US 20040261116A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0261116 A1

Mckeown et al. (43) Pub. Date: Dec. 23, 2004

(54) BROADBAND COMMUNICATIONS

(76) Inventors: **Jean Christophe Mckeown**, Mandelieu (FR); **Henri Chabrier**, Biot (FR)

Correspondence Address:
WOLF GREENFIELD & SACKS, PC
FEDERAL RESERVE PLAZA
600 ATLANTIC AVENUE
BOSTON, MA 02210-2211 (US)

(21) Appl. No.: 10/481,933

(22) PCT Filed: Jul. 3, 2002

(86) PCT No.: PCT/GB02/03074

(30) Foreign Application Priority Data

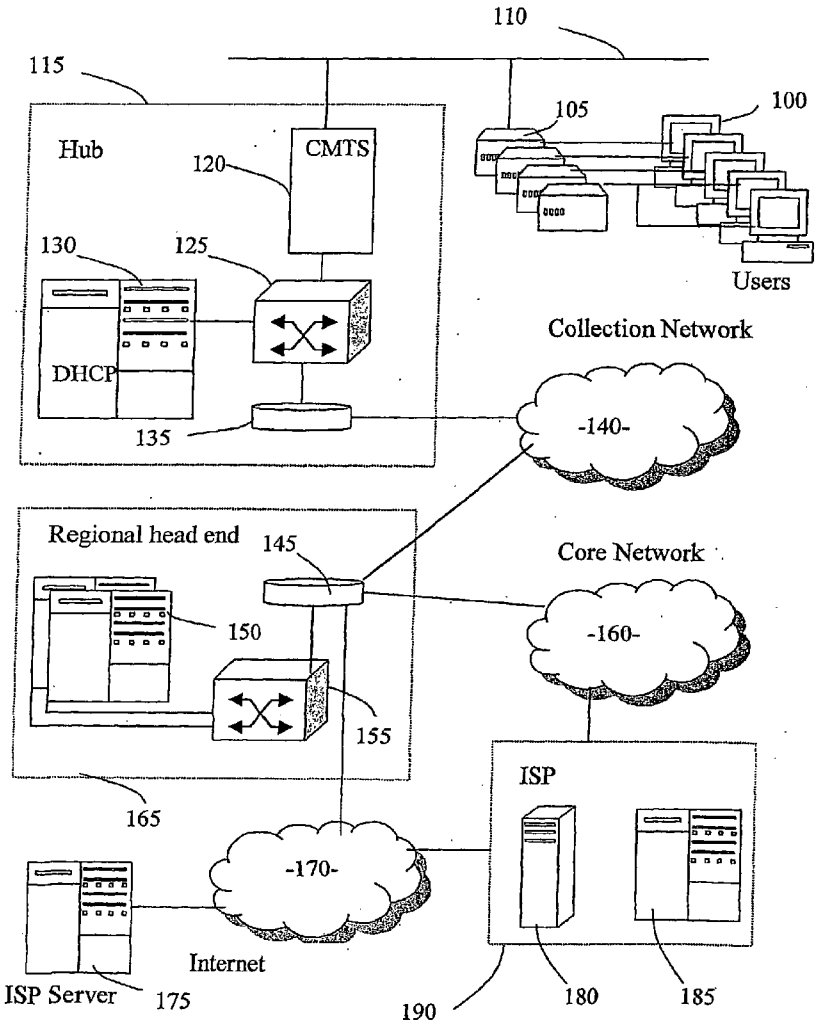
Jul. 3, 2001 (EP) 01401767.7
Mar. 26, 2002 (WO) PCT/GB02/01461
May 22, 2002 (WO) PCT/GB02/02372

Publication Classification

(51) Int. Cl.[7] H04N 7/173
(52) U.S. Cl. 725/109

(57) ABSTRACT

The invention relates to communications, particularly but not exclusively broadband communications. One facet of the present invention relates to provisioning of services in a communications network and finds particular, but not exclusive, application in a broadband network environment or other environment where services are provisioned. The provisioning of services will now be discussed in more detail.



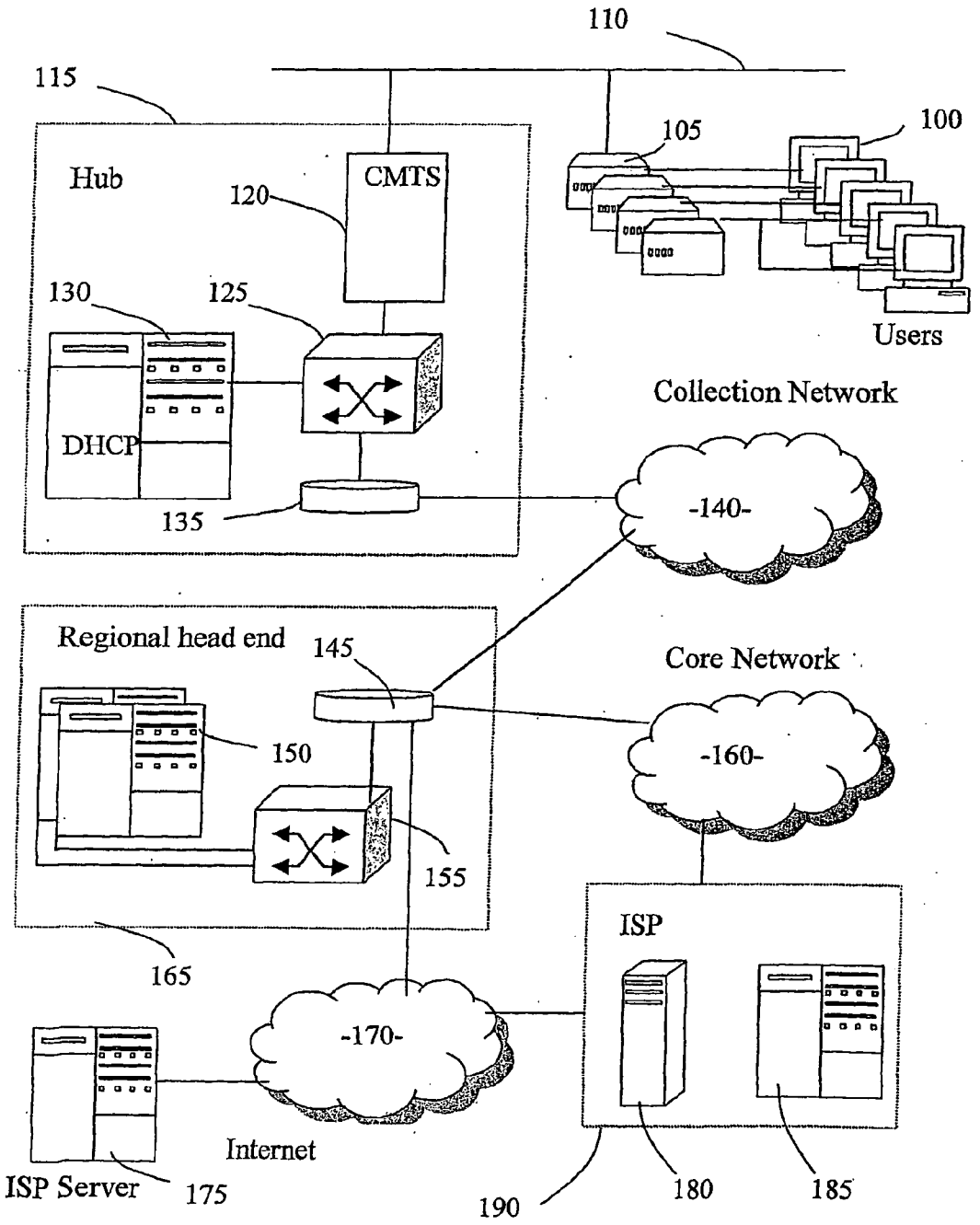

110
115
Hub
CMTS
120
105
100
130
125
Users
DHCP
Collection Network
-140-
135
Regional head end
145
Core Network
150
-160-
155
ISP
165
-170-
Internet
ISP Server
175
190
180
185

Fig. 1

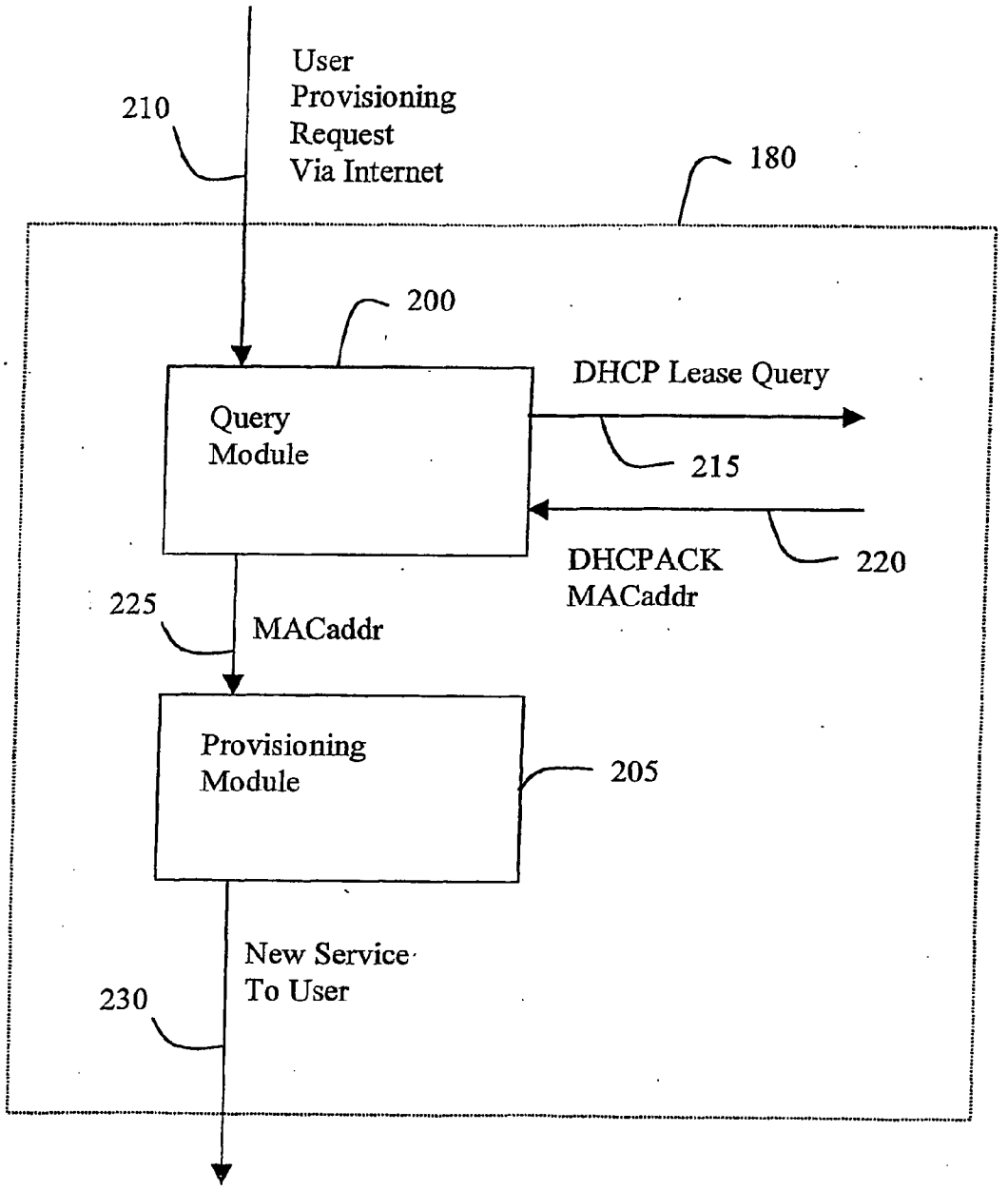

User
Provisioning
Request
Via Internet
210
180
200
Query
Module
DHCP Lease Query
215
DHCPACK
MACaddr
220
225
MACaddr
Provisioning
Module
205
New Service
To User
230

Fig. 2

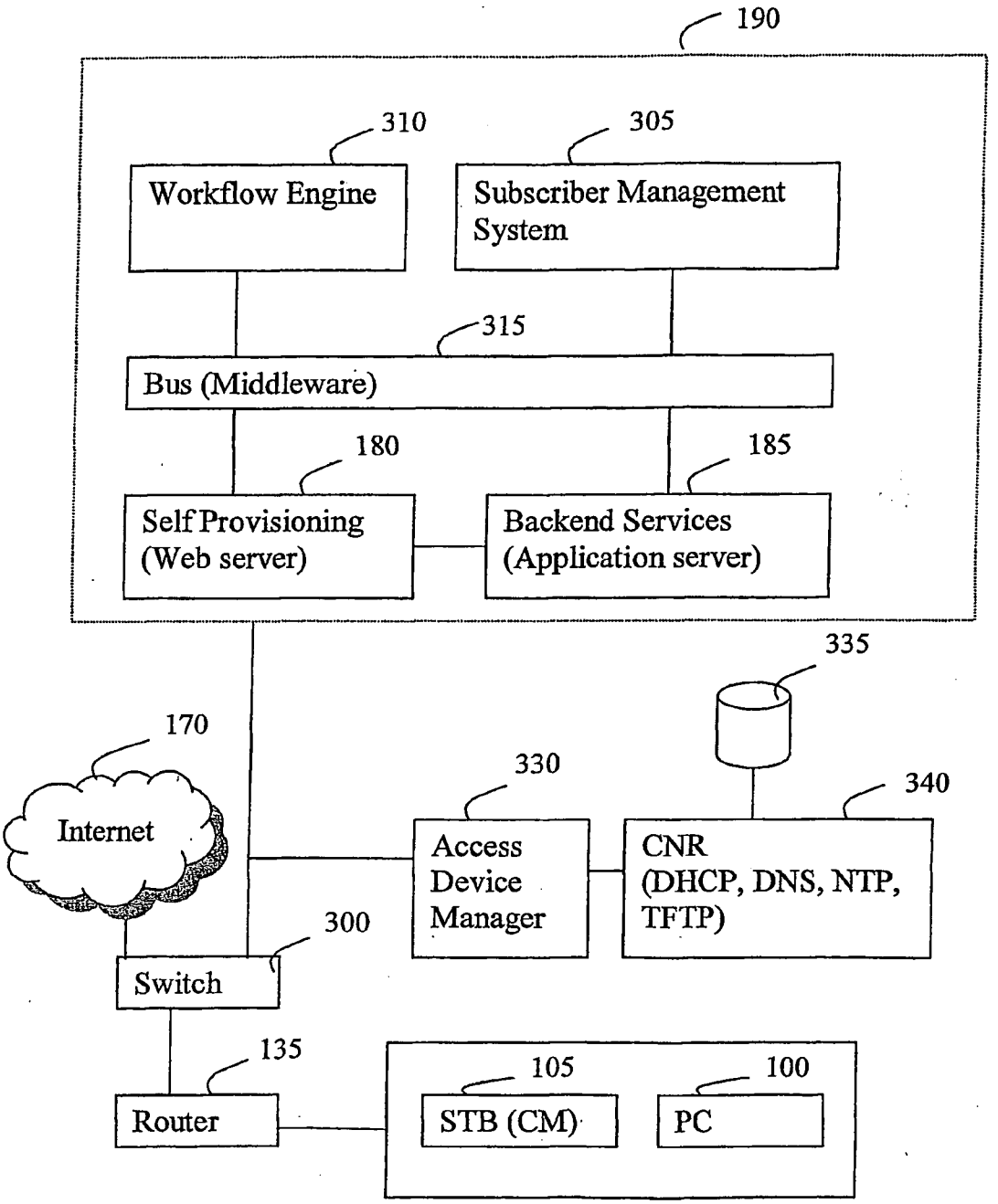

190
310
305
Workflow Engine
Subscriber Management System
315
Bus (Middleware)
180
185
Self Provisioning (Web server)
Backend Services (Application server)
335
170
330
340
Internet
Access Device Manager
CNR (DHCP, DNS, NTP, TFTP)
300
Switch
135
105
100
Router
STB (CM)
PC

Fig. 3

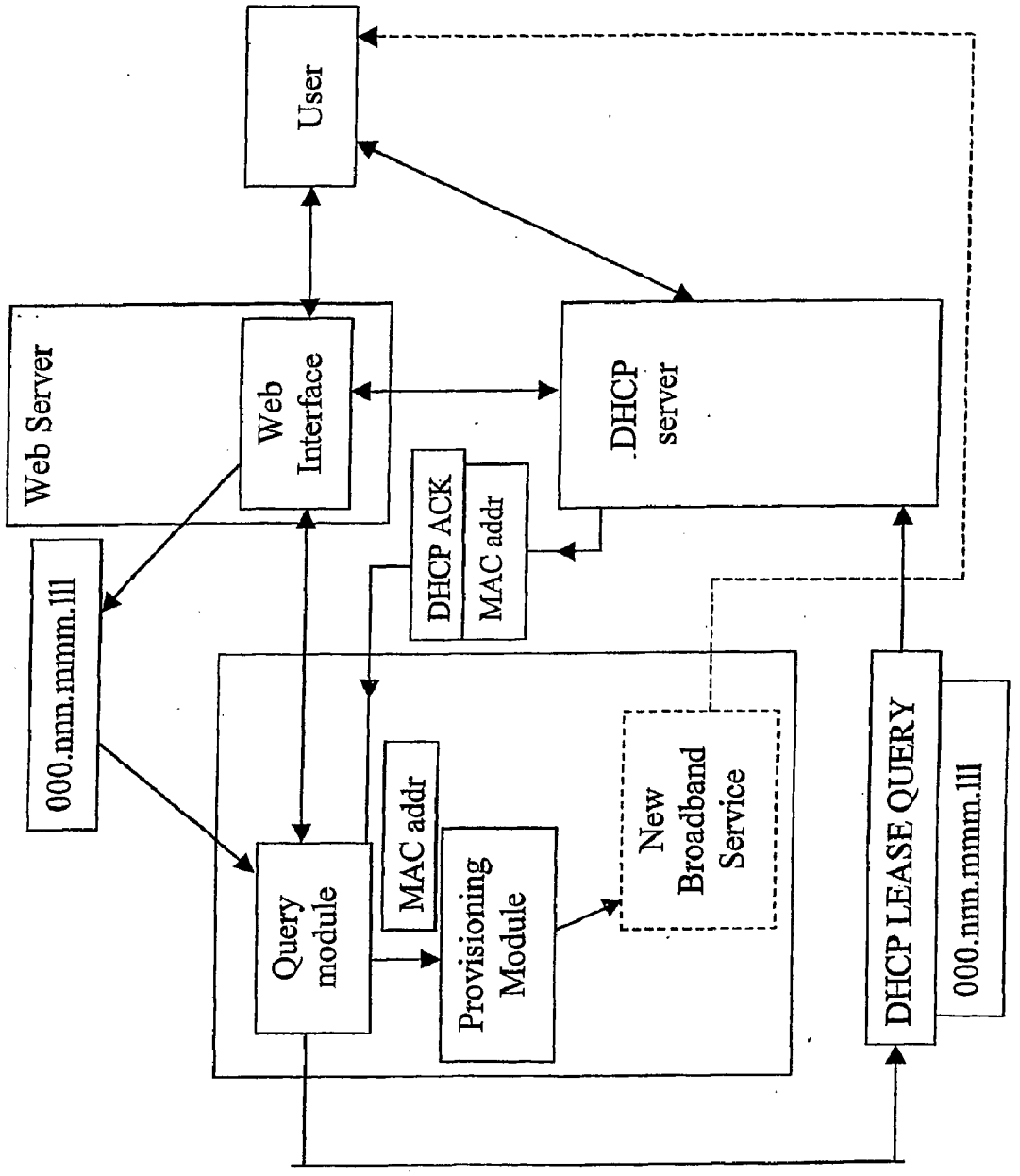

User
Web Server
Web Interface
DHCP server
DHCP ACK
MAC addr
000.nnn.mmm.lll
Query module
MAC addr
Provisioning Module
New Broadband Service
DHCP LEASE QUERY
000.nnn.mmm.lll

Fig. 4

Fig. 5

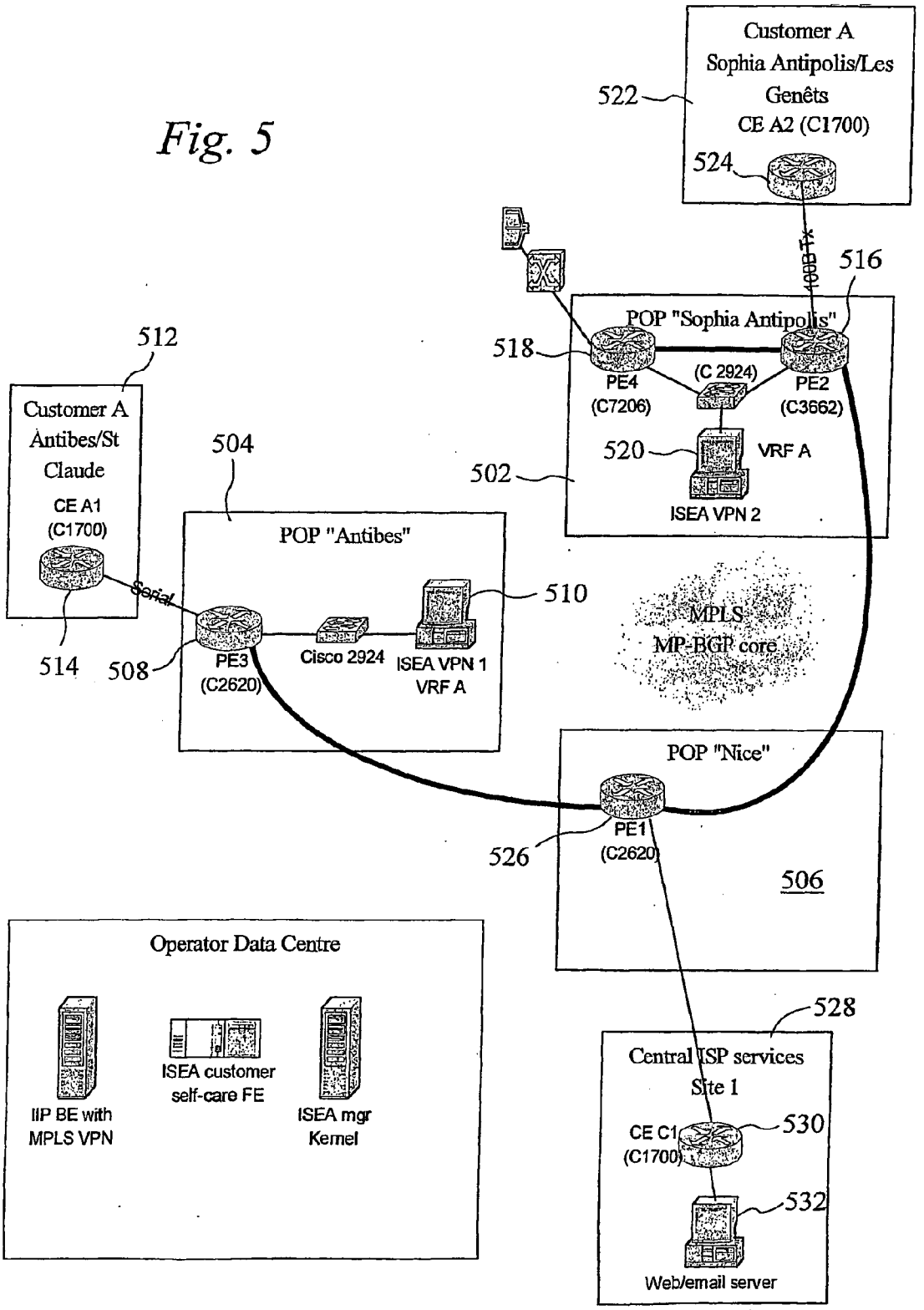

Customer A
Sophia Antipolis/Les Genêts
CE A2 (C1700)
522
524
516
POP "Sophia Antipolis"
518
PE4
(C7206)
(C 2924)
PE2
(C3662)
520
VRF A
502
ISEA VPN 2
512
Customer A
Antibes/St Claude
CE A1
(C1700)
504
POP "Antibes"
Serial
510
514
508
PE3
(C2620)
Cisco 2924
ISEA VPN 1
VRF A
MPLS
MP-BGP core
POP "Nice"
PE1
(C2620)
526
506
Operator Data Centre
IIP BE with
MPLS VPN
ISEA customer
self-care FE
ISEA mgr
Kernel
528
Central ISP services
Site 1
CE C1
(C1700)
530
532
Web/email server

Fig. 6

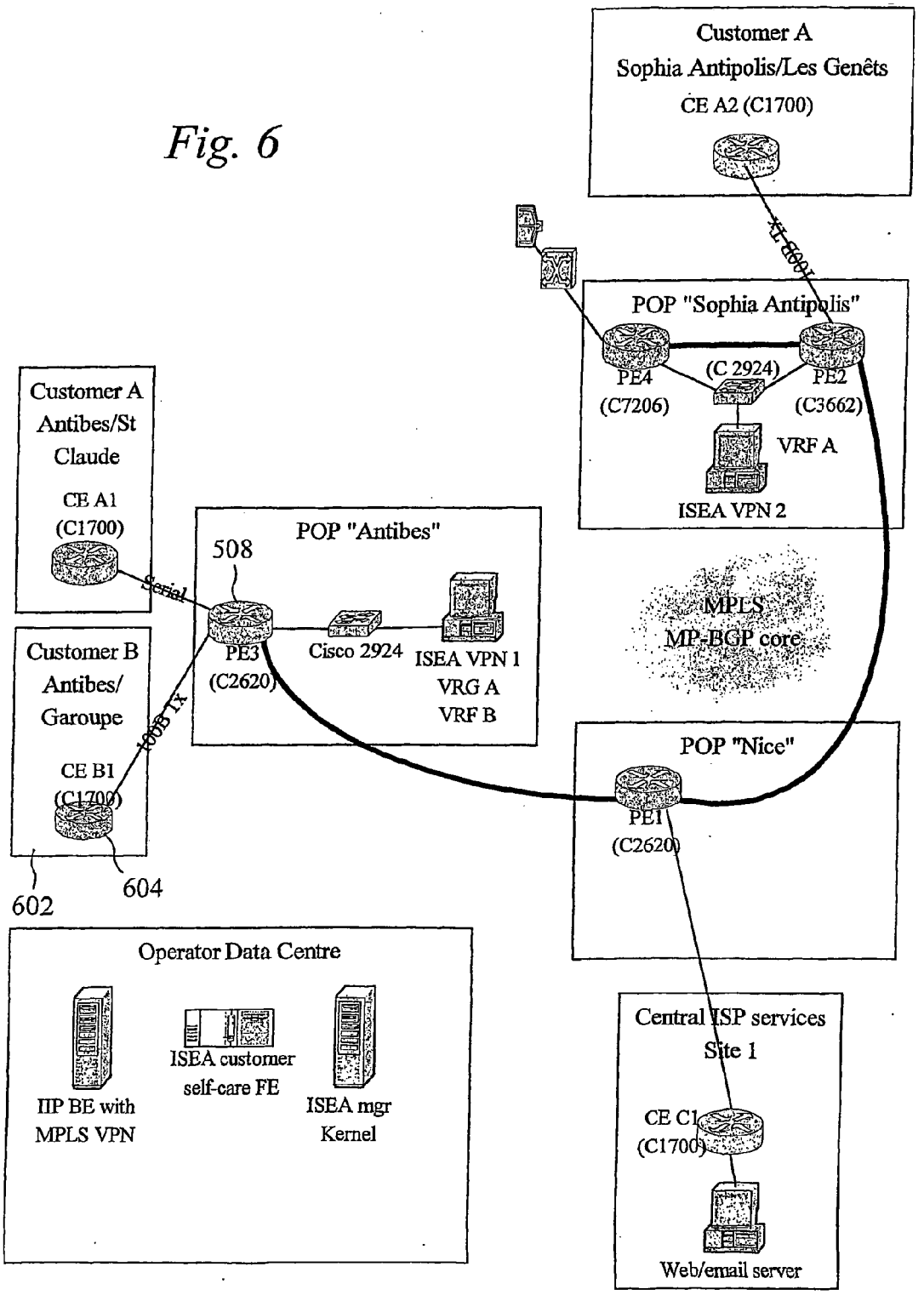

Customer A
Sophia Antipolis/Les Genêts
CE A2 (C1700)
100B-TX
POP "Sophia Antipolis"
PE4
(C7206)
(C 2924)
PE2
(C3662)
VRF A
ISEA VPN 2
Customer A
Antibes/St
Claude
CE A1
(C1700)
Serial
508
POP "Antibes"
PE3
(C2620)
Cisco 2924
ISEA VPN 1
VRG A
VRF B
MPLS
MP-BGP core
Customer B
Antibes/
Garoupe
CE B1
(C1700)
100B-TX
POP "Nice"
PE1
(C2620)
602
604
Operator Data Centre
IIP BE with
MPLS VPN
ISEA customer
self-care FE
ISEA mgr
Kernel
Central ISP services
Site 1
CE C1
(C1700)
Web/email server

Fig. 7

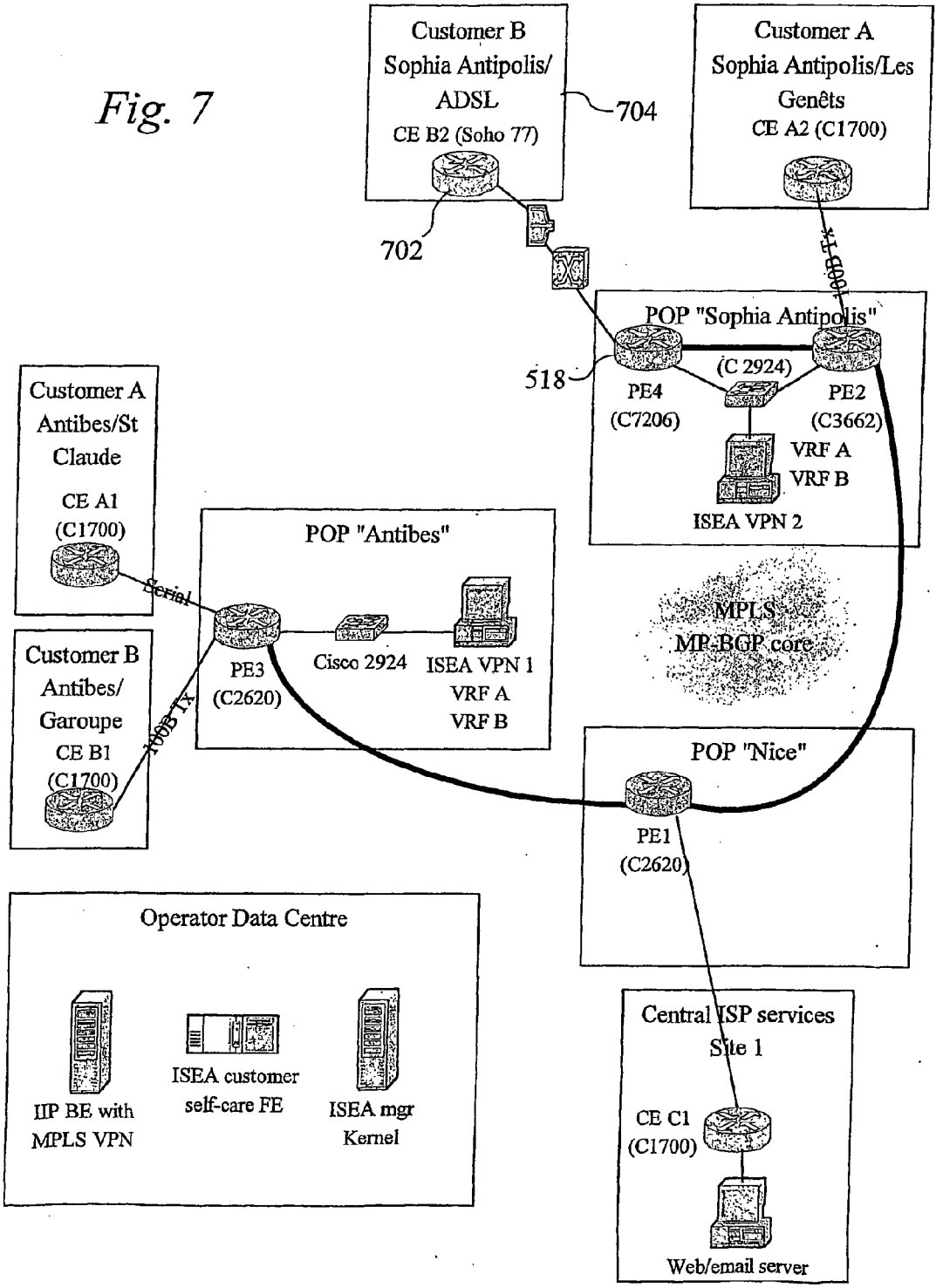
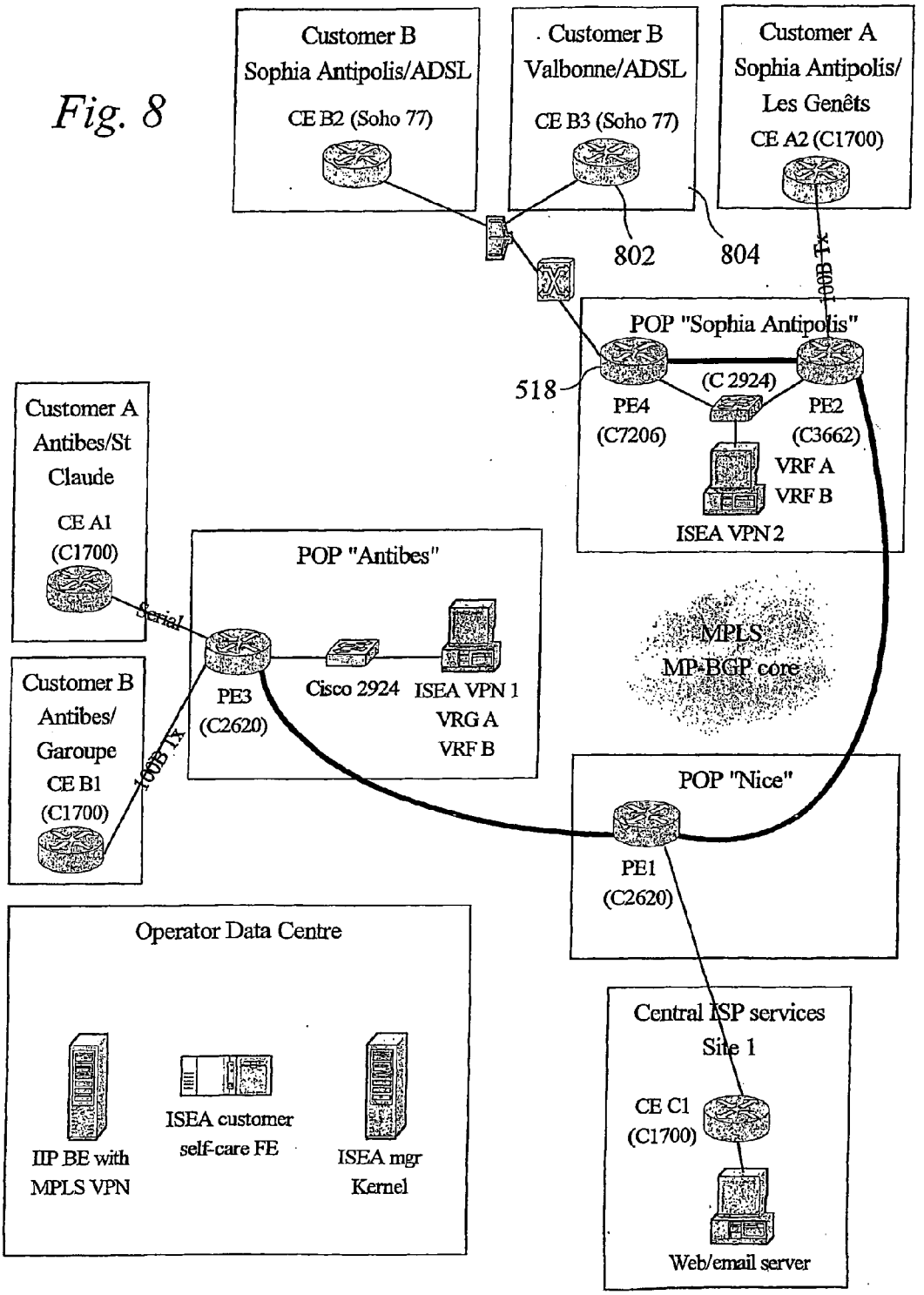

Customer B
Sophia Antipolis/
ADSL
CE B2 (Soho 77)
704
702
Customer A
Sophia Antipolis/Les
Genêts
CE A2 (C1700)
100B Tx
POP "Sophia Antipolis"
518
(C 2924)
PE4
(C7206)
PE2
(C3662)
VRF A
VRF B
ISEA VPN 2
Customer A
Antibes/St
Claude
CE A1
(C1700)
Serial
POP "Antibes"
PE3
(C2620)
Cisco 2924
ISEA VPN 1
VRF A
VRF B
MPLS
MP-BGP core
Customer B
Antibes/
Garoupe
CE B1
(C1700)
100B Tx
POP "Nice"
PE1
(C2620)
Operator Data Centre
IIP BE with
MPLS VPN
ISEA customer
self-care FE
ISEA mgr
Kernel
Central ISP services
Site 1
CE C1
(C1700)
Web/email server

Fig. 8


Customer B
Sophia Antipolis/ADSL
CE B2 (Soho 77)
Customer B
Valbonne/ADSL
CE B3 (Soho 77)
Customer A
Sophia Antipolis/
Les Genêts
CE A2 (C1700)
802
804
100B TX
POP "Sophia Antipolis"
518
(C 2924)
PE4
(C7206)
PE2
(C3662)
VRF A
VRF B
ISEA VPN 2
Customer A
Antibes/St
Claude
CE A1
(C1700)
Serial
POP "Antibes"
PE3
(C2620)
Cisco 2924
ISEA VPN 1
VRG A
VRF B
MPLS
MP-BGP core
Customer B
Antibes/
Garoupe
CE B1
(C1700)
100B TX
POP "Nice"
PE1
(C2620)
Operator Data Centre
IIP BE with
MPLS VPN
ISEA customer
self-care FE
ISEA mgr
Kernel
Central ISP services
Site 1
CE C1
(C1700)
Web/email server

