY BILLING, and MY ORDERS. The 'MY SERVICES' link is highlighted. To the right of the navigation bar is a '[Log Out]' link. Below the navigation bar is a 'My Services' section. On the left side of this section is a sidebar with links: Services Summary, Search, Modify Services, Manage Network, View Usage, View CDRs, Service Levels, Maintenance, and Home. The main content area is titled 'VIEW NETWORK ACTIVITY' and shows 'T3 for inCONTROL IP / Service ID: MS000020'. Below this is a description: 'View your network activity by type of traffic and/or a time interval.' There are two main sections: '1. Select the type of traffic you want to view:' and '2. Select a time interval:'. Section 1 has a list of checkboxes: Normal Traffic (Inbound, Outbound), Priority Traffic (Inbound, Outbound), Reserved Traffic (Inbound, Outbound), MS000022 inCONTROL Link (Inbound, Outbound), MS000024 inCONTROL Voice IP (Inbound, Outbound), MS000025 inCONTROL Video (Inbound, Outbound), and Total Traffic (Inbound, Outbound). Section 2 has two sub-sections: 'Daily' and 'Monthly'. The 'Daily' sub-section has a 'Date Range' section with 'Enter a date:' and a 'View' button, and a 'Date Range' section with a date range input and a 'View' button. The 'Monthly' sub-section has a 'Select a month:' dropdown and a 'View' button. The 'Year to Date' sub-section has an 'As of: 6/28/2002' input and a 'View' button. A footnote at the bottom states: '* Date must be in mm/dd/yyyy format.'

MASERGY
Customer Controlled Intelligent Networks

SERVICE CONTROL CENTER

HOME MY ACCOUNT MY SERVICES MY SUPPORT CENTER MY BILLING MY ORDERS

My Services [Log Out]

Services Summary

Search

Modify Services

Manage Network

View Usage

View CDRs

Service Levels

Maintenance

Home

VIEW NETWORK ACTIVITY

T3 for inCONTROL IP / Service ID: MS000020

View your network activity by type of traffic and/or a time interval.

1. Select the type of traffic you want to view:

☐ Normal Traffic (Inbound, Outbound)

☐ Priority Traffic (Inbound, Outbound)

☐ Reserved Traffic (Inbound, Outbound)

☐ MS000022 inCONTROL Link (Inbound, Outbound)

☐ MS000024 inCONTROL Voice IP (Inbound, Outbound)

☐ MS000025 inCONTROL Video (Inbound, Outbound)

☐ Total Traffic (Inbound, Outbound)

2. Select a time interval:

Daily

Enter a date:

(8/19/2001 to 6/28/2002 *)

Date Range

to

(8/19/2001 to 6/28/2002 *)

Monthly

Select a month:

Year to Date

As of: 6/28/2002

* Date must be in mm/dd/yyyy format.

Fig.13