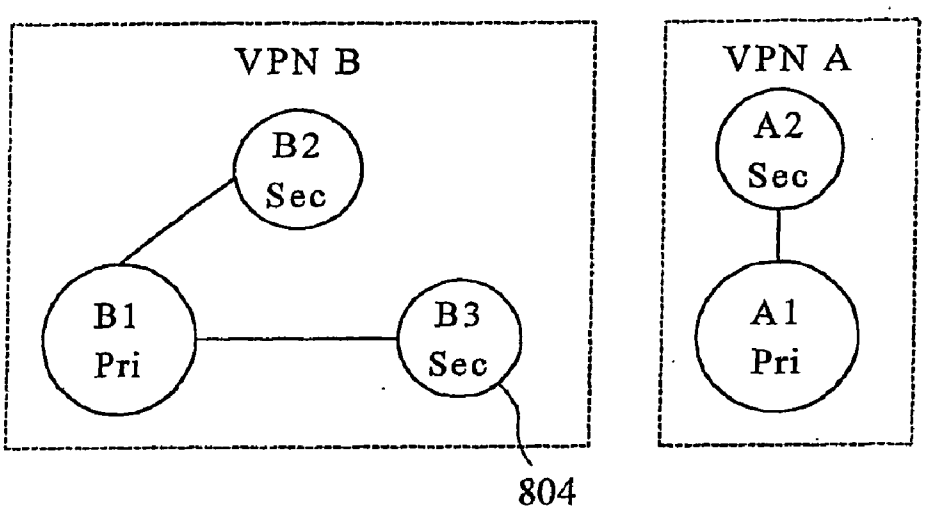

VPN B
B2
Sec
B1
Pri
B3
Sec
804
VPN A
A2
Sec
A1
Pri

Fig. 9

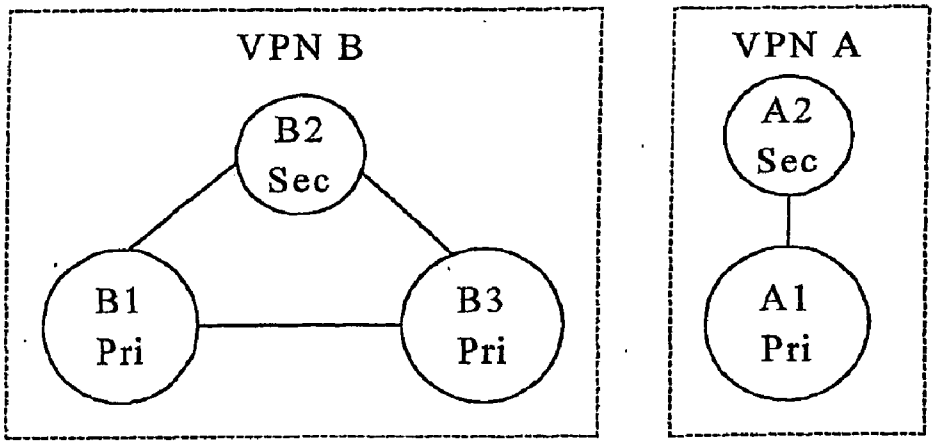

VPN B
B2
Sec
B1
Pri
B3
Pri
VPN A
A2
Sec
A1
Pri

Fig. 10

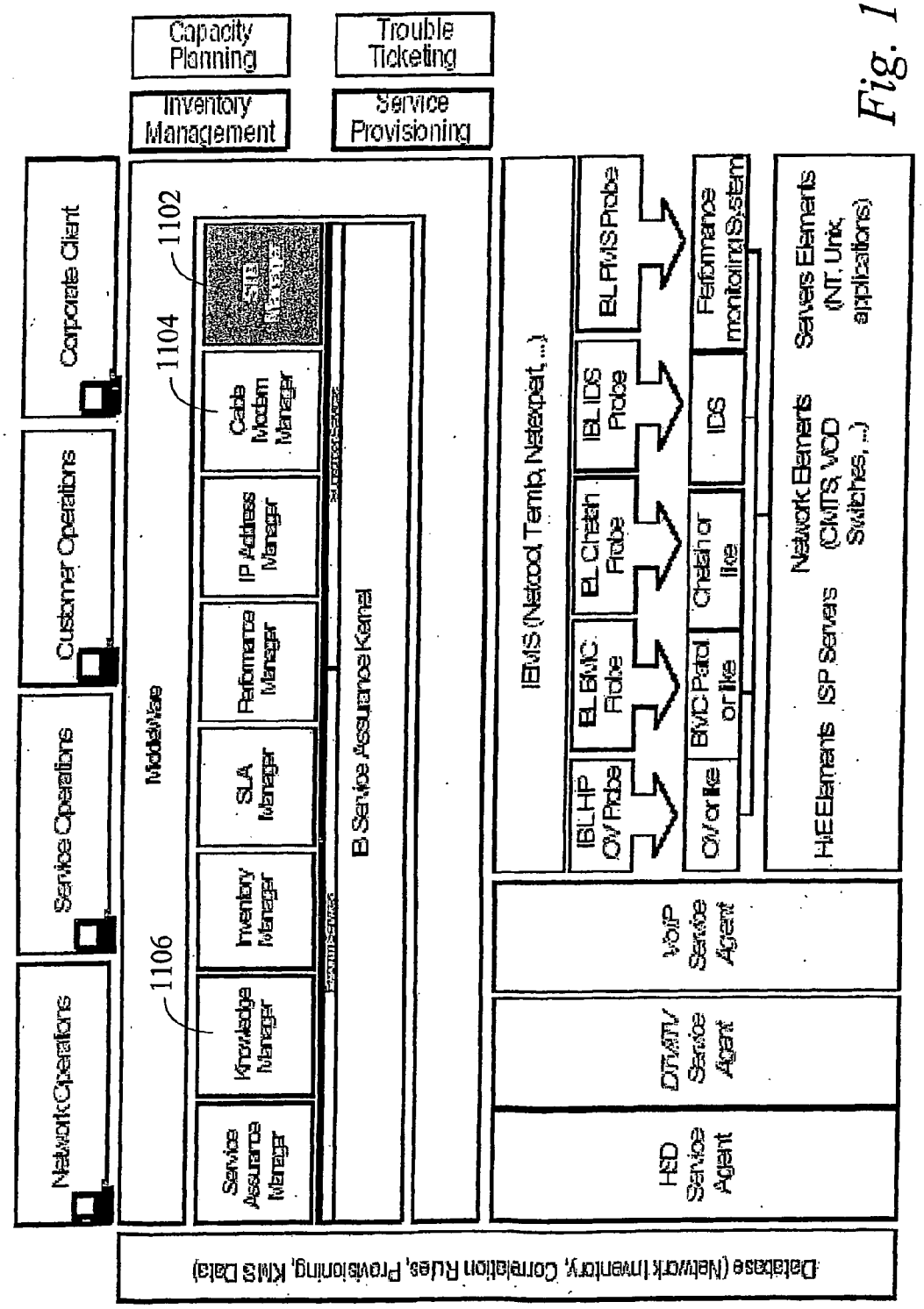

Capacity Planning
Trouble Ticketing
Inventory Management
Service Provisioning
Corporate Client
Customer Operations
Service Operations
Network Operations
1102
1104
1106
MidleWare
Cable Modem Manager
IP Address Manager
Performance Manager
SLA Manager
Inventory Manager
Knowledge Manager
Service Assurance Manager
B Service Assurance Kernel
IBMS (Netcool, Tembi, Netexpert, ...)
IBL PMS Probe
IBL IDS Probe
IBL Chatch Probe
IBL BMC Probe
IBL HP OV Probe
Performance monitoring System
IDS
Chatch or like
BMC Patrol or like
OV or like
Servers Elements (NT, Unix, applications)
Network Elements (CMTS, VOD Switches, ...)
ISP Servers
HiEElements
VoIP Service Agent
DTV/MTV Service Agent
HSD Service Agent
Database (Network Inventory, Correlation Rules, Provisioning, KMS Data)

Fig. 11

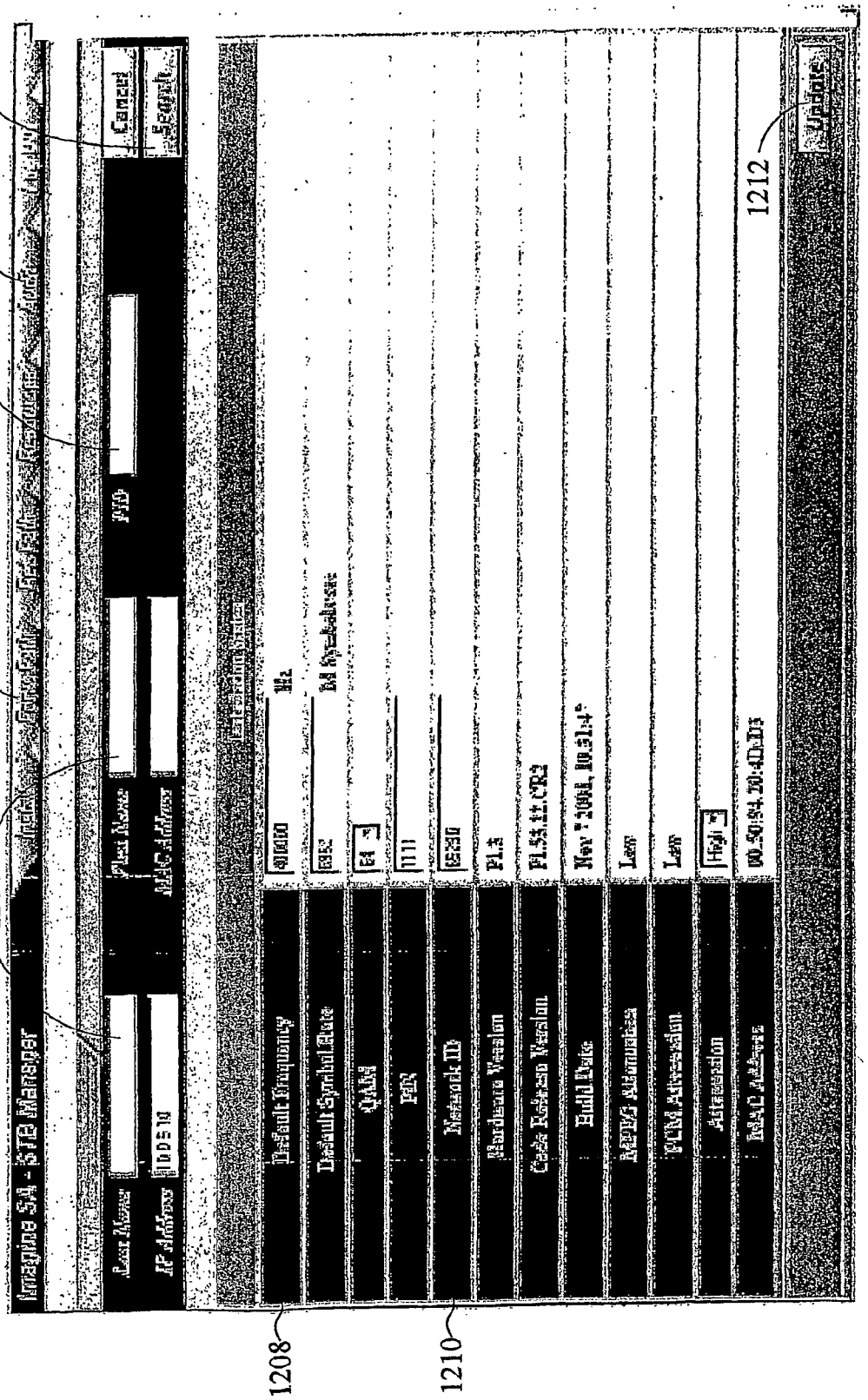

1206
1216
1202
1214
1204
1212
1208
1210
Cancel
Search
Update
Default Frequency
Default Symbol Rate
QAM
PIN
Network ID
Hardware Version
Code Release Version
Build Date
MPEG Attenuation
FCM Attenuation
Attenuation
MAC Address

Fig. 12

Fig. 13

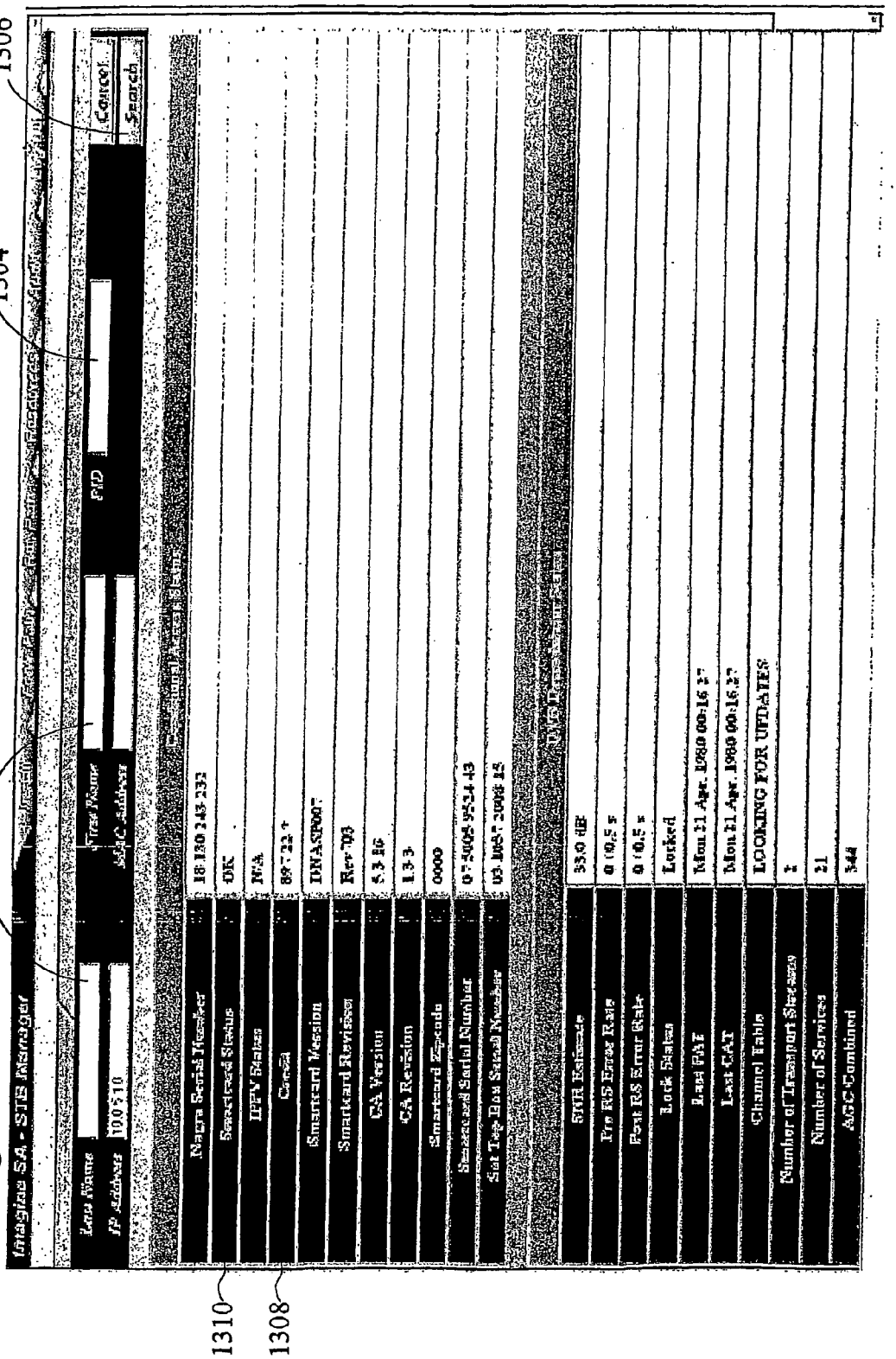
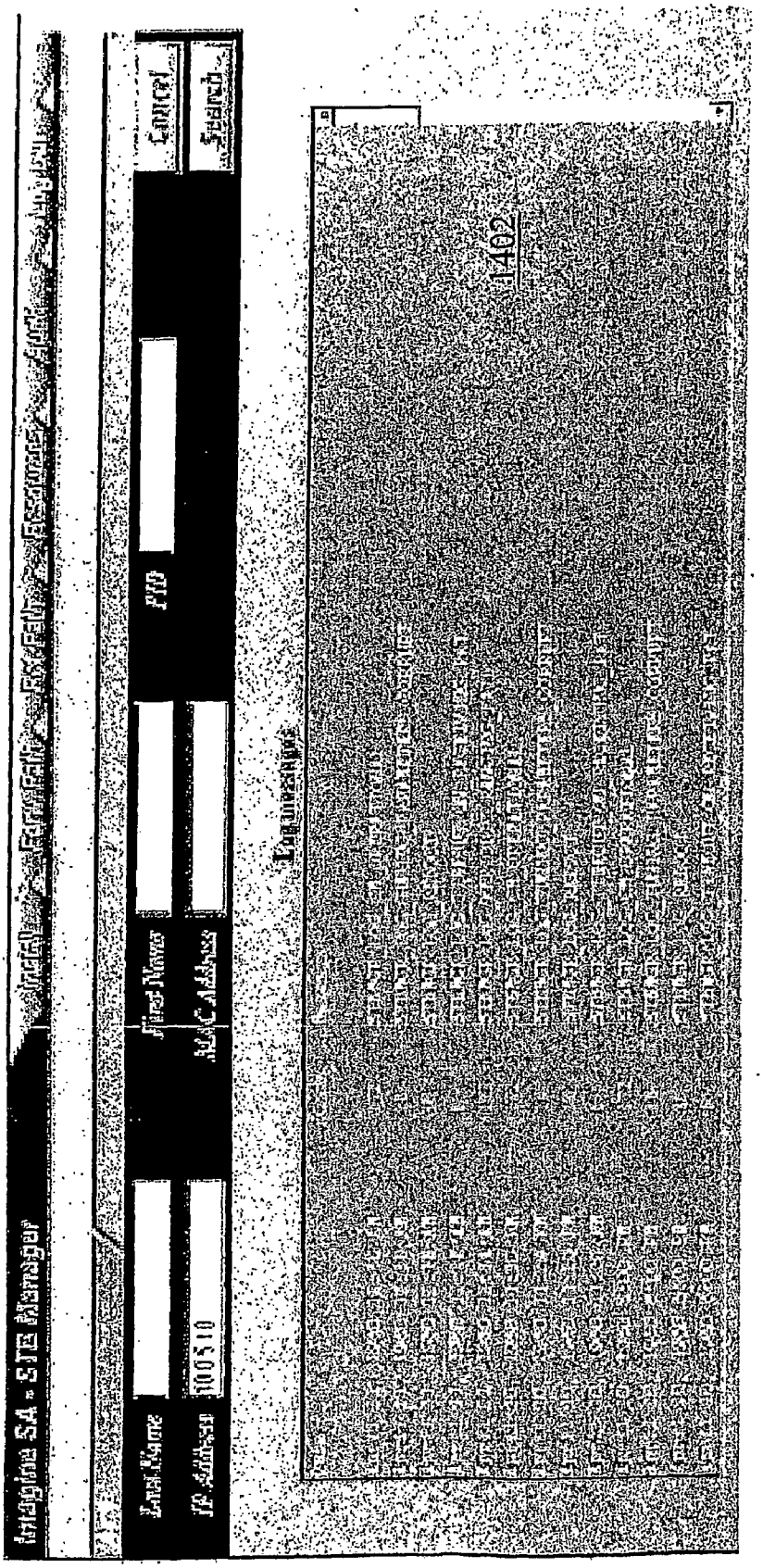

1306
1304
1302
1310
1308
Integrated SA - STB Manager
Low Name
IP Address
Test Name
MAC Address
PID
Cancel
Search
Nagra Serial Number
Smartcard Status
IPPV Status
Credit
Smartcard Version
Smartcard Revision
CA Version
CA Revision
Smartcard Zipcode
Smartcard Serial Number
Set Top Box Serial Number
SNR Estimate
Pre RS Error Rate
Post RS Error Rate
Lock Status
Last PAT
Last CAT
Channel Table
Number of Transport Streams
Number of Services
AGC Combined
Locked
LOOKING FOR UPDATES

Fig. 14


Imagine SA - STB Manager
Last Name
First Name
Cancel
Search
1402

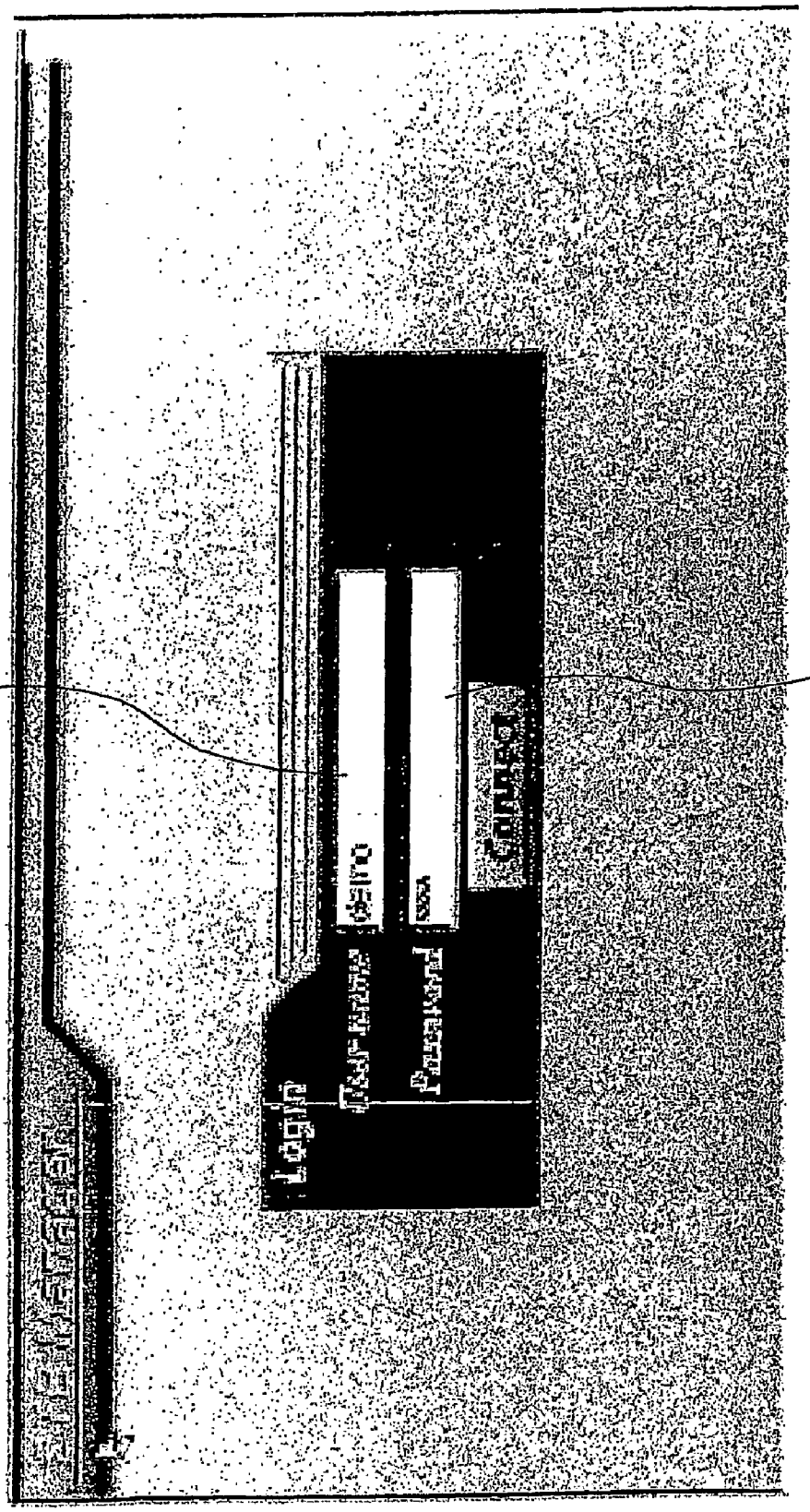


Fig. 15

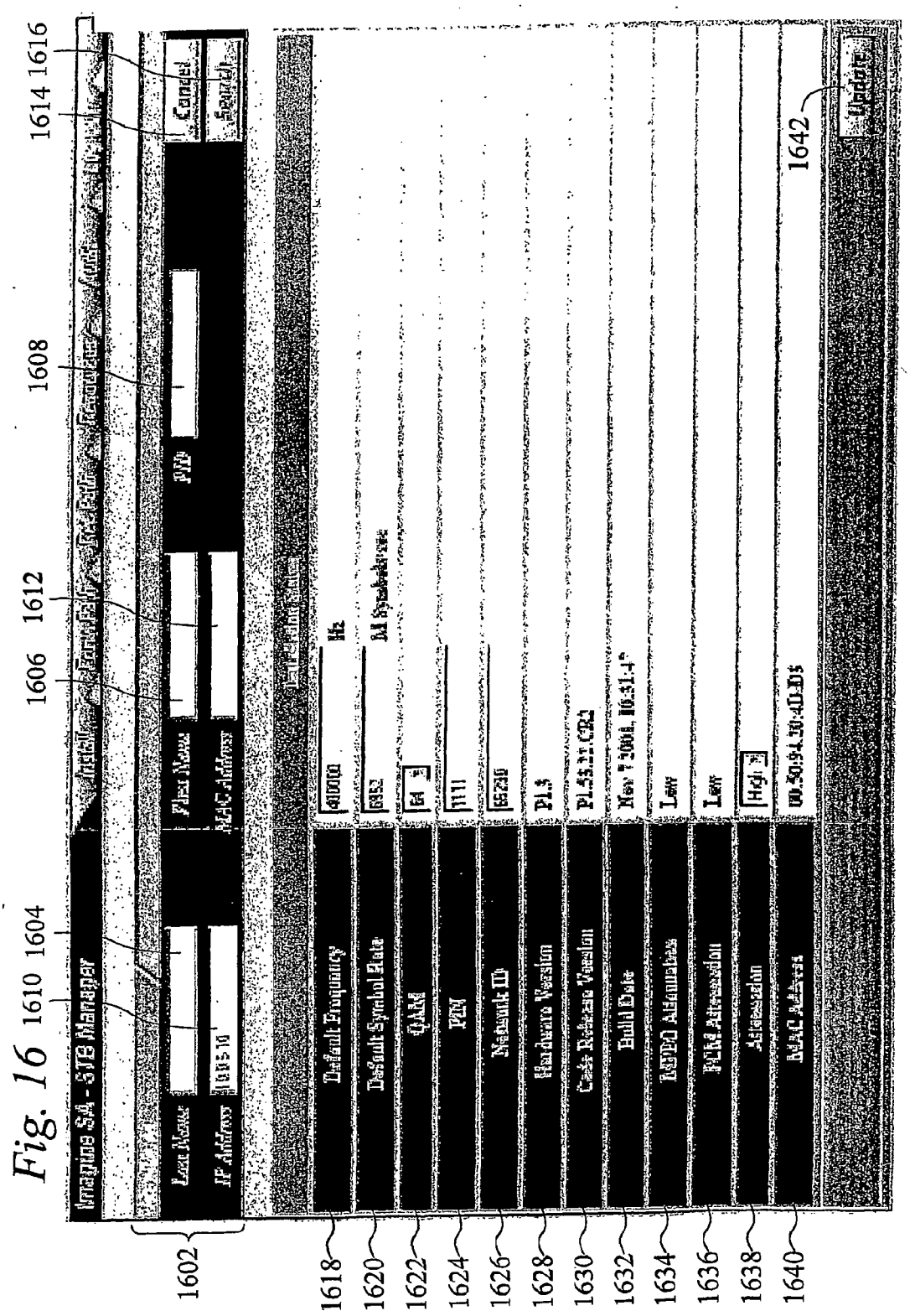

1602
1604
1606
1608
1610
1612
1614
1616
1618
1620
1622
1624
1626
1628
1630
1632
1634
1636
1638
1640
1642
Cancel
Search
Update

Fig. 16

Fig. 17

Integrated SA - STB Manager
Last Name
IP Address
First Name
MAC Address
RID
Cancel
Search
Nagra Serial Number
Smartcard Status
IPPV Status
Credit
Smartcard Version
Smartcard Revision
CA Version
CA Revision
Smartcard Zipcode
Smartcard Serial Number
Set Top Box Serial Number
SNR Estimate
Pre RS Error Rate
Post RS Error Rate
Lock Status
Last PAT
Last CAT
Channel Table
Number of Transport Streams
Number of Services
AGC Combined
Locked
LOOKING FOR UPDATES
1722
1724
1726
1728
1730
1732
1734
1736
1738
1740
1742
1702
1704
1706
1708
1710
1712
1714
1716
1718
1720

Fig. 18

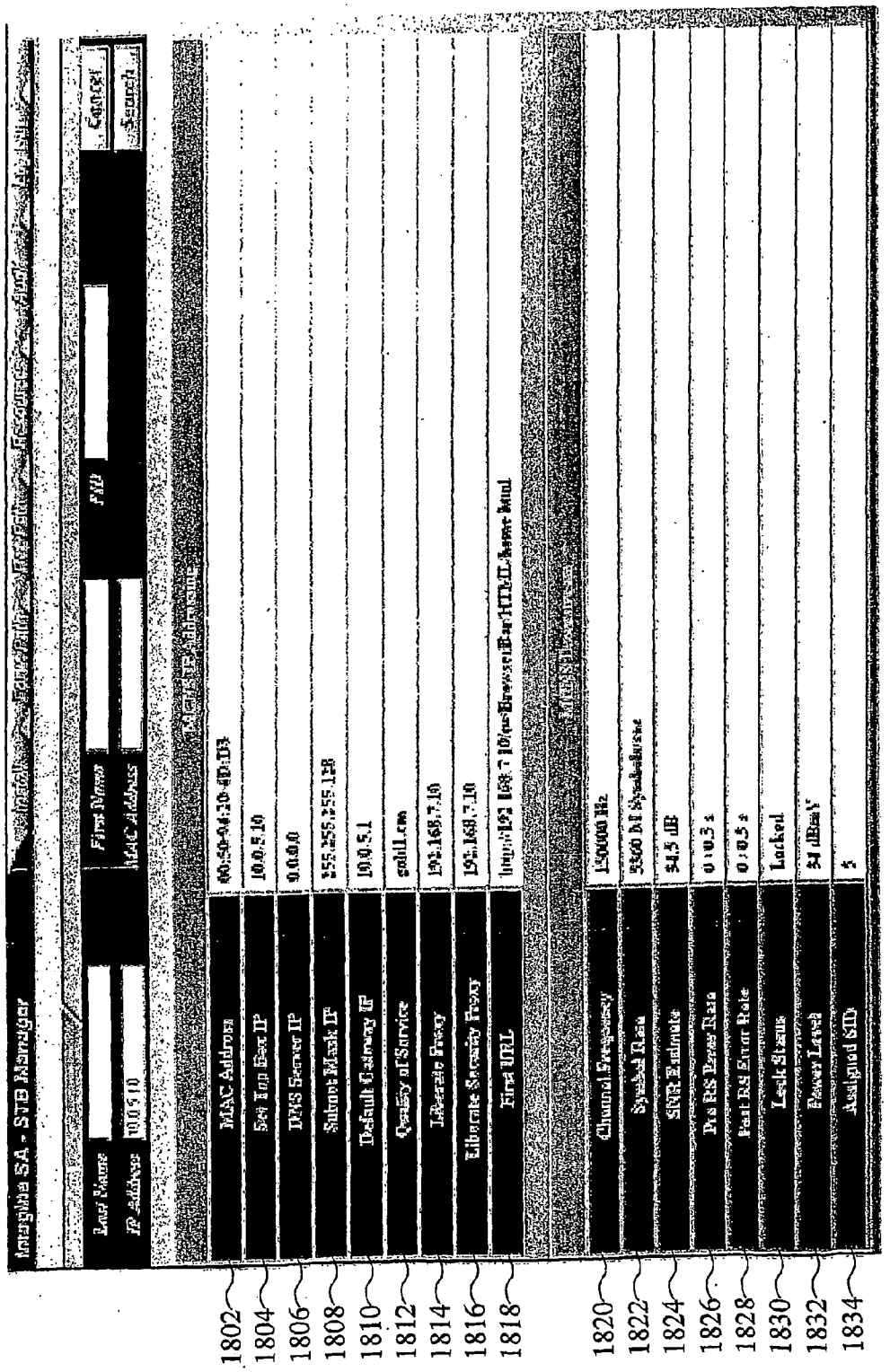
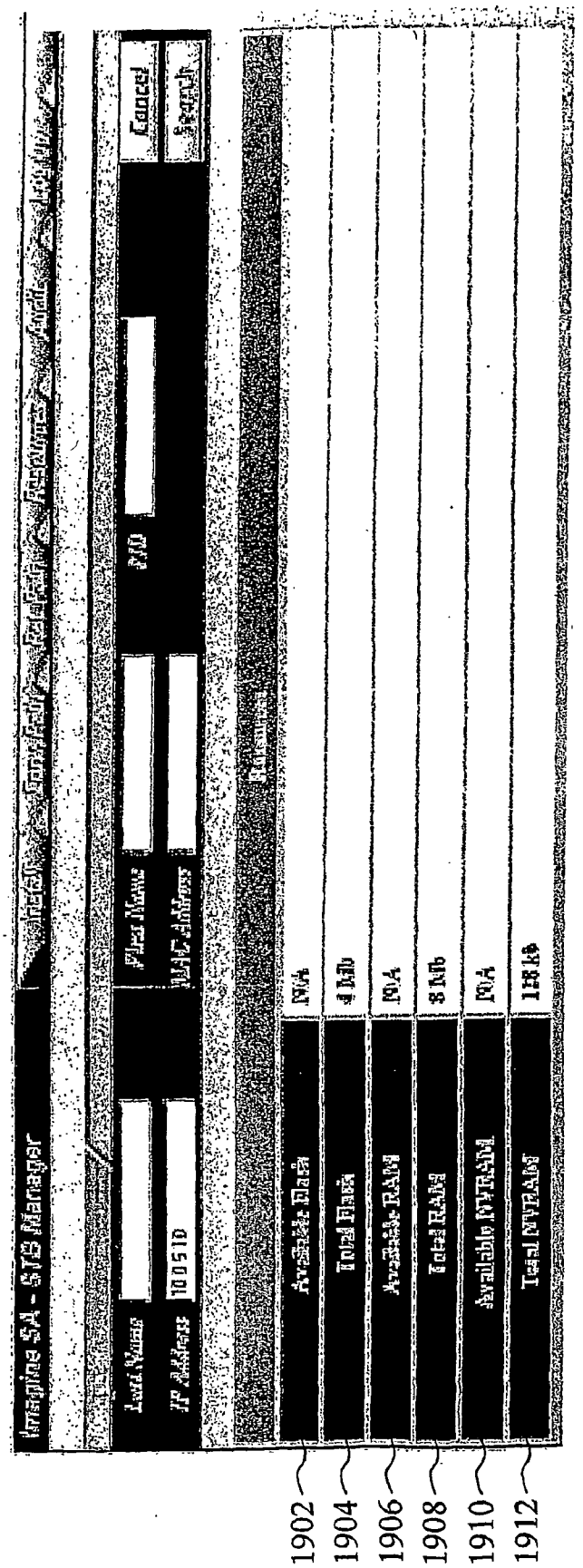

1802
1804
1806
1808
1810
1812
1814
1816
1818
1820
1822
1824
1826
1828
1830
1832
1834

Fig. 19


Imagine SA - STB Manager
Cancel
Search
Available Flash
Total Flash
Available RAM
Total RAM
Available NVRAM
Total NVRAM
1902
1904
1906
1908
1910
1912

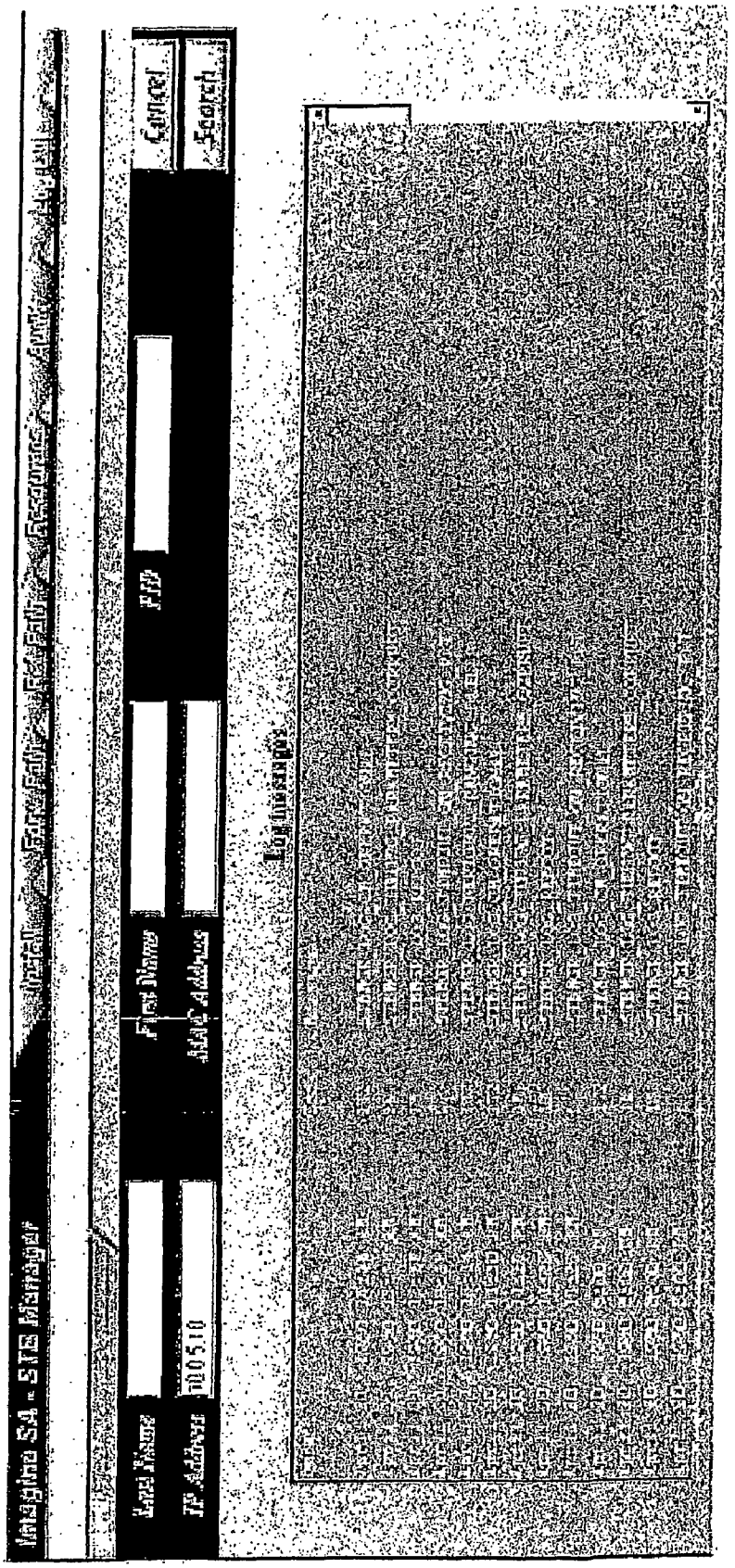


Fig. 20

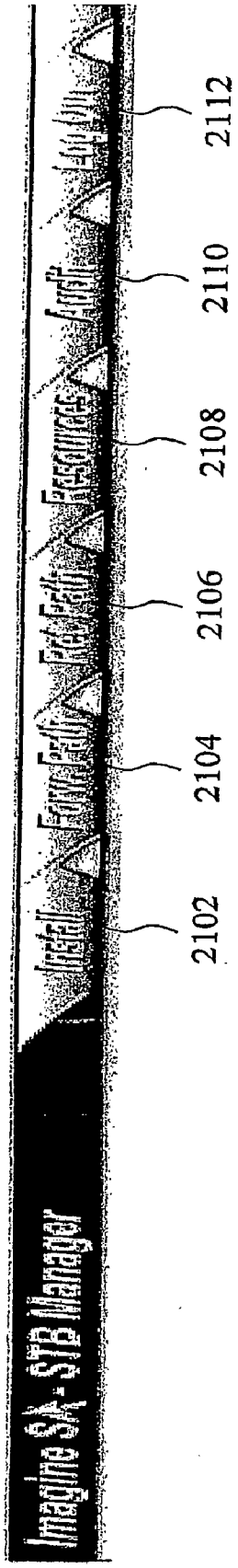

Imagine SA - STB Manager
Install
Fav Fath
Fed Fath
Resources
Audit
Log Out
2102
2104
2106
2108
2110
2112

Fig. 21

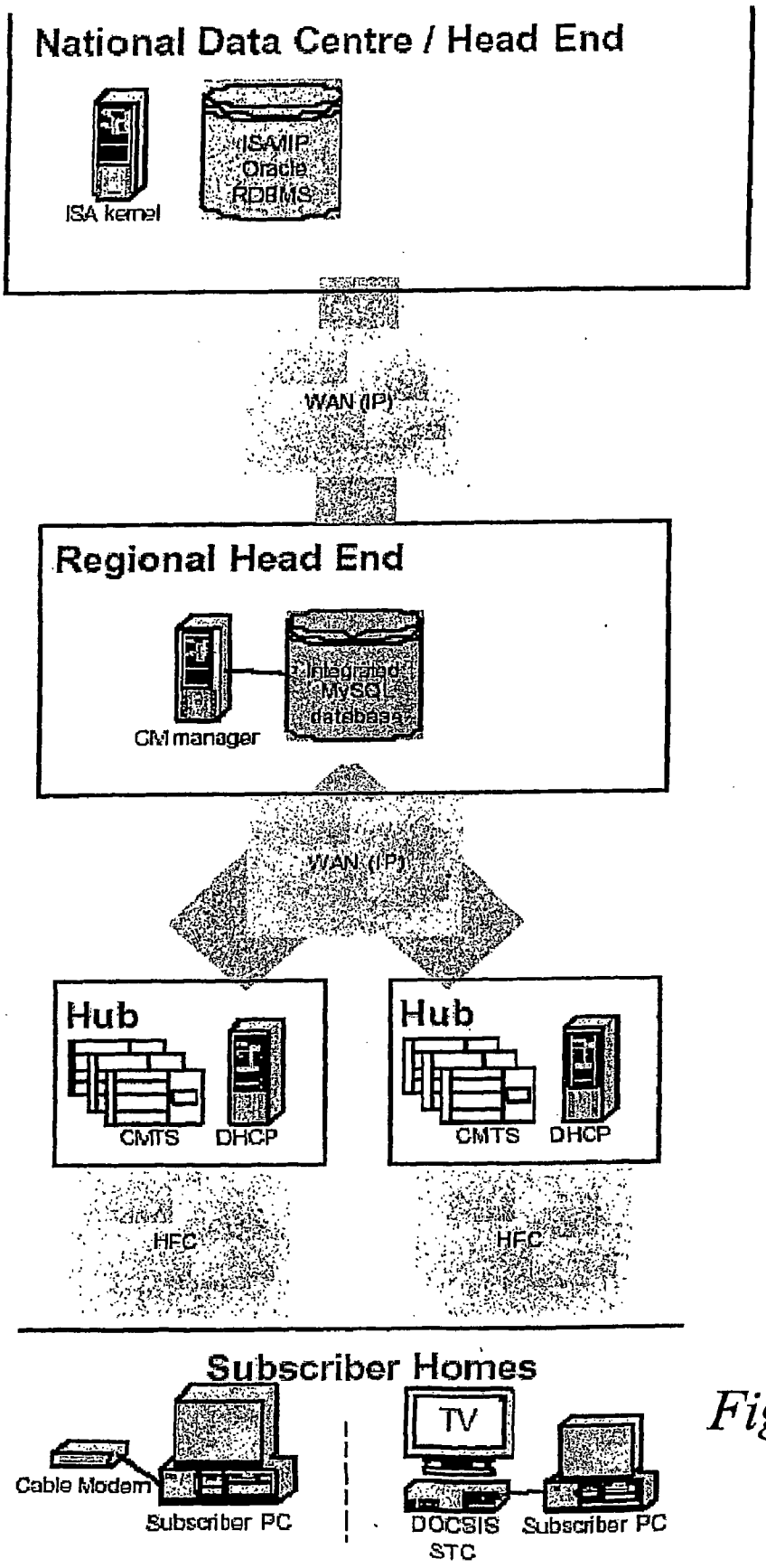

National Data Centre / Head End
ISA kernel
ISA/IP
Oracle
RDBMS
WAN (IP)
Regional Head End
CM manager
Integrated
MySQL
database
WAN (IP)
Hub
CMTS
DHCP
Hub
CMTS
DHCP
HFC
HFC
Subscriber Homes
Cable Modem
Subscriber PC
TV
DOCSIS
STC
Subscriber PC

Fig. 22

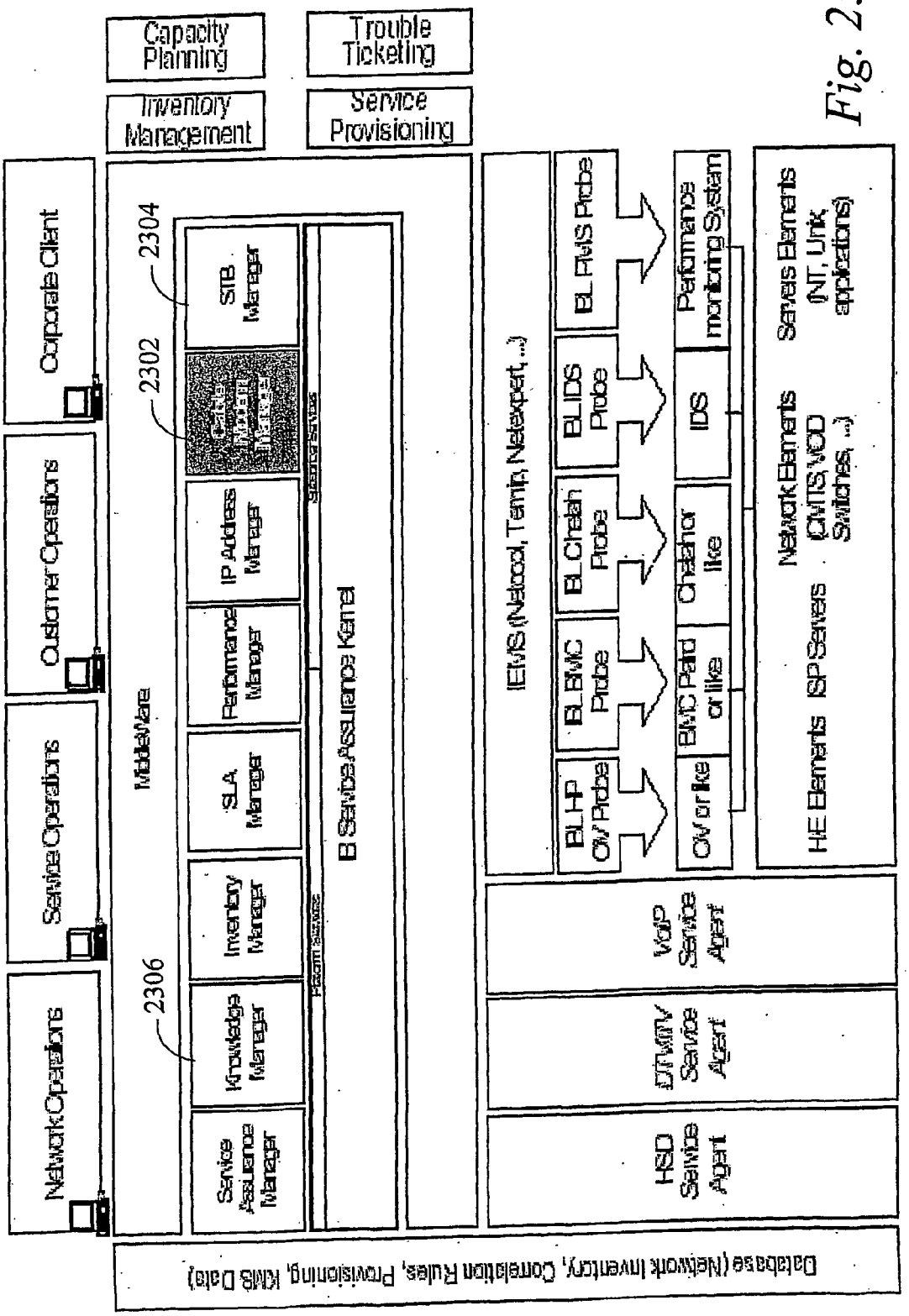

Capacity Planning
Trouble Ticketing
Inventory Management
Service Provisioning
Corporate Client
Customer Operations
Service Operations
Network Operations
MiddleWare
2304
2302
2306
STB Manager
Cable Modem Manager
IP Address Manager
Performance Manager
SLA Manager
Inventory Manager
Knowledge Manager
Service Assurance Manager
Platform Services
Service Services
B Service Assurance Kernel
IEMS (Netcool, Temip, Netexpert, ...)
BL PMS Probe
BL IDS Probe
BL Chelah Probe
BL BMC Probe
BL HP OV Probe
Performance monitoring System
IDS
Chelah or like
BMC Patrol or like
OV or like
Servers Elements (NT, Unix, applications)
Network Elements (CMTS, VOD Switches, ...)
ISP Servers
H/E Elements
VoIP Service Agent
DTMTV Service Agent
HSD Service Agent
Database (Network Inventory, Correlation Rules, Provisioning, KMS Data)

Fig. 23

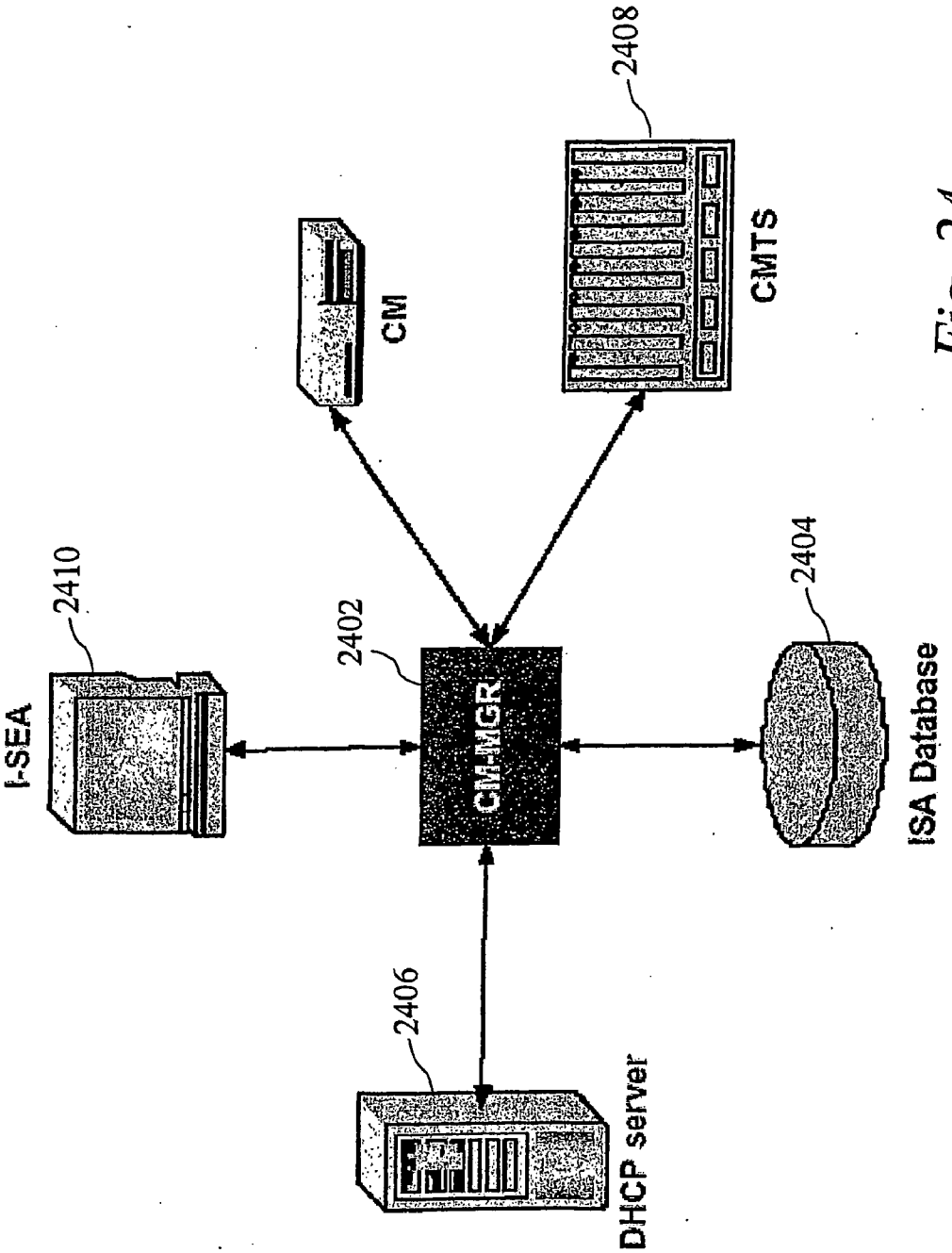
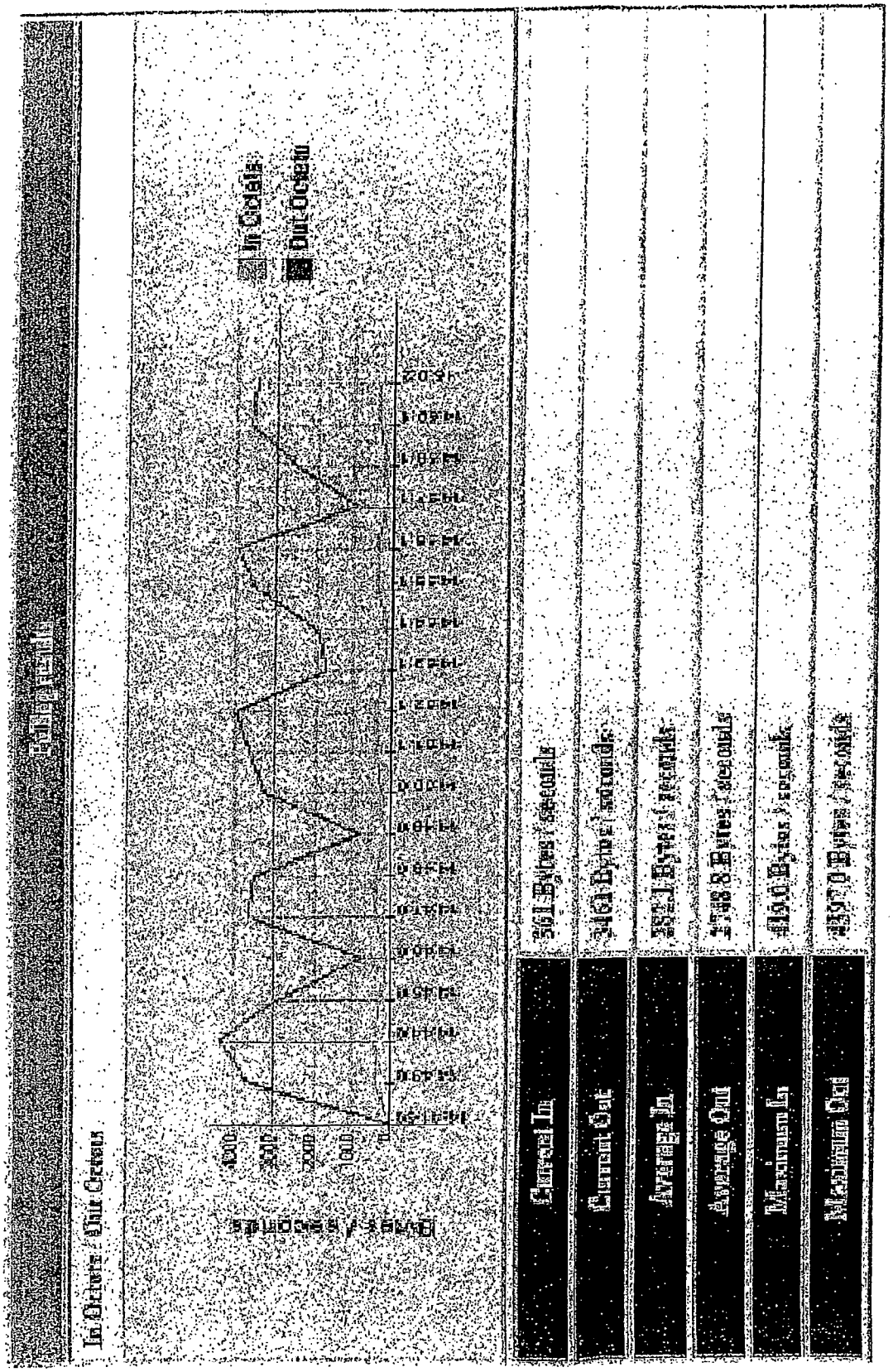

2410
I-SEA
2402
CM-MGR
CM
2408
CMTS
2404
ISA Database
2406
DHCP server

Fig. 24

Fig. 25


In Octets / Out Octets
Bytes / seconds
In Octets
Out Octets
Current In
Current Out
Average In
Average Out
Maximum In
Maximum Out

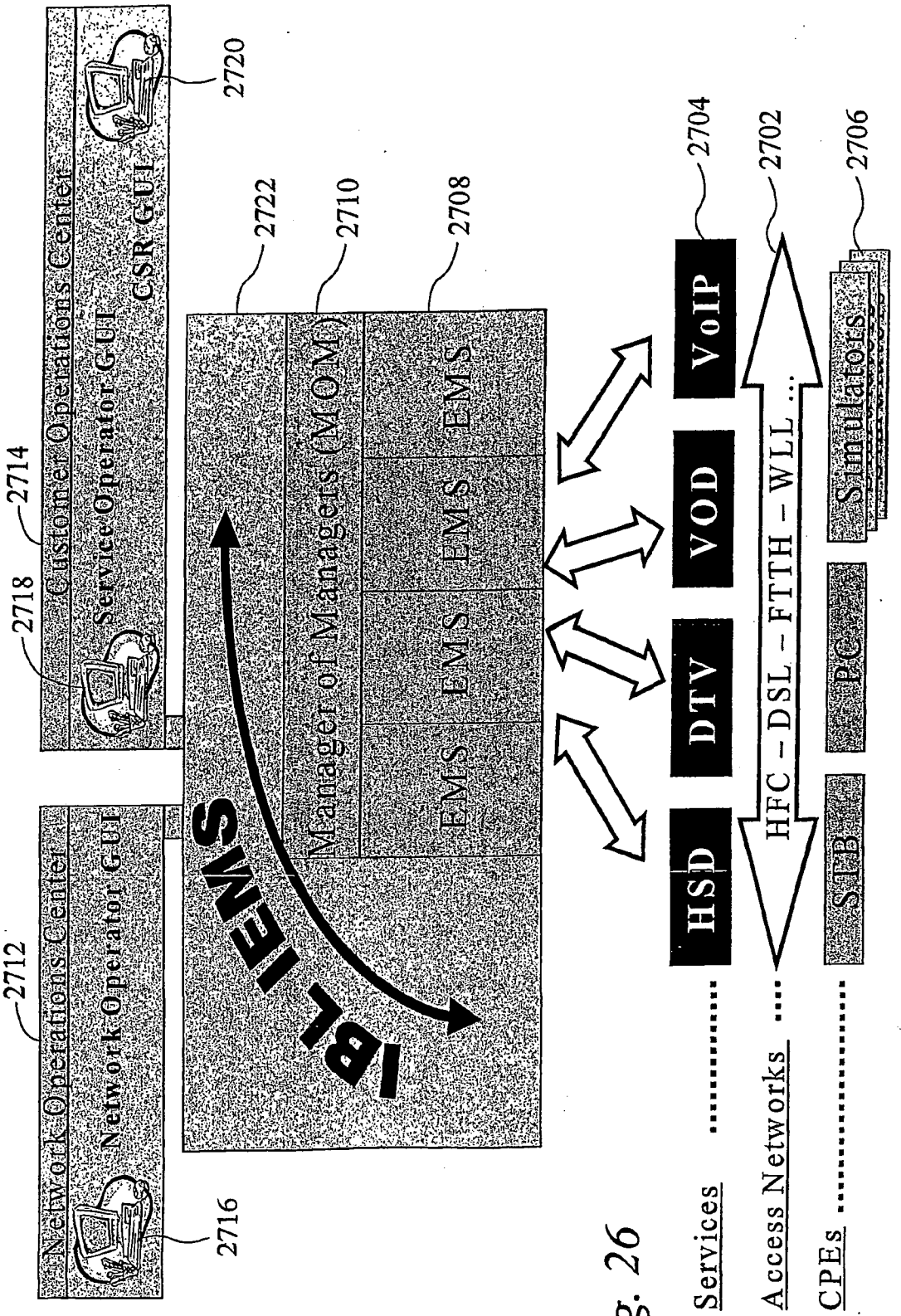

Network Operations Center
Network Operator GUI
Customer Operations Center
Service Operator GUI
GSR GUI
2712
2714
2716
2718
2720
2722
2710
2708
Manager of Managers (MOM)
EMS
EMS
EMS
EMS
BL-EMS
HSD
DTV
VOD
VoIP
2704
2702
HFC – DSL – FTTH – WLL ...
STB
PC
Simulators
2706
Services
Access Networks
CPEs

Fig. 26

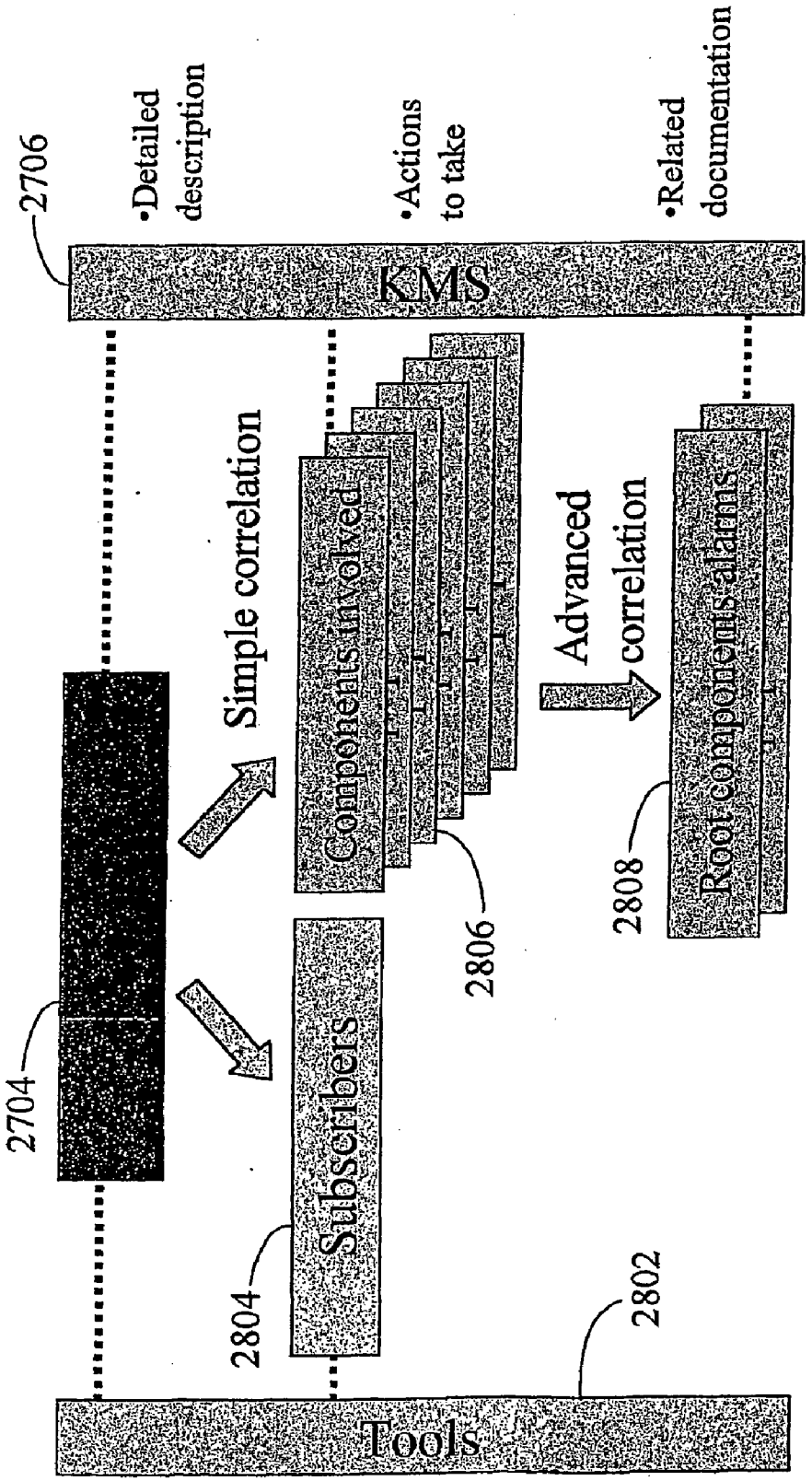

2706
•Detailed description
•Actions to take
•Related documentation
KMS
Simple correlation
Components involved
Advanced correlation
Root components/alarms
2808
2806
2704
Subscribers
2804
2802
Tools

Fig. 27

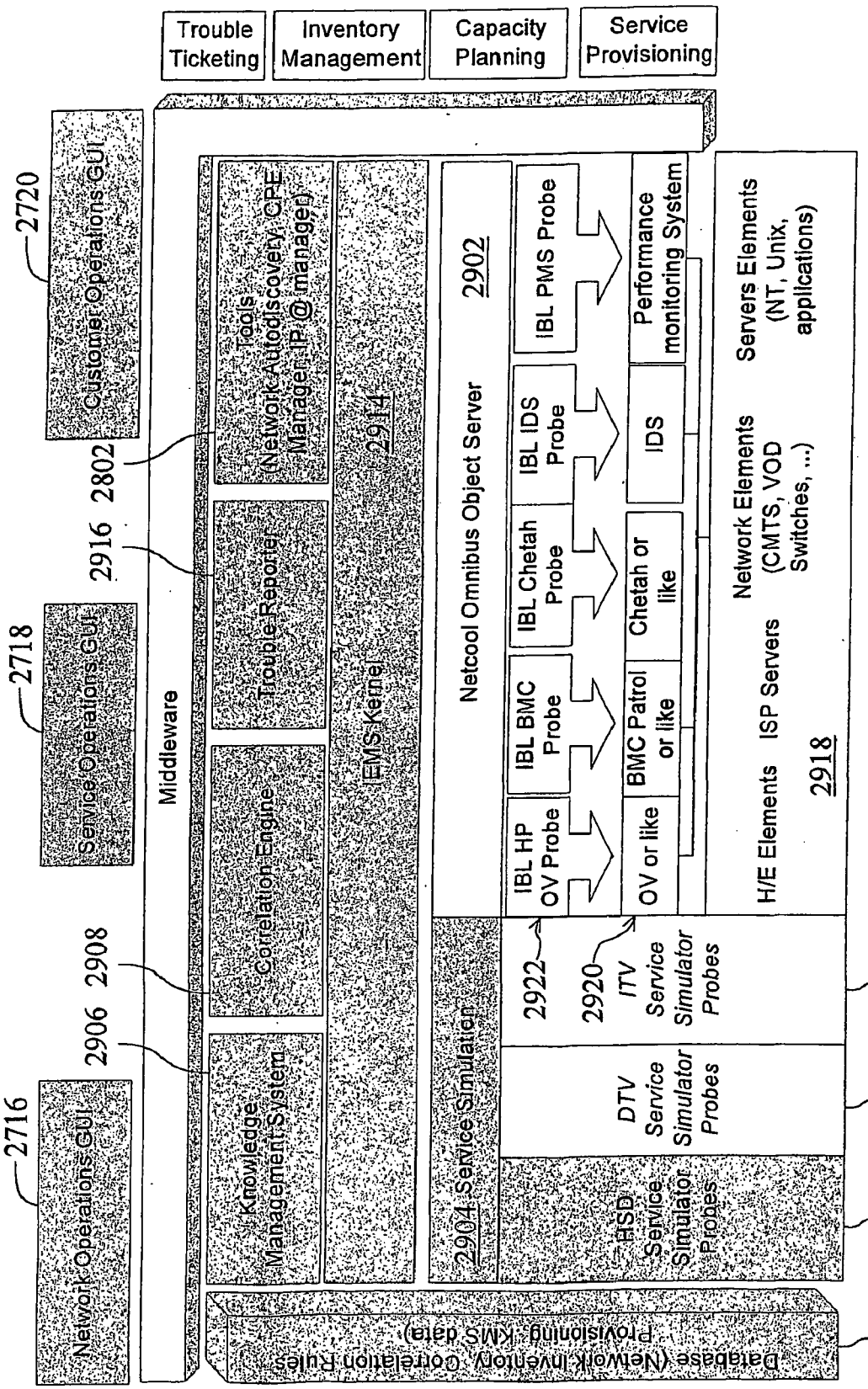

Trouble Ticketing
Inventory Management
Capacity Planning
Service Provisioning
Customer Operations GUI
2720
Service Operations GUI
2718
Network Operations GUI
2716
Middleware
Tools (Network Autodiscovery, CPE Manager, IP @ manager)
2802
Trouble Reporter
2916
Correlation Engine
2908
Knowledge Management System
2906
EMS Kernel
2914
Netcool Omnibus Object Server
2902
IBL HP OV Probe
IBL BMC Probe
IBL Chetah Probe
IBL IDS Probe
IBL PMS Probe
OV or like
BMC Patrol or like
Chetah or like
IDS
Performance monitoring System
Servers Elements (NT, Unix, applications)
Network Elements (CMTS, VOD Switches, ...)
H/E Elements
ISP Servers
2918
2922
2920
ITV Service Simulator Probes
2912
DTV Service Simulator Probes
2912
2904 Service Simulation
HSD Service Simulator Probes
2912
Database (Network Inventory, Correlation Rules, Provisioning, KMS data)
2910

Fig. 28

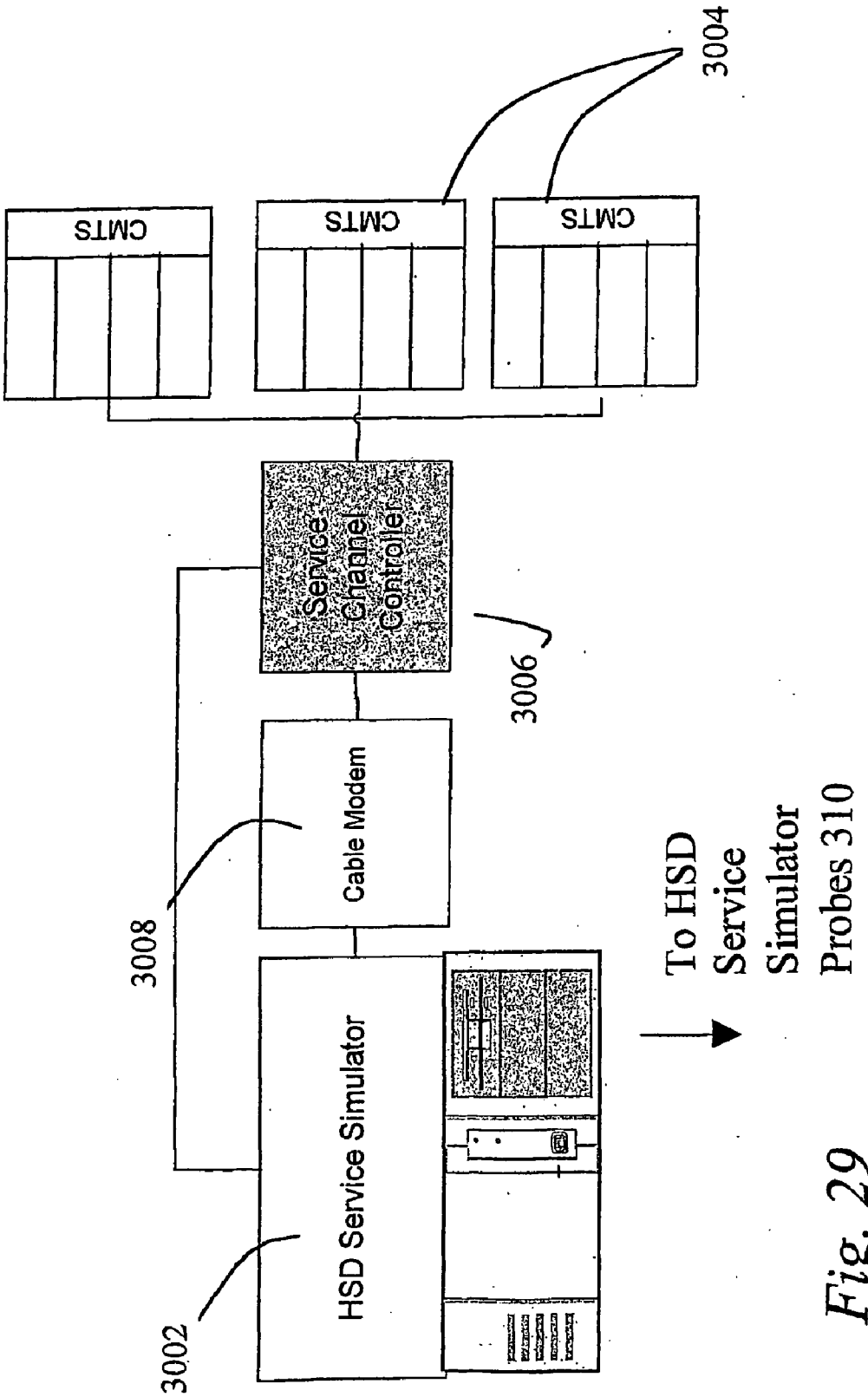

CMTS
CMTS
CMTS
3004
Service Channel Controller
3006
Cable Modem
3008
HSD Service Simulator
3002
To HSD Service Simulator Probes 310

Fig. 29

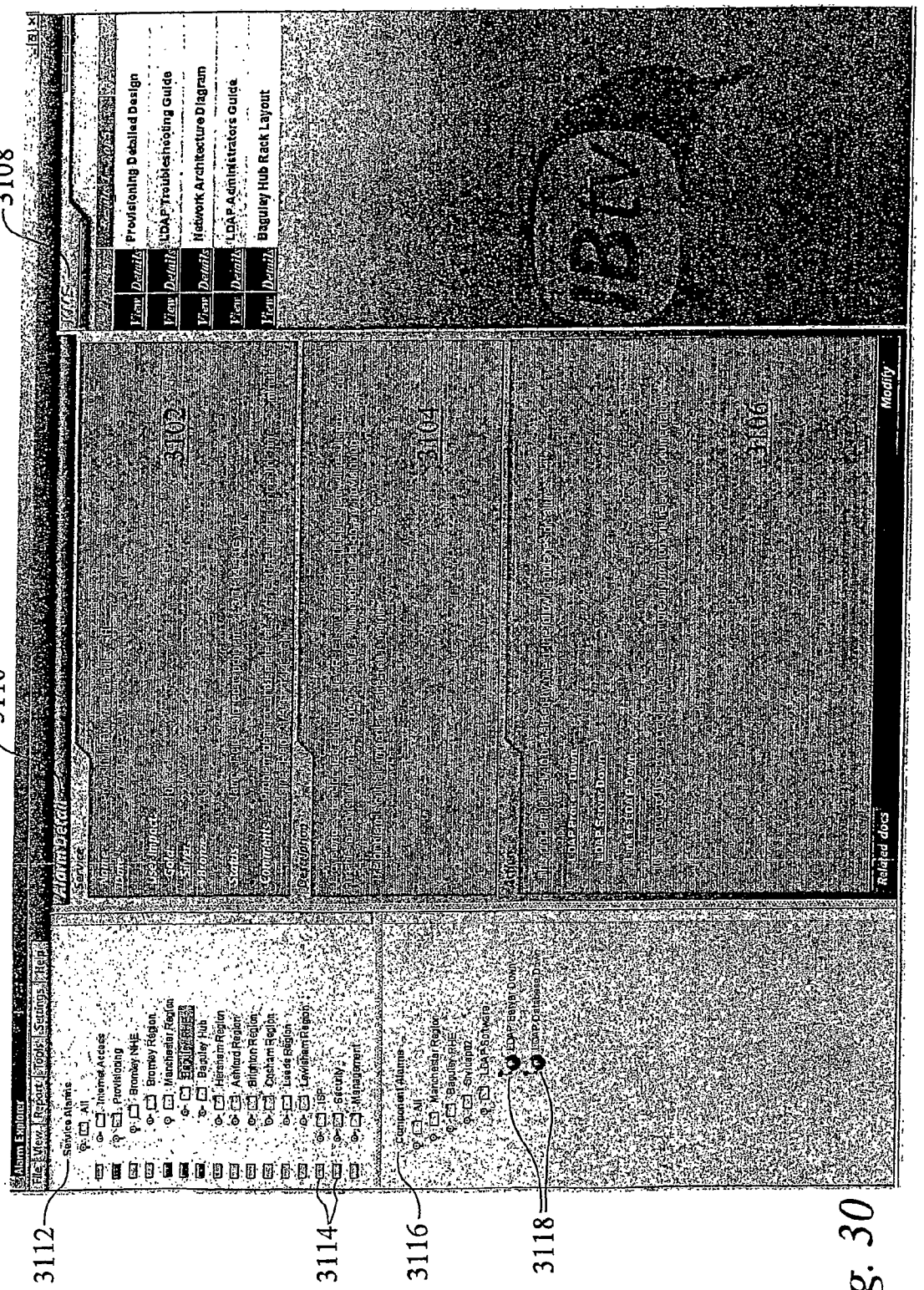

3108
3110
3112
3114
3116
3118
3102
3104
3106
Alarm Explorer
Alarm Detail
Provisioning Detailed Design
LDAP Troubleshooting Guide
Network Architecture Diagram
LDAP Administrators Guide
Baguley Hub Rack Layout
Related docs
Modify

Fig. 30

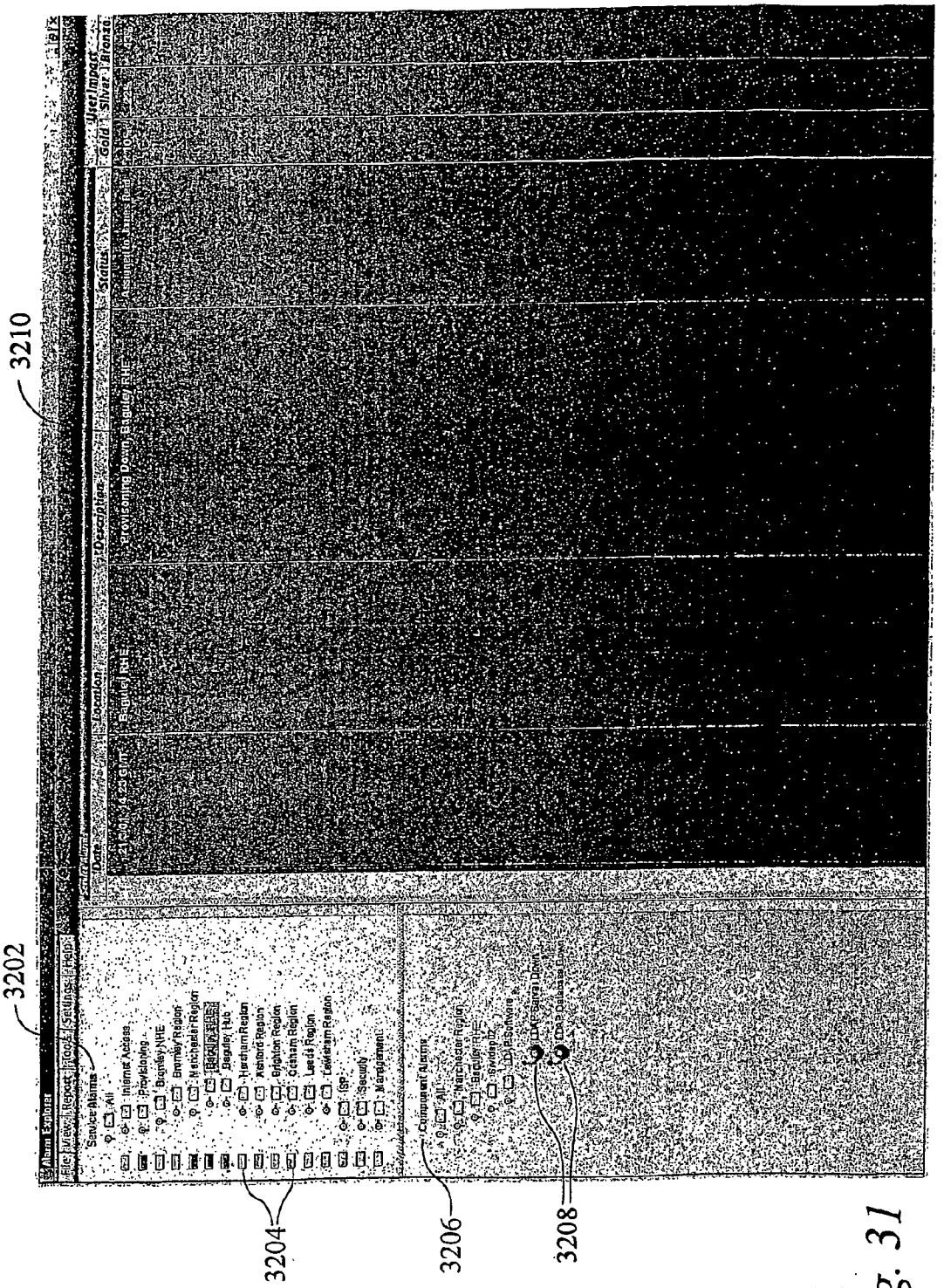


Fig. 31

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 031

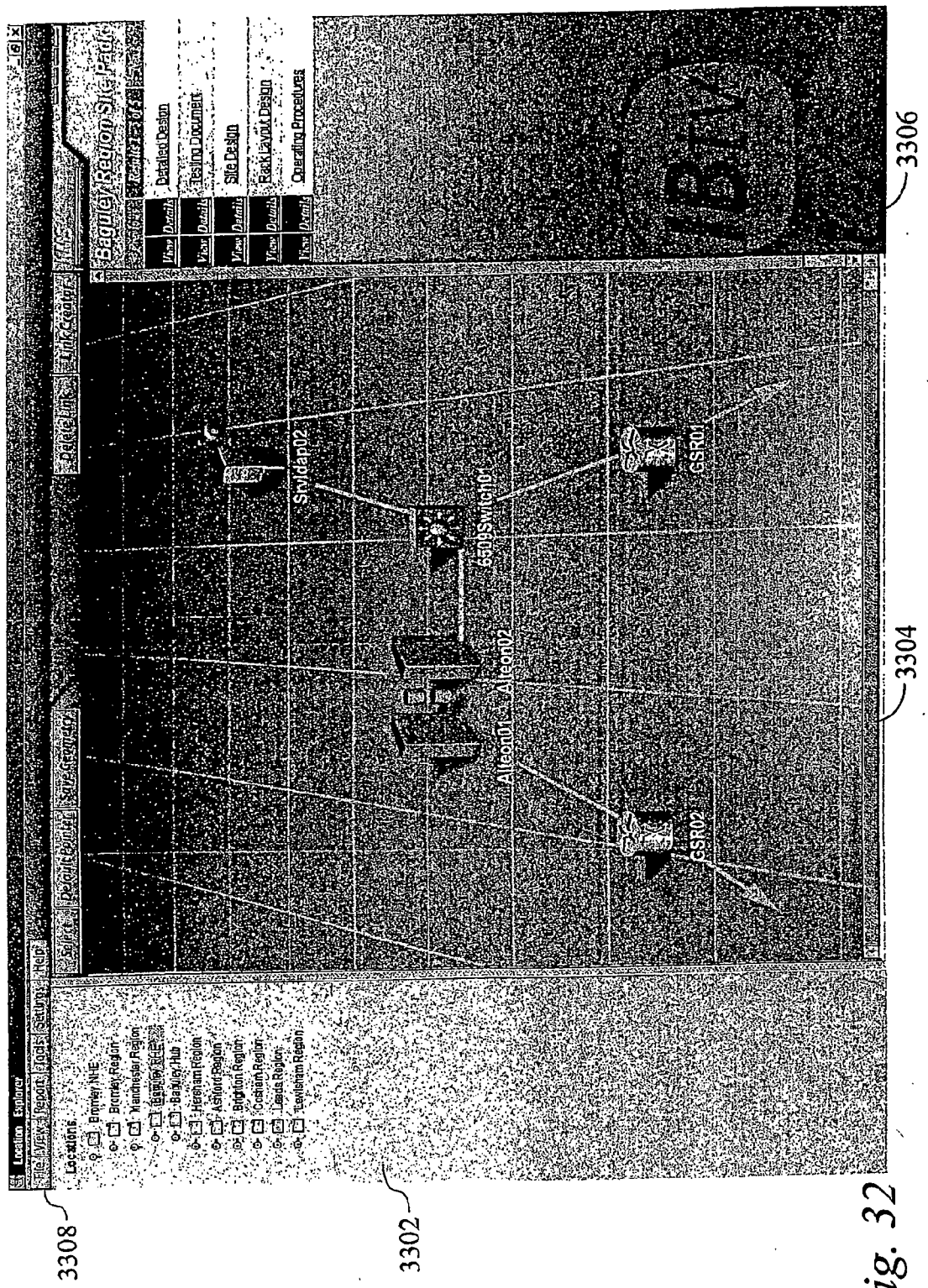

Location Explorer
File View Report Tools Settings Help
Locations
Bromley NHE
Bromley Region
Manchester Region
Bagley Hub
Hersham Region
Ashford Region
Brighton Region
Cosham Region
Leeds Region
Lewisham Region
Select
Default Pointer
Save Geometry
Delete Link
Link Creator
Bagley Region Site Pack
Detailed Design
Testing Document
Site Design
Rack Layout Design
Operating Procedures
View Details
Srvldap02
6509Switch01
Alteon01
Alteon02
GSR01
GSR02
3306
3304
3308
3302

Fig. 32

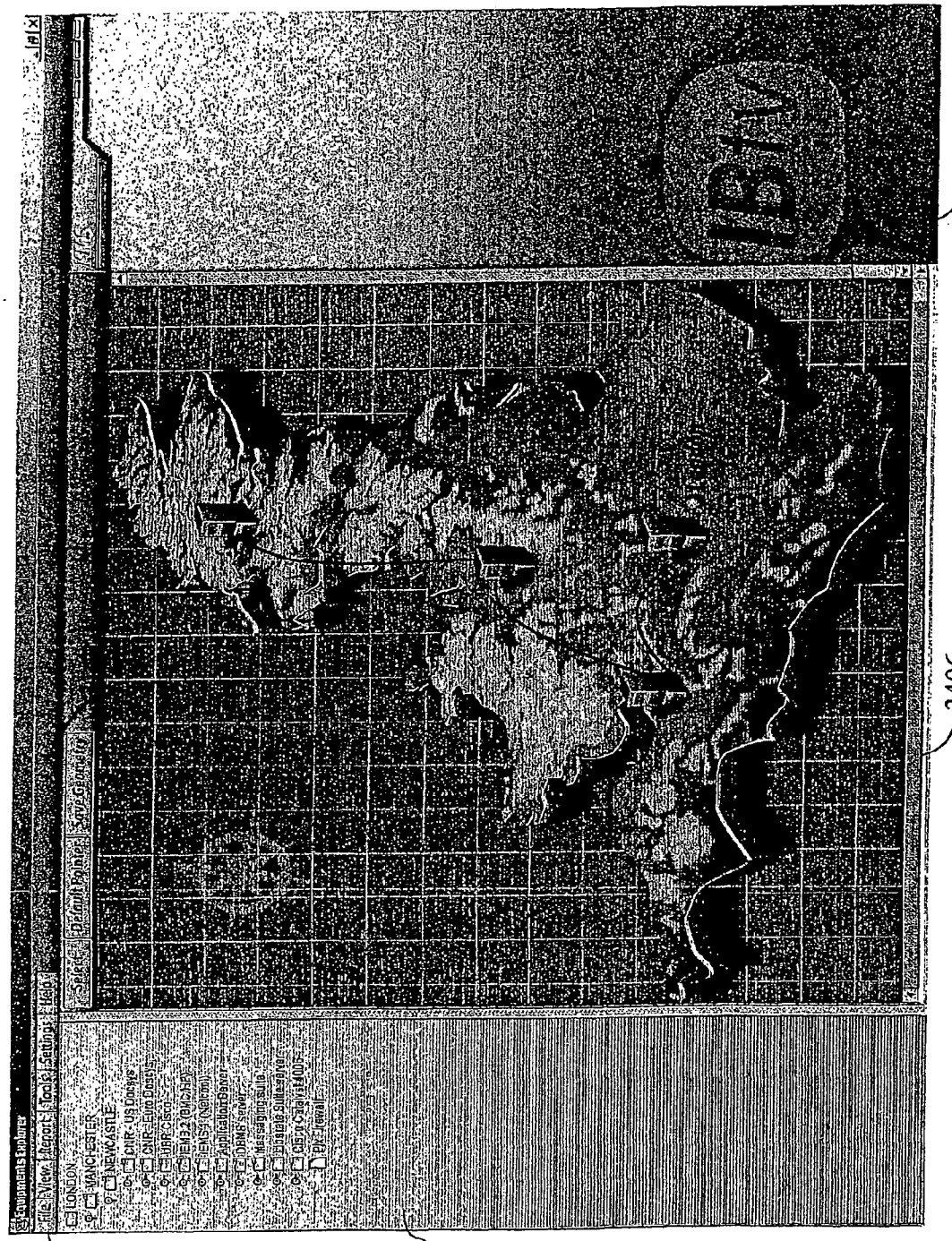

Equipment Explorer
File View Report Tools Settings Help
LONDON
MANCHESTER
NEWCASTLE
Select
Default Points
Save Current
3402
3404
3406
3408

Fig. 33

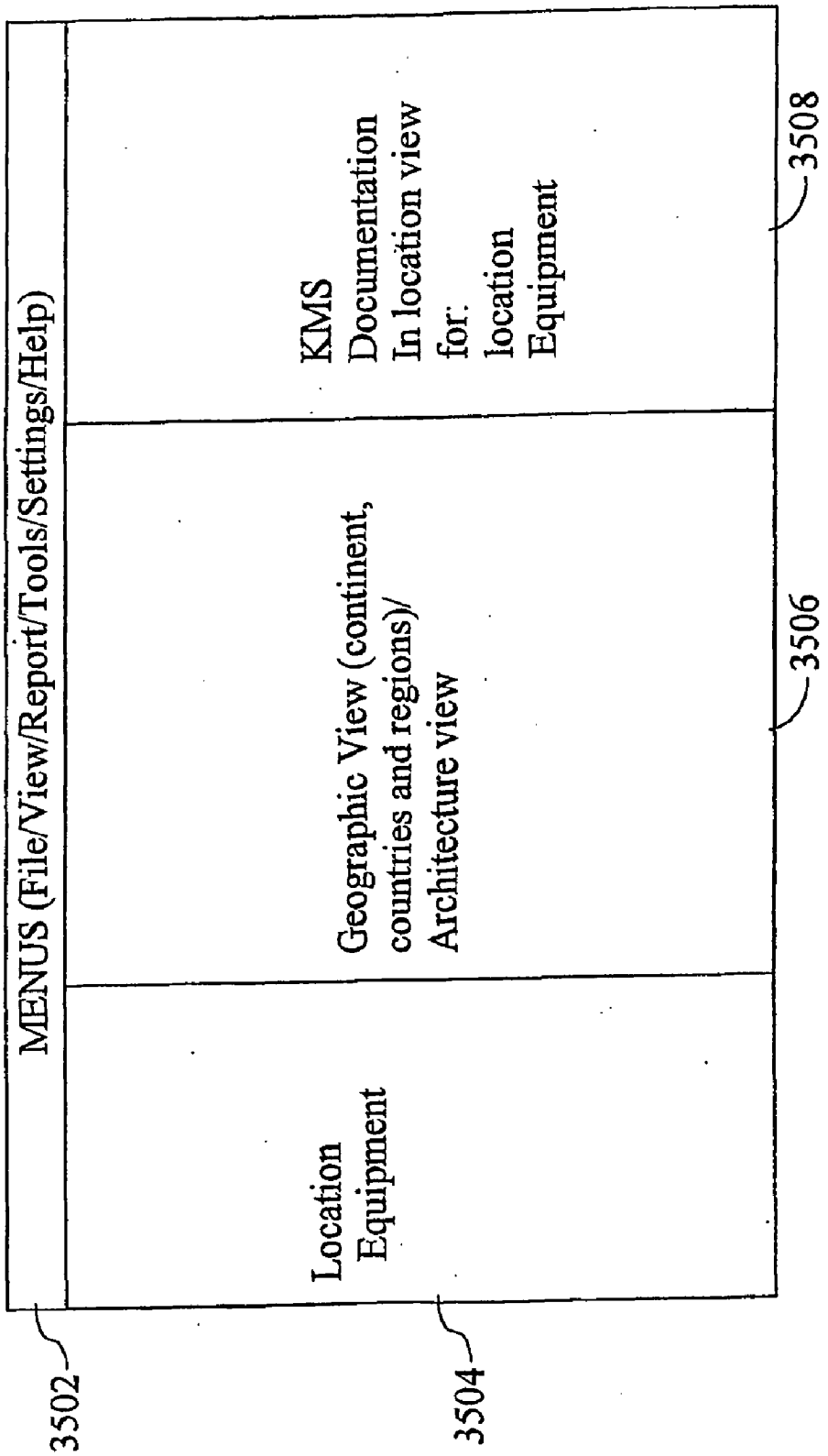

MENUS (File/View/Report/Tools/Settings/Help)
Location
Equipment
Geographic View (continent, countries and regions)/ Architecture view
KMS
Documentation
In location view
for:
location
Equipment
3502
3504
3506
3508

Fig. 34

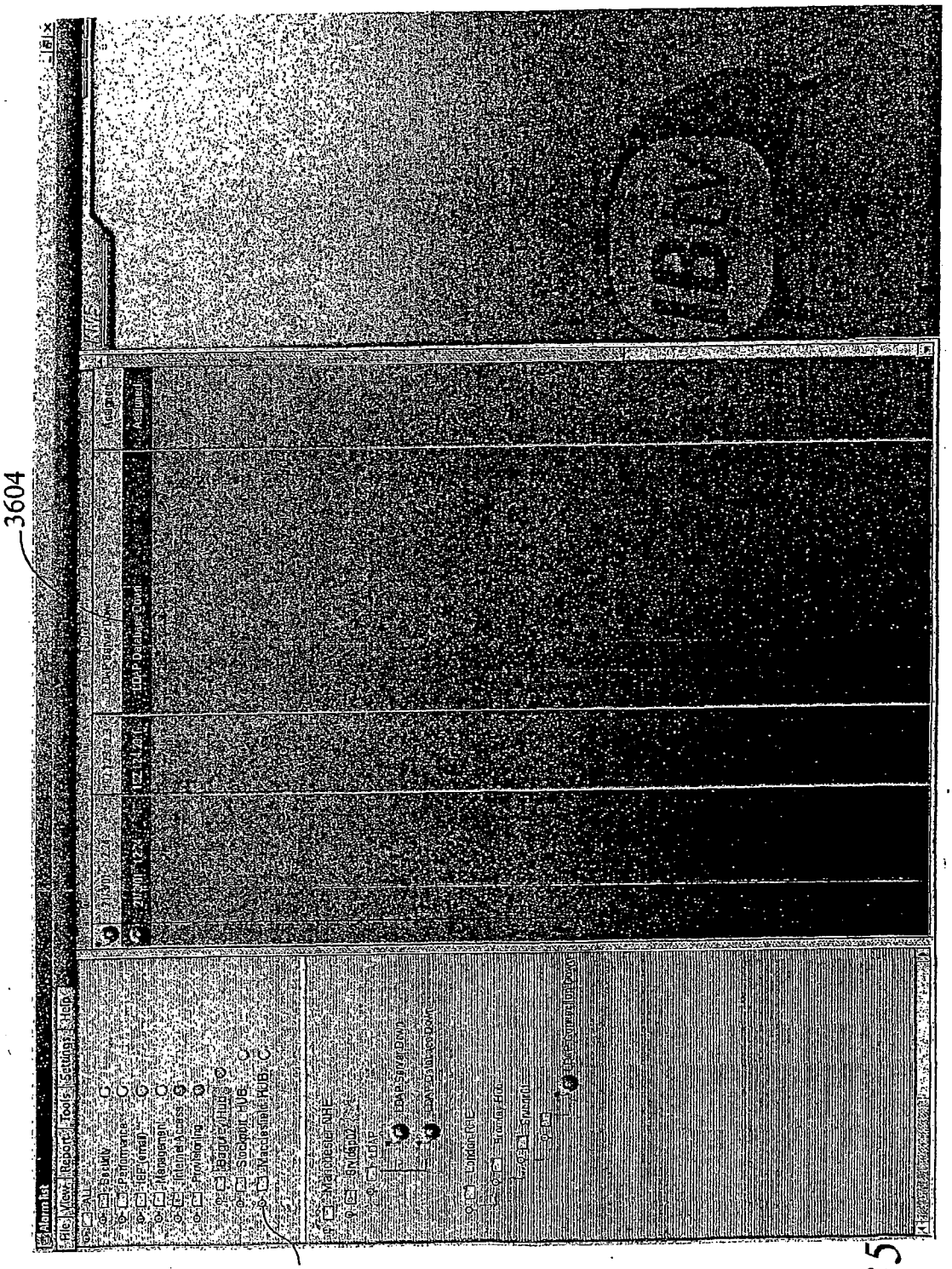


Fig. 35

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 035

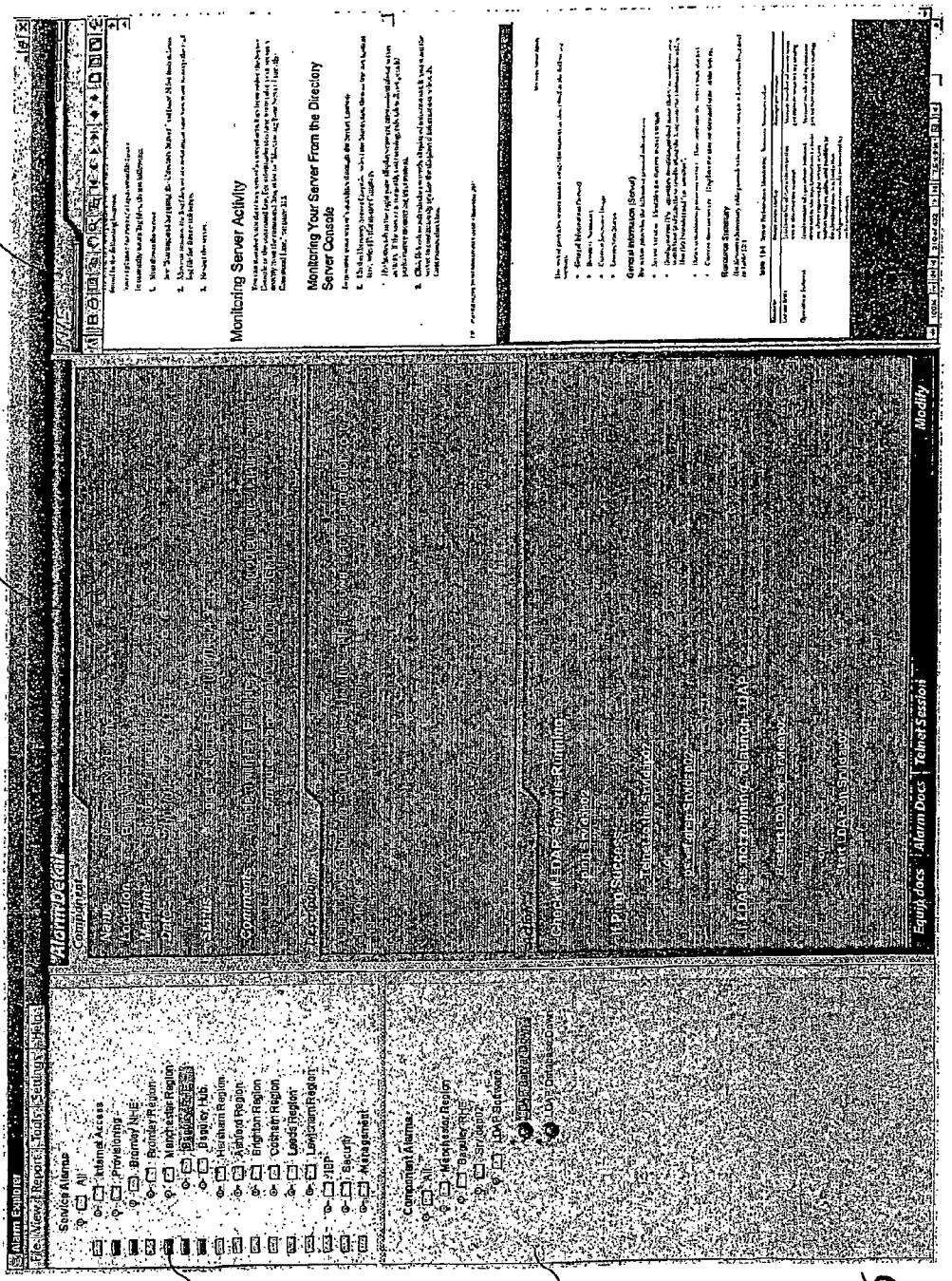

3706
3708
3702
3704
Alarm Explorer
Alarm Detail
Monitoring Server Activity
Monitoring Your Server From the Directory Server Console
Modify

Fig. 36

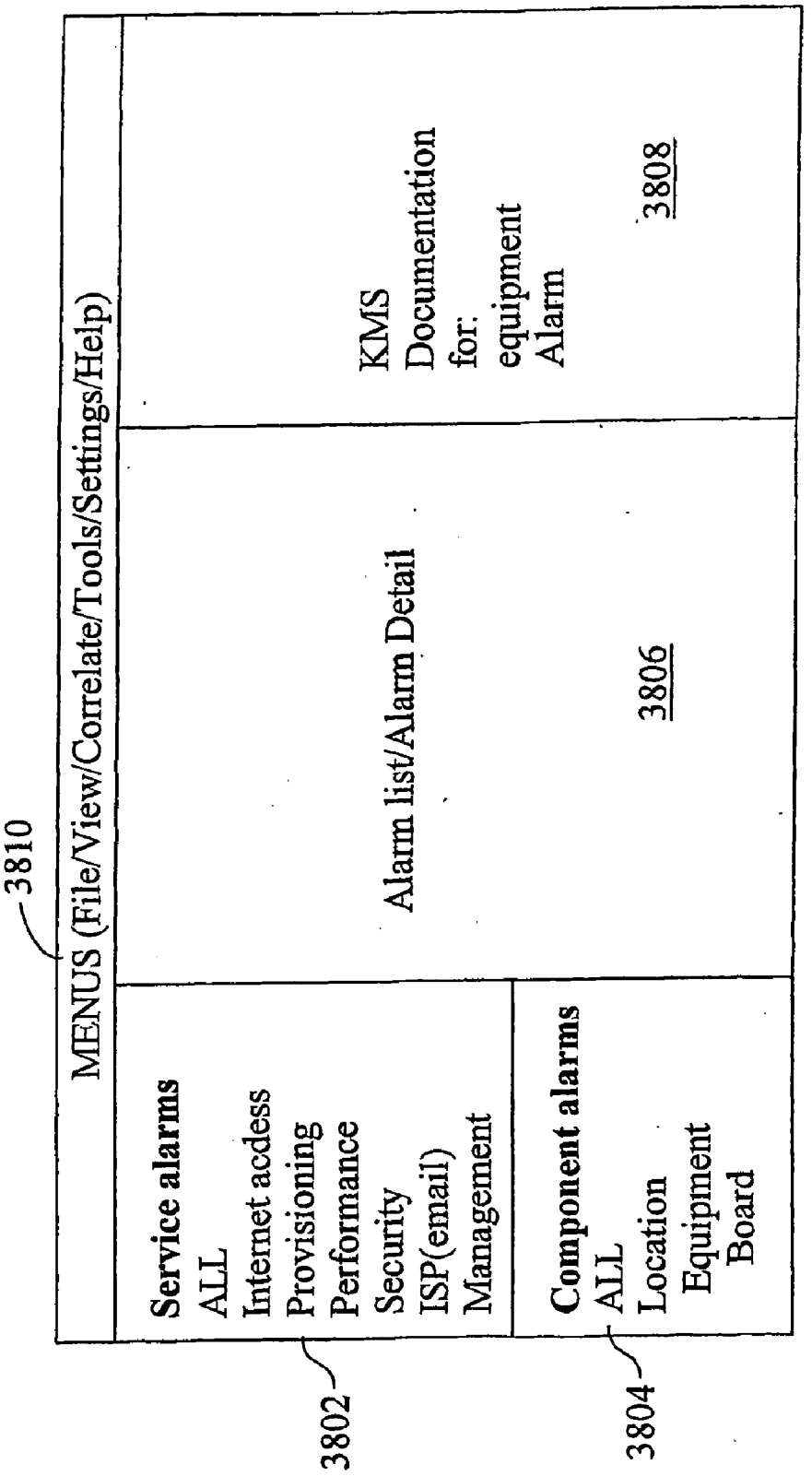

3810
MENUS (File/View/Correlate/Tools/Settings/Help)
Service alarms
ALL
Internet acdess
Provisioning
Performance
Security
ISP(email)
Management
3802
Component alarms
ALL
Location
Equipment
Board
3804
Alarm list/Alarm Detail
3806
KMS
Documentation
for:
equipment
Alarm
3808

Fig. 37

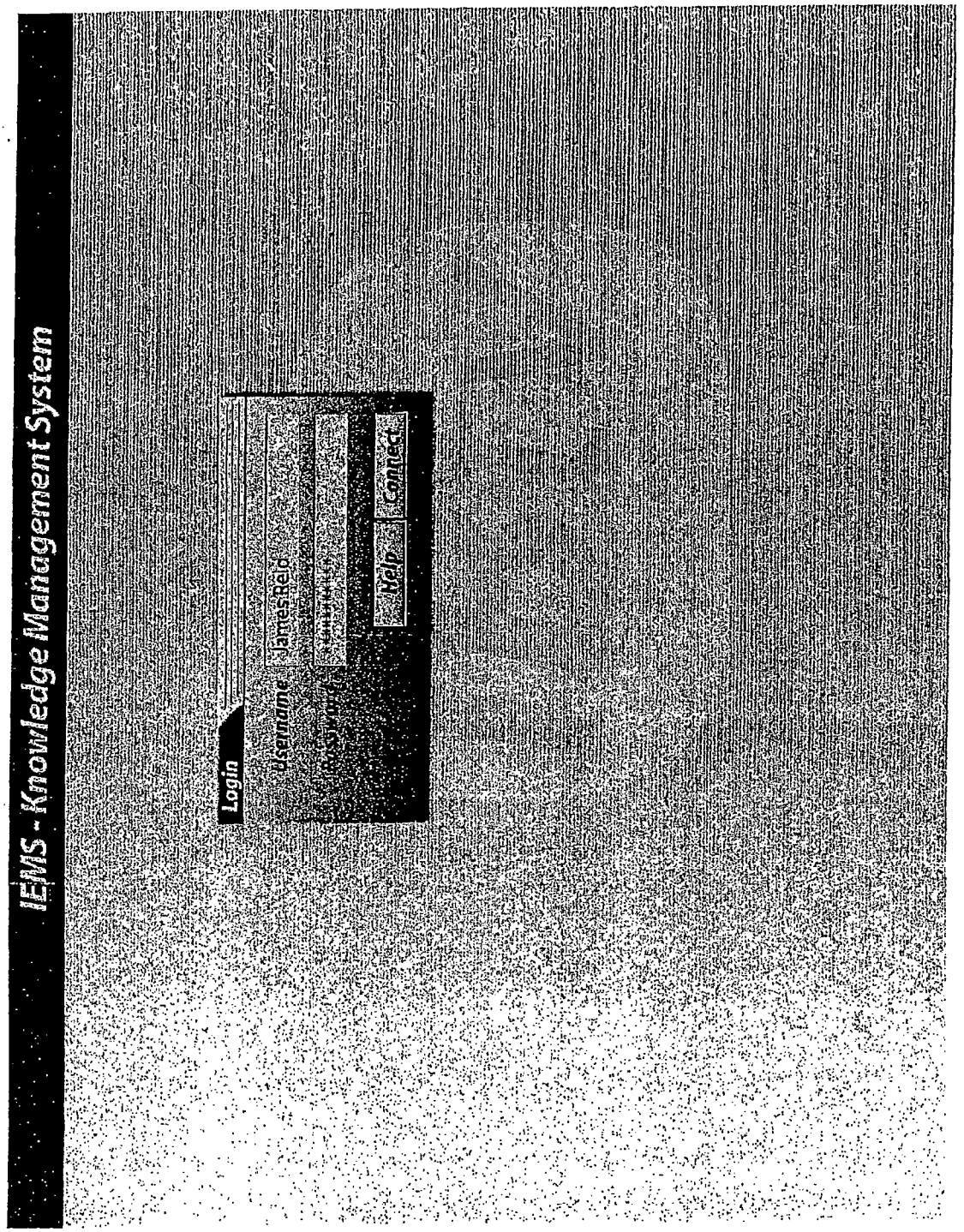

IEMS - Knowledge Management System
Login
Username
Help
Connect

Fig. 38

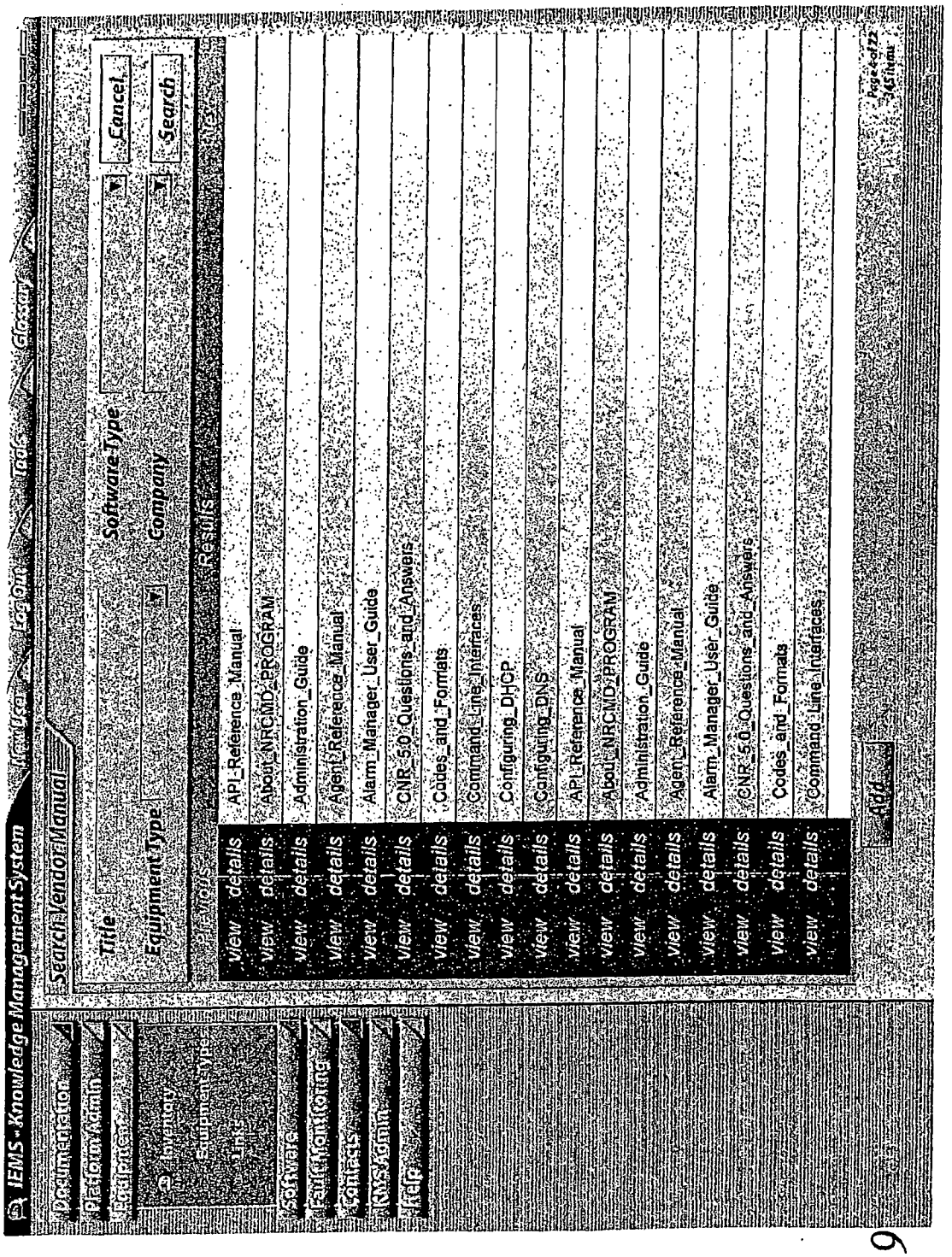

IEMS - Knowledge Management System
New User
Log Out
Tools
Glossary
Documentation
Platform Admin
Equipment
Inventory
Equipment Type
Links
Software
Fault Monitoring
Contacts
KMS Admin
Help
Search Vendor Manual
Title
Software Type
Cancel
Equipment Type
Company
Search
Previous
Results
Next
view details
API_Reference_Manual
About_NRCMD_PROGRAM
Administration_Guide
Agent_Reference_Manual
Alarm_Manager_User_Guide
CNR_5.0_Questions_and_Answers
Codes_and_Formats
Command_Line_Interfaces
Configuring_DHCP
Configuring_DNS
Add

Fig. 39

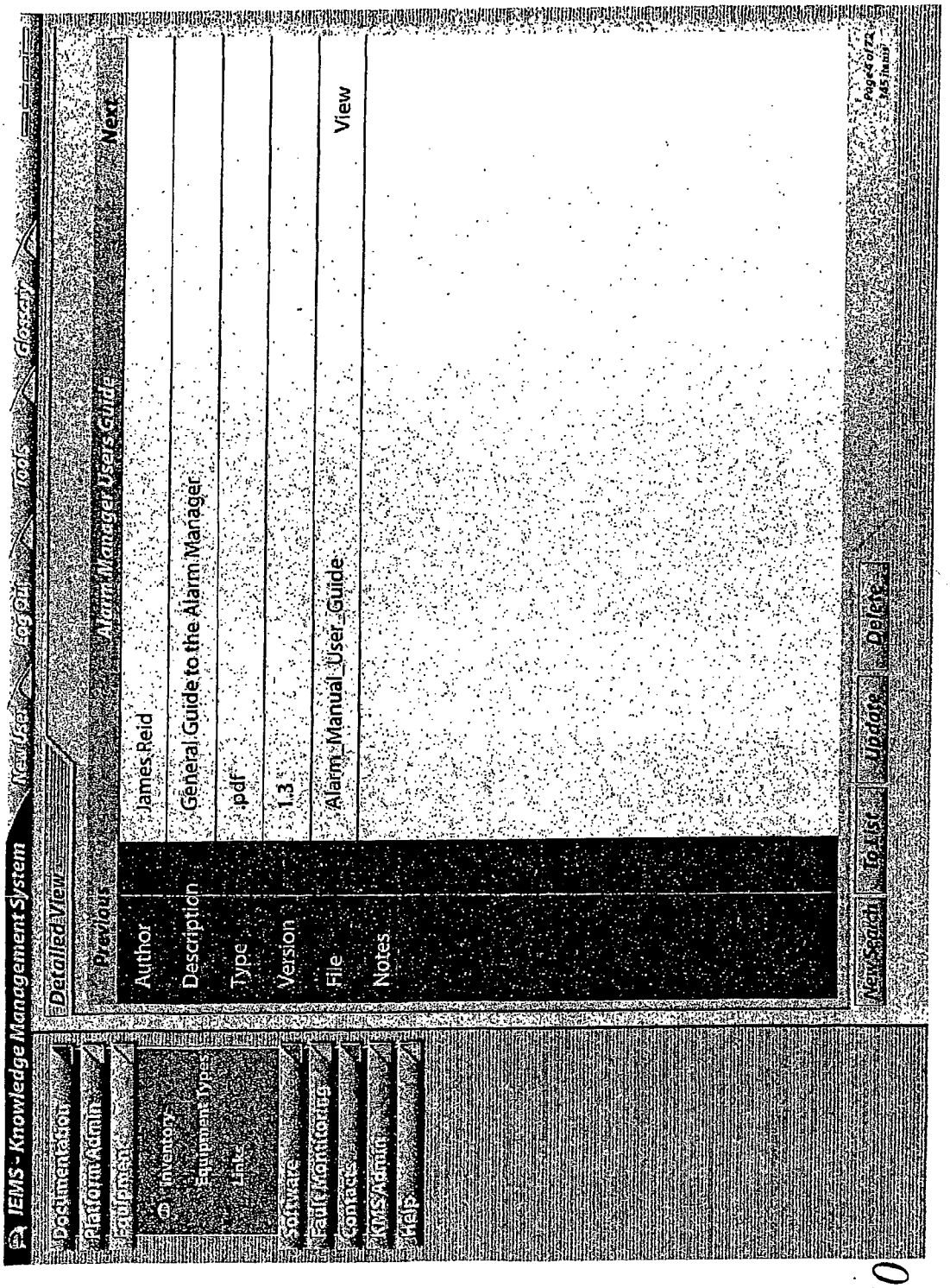

IEMS - Knowledge Management System
New User
Log Off
Tools
Glossary
Documentation
Platform Admin
Equipment
Inventory
Equipment Types
Links
Software
Fault Monitoring
Contacts
KMS Admin
Help
Detailed View
Previous
Next
Alarm Manager Users Guide
Author
James Reid
Description
General Guide to the Alarm Manager
Type
.pdf
Version
1.3
File
Alarm Manual User Guide
View
Notes
New Search
To List
Undate
Delete

Fig. 40

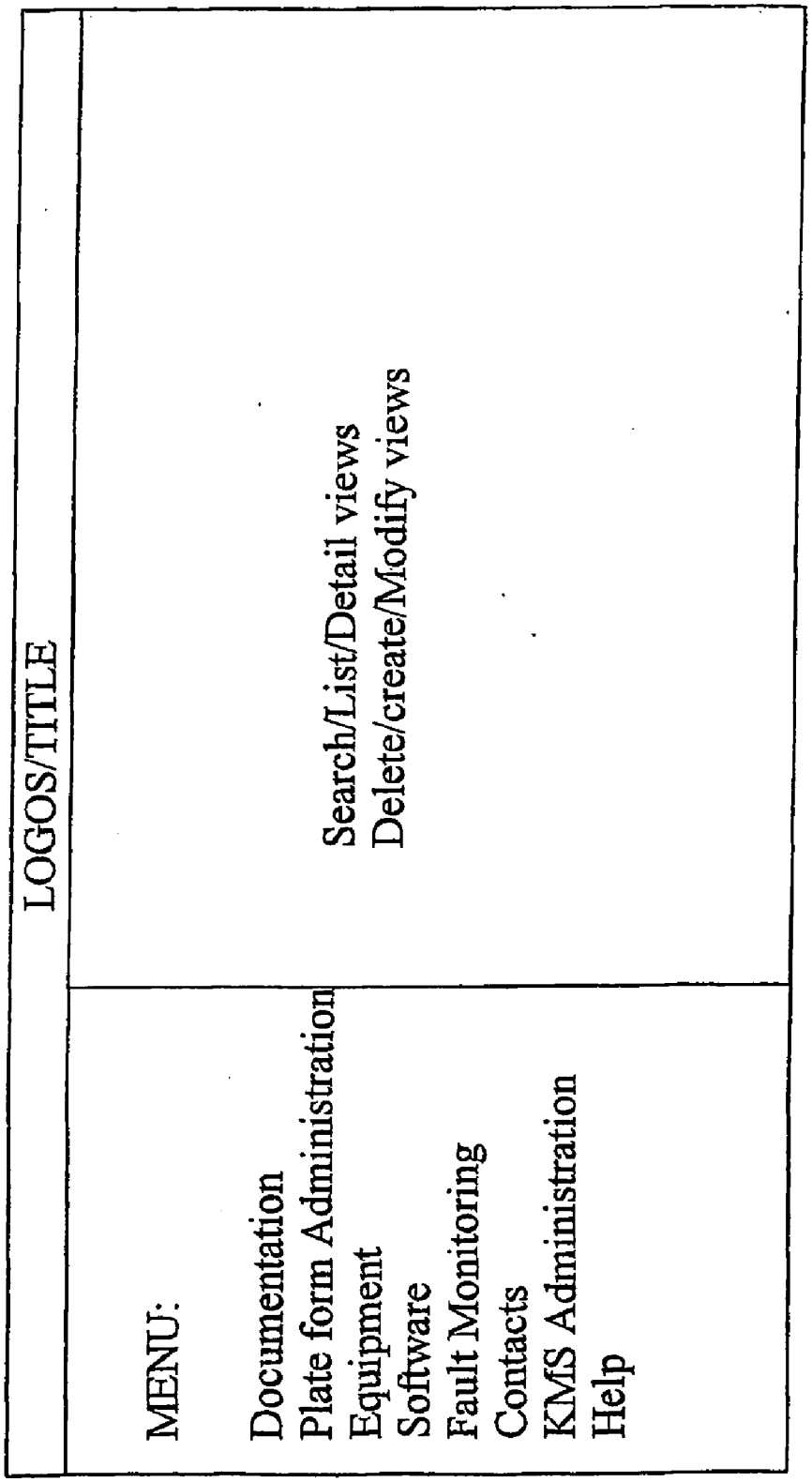

LOGOS/TITLE
MENU:
Documentation
Plate form Administration
Equipment
Software
Fault Monitoring
Contacts
KMS Administration
Help
Search/List/Detail views
Delete/create/Modify views

Fig. 41

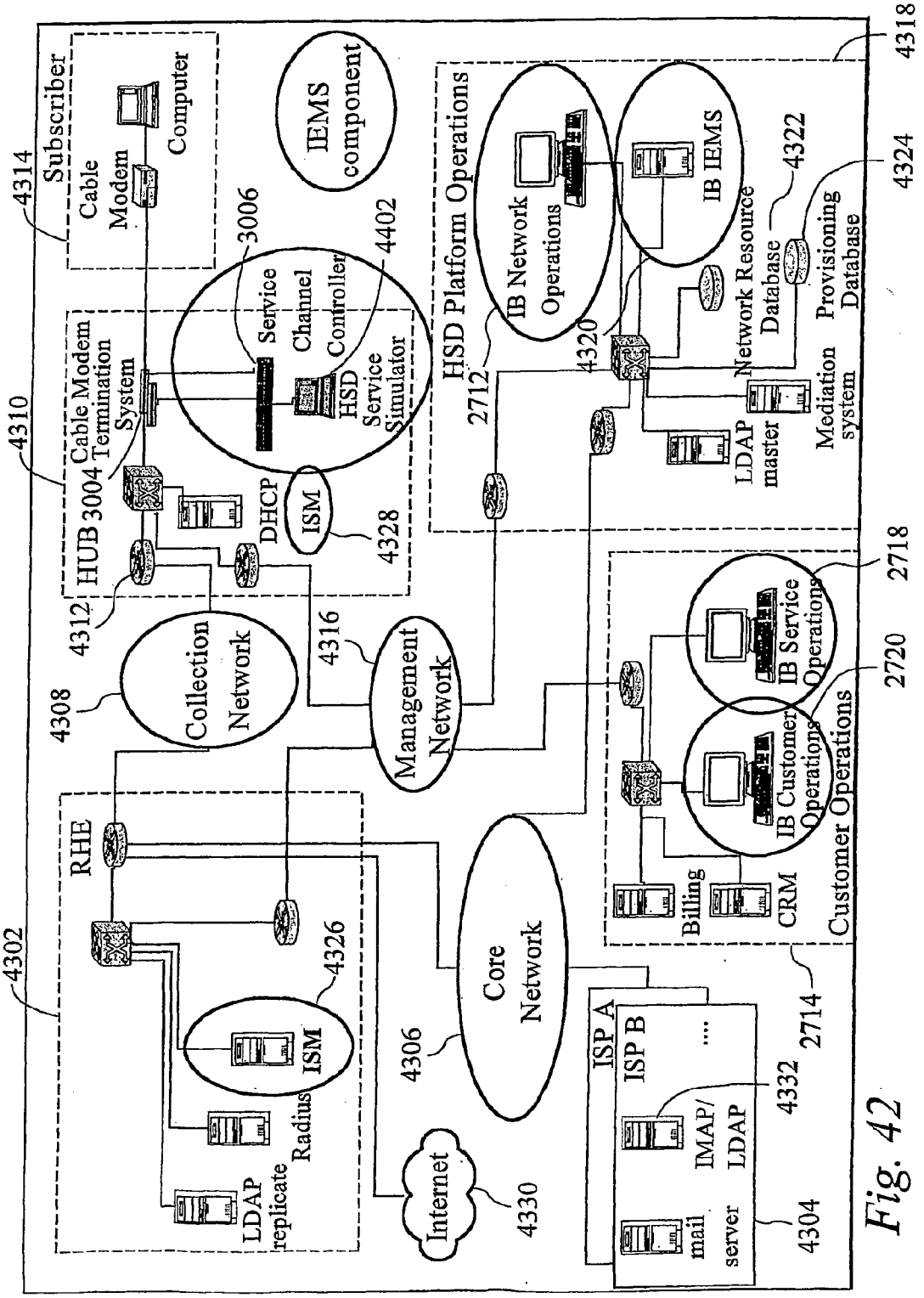

Subscriber
Cable Modem
Computer
4314
IEMS component
3006
Service Channel Controller
4402
HSD Service Simulator
Cable Modem Termination System
HUB 3004
4310
DHCP
ISM
4328
4312
Collection Network
4308
4316
Management Network
HSD Platform Operations
IB Network Operations
IB IEMS
4318
4322
4324
Network Resource Database
Provisioning Database
4320
2712
Mediation system
LDAP master
2718
IB Service Operations
2720
IB Customer Operations
Customer Operations
Billing
CRM
2714
RHE
4302
4326
ISM
Radius
LDAP replicate
Core Network
4306
Internet
4330
ISP A
ISP B
IMAP/ LDAP
mail server
4332
4304

Fig. 42

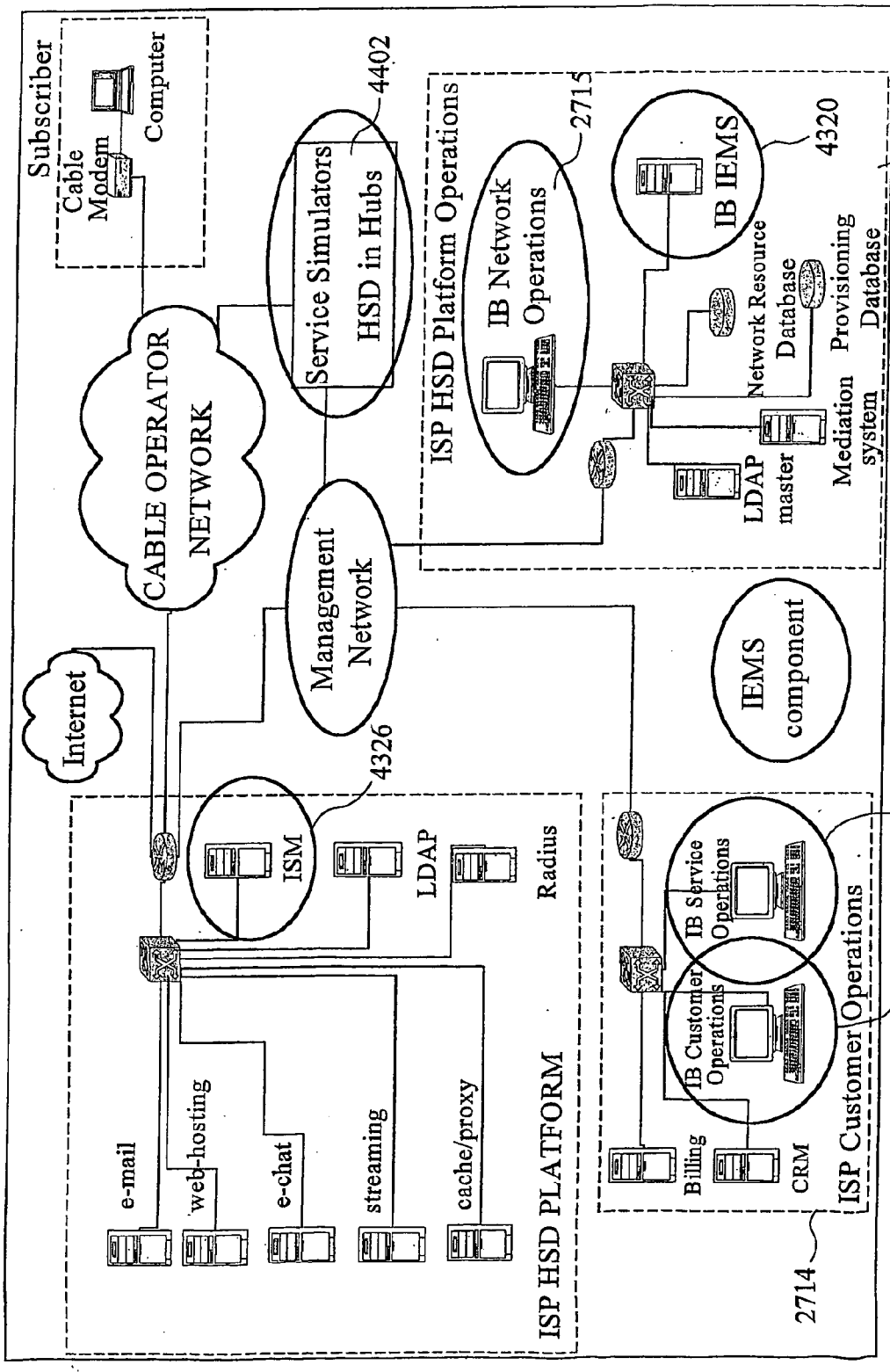

Subscriber
Cable Modem
Computer
CABLE OPERATOR NETWORK
Service Simulators
HSD in Hubs
4402
ISP HSD Platform Operations
IB Network Operations
2715
IB IEMS
4320
4318
Network Resource Database
Provisioning Database
Mediation system
LDAP master
Management Network
IEMS component
Internet
4326
ISM
LDAP
Radius
e-mail
web-hosting
e-chat
streaming
cache/proxy
ISP HSD PLATFORM
IB Service Operations
IB Customer Operations
2718
2720
Billing
CRM
ISP Customer Operations
2714

Fig. 43

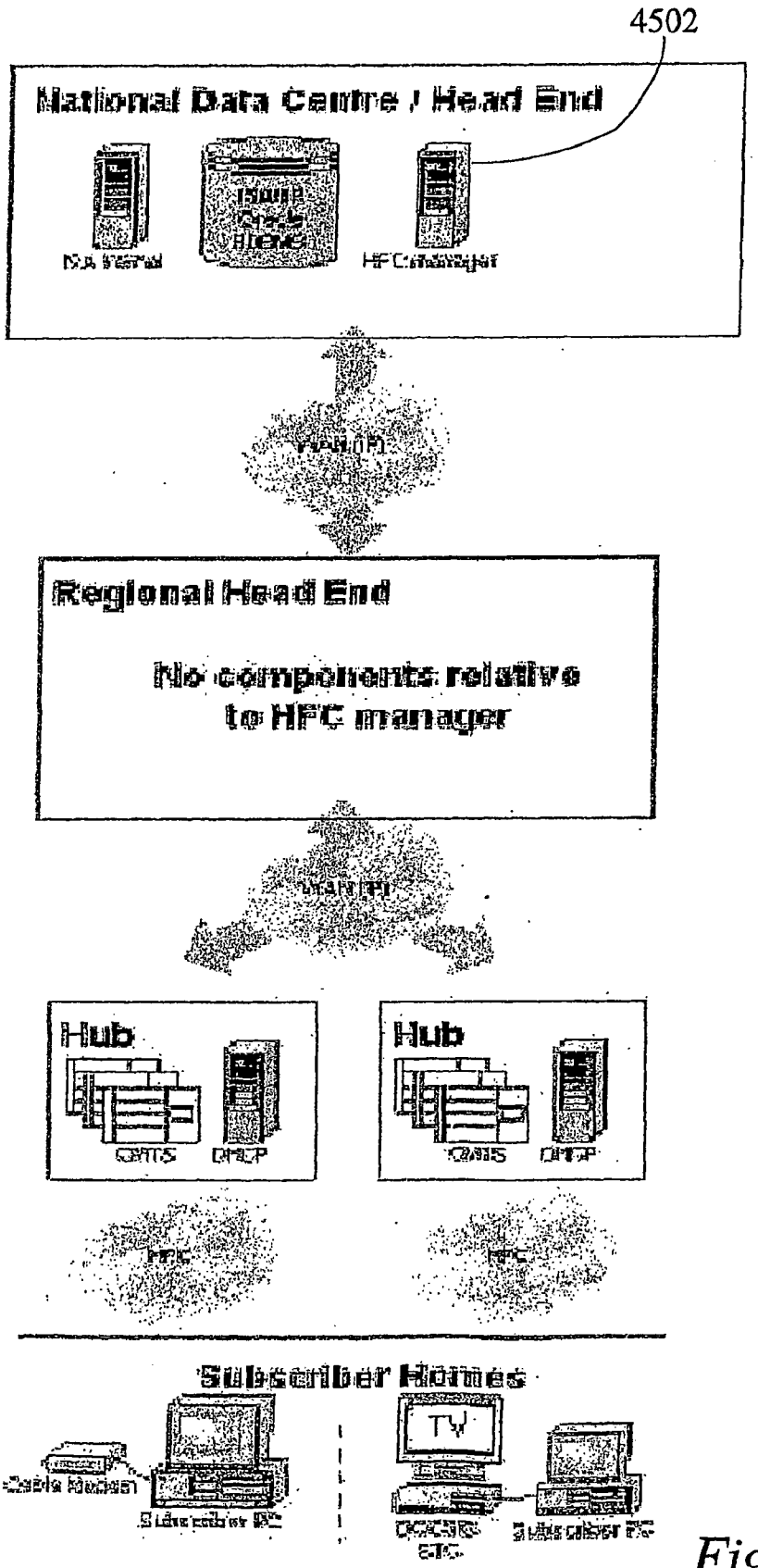

4502
National Data Centre / Head End
Regional Head End
No components relative to HFC manager
Hub
Hub
Subscriber Homes
TV

Fig. 44

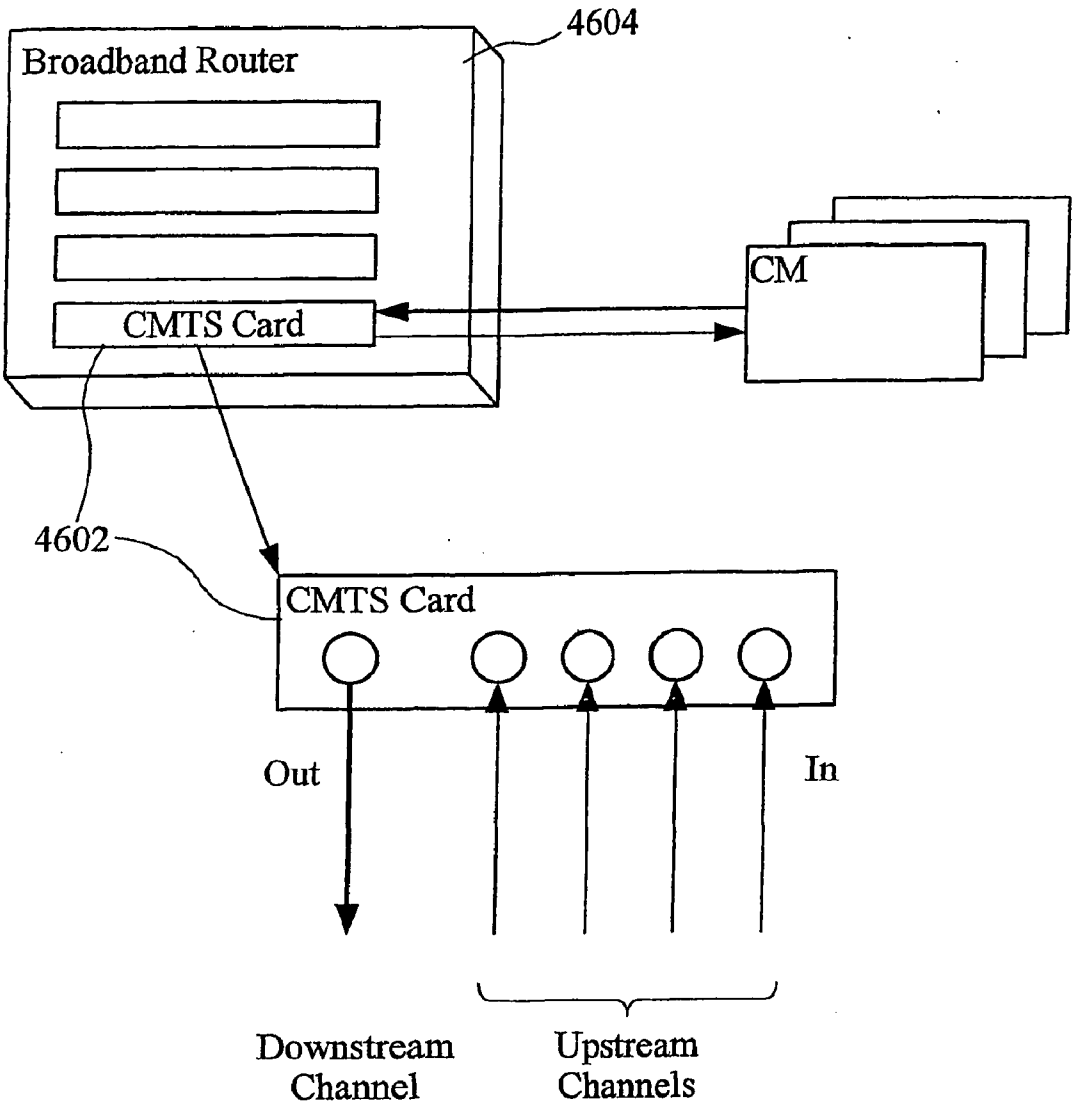

4604
Broadband Router
CMTS Card
CM
4602
CMTS Card
Out
In
Downstream Channel
Upstream Channels

Fig. 45

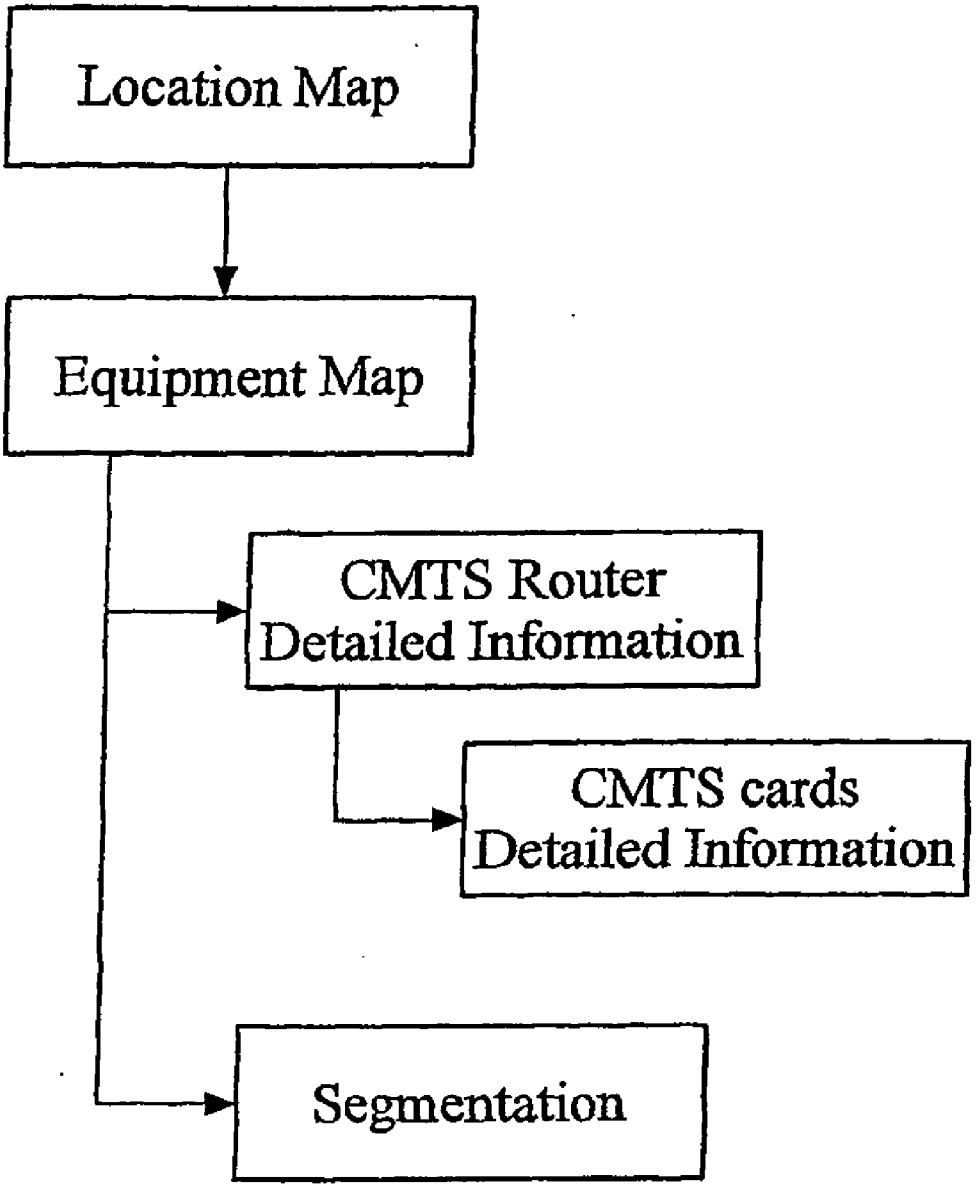

Location Map
Equipment Map
CMTS Router Detailed Information
CMTS cards Detailed Information
Segmentation

Fig. 46

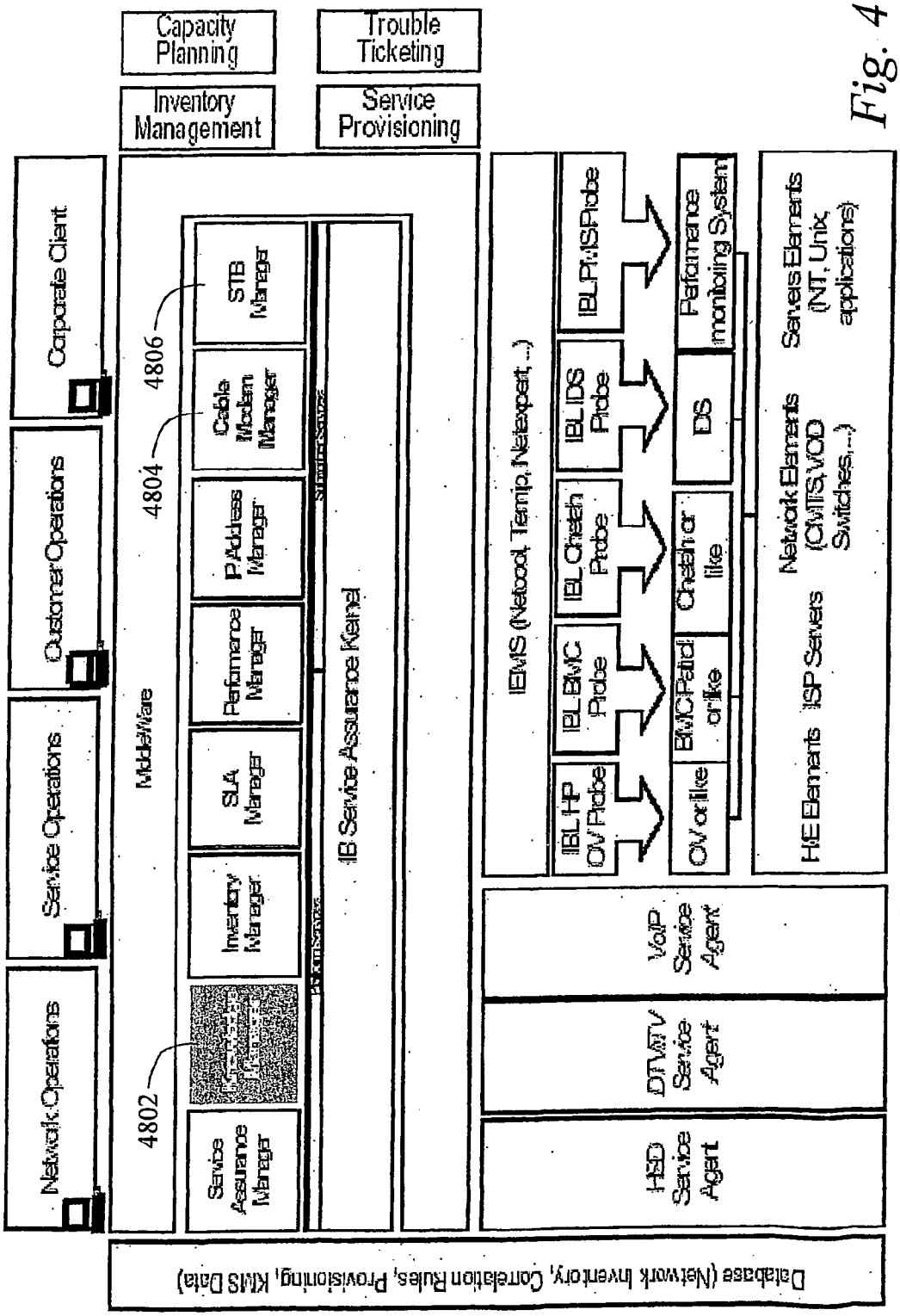

Capacity Planning
Trouble Ticketing
Inventory Management
Service Provisioning
Corporate Client
Customer Operations
Service Operations
Network Operations
Middleware
4802
4804
4806
Service Assurance Manager
Inventory Manager
SLA Manager
Performance Manager
IP Address Manager
Cable Modem Manager
STB Manager
IB Service Assurance Kernel
IEMS (Netcool, Temip, Netexpert, ...)
IBL HP OV Probe
IBL BMC Probe
IBL Chetah Probe
IBL IDS Probe
IBL PMS Probe
OV or like
BMC Patrol or like
Chetah or like
DS
Performance monitoring System
H/E Elements
ISP Servers
Network Elements (CMTS, VOD Switches, ...)
Servers Elements (NT, Unix, applications)
HSD Service Agent
DTV/TV Service Agent
VoIP Service Agent
Database (Network Inventory, Correlation Rules, Provisioning, KMS Data)

Fig. 47

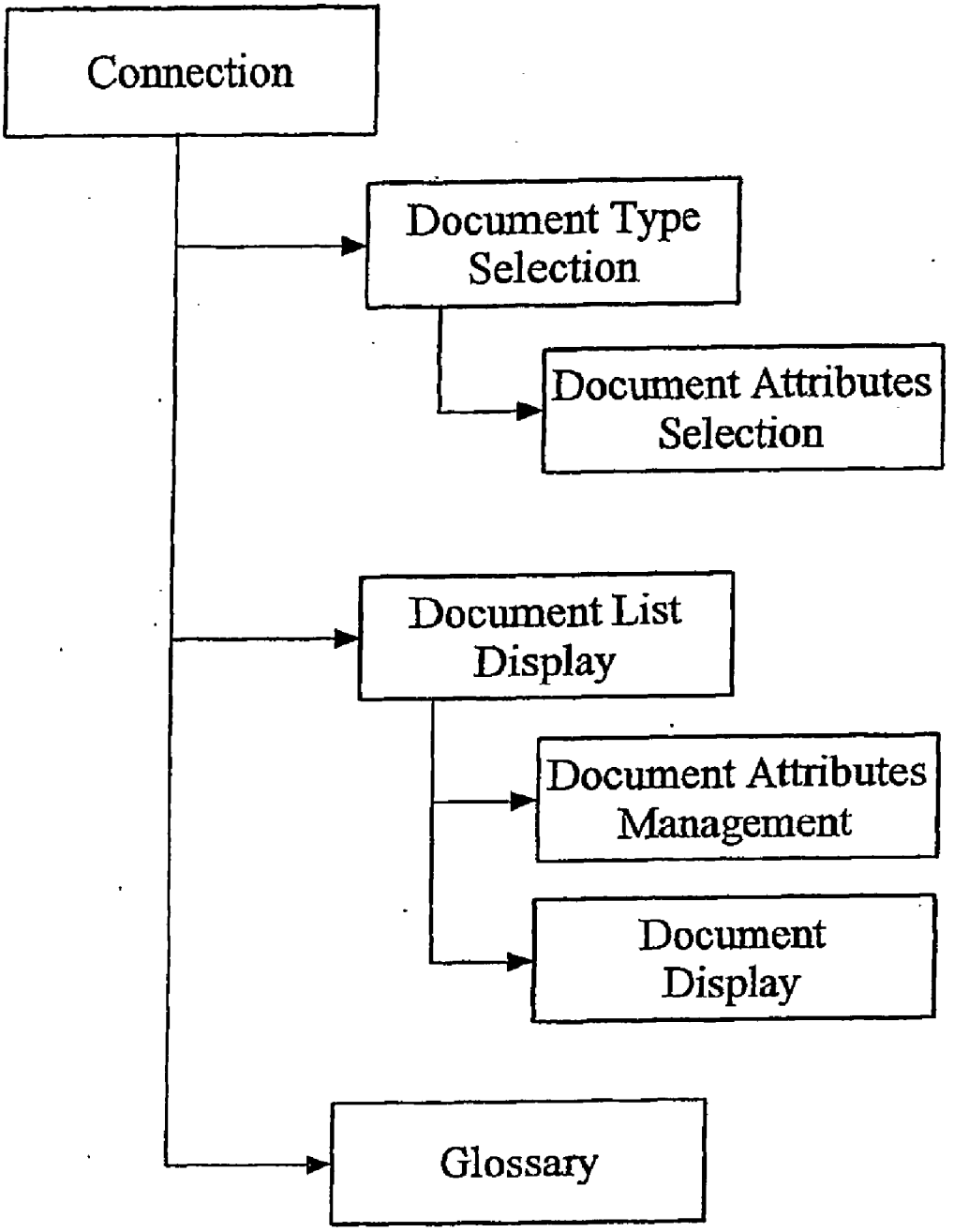

Connection
Document Type Selection
Document Attributes Selection
Document List Display
Document Attributes Management
Document Display
Glossary

Fig. 48

XML tag	Description	Value
<Connection>	Start tag for the Connection section	
<Type>	Sets the type of the connection	Fixed Value Direct = Management Switch = Switch CableModem = Cable modem DSLModem= DSL Modem
<Interface>	Sets the Interface used for the Management connection	Fixed Value Eth0 = Management Eth1= switch or Cable Modems
<IPAddress>	Sets the IP Address of the Switch	Fixed Value
<Community>	Sets the community of the Switch	Public Private
<PortOid>	Sets the Port Object Identification	
<TypeOid>	Sets the type of the UpOid and the DownOid	Fixed Value – Integer
<UpOid>	Sets 1 if the port of the switch is opened	1
<DownOid>	Sets 2 if the port of the switch is closed	2
<AgentPort>	Sets the Port for the connection with the ISEA Agent	What ever port number on the switch as long as it is only used to connect the ISEA to the switch
<ManagementPort>	Sets the Port used for the connection with the Management	What ever port number on the switch as long as it is only used to connect to the management network. It must be unique and different that the Agent Port
</Connection>	End tag for the Connection section	

Fig. 49

XML tag	Description	Value
<Connection>	Start tag for the Connection section	
<Type>	Sets the type of the connection	Fixed Value Direct = Management Switch = Switch CableModem = Cable modem DSLModem = DSL Modem
<Interface>	Sets the port of the switch where the cable modem is connected (Caveat to not use the switch port)	Fixed Value 1 to 8 1 to 24
<Location>	Sets the Location of the Cable Modem connection to the switch	Fixed value
<IPAddress>	Sets the IP Address of the Cable Modem. The cable modem must be provisioned	Fixed value
<MACAddress>	Sets the MAC Address of the Cable Modem. The cable modem must be provisioned	Fixed value
<Community>	Sets the community of the Cable Modem	Public Private
<CommandToKill>	Deprovision the Cable Modem	dhcpcd -k #interface#
<CommandToLaunch>	Provision the Cable Modem	dhcpcd -d -t #timeout# #interface#
<WaitedResponse>	Returns the message: "dhcpcd: your IP address"	Fixed value
<Timeout>	Sets the connection Time out in seconds	
</Connection>	End tag for the Connection section	

Fig. 50

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 050

XML tag	Description	Value
<?xml version="1.0" … ?>	Xml file header	Fixed Value
<SchedulerManager>	Start tag for the File Name	Fixed value
- <!-- Common Part -->	Commentary	
<DebugName>	Sets the Scheduler Manager Name used for the Debug mode	SchedulerManager
<DebugLevel>	Sets the debug level used by the application to log debugging info.	Info = all Agent activities Warning = abnormal activities Error = Error activities Critical = Agent is down
<AlarmWriter>	Sets a file as a default Alarm Writer	FlatFile
<AlarmWriter>	Sets a mail account as a default Alarm Writer	Mail
<AlarmHandler>	Start tag for the Alarm handler section	
<DebugName>	Sets the Alarm Handler Name used for the Debug mode	AlarmHandler
<DebugLevel>	Sets the debug level used by the application to log debugging info.	Info = all Agent activities Warning = abnormal activities Error = Error activities Critical = Agent is down

Fig. 51a

XML tag	Description	Value
<SleepTime>	Sets the time interval during which the alarm is not activated in milliseconds	5000
<AlarmWriter>	Start tag for the Alarm Writer section	
<Type>	Sets the type of the file Alarm Writer	FlatFile
<Path>	Sets the file path	test.alarms
</AlarmWriter>	End tag for the file Alarm Writer section	
<AlarmWriter>	Start tag for the mail Alarm Writer section	
<Type>	Sets the type of the Alarm Writer	Mail
<From>	Sets the alarm IP Address as defined in the Xmail Configuration	Fixed Value alarm@hostname.domain
<To>	Sets the destination IP Address as defined in the Xmail Configuration	Fixed Value alarm@hostname.domain
<Host>	Sets the Agent IP Address	Fixed value
<Port>	Sets the port used for the mail	Fixed Value - 25
</AlarmWriter>	End tag for the Alarm Writer section	
</AlarmHandler>	End tag for the Alarm Handler section	

Fig. 51b

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 052

XML tag	Description	Value
<Protocol>	Start tag for the Protocol section	
<Name>	Sets the Name of the Protocol	Fixed value - DHCP
<CommandToKill>	Sets the command used to kill the protocol	Fixed value /sbin/dhcpcd -k #interface#
<CommandToLaunch>	Sets the command used to launch the protocol	Fixed value /sbin/dhcpcd -d -t #timeout# #interface#
<WaitedResponse>	Returns a message: "dhcpcd: your IP address ="	Fixed Value
</Protocol>	End tag for the Protocol section	

Fig. 52

XML tag	Description	Value
<Scenario>	Start tag for the Scenario section	
<Name>	Sets the Name of the Scenario	Test
<Location>	Start tag for the location section	
<Code>	Sets the location code of the Cable modem	Fixed value Same as defined in the IBSAAgent.xml file
<Action>	Start tag for the Action section	
<ServiceName>	Sets the Name of the Service, as defined in the Service section	Provisioning
<Timeout>	Sets the global time out of the specific Action in milliseconds	10000
<HSDCode>	Sets the alarm Class (i.e. HSD_0_x00000)	x = Service code: 0 = Management 1 = Internet Access 2 = Provisioning 3 = Mail (ISP) 4 = Security 5 = Performance
</Action>	End tag for the Scenario section	
<Action>	Start tag for the Action section	
<ServiceName>	Sets the Name of the Service, as defined in the Service section	InternetAccess
<Timeout>	Sets the global time out of the specific Action in milliseconds	50000

Fig. 53a

XML tag	Description	Value
<HSDCode>	Sets the alarm Class (i.e. HSD_0_x00000)	x = Service code: 0 = Management 1 = Internet Access 2 = Provisioning 3 = Mail (ISP) 4 = Security 5 = Performance
</Action>	End tag for the Action section	
<Action>	Start tag for the Action section	
<ServiceName>	Sets the Name of the Service, as defined in the Service section	ISP
<Timeout>	Sets the global time out of the specific Action in milliseconds	10000
<HSDCode>	Sets the alarm Class (i.e. HSD_0_x00000)	x = Service code: 0 = Management 1 = Internet Access 2 = Provisioning 3 = Mail (ISP) 4 = Security 5 = Performance
<AlarmLocation>	Sets the Location of the Alarm (Hub)	Fixed Value
</Action>	End tag for the Action section	
<Action>	Start tag for the Action section	
<ServiceName>	Sets the Name of the Service, as defined in the Service section	Security
<Timeout>	Sets the global time out of the specific Action in milliseconds	10000

Fig. 53b

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 055

XML tag	Description	Value
<HSDCode>	Sets the alarm Class (i.e. HSD_0_x00000)	x = Service code: 0 = Management 1 = Internet Access 2 = Provisioning 3 = Mail (ISP) 4 = Security 5 = Performance
<AlarmLocation>	Sets the Location of the Alarm (Hub)	Fixed Value
</Action>	End tag for the Action section	
</Location>	End tag for the Location section	
</Scenario>	End tag for the Scenario section	

Fig. 54

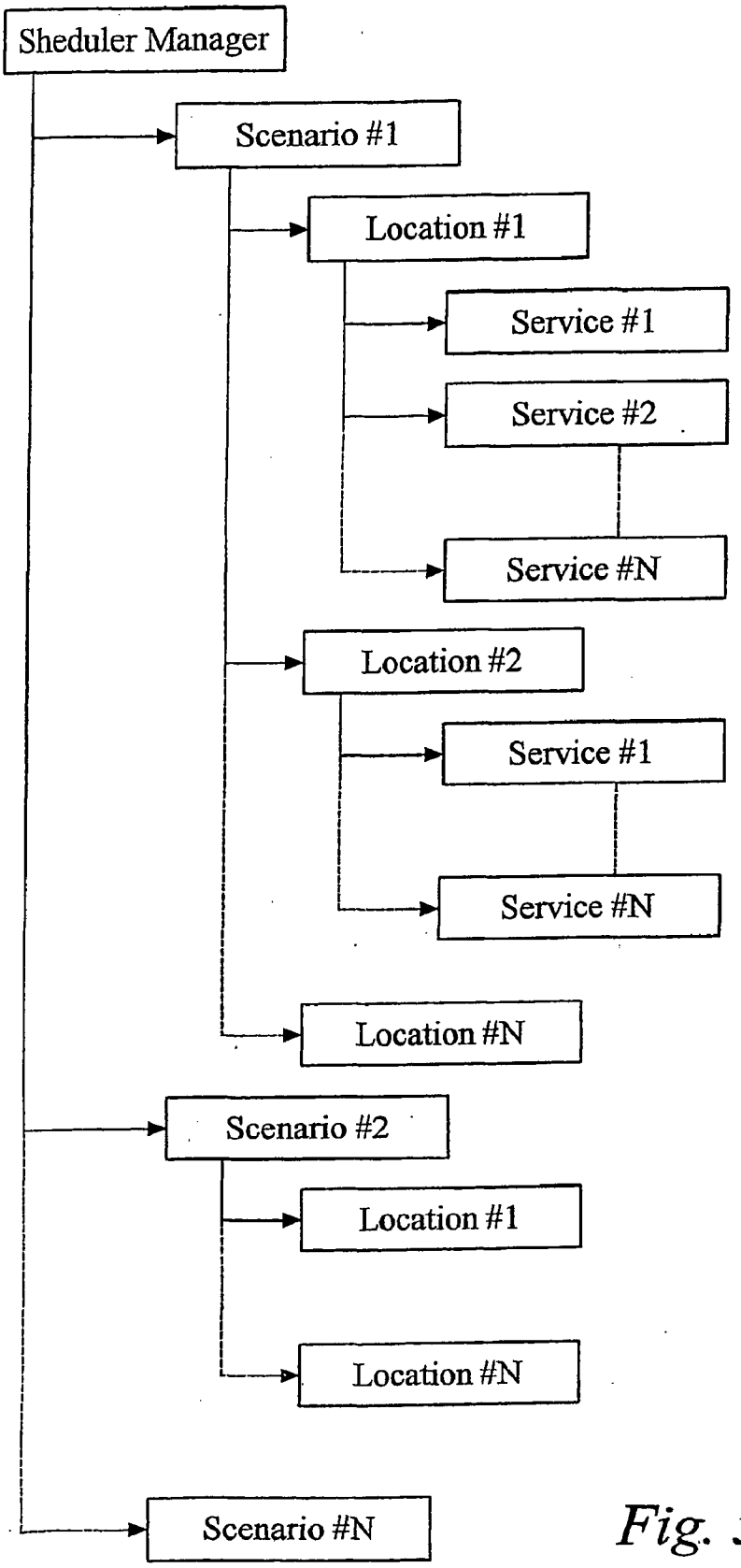

Sheduler Manager
Scenario #1
Location #1
Service #1
Service #2
Service #N
Location #2
Service #1
Service #N
Location #N
Scenario #2
Location #1
Location #N
Scenario #N

Fig. 55

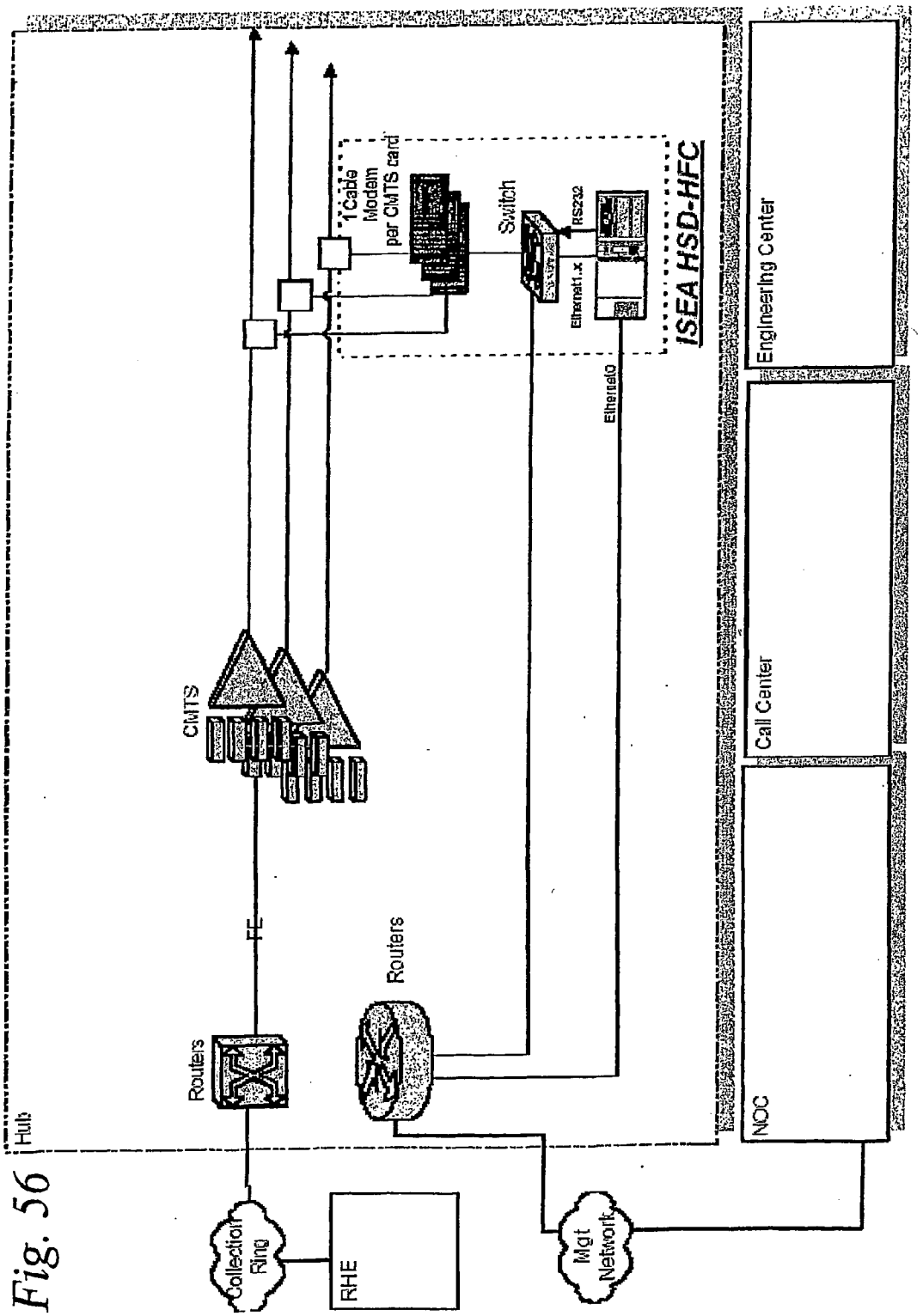

Hub
Collection Ring
RHE
Routers
FE
CMTS
Routers
Mgt Network
1 Cable Modem per CMTS card
Switch
Ethernet1.x
RS232
Ethernet0
ISEA HSD-HFC
Engineering Center
Call Center
NOC

Fig. 56

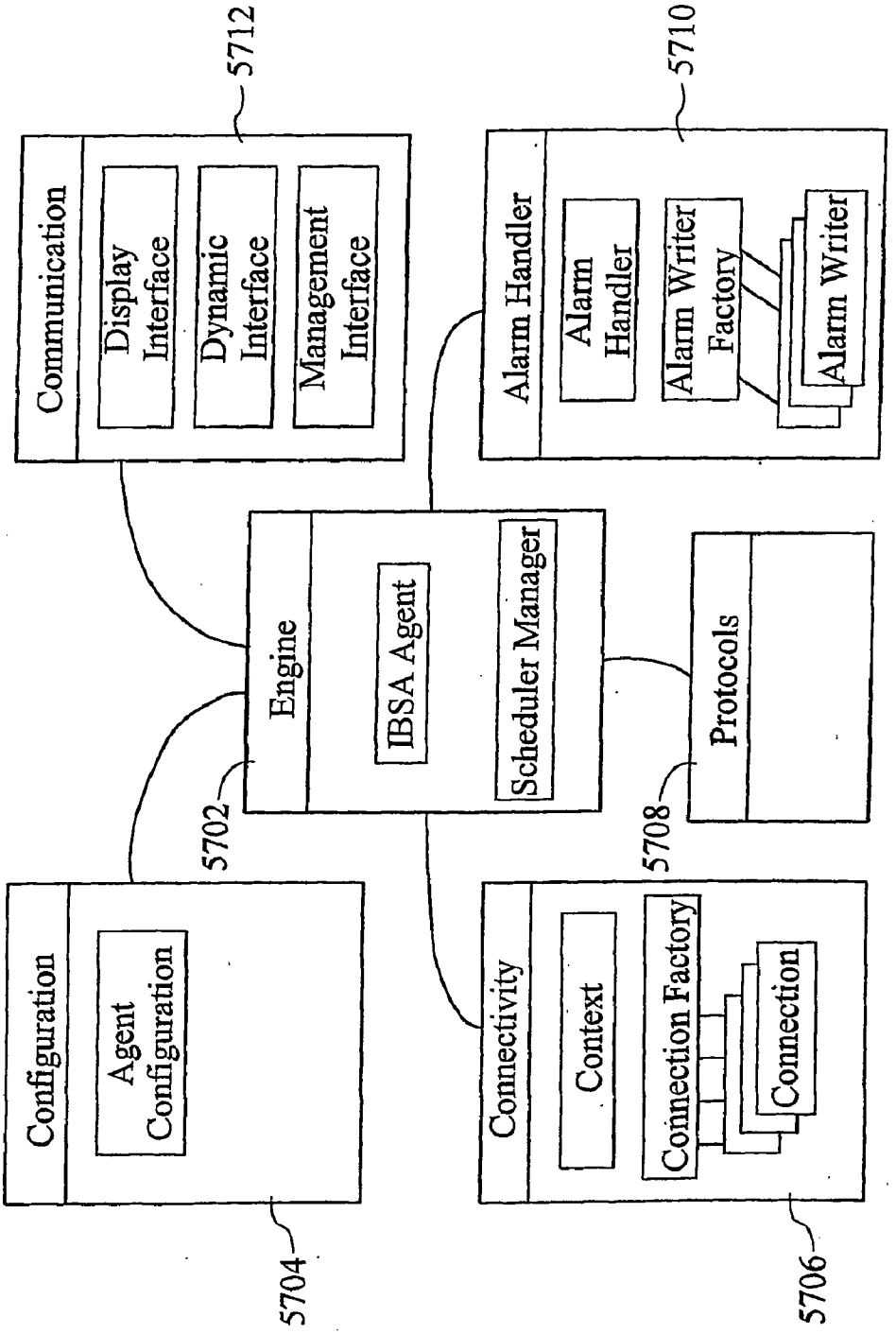

Communication
Display Interface
Dynamic Interface
Management Interface
5712
Alarm Handler
Alarm Handler
Alarm Writer Factory
Alarm Writer
5710
Engine
IBSA Agent
Scheduler Manager
5702
Protocols
5708
Configuration
Agent Configuration
5704
Connectivity
Context
Connection Factory
Connection
5706

Fig. 57

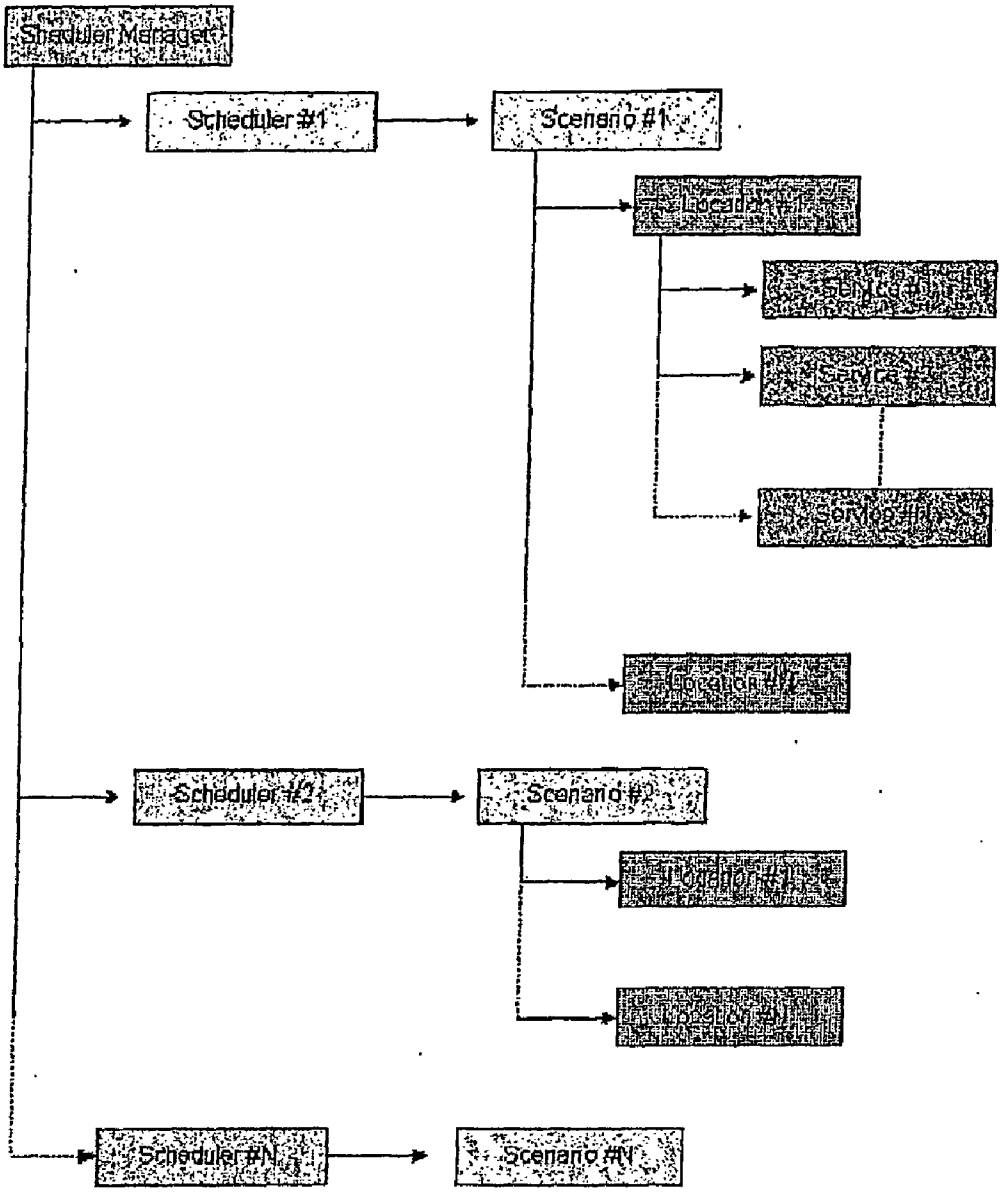

Scheduler Manager
Scheduler #1
Scenario #1
Scheduler #2
Scenario #2
Scheduler #N
Scenario #N

Figure 58

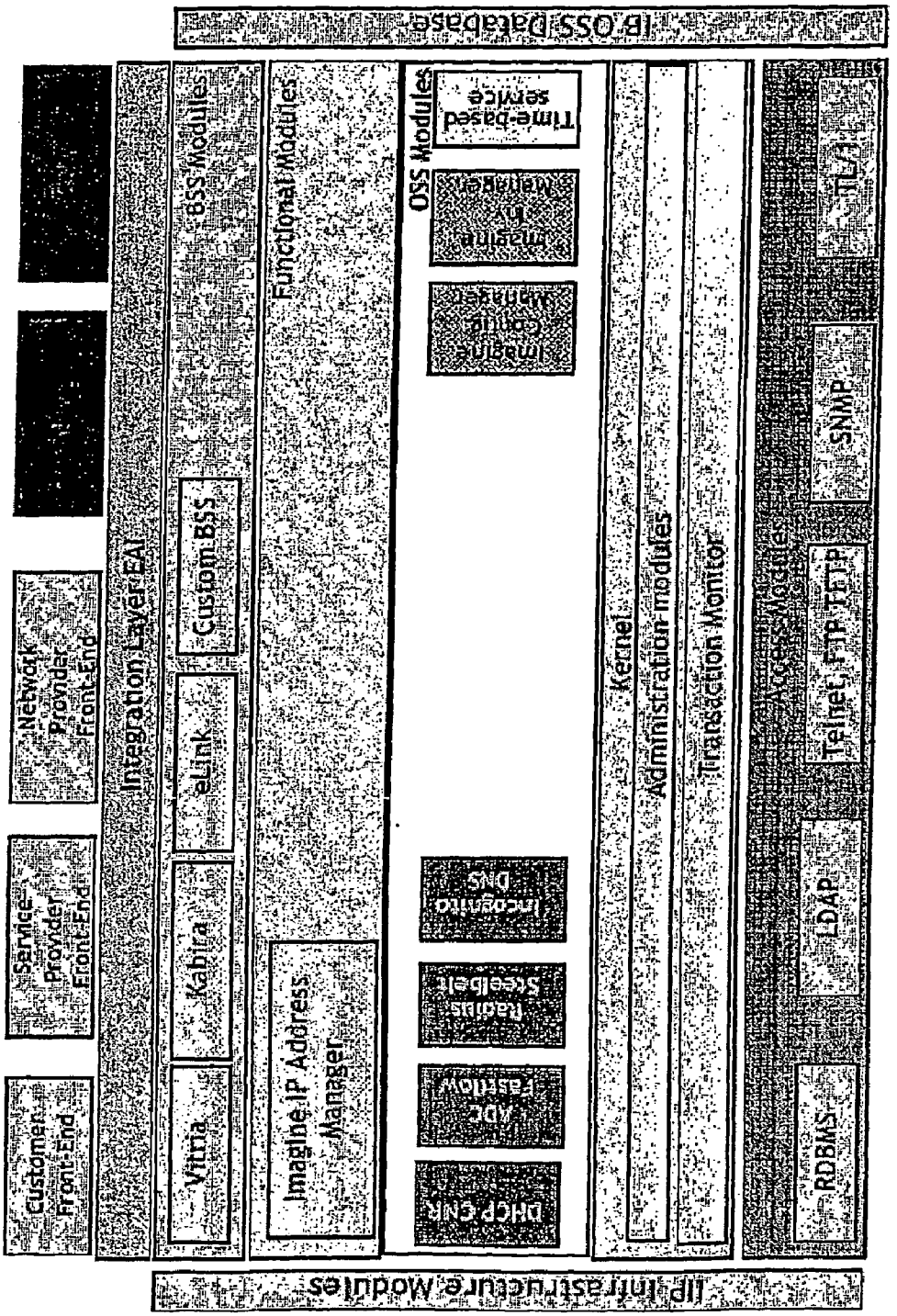

IB OSS Database
Customer Front-End
Service Provider Front-End
Network Provider Front-End
Integration Layer EAI
Vitria
Kabira
eLink
Custom BSS
BSS Modules
Imagine IP Address Manager
Functional Modules
DHCP CNR
ADC Fastflow
Radius Steelbelt
Incognito DNS
Imagine Config Manager
Imagine In Manager
Time-based service
OSS Modules
Kernel
Administration modules
Transaction Monitor
RDBMS
LDAP
Telnet, FTP, TFTP
SNMP
TL/1
Access Modules
IIP Infrastructure Modules

Figure 59

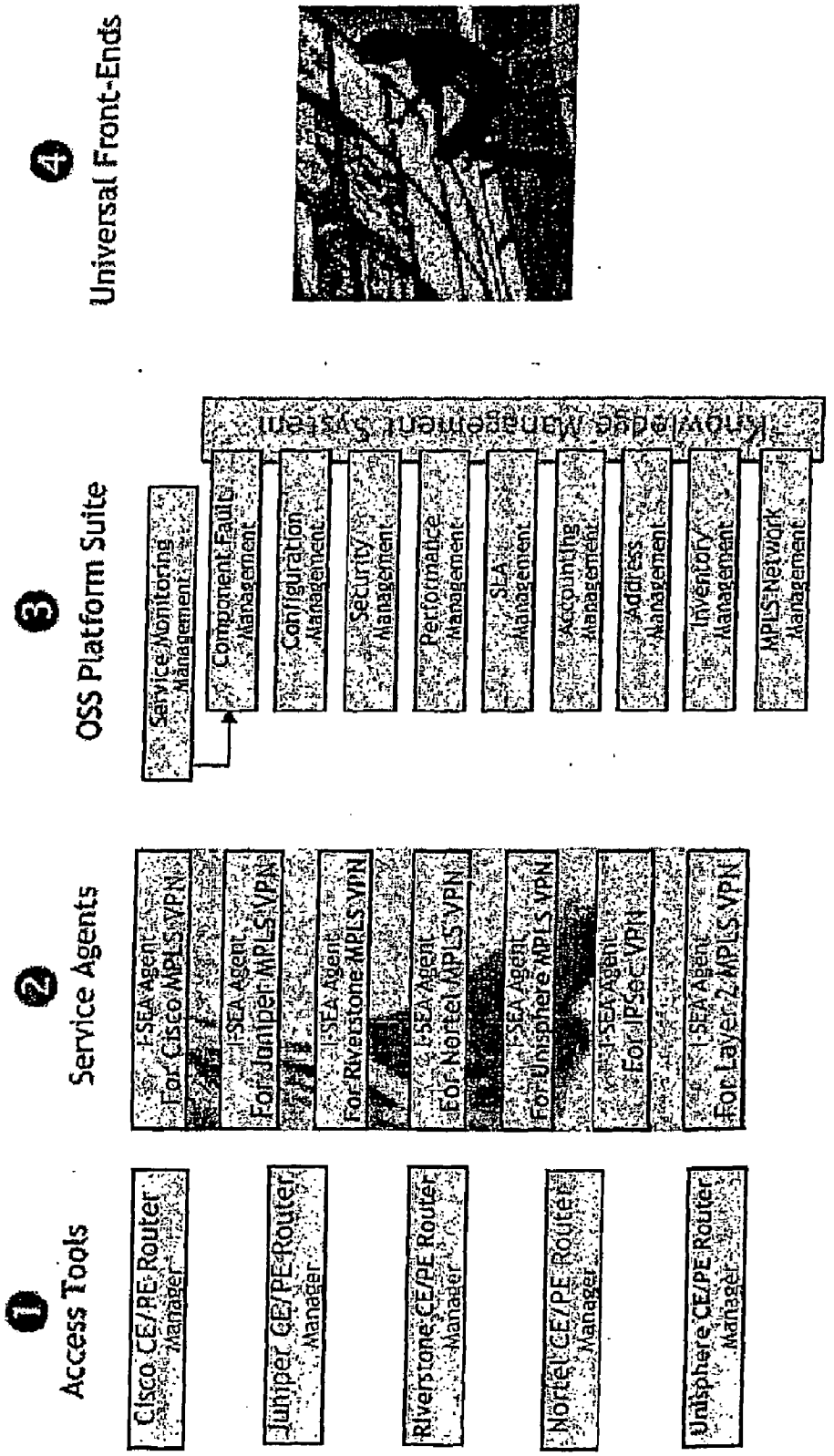

1
Access Tools
Cisco CE/PE Router Manager
Juniper CE/PE Router Manager
Riverstone CE/PE Router Manager
Nortel CE/PE Router Manager
Unisphere CE/PE Router Manager
2
Service Agents
ISEA Agent For Cisco MPLS VPN
ISEA Agent For Juniper MPLS VPN
ISEA Agent For Riverstone MPLS VPN
ISEA Agent For Nortel MPLS VPN
ISEA Agent For Unisphere MPLS VPN
ISEA Agent For IPSec VPN
ISEA Agent For Layer 2 MPLS VPN
3
OSS Platform Suite
Service Monitoring Management
Component Fault Management
Configuration Management
Security Management
Performance Management
SLA Management
Accounting Management
Address Management
Inventory Management
MPLS Network Management
Knowledge Management System
4
Universal Front-Ends

Figure 60

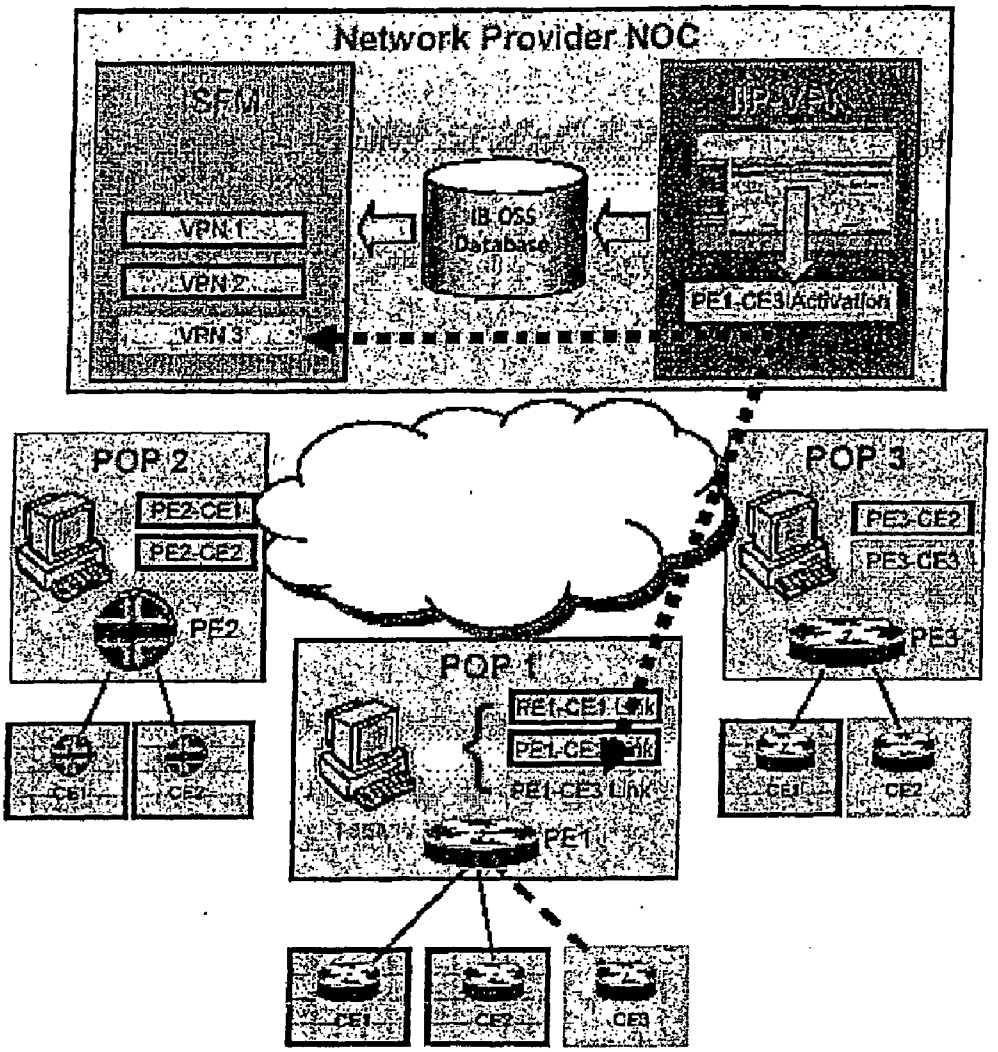

Network Provider NOC
ISFM
VPN 1
VPN 2
VPN 3
IB OSS Database
PE1-CE3 Activation
POP 2
PE2-CE1
PE2-CE2
PE2
POP 3
PE2-CE2
PE3-CE3
PE3
POP 1
PE1-CE1 Link
PE1-CE3 Link
PE1
CE1
CE2
CE3

Figure 61

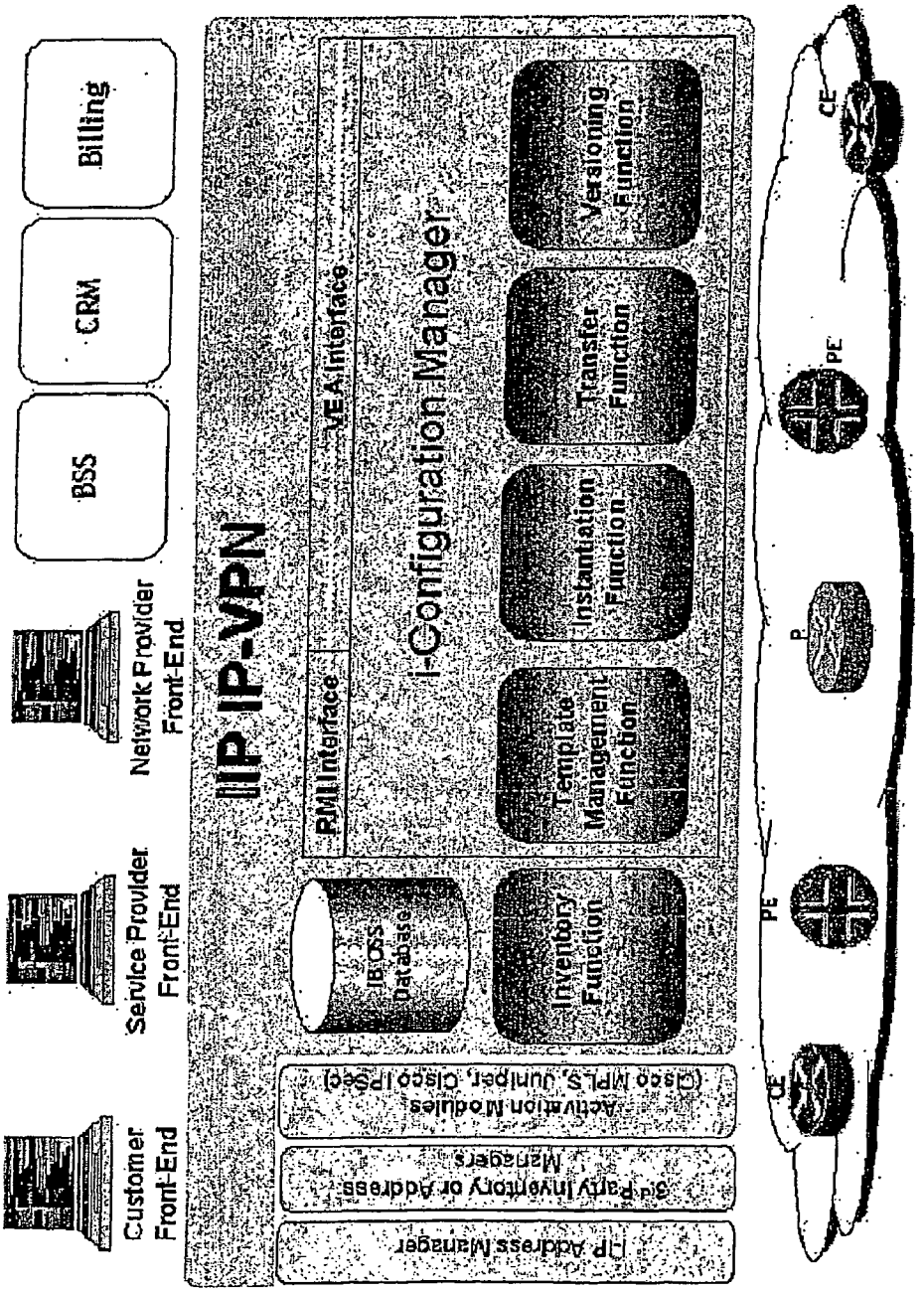

Billing
CRM
BSS
Network Provider Front-End
Service Provider Front-End
Customer Front-End
IIP IP-VPN
RMI Interface
VEA Interface
i-Configuration Manager
Versioning Function
Transfer Function
Instantiation Function
Template Management Function
Inventory Function
IBOSS Database
Activation Modules (Cisco MPLS, Juniper, Cisco IPsec)
3rd Party Inventory or Address Managers
IP Address Manager
CE
PE
P
PE
CE

Figure 62

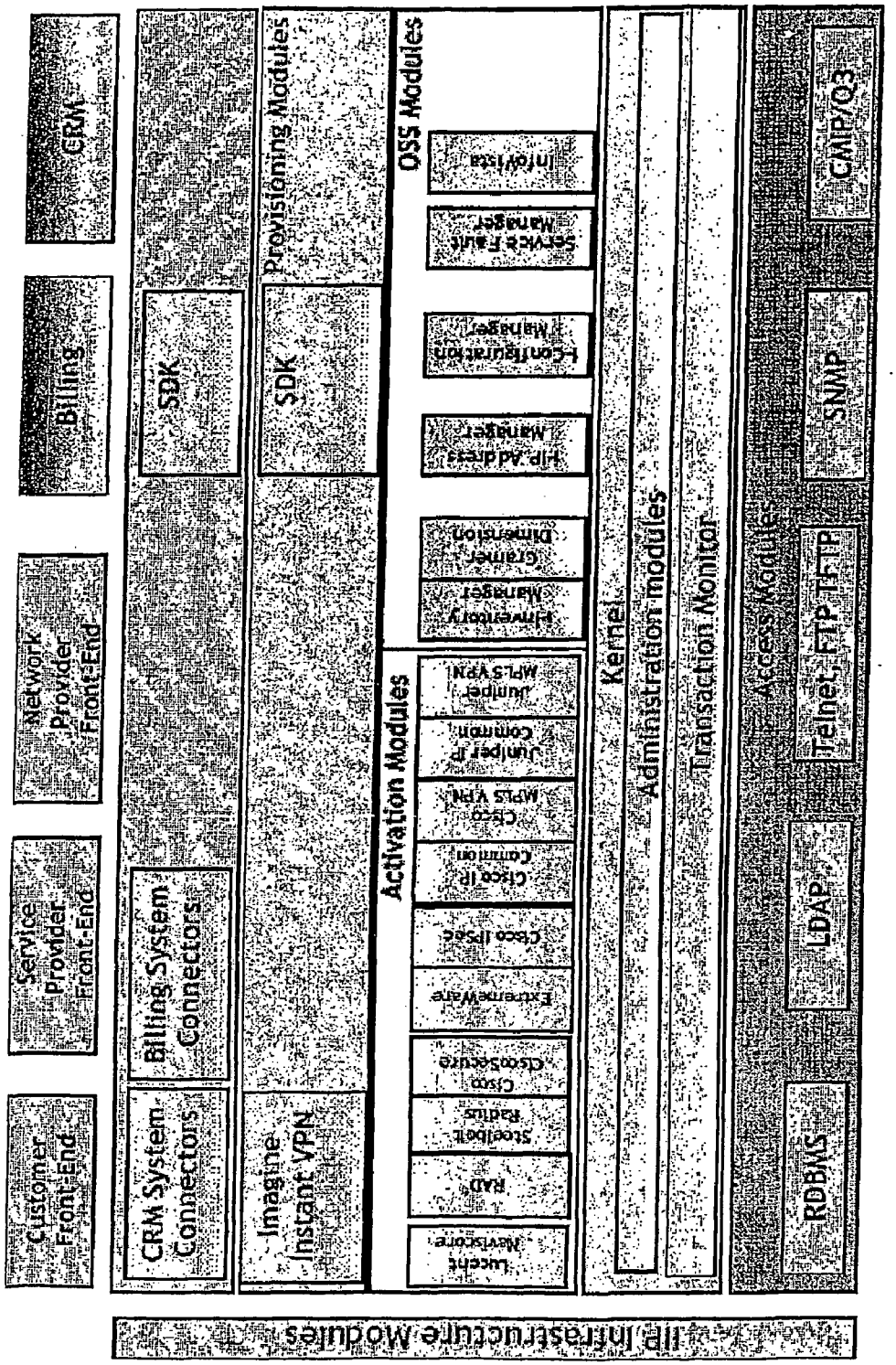

Customer Front-End
Service Provider Front-End
Network Provider Front-End
Billing
CRM
CRM System Connectors
Billing System Connectors
SDK
Imagine Instant VPN
SDK
Provisioning Modules
Activation Modules
Lucent Maviscore
RAD
Steelbolt Radius
Cisco CiscoSecure
ExtremeWare
Cisco IPSec
Cisco IP Common
Cisco MPLS VPN
Juniper IP Common
Juniper MPLS VPN
I-Inventory Manager
Cramer Dimension
I-IP Address Manager
I-Configuration Manager
Service Fault Manager
InfoVista
OSS Modules
Kernel
Administration modules
Transaction Monitor
Access Modules
RDBMS
LDAP
Telnet, FTP TFTP
SNMP
CMIP/Q3
IIP Infrastructure Modules

Figure 63

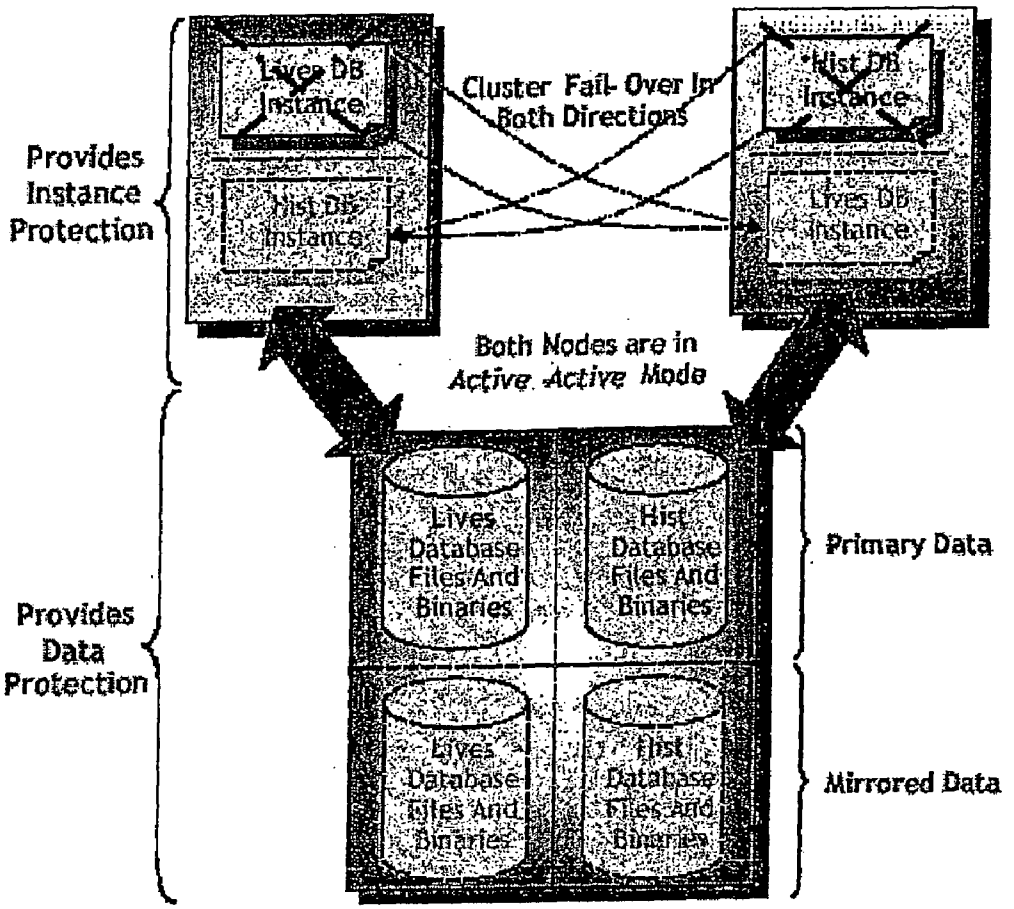

Lives DB Instance
Hist DB Instance
Cluster Fail-Over In Both Directions
Hist DB Instance
Lives DB Instance
Provides Instance Protection
Both Nodes are in Active Active Mode
Lives Database Files And Binaries
Hist Database Files And Binaries
Primary Data
Provides Data Protection
Lives Database Files And Binaries
Hist Database Files And Binaries
Mirrored Data

Figure 64

BROADBAND COMMUNICATIONS

[0001] According to one embodiment, the broadband network may be, but is not limited to, an MPLS (Multi-Protocol Label Switching) or an IPSec (IP Security) network and the service may be provisioned via a Virtual Private Network (VPN) connection.

[0002] Provisioning is a fundamental step in establishing a connection with a user. The user is normally provided with a user device, a non-limiting but illustrative example of which includes a Personal Computer (PC) and an access device. For example, in a broadband network, a cable modem or Digital Subscriber Line (DSL) modem normally provided as an access device to connect the user device to the broadband network. With a conventional dial up network, any user with a suitable modem and is able to dial into a service (although some service may request a password following connection whereas others may allow open or guest access). Similarly, with Internet services, any user with access to the Internet can access a desired web address, although some sites may require passwords. In both cases, however, it is not necessary for the service to have details of the user equipment in advance of connection. In contrast, broadband services must be specifically provisioned for a given user. In order to provision services for a broadband connection, it is necessary for the provisioning application to have a unique "physical" identifier of the user with whom the service is being provisioned. In the case of a cable modem connection in particular, this may be referred to variously as physical address or identifier, hardware address or Media Access Control (MAC) address. This may be achieved by, for example, a user manually reading an identifier of a hardware product (for example cable modem) printed on the packaging and communicating this, for example by telephone, to the service provider. This manual provisioning method obviously has drawbacks; it is labour intensive and renders rapid provisioning of new services cumbersome.

[0003] In the case of a DSL connection, the DSL modem does not have a MAC address nor a permanent IP address but the PVC ID used for the connection between a DSL modem and a Broadband Access Router (BRAS) is used to identify the user; provisioning is carried out by managing the software PVC between the BRAS and DSL modem. Class of service and Quality of service are managed through the settings of the PVC. When connecting the PC to the modem and booting the system, the actual PVC ID is transmitted across the network and can be used for user association. Thus, in the case of a DSL connection, although the relevant "physical address" which identifies the DSL modem is in fact that of an ATM virtual connection, pursuant to the invention it has been appreciated that this can be regarded as a physical or hardware address for the purpose of provisioning and treated in a similar manner to a cable modem MAC address. As used in this specification, the term "hardware address" or "physical address" is intended to encompass a PVC ID in the case of a DSL connection. The terms may encompass another address or identifier which uniquely characterises a connection to a specific access device in other contexts. The terms are intended to distinguish from higher level identifiers, such as an IP address or email address, which is not directly associated with a particular access device.

[0004] It is also possible to provide web-based applications for provisioning for a cable modem whereby a user enters a MAC address (as defined below) or physical device identifier into an interactive website; this reduces labour at the provisioning end but still requires a user to provide a (normally lengthy) physical identifier correctly. In prior art systems, the access device generally connects substantially transparently and the physical address (MAC address) of the user device (PC) is normally used to define the connection.

[0005] It has been proposed to provide specific application software to read the hardware address details and communicate these to a provisioning service provider and the provision of high-level application software at the user end may facilitate automatic provisioning of services. It does, however, of course require specialist software at the user end, which must be provided, adding to costs and complexity, and which may not always be present so may need to be installed by a user.

[0006] Aspects of the invention are set out in the independent claims to which reference should be made. Preferred features are set out in the dependent claims. Representative and further aspects are discussed below.

[0007] There is herein provided a method of providing an assured service to a user via a virtual private connection in a distributed network, the method comprising providing an agent in the network and configuring the agent to monitor the virtual private connection by simulating communication over the connection.

[0008] Preferably, the agent is arranged to reside on a node of the network other than the user's end node.

[0009] Further preferably, the agent is arranged to receive configuration information identifying a connection to monitor.

[0010] According to a further preferable feature, a single agent is arranged to receive configuration information identifying a plurality of independent connections to monitor.

[0011] Preferably, the method further comprises configuring the agent to pass a fault report to a remote network monitoring component in the event that a fault is detected in the provisioned virtual private connection.

[0012] There is also herein described a method of providing an assured service to a user via a virtual private connection in a distributed network, the method comprising provisioning a virtual private connection based on provisioning information and, based on the provisioning information, configuring an agent in the network to monitor the provisioned virtual private connection by simulating communication over the connection.

[0013] Preferably, configuration information is sent to a pre-existing agent.

[0014] According to an alternative preferable feature, an agent is launched if no preexisting agent is available to monitor the provisioned connection.

[0015] Preferably, the agent is further configured to pass a fault report to a remote network monitoring component in die event that a fault is detected in the provisioned virtual private connection.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 067

[0016] According to a further aspect, there is provided a method of provisioning a desired communications service for a user across a network, the method comprising obtaining information for a desired communications service to be provisioned based on information associated with an existing connection for the user and provisioning the desired communications service based on the information obtained.

[0017] This may facilitate provisioning by making use of an existing connection as a source of information on which to base provisioning of a new connection.

[0018] According to a preferred embodiment, there is provided a method of provisioning a service in a broadband network to a user device having an internetwork protocol address, the method comprising:

[0019] obtaining an internetwork protocol address of a user device for whom a service is to be provisioned;

[0020] sending a configuration protocol query message to a configuration related address server, the message containing the internetwork protocol address of the user device;

[0021] waiting for a response message from the server;

[0022] extracting a hardware address related to the user device from the response message;

[0023] provisioning a network connection with the user device based on the hardware address obtained from the response message.

[0024] There is herein described an improved and simplified method of facilitating provisioning in communications networks, particularly broadband networks. Preferably a user may be able to purchase an access device, such as a cable or DSL modem, "off the shelf" and services may be provisioned for the access device without the service provider having pre-provisioned the access device or supplied specialist software.

[0025] According to one embodiment, the broadband network may be an MPLS or an IPSec network. The user device may be provisioned via a Virtual Private Network (VPN) connection and, in particular, via an IP VPN connection.

[0026] There is described herein a method of provisioning a communications service for a user, the method comprising obtaining a hardware address for an access device, for example a cable modem MAC address or PVC ID in the case of a DSL connection, based on a communications protocol address, such as an Internet Protocol address, of a user device, for example a PC, and provisioning a service based on the hardware address obtained. The hardware address can be obtained using a low level protocol, for instance DHCP lease query.

[0027] Also described is the use of a communications protocol address, such as an Internet Protocol (IP) address, of a user device to obtain a physical address of an access device for use in provisioning a service for the user via the access device.

[0028] Further, there is also described herein a method of provisioning a service for a network access device comprising receiving a request from a user for a service which request does not include the physical address of the access device and provisioning a service based on obtaining the physical address of the access device using a communications protocol address, such as an Internet Protocol (IP) address, for the user.

[0029] A provisioning application is also described, which comprises means for receiving a communications protocol address, such as an Internet Protocol (IP) address, of a user device; means for discovering the physical address of an access device associated with tile user device based on the communications protocol address and means for provisioning a service for the access device based on the discovered physical address.

[0030] The methods and apparatus described above preferably operate without requesting the user to supply a physical address for the access device and without requiring the user to install software specific to the service provider.

[0031] It has been appreciated that it is possible to obtain or verify the physical device address of a user device such as a PC by a "brute force" trawl through IP servers in an IP environment. However, such a method is not particularly efficient in terms of resources and a more elegant method has been developed; this can drastically reduce time taken to obtain a physical address corresponding to an IP address.

[0032] There is further herein-described a method of provisioning a service in a communications network for a user having an communications protocol address, such as an IP address, the method comprising:

[0033] obtaining a communications protocol address of a user for whom a service is to be provisioned;

[0034] sending a DHCP lease query message to a DHCP server, the message containing the communications protocol address of the user;

[0035] waiting for a DHCP response packet from the server,

[0036] extracting a hardware address, such as the MAC address or the PVC ID, of the user from the DHCP response packet;

[0037] provisioning a network connection with the user based on the hardware address obtained from the DHCP response packet.

[0038] By way of additional background, it is noted that the method described above makes use of the well established Dynamic Host Configuration Protocol (DHCP), details of which can be found in RFC 2131 of the Internet Community dated March 1997 and available, inter alia, at http://www.dhcp.org/rfc2131.html, the contents of which are incorporated herein by reference. The method also makes use of the draft DHCP Lease Query message protocol, details of which may be found on the ietf.org website and are summarised below. As those skilled in the art will appreciate, DHCP is an established low-level protocol for managing IP connections. DHCP presupposes that services have been previously provisioned for the user with whom a connection exists and does not directly concern itself with provisioning.

[0039] Those skilled in the art will appreciate that provisioning of services is normally a distinct process from low level communication between access concentrators and DHCP is not normally considered directly relevant to provisioning applications. In particular, die DHCP lease query

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 068

has been designed for access concentrators within a network to rebuild address information gleaned from their access relay function after rebooting or replacement. However, it has been appreciated that features of DHCP can in fact also be used to simplify provisioning. A user for whom a service is to be provisioned will often have a pre-existing IP address. Using DHCP Lease Query, the hardware parameters associated with that address can be identified from the DHCP server without the need for specialist application software at the user end nor for manual provision of the hardware identifier and this information can be used to provision a new service. Thus, surprisingly, DHCP lease query can be used in a provisioning context to facilitate automatic provisioning.

[0040] It is particularly advantageous that an address allocated in an internetworking environment, such as the Internet environment, can be used to obtain a hardware address. Within a network, the arrangement is usually that the network has at least one server, such as a DHCP server, which controls allocation of a block of internetworking protocol addresses (e.g. IP scope), which can be used across the internetworking environment, to individual hardware devices connected within the network. The mapping between internetworking protocol addresses and hardware addresses is then only known within the network doing the allocation and the DHCP lease query is only a low level communication designed for use by access concentrators in a network to rebuild data for use in carrying traffic. Increasingly, however, there is a demand for open access services in which networks carry services provided by off-net service providers but that means provisioning has to be done for new access devices, or new services to be provided to existing access devices, by off-net service providers. Here a further problem arises since an off-net service provider doesn't have access at all to the DHCP server.

[0041] This further problem may be solved using a facility of internetworking protocols known as tunnelling. In tunnelling, a datagram is encapsulated in a protocol from a higher or the same level and passed across the transport system to an endpoint where it is decapsulated. There are various forms of tunnelling, including Virtual Local Area Network (VLAN) encapsulation and source network address routing but a form that is likely to be particularly appropriate is Point-to-Point Protocol (PPP), for example PPP over Ethernet (PPPoE). This is described in an Internet Engineering Task Force (IETF) Draft, a list of current Drafts being available at http://www.ietf.org/ietf/lid-abstracts .txt. Increasingly, networks such as broadband networks will support tunnelling and this is exploited in the apparatus and methods herein described.

[0042] The user access device IP address may be obtained by means of an existing internetworking connection such as a TCP/IP connection For example, most conveniently a user may be required or requested to visit a website in order to obtain a new service and the user's access device IP address may be captured from this website for use in formulating a DHCP lease query for a provisioning application. Other TCP/IP transactions may be used to obtain an IP address for the user access device.

[0043] There is also herein described use of a DHCP lease query message to obtain a physical hardware identifier of a user device for use in a provisioning application to provision a broadband service for the user.

[0044] Further, there is also described a provisioning application having means, preferably a provisioning module, for provisioning a broadband service based on an access device physical address characterised by means, preferably a query module, for obtaining the user hardware identifier based on a DHCP lease query message submitted to a DHCP server and containing an IP address related to the access device. The access device may be a cable modem or DSL modem and the physical address may be a MAC address or PVC ID.

[0045] There is also herein described a computer program or computer program product, preferably stored on a computer readable medium, for performing any method described herein, preferably containing instructions for:

[0046] generating a DHCP query message containing an identifier related to an access device;

[0047] obtaining from a response to said message a hardware identifier of the access device;

[0048] provisioning a service for the access device based on the hardware identifier obtained.

[0049] Whilst the use of DHCP lease query may provide a particularly preferred, efficient and elegant implementation, other mechanisms may alternatively be used which allow an access device physical address to be returned using an internetworking address (or other pre-existing identifier related to the user of the access device) and preferably without requiring specialised software on the user machine.

[0050] Prior art provisioning methods generally provision services based on physical addresses (MAC addresses) of user devices such as PCs. Further, there is also herein described a method of provisioning a service for a user having a user device connected to a broadband network via a broadband access device, the user device and the broadband access device each having a respective physical address, the method comprising provisioning a service based on the physical address of the access device.

[0051] This allows the user to replace a user device, for example to connect multiple PCs without having to re-provision each device, which can be a cumbersome process, particularly with prior art provisioning methods. It also reduces the risk of fraudulent access as the service is made to the nearest point to the broadband network, namely the access device. Thus, if the access device is swapped, the service will need to be re-provisioned.

[0052] A significant advantage of the methods and apparatus described above is that they may facilitate more rapid expansion of services as users may purchase suitable access devices from retail outlets without requiring pre-provisioning or specialist skills to install the devices.

[0053] It has been further appreciated that because the novel provisioning application described can autonomously propagate services, it is desirable to integrate this with or tie the provisioning application to a capacity management application.

[0054] Thus preferably the provisioning method or provisioning application includes the step of or means for communicating with a capacity management application and such a method or application may be independently provided.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 069

[0055] The method may include checking for available capacity prior to provisioning a service and/or reporting provisioning of a service to a capacity management application after provisioning.

[0056] Conventionally, provisioning and capacity planning are distinct and this reflects conventional provisioning processes; problems have hitherto not been appreciated. However, this method may enable provisioning to be controlled at a higher level before problems arise; thus this solves a surprising and hitherto unappreciated problem which studies reveal might arise were efficiency of existing provisioning processes improved. The benefits of this method may be realised even with conventional provisioning processes.

[0057] The system described herein further extends to a capacity management application having means for communicating with a provisioning application. The capacity management application will normally have means for storing data relating to network capacity and user interface for communicating the stored data with a user. The capacity management application will normally provide a graphical interface and may include conventional statistical and graphing tools for displaying information concerning present, historical or predicted network capacity. The details of the capacity planning application are not critical and may be based on existing network planning applications. According to the inventive development, the application has means for communicating (preferably dynamically/in real time) with a provisioning application. Thus a provisioning application can report provisioning of new services and thus advise that capacity will be reduced before this would normally be featured in capacity planning considerations (for example before an actual increase in traffic can be detected). Particularly in the case of rapid roll out of services, this may lead to a significant increase in reliability of predictions. Alternatively or in addition, the capacity management application may feed information back to the provisioning application and may inhibit provisioning if capacity is unavailable, or may limit the capacity that can be provisioned. Again this may be advantageous particularly in the case of rapid roll out as it may reduce the risk of a service being provisioned and leading to network overload or the service being unsatisfactory to a user.

[0058] Preferably a network management tool comprises means for displaying at least one of performance, no of modems on a given node, quality of service, duration of connection, uptime, identifiers of faulty modems. Preferably a network management tool has means for communicating with an agent associated with a network component for receiving information from the agent. Preferably the network management tool comprises means for displaying information based on network usage at the level of network segments, preferably wherein a network segment corresponds to a card of a universal broadcast router or cable modem termination system. Preferably an agent is provided to report usage at the segment level. Preferably the management tool has means for displaying an indication of subscriber types as well as traffic information. A network management tool having any of the preferred features disclosed herein may be independently provided.

[0059] Information gathered by agents associated with at least some of the individual network components may allow the remote network component, which may be, for example, a network monitoring component, to be provided with realtime data from that point in the network. The information provided to the remote network component may allow the remote network component, for example, to monitor services provided to users and to identify quickly the source of a fault in the network. The remote network component may use the information to monitor the status of the network as a whole, or the status of a portion of the network.

[0060] Information other than the equipment status information may also be passed to the remote network component. For example, identification information for the network component may be transmitted, or service data, such as the rates at which data is being transmitted through the component, may also be transmitted to the remote network component.

[0061] Preferably, the agent further comprises means for receiving a configuration instruction. The presence of the agent on the network component may allow the network component to be configured remotely. If the network component stores service parameters for a user, then the agent may allow the remote modification of these service parameters, for example by the end user, or by a control centre.

[0062] Preferably at least a portion of the operation of the agent is configurable by means of a script. Hence the agent may be configured to send different types of data to the remote network component or to send data at predefined intervals.

[0063] As discussed above, the remote network component may be a network management tool which may be used to monitor and control the network and individual components within the network. In addition, or alternatively, the remote network component may be a planning tool or a provisioning tool, the network component may pass information regarding new user devices that connect to it to these remote components. Planning tools or provisioning tools may also receive information from the network component regarding traffic flow through the network component to allow the tools to plan for future provisioning requests.

[0064] According to a highly preferable feature, at least a portion of the operation of the agent is configurable to simulate activity of other network components at the network component incorporating the agent. Hence the agent may test the operation of the network component by simulating the activity of other network components. For example, the agent may simulate the process whereby another network component connects to or sends data to the network component. This may allow the agent to detect faults in the network component or in the network. The agent may signal an alarm to the remote network component in the event of detection of a fault condition in the network or in the network component on which the agent is running.

[0065] Preferably, the agent further comprises means for sending a report on the simulated activity of the other network components to the remote network component. This may allow the remote network component to detect and to debug faults in the network component incorporating the agent or in the network itself.

[0066] According to a preferable embodiment, the network component is a Point-of-Presence in a broadband network.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 070

[0067] According to a further aspect, there is also herein provided a method of monitoring and controlling network components in a broadband network, comprising:

[0068] providing an agent at each of a plurality of network components in the broadband network;

[0069] receiving data from each agent regarding the operation and status of the network component;

[0070] processing the data to determine the status and operation of the broadband network and of service provision in the broadband network.

[0071] Hence data corresponding to the network components may be sent from the agents to a central network monitoring component to allow monitoring and control of the network.

[0072] Preferably, the agent provided at each of the plurality of network component comprises an agent according to the agent aspect outlined above.

[0073] Preferably the step of processing the data comprises passing the data to a network monitoring tool and allowing access to the data at a user interface. Hence a network operator may monitor the network using the user interface and the data that has been passed to the network monitoring tool.

[0074] A further preferable feature of the provisioning aspect may be that:

[0075] At least one of the components in the broadband network incorporates an agent for passing information concerning the network component to a remote network component such that the method of provisioning a service may further comprise sending a provisioning information message to the or each agent. If the provisioning tool communicates details of any newly provisioned service to the or each agent, then the agent may begin to monitor the newly provisioned service immediately and, as a further advantage, agents associated with the newly provisioned service may be set up to monitor the service and the network components associated with it.

[0076] Preferably, the method of provisioning a service further comprises storing individual user parameters for the service, configuring the service provision based on a set of core configuration parameters and customising die service provision based on the stored individual parameters for the user. Hence the basic service may be provisioned according to a standard procedure and set of parameters and further steps may then be taken customize the service for each individual user.

[0077] Preferably, the method further comprises identifying new connections to the broadband network and automatically initiating a provisioning procedure for provisioning a service to the user device corresponding to the newly connected user. This may allow end-to-end provisioning of the user device. A user may connect a user device to the network and the new device may be provisioned automatically on connection. The provisioning of the user device should be dependent on the type of the user device, for example a cable modem or a set top box would be provisioned differently.

[0078] According to one preferable embodiment, the identifying step comprises receiving a message when the user device connects to the network.

[0079] According to a further preferable embodiment, the identifying step comprises monitoring the network to detect new connections to the network.

[0080] According to a further aspect there is provided a method of provisioning a service for a user device in a broadband network, the method comprising:

[0081] provisioning the service over the broadband network based on obtaining a physical address of the broadband access device;

[0082] storing individual service parameters for the user device from a database of service parameter information;

[0083] determining the individual service parameters for the user device and providing the service to the user device based on the determined service parameters.

[0084] This aspect may allow a service to be provisioned for a user device according to parameters defined by the user. The user may provide the desired parameter values either before or during provisioning and some parameters may be determined automatically from querying the user device itself.

[0085] Preferably, the method further comprises providing a user interface to allow a network operator or a user to access and to amend the stored service parameters for the provisioned service. This may allow the user parameters to be amended after provisioning.

[0086] According to one preferable feature, at least some of the individual service parameters may be applied to a predefined plurality of user devices. This may allow a user to set the service parameters for, for example, a whole network of user devices.

[0087] According to a further aspect, there is provided a method of provisioning a connection between a remote user device and a virtual private network of user devices comprising provisioning the connection such that: the virtual private network appears to be connected directly to the remote user device; and the remote user device appears to be connected directly to the remote user device.

[0088] Preferably, the method further comprises provisioning a service to the remote user device via the virtual private network (VPN).

[0089] According to one preferable aspect, the network is a broadband network and the provisioned service is a broadband service.

[0090] Preferably, the provisioning a service step comprises receiving a request from a user of the remote user device, which request does not include the physical address of the remote user device and provisioning a service based on obtaining the physical address of the remote user device.

[0091] Further preferably, the physical address of the remote user device is obtained by using the local address of the remote user device within the VPN.

[0092] According to an alternative preferable embodiment, the physical address of the remote user device is obtained by using an IP address of the remote user device.

[0093] The invention further provides provisioning tools, planning tools, user interfaces, methods, inventory tools,

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 071

agents for devices, data packets, computer programs, computer program products, apparatus, systems, and computer implemented methods. Features and preferred features of each category may be applied to other categories unless otherwise stated. References to tools are intended to encompass without limitation applications or applets, software modules, combinations of hardware and software and to include both stand-alone modules, modules or code integrated into larger applications and modules which may stand alone and/or be provided as part of a suite of components. In most cases, these tools may be embodied as computer programs and computer program products and may be supplied as data packets or signals, but may include either general purpose or dedicated hardware.

[0094] A further aspect provides a provisioning tool for a broadband network comprising means for discovering information concerning a service to be provisioned based on information associated with an existing connection.

[0095] A further aspect provides a provisioning tool for provisioning a broadband service over at least one specified hardware connection, the provisioning tool comprising a module for performing an activation action and an activation script processor for processing an activation script defining a workflow sequence including at least one activation action.

[0096] Conventionally the workflow sequence would be implicit in the operation of any activation module for a particular hardware connection. However, pursuant to the invention, it has been appreciated that similar steps may be performed for different hardware connections and changes may be made dependent on the network configuration. By providing a module for performing an activation action and an activation script, definition of the necessary steps for a variety of hardware connections (cable, dsl modems of varying types, MPLS and VPN connections) may be accommodated more easily without requiring complex dedicated programming for each type of hardware; basic actions may be defined and then these may be put together using a script.

[0097] Preferably the script is user viewable and/or editable. In a highly preferred embodiment, the activation script is executed in a structured document, particularly a markup language such as SGML or most preferably XML (extensible markup language)—XML provides a readily editable and readily processed compact language having sufficient flexibility to implement an activation script. The provisioning tool may provide means for storing a plurality of activation scripts for mutually distinct hardware connections and means for selecting an executing an appropriate script for a hardware connection in response to an activation request.

[0098] Preferably the provisioning tool has means for receiving an identifier of a client device and means for selecting an activation script based on the identifier. The identifier may include an identifier of equipment type for at least some components in the network, preferably for all components. The equipment type information preferably includes manufacturer and model information—this enables different procedures for different versions of the same type of device (e.g. switch, cable modem) to be accommodated. This is particularly beneficial when scripts govem workflow as the workflow for a variety of similar devices from different manufacturers may be similar or identical but the precise activation actions may differ. Multiple devices may be catered for efficiently by essentially duplicating activation scripts but providing device specific activation modules as needed.

[0099] The identifier may be user input or may be based on information gained from a discovery process. Preferably each activation action comprises a low-level action, i.e. without complex flow control and action flow control is defined by the script. Preferably each action corresponds to a defined step or unit of time. Preferably actions correspond to verbs of the activation scripts.

[0100] Preferably the provisioning tool has means for recording transactions (with a device to be provisioned such as a modem) during activation of a service. Preferably transactions are recorded so that individual transactions can be replayed, viewed or analysed. Pursuant to the invention, it has been appreciated that this can provide a surprisingly useful insight into any network problems as compared to the conventional approach of logging internal success or error reports and may enable configuration scripts to be optimised. This feature is particularly useful when provided in conjunction with the scripting of actions but may be provided independently.

[0101] A further aspect provides a provisioning tool for a broadband network comprising means for executing a sequence of actions to activate a broadband service via a client device, the provisioning tool having means for recording transactions with the client device.

[0102] The provisioning tool may have means for receiving stored data indicative of a network configuration and client data identifying the client device to be provisioned and means for determining a sequence of actions based on the stored data and client data. This may simplify a process, as compared to a conventional process in which a user specifies network components to be configured.

[0103] A further aspect provides a provisioning tool for a broadband network comprising means for receiving stored configuration data indicative of a network configuration and client data identifying the client to be provisioned and means for determining a sequence of actions based on the stored configuration data and client data. The client data may be determined from a user interface.

[0104] The provisioning tool preferably has a graphical user interface for displaying a representation of at least a part of the network. The client data may be determined based on a user input from the graphical user interface. More preferably the provisioning tool has means for receiving an input command based on the graphical user interface and determining at least one provisioning action in response thereto based on the stored configuration data. In a preferred application, the input command may include a drag and drop command. Preferably the provisioning tool is arranged to interpret a user action based on the graphical interface and the configuration data. Advantageously the provisioning tool has means for storing at least one rule or configuration script for use in determining at least one provisioning action. The storage of rules may facilitate generation of complex sequences of action based on simple user inputs.

[0105] In a preferred embodiment, the invention provides a provisioning tool for a broadband network comprising means for storing a representation of network configuration, means for storing rules governing activation actions, a

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 072

(preferably graphical) user interface for providing a user with a representation of a network configuration, means for receiving a user input to provision a service for a client, means for processing the input based on the stored representation of the network configuration and the stored rules to generate a sequence of at least one activation action. The provisioning tool typically has means for performing at least one activation action.

[0106] A further aspect provides a provisioning tool for a broadband network comprising means for storing network configuration information including information concerning network topology and information concerning configuration actions, a drag and drop graphical user interface for receiving a user command to provision a service and means for generating an activation sequence containing at least one activation action based on the received command and the stored network configuration information.

[0107] The provisioning tool may have means for communicating with an agent associated with a client device to communicate configuration information therewith. By providing an agent on the client device, greater flexibility may be achieved and enhanced functionality may be achieved as compared to communicating directly with the client device. The agent may be independently provided.

[0108] A further aspect provides an agent for a client device in a broadband network, the agent having means for communicating configuration information for the client device to a remote network configuration or management tool, advantageously from a provisioning tool.

[0109] The provisioning tool may have means for communicating with a network inventory tool for receiving network configuration information. The network inventory tool preferably has means for discovering network configuration information based on communicating with network components. The network inventory tool may (additionally, or less preferably alternatively) have means for receiving information describing network configuration via a user interface. It is a preferred feature of the provisioning tool aspects that the network configuration information includes an identifier of equipment type for at least some components in the network, preferably for all components. The equipment type information preferably includes manufacturer and model information. This greatly enhances the flexibility of the method as actions specific for a particular type of component may be correctly generated in an automated fashion. This is particularly advantageous in combination with aspects which provide for selection of activation actions. Preferably the network inventory tool has means for storing information concerning (a) equipment type identifiers for network components type and (b) interconnections between network components. Thus, as well as a user being able to view network topology and see which components may be affected by a proposed action, the configuration actions may be tailored to specific hardware equipment type. The inventory tool may be integrated with the provisioning tool or may be provided independently. The provisioning tool and inventory tool advantageously communicate by sharing a database.

[0110] A further aspect provides a network inventory tool for a broadband network comprising means for storing network configuration information including first information including an equipment type identifier for each of a plurality of network components and second information identifying interconnections between network components.

[0111] The inventory tool may be arranged to discover network configuration information by interrogating network components. The inventory tool is preferably arranged to communicate the network configuration information to at least one other tool, optionally by storing the information in a commonly accessible database. The inventory tool is preferably arranged to communicate with an agent operating on a network component to discover information about the network component. This may simplify operation of the inventory tool and/or increase the amount of information that the tool can discover and/or facilitate operation with a variety of types of hardware. Agents may be configured to operate on specific network components. The agents may be independently provided.

[0112] A further aspect provides an agent for a network component of a broadband network, the agent comprising means for passing equipment status or identification information concerning the network component to a remote network component, preferably a network inventory tool.

[0113] The agent may further comprise means for receiving a configuration instruction, optionally from a provisioning or configuration or management tool. At least a portion of the operation of the agent is preferably configurable by means of a script, preferably an XML script.

[0114] Preferably, the remote network component includes a provisioning tool incorporated into a broadband network.

[0115] Further preferably, the remote network component includes a planning tool incorporated into a broadband network.

[0116] Further preferably, the remote network component includes a network management tool.

[0117] According to a highly preferable embodiment, at least a portion of the operation of the agent is configurable to simulate user activity at the network component. Hence different situations and scenarios of user activity may be simulated on demand from an operator at a remote network component. This may allow the operator of the remote network component to de-bug a fault in the operation of the network component.

[0118] Preferably, the user activity comprises at least one of:

[0119] connecting to a broadband network;

[0120] verifying the identity of the user or the network component over the broadband network;

[0121] accessing a service via the broadband network using configured and/or preset parameters;

[0122] amending at least one preset parameter and accessing a service via the broadband network using the at least one amended parameter.

[0123] Preferably, the agent further comprises means for sending a report on the simulated user activity to the remote network component.

[0124] According to one preferable embodiment, the network component is a Set Top Box.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 073

[0125] According to a further preferable embodiment, the network component is a Cable Modem.

[0126] Preferably, the agent further comprises means for accessing a communication service and means for signalling an alarm to a remote network component in the event oF detection of a fault condition. Hence the agent may be used to monitor access of the network component to the communication service and report any problems with access immediately. This may reduce reliance on a user to report a fault, or a central network monitoring centre to detect the fault.

[0127] A further aspect provides a method of operating a network component of a broadband network, the method comprising passing equipment status or identification information concerning the network component to a remote network component.

[0128] The method may have preferable features corresponding to the preferable features of the agent aspect described above.

[0129] The provisioning tool and/or inventory tool may operate in conjunction with a planning tool.

[0130] A further aspect provides a planning tool comprising a user interface for communicating information relating to network capacity or a planned service with a user, the planning tool characterised by means for communicating with a provisioning tool and/or inventory tool network or service configuration information.

[0131] In a preferred implementation, the planning tool may provide means for defining one or more planned services based on at least one of: location; customer profile; quality of service; network availability; availability of other services.

[0132] The provisioning tool is preferably arranged to operate in conjunction with a customer front end for communicating user information. The user information may include authentication information. The user information may include an indication or selection of one or more desired services. The provisioning tool may include means for re-provisioning a service based on information received from a user and/or may include means for communicating available services to a user, preferably by means of a customer front end tool.

[0133] A further aspect provides a customer front end tool for a client device in a broadband network, the customer front end tool having means for receiving user information and communicating the user information to a remote provisioning tool.

[0134] This may facilitate configuration. The customer front end tool may include means for communicating an identifier of the client device to the provisioning tool. The customer front end tool may operate over an internet connection and the internet connection may be used by the provisioning tool in identifying the client device. The customer front end may be arranged to enable a user to enter user authentication information in the event that a client device configuration is changed, for example in the event that one device (e.g. a cable modem) is swapped for another and/or the device is physically connected at a new location. Particularly in combination with the automatic discovery procedure mentioned, this may greatly facilitate use of a service for a user who modifies equipment as, rather than having to undergo a new manual provisioning step each time a change is made to the location of equipment or equipment hardware, the user need simply supply authentication information and the previous service can be re-provisioned to operate with the new configuration.

[0135] A further advantage of the provisioning techniques and tools is that, because provisioning is straightforward and in preferred embodiments can be performed without end user interaction, new or modified services can be delivered. In particular, a service may be dynamically altered by re-provisioning, or new services made available periodically. This may facilitate content delivery and may increase uptake of new services.

[0136] A further aspect provides a provisioning tool for provisioning a service in a broadband communications network having means for provisioning a service characterised by means for storing information relating to a service parameter which varies with time and means for altering a characteristic of the service based on the stored information.

[0137] Preferably the means for altering is arranged to re-provision the service.

[0138] A further aspect provides a method of providing a service in a broadband communication network comprising storing information relating to a service parameter which varies with time and periodically re-configuring the service based on the stored information.

[0139] A further aspect provides use of a provisioning function to effect delivery of a communication service having at least one time-varying service characteristic based on periodic re-provisioning of the service.

[0140] The time varying characteristic may include one or more of bandwidth, quality of service, access to specified services. The time varying characteristic may include variation at least once a week and preferably at least once a day. The characteristic may be varied in response to usage or based on information from a source such as a congestion detector or a billing system, in addition to or instead of in response to stored data of a time characteristic.

[0141] Additionally or alternatively, a service having a time-varying characteristic may be implemented based on reconfiguring a network component, preferably by communicating with an agent provided on the network component, particularly wherein the network component comprises a user access device.

[0142] The invention may provide a method of providing a communication service to a user via a user access device, the method comprising dynamically remotely re-configuring the user access device to modify a characteristic of the service delivered.

[0143] By dynamically is preferably meant online and/or while the service is available substantially uninterrupted and/or in response to a real time input, and most preferably without operator intervention.

[0144] Services may be provided to a plurality of users and the method may include selectively re-configuring an individual user access device to modify selectively a characteristic of service for the individual user.

[0145] Modification may be in response to stored information relating to a time varying characteristic, as afore-

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 074

mentioned. Additionally or alternatively, modification may be in response to usage or billing system information—for example a service may be downgraded for a user who is behind with payments or who has previously exceeded a usage quota.

[0146] Another advantageous use of data captured during provisioning may be in service assurance. It can be important in offering a communications service that the ongoing quality of service provided to customers can be monitored. New customers will generally have an expectation of an acceptable quality of service and may indeed have a service level agreement with a service provider. Existing customers will not expect the quality of service to become degraded because other customers have been newly provisioned.

[0147] By sharing data, for instance by sharing a data model and access to the same data storage, a provisioning application, working in conjunction with a service assurance application, can offer a particularly efficient use of data for diagnostics. Service assurance products may for instance receive alarm signals or data arising in use of a network to provide an identified service. Since a provisioning application may gather subscriber-related address data in relation to services provisioned, the service assurance product can be enabled to relate alarm data not just to services but also to relevant service subscribers.

[0148] Further advantages of the methods and apparatus herein described lie in the fact that a service provider has the physical address of a user's access device. For instance, the service provider can also provide a measure of fraud management in that, if fraud is detected in association with an access device, the service provider can suspend or deactivate the device in relation to a service, or can downgrade the level of service to that device.

[0149] Also, prior to service provision, the service provider can identify cases where a user's situation is simply not able to support a service. For instance, where a user wants to subscribe to a Video on Demand (VoD) service over Digital Subscriber Lines (DSL), the service provider can check whether the user's access device is physically close enough to a Digital Subscriber Line Access Multiplexer (DSLAM) to have sufficient bandwidth.

[0150] Further incorporated herein are methods which correspond to the apparatus and vice versa and to computer programs and computer program products for implementing such methods. Preferred and optional features of the methods and apparatus disclosed may be applied to all other methods and apparatus unless otherwise stated or apparent from the context.

[0151] Further aspects and preferred features of the invention are described below:

[0152] A method of testing a broadband network, the network comprising a head end for receiving one or more communications services from service providers and transmitting the one or more services towards end user equipment, and comprising at least one node for receiving said one or more services from the head end and delivering the service(s) towards end user equipment, which method comprises launching a test signal to the network at said at least one node and monitoring a response by the network thereto.

[0153] The test signal may be launched by computing equipment provided at said at least one node. The test signal may be provided by an agent associated with the node. The method may further comprise receiving one or more control signals at said computing equipment (or agent), the control signals having been transmitted over the network to control said launch of a test signal. The test signal may be launched via a first signal path from the computing equipment (or agent) to the network and said one or more control signals may be received via a second signal path from the network to the computing equipment (or agent), said first and second signal paths being different. The first and second signal paths may differ at least in that said first signal path comprises transmission by a cable modem termination system. A selected one or more of a plurality of different test signals may be used. The agent or system may be programmed to launch one or more test signals at one or more predetermined times. One or more control signals may comprise means to trigger launch of one or more test signals by the computing equipment.

[0154] In one embodiment at least one node comprises a provisioning server, for dynamic assignment of addresses to end user equipment, and said test signal in use requires assignment of an address by said provisioning server and a monitored response comprises said assignment of an address.

[0155] One or more of said test signals may simulate a request received from user equipment for service delivery by means of the network.

[0156] The invention may provide a method of testing a broadband network, the network comprising a head end for receiving one or more communications services from service providers and transmitting the one or more services towards end user equipment, and comprising at least one node for receiving said one or more services from the head end and delivering the service(s) via a cable modem termination system towards end user equipment, which method comprises transmitting a control signal to an agent or other computing means at the node, said control signal comprising a rigger to launch a service request to the network via the cable modem termination system at said at least one node, said method further comprising monitoring a response by the network to the launched service request.

[0157] There may be provided a node of a broadband communications network, for receiving one or more communications services from service providers and transmitting the one or more services towards end user equipment, which node comprises an agent or other programmable end user simulation equipment for launching a service request to the network.

[0158] The node may further comprise a first signal path for delivering control signals to the simulation equipment and a second path for transmitting a launched service request from the simulation equipment to the network, said first and second paths being different. Then second path may comprise a cable modem termination system.

[0159] There may be provided a network management system comprising a fault detector and fault processor for detecting faults in the network or services provided over the network, and for analysing detected faults with the purpose of generating solutions to the faults, wherein the system further comprises context sensitive help for providing information to the user in relation to one or more faults being analysed.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 075

[0160] The context sensitive help may comprise a knowledge management system having a search engine and the search engine runs a search on data stored for the knowledge management system, said search being based on the one or more faults being analysed.

[0161] There may be provided a communications network management system, for receiving and processing fault reports in respect of a network and/or one or more services supported by the network, the system being provided with a data store for storing data in respect of said network and/or services and processes fault reports in the light of stored data to generate corrective solutions to received fault reports, wherein the system is further provided with at least one simulator for requesting service provision over the network such that the network and one or mole services can be proactively tested. Preferably the simulator simulates user activity. The simulator may comprise an agent associated with a network component. Preferably the network is a broadband network and the simulator is provided at a node of the network.

[0162] There may be provided a communications network management system, which system comprises:

[0163] a) an input for receiving Fault reports in respect of a network and/or one or more services supported by a network,

[0164] b) a data store for storing data in respect of said network and/or services,

[0165] c) a fault processor for processing fault reports received via the input, using data stored in the data store, to generate corrective solutions, and

[0166] d) a simulator for triggering a service provision response by the network

[0167] wherein the simulator has an output to the network to trigger a service provision response, such that a fault report in respect of said response will be received at the input and processed by the fault processor.

[0168] The communications network management system may further comprise means to apply a generated corrective solution to the network and to trigger a service provision response by use of the simulator such as to validate the applied corrective solution.

[0169] The input for receiving fault reports may be adapted to receive both fault reports in respect of services provided by said network and component alarms from components of said network, and said fault processor comprises a correlation engine for correlating received fault reports in respect of one or more services with received component alarms.

[0170] The data store may be structured to hold one or more problem descriptions in addition to one or more fault reports and/or one or more component alarms, at least one stored problem description comprising data received in respect of historic component behaviour, said fault processor being adapted to access data received in respect of historic component behaviour for use in processing fault reports to generate one or more corrective solutions.

[0171] There may be provided a communications network management system, which system comprises:

[0172] a) an input for fault reports in respect of a network and/or one or more services supported by a network,

[0173] b) a data store structured to store data in respect of said network and services, and

[0174] c) a fault processor for processing fault reports received via the input to generate corrective solutions,

[0175] wherein the data store is further structured to store customer data in relation to services and the fault processor comprises a correlation engine for correlating received fault reports in respect of one or more services with customer data, and wherein the fault processor further comprises sorting apparatus for sorting fault reports in an order determined by correlated customer data.

[0176] A further aspect provides a service provisioning and assurance tool for use in the supply of one or more communications services to at least one user via a network, comprising:

[0177] i. means for provisioning a service, selected by a user or user representative, in relation to a hardware address of the user;

[0178] ii. means for storing data relating the selected service, the hardware address and the user;

[0179] iii. means for supplying the selected service to the hardware address;

[0180] iv means for receiving one or more alarms in respect of the supplied service; and

[0181] v. means for analyzing received alarms

[0182] wherein the means for analyzing is arranged to access the stored data

[0183] Hence the tool can be used to provision, supply and monitor a service to a user over a network. Analysis of alarms received may incorporate an analysis of the present fault in view of previous faults at that user equipment or in view of previous similar faults in other sections of the network.

[0184] Preferably, the service provisioning and assurance tool further comprises means for obtaining information relating to the selected service, the hardware address and the user fri-om components over a network, wherein the components include at least one of:

[0185] a DHCP server;

[0186] an agent associated with user equipment, wherein the user equipment may comprise a Set Top Box or a Cable Modem;

[0187] a system database;

[0188] a Cable Modem Termination System.

[0189] Preferably, the service provisioning and assurance tool further comprises display means for displaying at least one of:

[0190] parameters corresponding to the configuration of a service for a particular user;

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 076

[0191] information regarding use of a service by a particular user or group of users;

[0192] information regarding the provisioning and performance of a particular service;

[0193] and wherein the display means further comprises means for adjusting parameters corresponding to the configuration of a service for a particular user.

[0194] Hence an operator may use the tool to analyse the setup and use of a particular item of user equipment, and may, for example by accessing a secure area of the operator interface, alter parameters corresponding to service provision for a particular user.

[0195] According to a highly preferable feature, there is further provided means for configuring an agent associated with the user equipment to test at least one aspect of service provision by simulating user activity at the user equipment.

[0196] Hence the functionality of user equipment may be tested remotely by using the tool to configure an agent associated with the user equipment. This may mean that it is not necessary for an operator or engineer to go to the user equipment in order to test it.

[0197] Preferably, there is further provided means for amending service provision parameters for a particular item of user equipment and means for configuring the agent to simulate user activity at the user equipment using the amended parameters.

[0198] The functionality of the system may also be tested with amended parameters. Hence it may be possible for a network engineer, or operator to solve problems with the users equipment remotely by changing service parameters for the user and testing the new parameters using the agent associated with the user equipment.

[0199] According to a further preferable feature, the service provisioning and assurance tool further comprises:

[0200] means for receiving information from the agent regarding the simulation of user activity at the user equipment;

[0201] in the case of successful provision of a service, means for transferring the amended service provision parameters for the user to the system database.

[0202] This may allow any successful amendment to the parameters to be detected by the tool. The amended parameters may then be saved in die system database for that user.

[0203] According to a further aspect, there is also provided a method corresponding to the service assurance tool described above with corresponding preferable features.

BRIEF DESCRIPTION OF DRAWINGS

[0204] The provisioning of services in a communications network and the management of such a network will now be described further, by way of example only, with reference to the accompanying drawings in which:

[0205] **FIG. 1** is a schematic diagram of a network environment for provisioning apparatus in accordance with one example of the system and methods herein described;

[0206] **FIG. 2** is a schematic diagram of message flow in provisioning apparatus carrying out provisioning according to one example of the systems and methods herein described;

[0207] **FIG. 3** is a schematic diagram of an architecture for a service management system using the provisioning apparatus of **FIGS. 1 and 2**;

[0208] **FIG. 4** is a schematic diagram of message flow in provisioning apparatus carrying out provisioning according to a further example of the systems and methods herein described;

[0209] **FIG. 5** is a schematic diagram of an initial set-up of a network environment for provisioning apparatus in accordance with a further example of the system and methods herein described;

[0210] **FIG. 6** is a schematic diagram of a network environment for provisioning apparatus in accordance with the example illustrated in **FIG. 5** after a new customer edge router has been added to the network according to an example process;

[0211] **FIG. 7** is a schematic diagram of a network environment for provisioning apparatus in accordance with the example illustrated in **FIG. 5** or **6** after a new customer edge router has been added to the network according to a further example process;

[0212] **FIG. 8** is a schematic diagram of a network environment for provisioning apparatus in accordance with the example illustrated in **FIG. 5, 6** or **7** after a new customer edge router has been added to the network according to a further example process;

[0213] **FIG. 9** is a schematic diagram of an initial topology of the network environment for provisioning apparatus, before modification has taken place, according to an example of the system and methods herein described;

[0214] **FIG. 10** is a schematic diagram of a final topology of the network environment for provisioning apparatus, after modification has taken place, according to an example of the system and methods herein described;

[0215] **FIG. 11** is a schematic diagram of how the Set-Top Box Manager application may be incorporated into a network environment for provisioning apparatus according to one embodiment of the systems and methods herein described;

[0216] **FIG. 12** is a schematic diagram of an example of a Set-Top Box Manager screen display according to one embodiment of the systems and methods herein described;

[0217] **FIG. 13** is a schematic diagram of an example of a further Set-Top Box Manager screen display according to one embodiment of the systems and methods herein described;

[0218] **FIG. 14** is a schematic diagram of an example of a further Set-Top Box Manager screen display, which may be used to show 'Audit' information, according to one embodiment of the systems and methods herein described;

[0219] **FIG. 15** is a schematic diagram of a 'Connection Window' screen display according to one embodiment of the systems and methods herein described;

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 077

[0220] **FIG. 16** is a schematic diagram of an 'Install' Results List Panel screen display according to one embodiment of the systems and methods herein described;

[0221] **FIG. 17** is a schematic diagram of a 'Forward Path' Results List Panel screen display according to one embodiment of the systems and methods herein described;

[0222] **FIG. 18** is a schematic diagram of a 'Reverse Path' Results List Panel screen display according to one embodiment of the systems and methods herein described;

[0223] **FIG. 19** is a schematic diagram of a 'Resources' Results List Panel screen display according to one embodiment of the systems and methods herein described;

[0224] **FIG. 20** is a schematic diagram of an example of a further Set-Top Box Manager screen display, which may be used to show 'Audit' information, according to one embodiment of the systems and methods herein described;

[0225] **FIG. 21** is a schematic diagram of a Set-Top Box Manager Top Bar according to one embodiment of the systems and methods herein described;

[0226] **FIG. 22** is a schematic diagram of a one embodiment of the architecture of the Set-Top Box Manager;

[0227] **FIG. 23** is a schematic diagram of a Cable Modem Manager integrated into a distributed system according to one embodiment of the systems and methods herein described;

[0228] **FIG. 24** is a schematic diagram of a technical architecture overview of the Cable Modem Manager according to one embodiment of the systems and methods herein described;

[0229] **FIG. 25** is a schematic diagram of a screen display which may be generated by the Cable Modem Manager to display data according to one embodiment of the systems and methods herein described;

[0230] **FIG. 26** shows a schematic view of where the network management system sits in relation to interfaces for use by users, including customers, service operators and network operators, and the services and network elements being managed;

[0231] **FIG. 27** shows a schematic view of the primary components of the network management system;

[0232] **FIG. 28** shows a more detailed view of components of the network management system together with tools and other systems with which it interacts;

[0233] **FIG. 29** shows a simulator for use in the network management system of **FIG. 26** and its connection into a network to be tested;

[0234] **FIG. 30** shows a screen view from a graphical user interface reviewing an alarm by means of the network management system, with access available to a knowledge management system for further analysis;

[0235] **FIG. 31** shows a screen view from a graphical user interface reviewing an alarm in terms of user impact;

[0236] **FIG. 32** shows a screen view from a graphical user interface reviewing an alarm with reference to its network location, with access available to the knowledge management system for further analysis;

[0237] **FIG. 33** shows a screen view from a graphical user interface providing equipment information, with access available to a knowledge management system for further analysis;

[0238] **FIG. 34** shows the options available for a screen view layout as shown in **FIG. 33**;

[0239] **FIG. 35** shows a screen view from a graphical user interface providing an alarm list with access to the knowledge management system for further analysis of selected alarms;

[0240] **FIG. 36** shows a screen view similar to that of **FIG. 30** in which the knowledge management system has been accessed for further relevant information;

[0241] **FIG. 37** shows the options available for a screen view layout as shown in **FIG. 36**;

[0242] **FIG. 38** shows a login screen for a user accessing the knowledge management system;

[0243] **FIG. 39** shows a screen view available to a user of the knowledge management system;

[0244] **FIG. 40** shows a further screen view available to a user of the knowledge management system;

[0245] **FIG. 41** shows the options available for a screen view layout as shown in **FIG. 39** or **40**;

[0246] **FIG. 42** shows a network context for the network management system in which a global infrastructure provider controls the end-to-end network;

[0247] **FIG. 43** shows a network context for the network management system in which a service provider uses the network management system to control the service provider's part of the network;

[0248] **FIG. 44** shows a sample Hybrid Fibre-Coax manager deployment according to one embodiment of the systems and methods described herein;

[0249] **FIG. 45** illustrates CMTS router and CMTS card relationships according to one embodiment of the systems and methods described herein;

[0250] **FIG. 46** shows an HFC manager user interface overview for a preferred embodiment of the systems and methods described herein;

[0251] **FIG. 47** illustrates a Knowledge Management System integrated with Imagine Service Emulation Agent modules according to one embodiment of the systems and methods described herein;

[0252] **FIG. 48** illustrates a graphical User Interface structure for a preferred Knowledge Management System according to one embodiment of the systems and methods described herein;

[0253] **FIG. 49** is an XML section of command script for the switch configuration for use with a preferred ISEA according to one embodiment of the systems and methods described herein;

[0254] **FIG. 50** is an XML section of command script for a cable modem configuration for use with a preferred ISEA according to one embodiment of the systems and methods described herein;

[0255] **FIGS. 51***a* and **51***b* are an XML sections of command script for a scheduler manager configuration for use with a preferred ISEA according to one embodiment of the systems and methods described herein;

[0256] **FIG. 52** is an XML section of command script for a DHCP protocol configuration for use with a preferred ISEA according to one embodiment of the systems and methods described herein;

[0257] **FIGS. 53***a* and **53***b* are an XML sections of command script for use with a preferred ISEA to configure a scenario named 'Test' for one location, containing three services; provisioning, internet access, mail (ISP) according to one embodiment of the systems and methods described herein;

[0258] **FIG. 54** is a continuation of the XML section of command script of **FIGS. 53***a* and **53***b* according to one embodiment of the systems and methods described herein;

[0259] **FIG. 55** illustrates scenario organization for an ISEA according to one embodiment of the systems and methods described herein;

[0260] **FIG. 56** shows a preferred hardware architecture for an ISEA according to one embodiment of the systems and methods described herein;

[0261] **FIG. 57** illustrates the six key components comprising a preferred ISEA architecture according to one embodiment of the systems and methods described herein;

[0262] **FIG. 58** illustrates one embodiment of the scenario organisation for a HSD agent according to one embodiment of the systems and methods described herein;

[0263] **FIG. 59** is a schematic diagram of the IP address manager integrated into a service assurance suite according to one embodiment of the systems and methods described herein;

[0264] **FIG. 60** is a schematic diagram of an overview of one embodiment of the architecture of the VPN service assurance suite;

[0265] **FIG. 61** illustrates one embodiment of the operation of an agent on provisioning of a new PE-CE link;

[0266] **FIG. 62** illustrates one embodiment of the architecture of the Configuration Manager and the integration of the Configuration Manager into a VPN provisioning network;

[0267] **FIG. 63** illustrates how a VPN provisioning system may be incorporated into a network according to one embodiment of the systems and methods described herein;

[0268] **FIG. 64** illustrates one embodiment of the OSS database with the high availability cluster in active-active mode.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0269] Provisioning

[0270] Discovery of Device Details for Use in Provisioning

[0271] Referring to **FIG. 1**, a network environment in which provisioning apparatus might be used is a cable network providing broadband services. User terminals **100** such as PCs are connected to a cable network via modems **105**. A cable modem termination system **120** connects the modems **105** to an access concentrator **125** which in turn is connected at or via a hub **115** of the network to a DHCP server **130**.

[0272] The network hub **115** is connected over a collection network **140** to a regional head end **165** for the network and an Internet Service Provider (ISP) platform **190** is connected to the regional head end **165** by a core network **160**. The ISP platform **190** also has access to the Internet **170** and may provide services from an Internet-based server **175** and/or from a server **185** within its own platform **190**.

[0273] Importantly, in an open access environment, there may be service provider platforms **190** which only have connection to the cable network via the Internet **170**.

[0274] In a known provisioning arrangement, when a new access device **105** is added to the cable network, at a hardware address in the network, the DHCP server **130** will allocate it an Internet Protocol (IP) address. The DHCP server **130** maintains a record of the allocated 1P addresses mapped against the hardware addresses.

[0275] If a user now wishes to subscribe to a new service, using the same access device **105**, the relevant service provider needs to know the hardware address in order to provision the new service to that user and the hardware address can be obtained from the DHCP server **130** using a DHCP lease query message, as long as the user's access device IP address is known.

[0276] One way of enabling service provisioning can be done in response to a user's request over the Internet. In **FIG. 1**, the user may use their user equipment **100**, connected to an access device **105**, to access an interactive Web interface of the service provider's, installed on an Internet host **175**. The Web interface will automatically pick up an rP address for the user's access device **105** which the service provider can use in querying the DHCP server **130** from their ISP platform **190**.

[0277] Referring to **FIG. 2**, in more detail, the ISP platform **190** comprises a provisioning server **180** which supports a provisioning module **205** and a query module **200**. When the user interacts with the Web interface to request a new service, the query module receives (Step **210**) an IP address associated with the user's access device **105** from the Web interface, for instance in the form "000.nnn.mmm.111". The query module **200** formulates a DHCPLEASEQUERY message containing the IP address and sends it (Step **215**) to the DHCP server **130** which returns (Step **220**) a DHCPACK response packet from which the user's hardware address (MACaddr) is extracted by the query module **200** and passed (Step **225**) to the provisioning module **205**. The provisioning module, having a hardware address for the user's access device, can then perform provisioning in a conventional manner.

[0278] An exemplary method of operation will now be summarised.

[0279] (A) A user visits a website hosted on an ISP server **175** and requests a new service. This request contains the user's IP address and identifies the service requested. The request is communicated to the service

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 079

provider's Web interface which communicates the request or a portion thereof to a provisioning application on a provisioning server **180**. The Web interface may be a part of the provisioning application, it may be separate but run on the same server, or it may run on a separate server altogether.

[**0280**] (B) The provisioning application receives the request (Step **210**), performs validation as required and formulates a DHCPLEASEQUERY message containing the IP address to send (Step **215**) to an appropriate DHCP server **130**. In **FIG. 2**, the query is formulated by a specific query module **200**, but this may be integrated seamlessly into the provisioning application.

[**0281**] (C) The DHCP server **130** receives the message and returns (Step **220**) the appropriate MAC address. If the DHCP server does not support DHCPLEASEQUERY or does not have the information then either no response will be sent or a null response, according to the circumstances and the DHCP protocol.

[**0282**] (D) The provisioning application processes the response packet, if any, and extracts a MAC address, if possible. In the event that the provisioning application cannot obtain a response from any DHCP server, then it must revert to other methods of obtaining a MAC address, for example by requesting the user to supply it. Even if it is available, the user may be requested to verify the information obtained.

[**0283**] (E) Provisioning is carried out as required, using the MAC address obtained to enable provision of the new service to the user (Step **230**) via the relevant access device; the remainder of the provisioning process may correspond to or be based on a known provisioning process.

[**0284**] The DHCP Lease Query protocol will be available to those skilled in the art and so is not described in detail. A list of drafts of the Internet Society may be found at http://www.ietf.org/ietf/lid?abstracts.txt. However, the following may assist in understanding the background and explaining the novel use made of this low level query, which was intended for use by access concentrators such as routers and not previously contemplated for use in provisioning applications.

[**0285**] Background to DHCPLEASEQUERY

[**0286**] The DHCPLEASEQUERY message is a new DHCP message type transmitted from a DHCP relay agent to a DHCP server. It is intended that a DHCPLEASEQUERY-aware relay agent would send the DHCPLEASEQUERY message when it needed to know the location of an IP endpoint. The DHCPLEASEQUERY-aware DHCP server would reply with a DHCPKNOWN or DHCPUNKNOWN message. The DHCPKNOWN response to a DHCPLEASEQUERY message would allow the relay agent to determine the IP endpoint location, and the remaining duration of the IP address lease.

[**0287**] Query by IP Address:

[**0288**] The system and methods herein descried may make use of this feature, which will be summarised briefly. (Words in capital letters are keywords which can be interpreted as described in the IETFs RFC 2119.)

[**0289**] For this query, the client passes an IP address to the DIICP server which returns any information that it has on the most recent client to use that IP address. Any server which supports the DHCPLEASEQUERY message MUST support query by IP address. If an IP address appears in the client IP address ("ciaddr") field, then the query MUST be by IP address regardless of the contents of the MAC address or client-id option (if any).

[**0290**] Definition of MAC Address

[**0291**] In the context of a DHCP packet, a MAC (Media Access Control) address consists of the fields: hardware type "htype", hardware length "hlen", and client hardware address "chaddr".

[**0292**] Sending the DHCPLEASEQUERY Message

[**0293**] Although it is envisaged in the draft protocol that a DHCPLEASEQUERY message would typically be sent by an access concentrator, in fact, in this embodiment, the message will be sent (or caused to be sent) by a provisioning application. The DHCPLEASEQUERY message uses the DHCP message format as described in [RFC 2131], and uses message number TBD in the DHCP Message Type option (option **53**). The DHCPLEASEQUERY message has the following pertinent message contents:

[**0294**] The gateway address (giaddr) MUST be set to the IP address of the requestor (i.e. the server running the provisioning application). The giaddr is independent of the ciaddr to be searched; it is simply the return address for the DHCPKNOWN or DHCPUNKNOWN message from the DHCP server.

[**0295**] The Parameter Request List SHOULD be set to the options of interest to the requestor.

[**0296**] The Reservation bit in the "flags" field of the DHCP packet (see [RFC 2131]) is used to specify if the response should include information encoded into reservations.

[**0297**] Specifically for Query by IP Address:

[**0298**] The values of htype, hlen, and chaddr MUST be set to 0.

[**0299**] The ciaddr MUST be set to the IP address of the lease to be queried.

[**0300**] The client-id option (option **61**) MUST NOT appear in the packet.

[**0301**] Processing the Response

[**0302**] If the DHCP server has information about the most recent device associated with the IP address specified in the ciaddr, then the DHCP server MUST encode the physical address of that device in the htype, hlen, and chaddr fields. Otherwise, the values of htype, hlen, and chaddr MUST be set to 0 in the DHCPKNOWN packet.

[**0303**] Thus, to extract the physical address, the provisioning application need simply read the htype, hlen and chaddr fields in a response packet. In the case of a cable modem, the MAC address is obtained and, in the case of a DSL modem, the PVC ID is obtained.

[**0304**] Referring to **FIG. 3**, the network environment in which services are administered and delivered can be complex. It may be that the service provider's platform **190** is

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 080

directly connected to the network to which the user's access device **105** is connected. In this case, the provisioning server **180** can easily send a DHCP Lease Query message to the DHCP server **130** for the relevant network. However, in an open access environment, it may be that the network is actually one of many which could be used by a service provider. In this environment, each broadband network may have an associated management platform comprising an access device manager, e.g. a cable modem manager **330** such as a cable modem termination system, and an address server of some sort which might be managed centrally for instance by a Cable Network Registrar (CNR) **340** as one of several network address servers across several networks. The CNR **340** may then have access over a core network to various address-related platforms, such as DHCP servers **130** and Domain Name Servers (DNS). The core network will also be connected to the Internet **170**.

[**0305**] An environment of this type is described in "Integration Solutions Guide for Managed Broadband Access Using MPLS VPNs for MultiService Operators", published by Cisco on the Internet at: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/mplscabl.htm.

[**0306**] Since multiple ISPs will have access to the same networks, a way in which such an environment might be managed is that each ISP has its own set of IP addresses and effectively its own Virtual Private Network (VPN) which may in practice be supported by several separate broadband networks. Whenever a user's access device such as a cable modem **105** is assigned an IP address belonging to a particular ISP, that cable modem along with all of the devices **100** connected to its Ethernet port are placed into that ISP's VPN. Thus, the user's PC can acquire an IP address in the ISP's address range directly from the ISP's DHCP server via the CNR **340**.

[**0307**] It is known in an environment of this general type, providing managed broadband access via logical separation, to use tunnelling for communication between an ISP's platform and the management platform supporting the CNR **340**. The use of this tunnelling may be extended to allow a provisioning server **180** of the ISP to obtain user access device hardware addresses via the CNR **340** of that management platform. The steps of **FIG. 2** can be repeated but the DHCP Lease Query message will be sent (Step **215**) and acknowledged (Step **220**) using a tunnelling protocol over a network such as the Internet itself, or another network such a management core network using the Internet Protocol.

[**0308**] Referring again to **FIG. 3**, once a service provider can obtain an access device hardware address for a user's service provision, there are several potential benefits which the service provider can exploit in relation to individual access devices. The service provider can provide various backend services via an application server **185** and can interface via middleware **315** to a workflow engine **310** and a subscriber-management system **305**. The following are examples of potential benefits:

[**0309**] end-to-end self provisioning for the user, including deprovisioning

[**0310**] using a single interface and PIN for provisioning

[**0311**] open access provisioning

[**0312**] resource management

[**0313**] fraud management

[**0314**] As mentioned above, the auto-discovery by the service provider platform of the user's access-device hardware address on service provisioning removes the need for the consumer to enter the physical address of an access device manually. The use of the hardware address of the access device means that the consumer devices don't have to be provisioned individually which provides greater flexibility in handling lifetime scenarios. For example, a user can change, upgrade his/her PC without having to go through the whole provisioning process.

[**0315**] Further methods and apparatus herein described can also simplify de-provisioning. The consumer can self de-provision services by accessing the interactive Web interface of the relevant service providers, installed on an Internet host **175**, and using substantially the same process as described above but now to de-provision the service. In this case, the Query Module **200** and Provisioning Module **205** of the ISP's provisioning server **180** will again query the relevant hardware address server, such as a DHCP server **130**, but the provisioning module **205** will de-provision the service in place of provisioning it as before.

[**0316**] By providing a simple authentication routine in, or accessible by, the provisioning module **205**, service provisioning and de-provisioning can be done through a single Web interface **175**, using a PIN and thus providing again greater flexibility. The same interface and application can then be used not only to provision multiple different services, over multiple end user termination devices **100**, but also for multiple subscribers and/or users.

[**0317**] By using a tunnelling protocol, an open access business model can be supported, which enables both a retail model (i.e. "plug and play" type provisioning of off-the-shelf access devices) and/or a wholesale business model (provision of services that are external to a management network which may again be external or independent of broadband networks used for the actual service provision). Since the service provider can auto-discover the access device identity, pre-provisioning is not required and any access device can be provisioned, whatever its origin. This tunnelling feature for provisioning means that service providers external to the broadband network itself can host their own service-provisioning in-house but through the operators network.

[**0318**] Through integration with a capacity management, or service assurance product, for instance accessible via the middleware **315** of the service provider's platform, the service provider can check that the relevant network resources are capable of handling the quality of service requested by the customer. To do this, the service provider needs to keep track of all the potential services to be delivered so as to aggregate at least loosely all impacted service levels and thus determine the potential risk and probability of resource congestion at peak time.

[**0319**] For example, if network equipment X serves 10,000 users with a back-plane capacity of 2 GB, then the service provider should only sell 80% of the equipment capabilities and only through a mix of various of qualities of service (QoS). A Gold service could be based on a capacity of 2 Mbps, a Silver service would be 1 Mbps, a Bronze

service would be 512 Kbs and a standard service would be 256 Kbps. Then the service provider needs to aggregate the content of all the service agreements entered into so as not to exceed the utilisation threshold decided by the operator. This will generally need to be adjusted to reflect peak usage time and other relevant factors.

[0320] When a customer uses self-provisioning, this aggregation may remain important. Although the service provider may not control every new instance of service provision, it remains important (or indeed is more so) that the service provider maintains a database and software to monitor service provision. Means to maintain such a database and software are already known. However, another aspect which arises with self-provisioning is ongoing service monitoring.

[0321] New customers will generally have an expectation of an acceptable quality of service and will often have a form of service level agreement with a service provider. Existing customers will not expect the quality of service to become degraded because other customers have been newly provisioned.

[0322] By sharing data, for instance by sharing a data model and access to common data storage, a provisioning application working in conjunction with a service assurance application may offer a particularly efficient use of data for diagnostics. The invention independently provides a method comprising sharing a data model between a provisioning application and a service assurance application, preferably dynamically, and further independently provides use of a common data model in a plurality of communications applications including at least two of: provisioning, service assurance, planning, inventory management, and network management. Service assurance products may for instance receive alarm signals or data arising in use of a network to provide an identified service. Since a provisioning application may gather subscriber-related address data in relation to services provisioned, by sharing access to that data the service assurance product can be enabled to relate alarm data not just to services but also to relevant service subscribers.

[0323] Referring further to **FIG. 3**, the service provider's platform **190** may be provided with a database accessible to several applications including backend services **185** and subscriber management **305** via the middleware **315**. Except perhaps for services paid in advance, when a subscriber triggers provisioning of a new service for instance by means of a self-provisioning module **180**, it is usually necessary that the subscriber provides identification, at least in the form of a billable account number, as well as identifying the service to be provided. If the provisioning module **180** writes this information to the database, it is relatively simple to give access to the same information for a service assurance application, particularly if they share the same data model. This represents a very convenient way to support analysis of service problems during use of a network in relation to individual customer accounts.

[0324] Tools for monitoring performance of networks and services in use are known, such as the Micromuse Netcool products.

[0325] An advantage of the service provider having knowledge of the access device address is that the service provider can determine the serviceability of the customer before trying to provide a service. This step can be used to ensure that the operator infrastructure can physically deliver services to the client since the service provider will be able to detect at least some shortcomings in the customers arrangement. For instance, if a customer wishes to subscribe to a VoD over DSL service, the service provider is enabled to check whether the customer's access device is actually physically close enough to a DSL Access Multiplexer (DSLAM) and that there is therefore enough bandwidth. The MAC address contains information on hardware type and this information is also therefore available to the service provider for use in checking serviceability.

[0326] The use of a limited IP scope at initial activation time limits greatly fraud by preventing an un-authorised access modem to access services. However, through management of the IP address scheme and physical address of the access devices, whether based on the MAC address of a cable modem or management of the PVC in the case of a DSL modem, it is possible for the service provider to detect the origination of fraudulent activity and to take action to avert the fraud for instance by suspending or de-activating service provision to the offender, or by downgrading level of service.

[0327] The methods and apparatus herein described can be used in relation to many different services, access networks and CPE types. For instance, the following can be supported:

[0328] IP Data Access

[0329] Service on Demand (video or games, i.e., any pay-per-use services . . .)

[0330] TV broadcast

[0331] Voice over IP

[0332] Cable networks (DOCSIS and DAVIC)

[0333] XDSL

[0334] Wireless Local Loop (WLL)

[0335] Fibre-to-the-Home (FITH)

[0336] Personal Computers

[0337] Set Top Boxes (STBs)

[0338] Personal Digital Assistants (PDAs)

[0339] mobile phones.

[0340] **FIG. 4** illustrates a further example of message flow in provisioning apparatus carrying out provisioning according to an embodiment of the systems and methods herein described.

[0341] Each feature disclosed may be provided independently, unless otherwise stated. In summary, the provisioning of communications services may be facilitated by a self-provisioning application which, in preferred applications, can operate with off the shelf access devices, such as cable modems, is disclosed; this makes use of an existing IP address to discover a unique "physical" address (e.g. MAC address for a cable modem or PVC ID for a DSL modem) thereby avoiding the need for a user or specialised user software to communicate the physical address of the access device prior to provisioning. A low level command, particularly DHCP lease query, is preferably used to obtain a

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 082

hardware address for use in provisioning of a new broadband service based on a user's existing IP address. Provisioning may be based on the access device physical address. The provisioning application may communicate with a capacity management application. It may also, or instead, share a data model and data storage with a service assurance application to enable data captured during service provision to be used in alarm analysis after a service has been provisioned and is in use.

[0342] Application to VPN MPLS

[0343] The systems and methods of the provisioning system and methods described herein will now be illustrated further by the following description of an Internet Infrastructure Provider (IIP) specific Virtual Private Network (VPN) Multiprotocol Label Switching (MPLS) provisioning system. This system is described by way of example only and the description is not intended to be limiting in any way. The terms "subscriber" and "customer" may be used in the following description to denote potential users of the system.

[0344] The test set up described below uses a plurality of simulated customers at geographically distinct sites and demonstrates many of the advantageous features which may be achievable in a typical implementation.

[0345] In the initial scenario for this example system, illustrated in **FIG. 5**, the core MPLS network has been set-up with 3 Points of Presence (POPs) **502**, **504**, **506**:Antibes POP **504** has one Provider Edge (PE) router **508** with an ISEA VPN **510**.

[0346] PE**3508** has a VRF (a VPN Routing and Forwarding device) for Customer A's Antibes/St Claude site **512** connected via serial interface to a C1700 Customer Edge (CE) router **514**.

[0347] Sophia Antipolis POP **502** has 2 PE routers **516**, **518**. ISEA **520** is connected to both PE routers.

[0348] PE**2516** has a VRF for Customer A's Sophia Antipolis/Les Genets site **522** connected via Fast Ethernet to a C1700 CE router **524**.

[0349] PE**4518** is connected to an ATM switch and to a DSLAM (Digital Subscriber Line Access Multiplexer). There are no VPN customers yet.

[0350] Nice POP **506** has one PE router **526** with no ISEA MPLS.

[0351] PE**1526** has a VRF for Central ISP services site **528** connected via Fast Ethernet to a C1700 CE router **530**. A web/email server **532** is located behind the CE router.

[0352] Customer A has already been provisioned using IIP VPN. Customer A has 2 sites

[0353] A primary CE A1 site located in Antibes/St Claude **512** connected to Antibes POP **504**.

[0354] A secondary CE A2 site located in Sophia Antipolis/Les Genets **522** connected to Sophia Antipolis POP **502**.

[0355] An example of the process of connecting a new CE router to the network in a new VPN with access to the centralised services web server and management VPN will now be described with reference to **FIG. 6**, which summarises an example network topology. In this example, all actions are carried out through the MPLS console/Graphical User Interface (GUI).

[0356] 1. A new customer called "Customer B" is created using the console.

[0357] 2. A new VPN is created for "Customer B" using the console

[0358] 3. A new primary CE site called "Antibes Garoupe"**602** is added for Customer B with ISEA monitoring (Ethernet 802.1Q sub-interface).

[0359] 4. An interface is provisioned on the PE router **508** for the PE-CE link

[0360] 5. A minimal "IP only" configuration file is created for the CE router **604**.

[0361] 6. The configuration file is manually loaded onto the CE router **604** and it is plugged in.

[0362] 7. When IP connectivity is established to the CE **604** the VPN/routing/CoS config file is downloaded to the router. This demonstrates the advantageous feature of the provisioning system in preparing configuration files.

[0363] 8. Customer B may then connect a PC behind CE router **604** and access centralised services.

[0364] By way of example, **FIG. 7** summarises the VPN topology and illustrates the process of connecting a new CE router **702** to the network in a new VPN with access to the centralised services web server and management VPN. In this example, all actions can be carried out through the MPLS console/GUI.

[0365] 1. A new secondary site called "Sophia Antipolis ADSL"**704** is added for Customer B (where ADSL indicates an Asynchronous Digital Subscriber Line).

[0366] 2. An interface (ATM sub interface) in a VRF is provisioned on the PE router **518** for the PE-CE link with ISEA monitoring (Ethernet 802.1 Q sub-interface).

[0367] 3. The full CE router configuration is provided to the customer via a File Transfer Protocol (FIP) download.

[0368] 4. The configuration file is manually loaded to the CE ADSL router **702** and it is rebooted.

[0369] 5. Customer connects a PC behind ADSL CE router and accesses centralised services.

[0370] The phase PE-CE link parameters for the CE router **702** added in above may be modified according to the following example procedure:

[0371] 1. In the MPLS console/GUI, browse to the PE-CE link edition screen.

[0372] 2. Edit the Class of Service (CoS) of the Ethernet PEACE link by choosing a Diffserv class and sub class and applying this to the Ethernet interface

[0373] 3. Deploy the configuration to the PE**4518** and CE B**2702** routers

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 083

[0374] **FIG. 8** illustrates an example of a VPN physical topology in which a new CE router **802** may be connected to the network in a new VPN with access to the centralised services web server. In this example, all actions may be carried out through a batch file using the VEA.

[0375] 1. A new secondary site called "Valbonne ADSL"**804** is added for Customer B.

[0376] 2. An interface (ATM sub interface) in a VRF is provisioned on the PE router **518** for the PE-CE link with ISEA monitoring (Ethernet 802.1 Q sub-interface).

[0377] 3. The full CE router configuration is provided to the customer via FTP download.

[0378] 4. The configuration file is manually loaded to the CE ADSL router **802** and it is rebooted.

[0379] 5. Customer connects a PC behind ADSL CE router **802** and accesses centralised services.

[0380] VPN topology may also be modified. An example of a process in which VPN B's topology is modified will be described below. **FIG. 9** summarises the VPN logical topology of the present example before the modification.

[0381] By way of example, Customer B has expressed a requirement that site B**3804** (currently secondary) is now becoming one of his major offices/data centres and it must be able to communicate with all primary and secondary sites in the network. In order to modify the topology accordingly, the following process may be implemented:

[0382] 1. In VPN console/GUI go to the properties of site B**3804**.

[0383] 2. Change the status of site B**3** from secondary to primary.

[0384] 3. The topology change is applied to the network elements.

[0385] 4. With a PC connected behind B**3804** show that all sites (B**1602**, B**2704**) can be pinged.

[0386] **FIG. 10** summarises the VPN logical topology after the modification.

[0387] Communications Network Management System

[0388] The provisioning system and methods described above may also be implemented in conjunction with a communications network management system, which may find particular but not exclusive application in management of systems supporting broadband services.

[0389] With the advent of higher transmission capacity networks, and particularly for instance broadband networks, network operators have to manage more and more complex infrastructure and to keep an always-increasing number of services up and running. As a result, subscriber satisfaction can drop if they perceive deficient service management and there is more subscriber "churn". Meanwhile, the operators already have to invest more in their operation support teams, taking on more people and/or improving the skills their people have. Hence it is a challenge to be able to provide cost effective management of complex services.

[0390] The sort of complexity involved is demonstrated by the services it may be important to support. For instance, these may include digital multiplexes of entertainment video, high speed connections with the Internet and local servers via cable modems, commercial enterprise Local Area Networks and Wide Area Networks, personal communication services over cable and telemetry, as well as traditional analogue TV.

[0391] The supporting "cable" network technology may also be complex, based partially on fibre as well as on coaxial cable. A typical architecture for a network operator might be a hybrid fibre coaxial (HFC) architecture in which there is a head end, where all the signal sources are collected and processed, connected for distribution over a fibre backbone to primary hubs, comprising switches or routers, which in turn distribute to secondary hubs which in turn distribute to fibre nodes. The fibre nodes convert the communications to radio frequency and use coaxial cable to reach the end-users who may be corporate or private. The head ends and hubs will also distribute to their local vicinities.

[0392] In the broadband domain, Such as services offered over cable networks, there are characteristics which differentiate today's services from those traditionally offered over telephone networks. For instance high speed data is often transmitted over always-on connections to customer personal computers (PCs) using cable modems (CMs). This means that cable operators need to provide a network which is working correctly throughout every day of every week to meet performance requirements compatible with service level agreements with customers. The always-on connection is vulnerable to non-subscribers trying to get free connections and the computer access is vulnerable to hackers.

[0393] Automated fault management tools are known but tend to be focused on equipment, tools and mechanical problems rather than trying to solve problems at other levels of customer service. Meanwhile, as customer expectation and competition in the market increase, operators are under pressure to offer not just consistent and high quality services to many customers using different types of customer equipment but also to take into account fraud and security management.

[0394] According to an aspect of the present invention, there is provided a communications network management system, which system comprises:

[0395] a) an input for fault reports in respect of a network and/or one or more services supported by a network,

[0396] b) a data store for storing data in respect of said network, and/or services,

[0397] c) a fault processor for processing fault reports received via the input, using data stored in the data store, to generate corrective solutions, and

[0398] d) a simulation engine for simulating one or more service instances wherein the simulation engine has an output to the network to trigger provision of said one or more service instances, such that a fault report in respect of said provision will be received at the input and processed by the fault processor.

[0399] The simulation engine can be used in embodiments of the present invention in providing service assurance to the end user by intelligent monitoring of complex platforms. In particular, the simulation engine could be used either pro-

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 084

actively, to run test service instances, or to validate the result of applying a corrective solution which has been generated by the fault processor. The simulation engine may be implemented by one or more agents running on a network component, for example a user access device such as a cable modem, or a switch or router or access concentrator.

[0400] The manner in which corrective solutions are generated is of course important, particularly in respect of the level at which they are targeted. It could be easy to meet the requirements of a received fault report but to fail to diagnose a more widespread problem that might continue to mean service failures.

[0401] According to a further aspect of the present invention, there is provided a communications network management system, which system comprises:

[0402] b) an input for receiving fault reports in respect of one or more services supported by a network, and for receiving component alarms from components of said network;

[0403] b) a data store for storing data in respect of said network and/or services; and

[0404] c) a fault processor for processing fault reports received via the input, using data stored in the data store, to generate corrective solutions,

[0405] wherein the fault processor comprises a correlation engine for correlating received fault reports in respect of one or more services with received component alarms.

[0406] Embodiments of the present invention including the correlation engine can provide improved fault processing in that they may be able to identify a root cause of faults which can affect more than one service, or service to more than one customer.

[0407] Preferably, the data store is structured to support fault processing of this type. For instance it may be structured to hold data relating a problem description to one or more fault reports and to corresponding one or more component alarms. A problem description may include data describing component behaviour and, preferably, data received in respect of historic component behaviour. In the relatively simple network and service provision of the past, historic behaviour is likely to reproduce predicted behaviour for a component However, in the much more complex networks and services being provided today, embodiments of the present invention recognise that component behaviour may no longer be fully predictable. Thus embodiments of the present invention which support fault processing in relation to historic component behaviour may be very valuable in providing a learning mechanism in fault processing.

[0408] Alternatively, the fault reports generated by problems with component behaviour might be unpredictable. Hence a problem description may instead or as well contain data defining fault reports in respect of past system behaviour, related to successful corrective solutions.

[0409] Known fault management systems for communication systems have relied principally on fault reports by end-users to locate faults and trigger a fault management process. Fault management has been done largely at the network level, with the aim of keeping a network fully functional. However, this means there will often be delays between identification of a fault and its correction. As mentioned above, embodiments of the present invention may use proactive simulation of service instances to trigger faults latent in the network but not yet exposed by customer requirements. A further improvement which can be provided by embodiments of the present invention is to relate fault processing to both service and customer data.

[0410] According to a further aspect of the present invention, there is provided a communications network management system, which system comprises:

[0411] c) an input for fault reports in respect of a network and/or one or more services supported by a network,

[0412] b) a data store structured to store data in respect of said network and services, and

[0413] c) a fault processor for processing fault reports received via the input to generate corrective solutions;

[0414] wherein the data store is further structured to store customer data in relation to services and the fault processor comprises a correlation engine for correlating received fault reports in respect of one or more services with customer data.

[0415] Preferably, the fault processor further comprises sorting apparatus for sorting fault reports in an order determined by correlated customer data. This could be very important in prioritising fault reports and thus the manner in which a network is repaired in order to restore services of highest priority for instance because they have an impact on a large number of customers or customers with stringent service levels agreed.

[0416] In practice, the correlation engine may combine the attributes of the correlation engines of the previous two aspects of the present invention and thus provide a two stage correlation mechanism, including both correlation of fault reports to component alarms and correlation of component alarns to customer data.

[0417] Advantageously, the customer data includes a measure or priority of service provision in relation to an identified customer and an identified service. This enables a further level of flexibility for the manner in which the network is repaired which might be inherited from priority values in contractual data for the respective customer.

[0418] In an alternative to the previous aspect of the present invention, the data store may be further structured to store not necessarily customer data but a priority parameter in respect of at least one identified service and the fault processor may comprise a correlation engine for correlating received fault reports in respect of one or more services with the respective priority parameter(s). In this alternative, there is no need to rely on customer data to identify important services and thus to be able to prioritise fault reports or component alarms for repair.

[0419] It is intended in embodiments of the present invention that a network operator, such as a cable operator, should be able to deal efficiently, and preferably proactively, with problems relating to access loss, performance, fraud and security. Further, it is intended that the operator should be able to analyse the impact of a problem in more than one context, including preferably the impact on a service in

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 085

relation to the location in a network, the subscribers (customers) affected and the nature of the impact such as lost access or limited performance. Then the operator should preferably be able to identify the equipment generating a problem, current or pending, fix the problem at the equipment level and log it for future analysis. This last may be particularly useful if the operator can use past problems in diagnosing future ones.

[0420] Embodiments of the present invention may take advantage of a particularly advantageous arrangement for launching test signals into the network. According to a further aspect of the present invention, there is provided a method of testing a broadband network, the network comprising a head end for receiving one or more communications services from service providers and transmitting the one or more services towards end user equipment, and comprising at least one node for receiving said one or more services from the head end and delivering the service(s) towards end user equipment, which method comprises launching a test signal to the network at said at least one node and monitoring a response by the network thereto.

[0421] A way of doing this is to install a personal computer, or like computing platform, in the node. The personal computer could be pre-programmed, or controlled from elsewhere, to launch the test signals. For instance, it could be controlled via the head end relevant to the node. In order to test the response of the network to something as close as possible to user signals, if the node is a node in which optical to electrical signal conversion takes place, at a cable modem termination system, the personal computer can be arranged to launch the test signals via the cable modem termination.

[0422] If there is a significant problem in the signal path used to launch one or more test signals, the same problem could affect incoming control signals to the personal computer. It is therefore particularly advantageous if the signal path used to carry control signals to the personal computer is different from the signal path used to launch one or more test signals from the personal computer. A way of providing these different paths is to launch the test signals via the cable modem termination system, which also means that the test signals closely emulate user signals such as service requests, but to carry the control signals to the personal computer without going through the cable modem termination system. Alternatively or as well, out of band signalling can be used for the control signals.

[0423] A network management system according to an embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawings (FIGS. **26** to **43**):

[0424] Glossary

[0425] (The following will not necessarily be the only expansions or explanations relevant and are here to give at least one option rather than to be taken as limiting the meaning of an acronym, word or phrase in any way.)

[0426] ACL: Access Control List

[0427] CM: cable modem

[0428] CMTS: Cable Modem Termination System

[0429] CRM: Customer Relationship Management

[0430] DHCP: Dynamic Host Configuration Protocol

[0431] DLC: Data Link Control. A service provided by the Data Link Layer of a function defined in the Open Systems Interconnection (OSI) Model for network communications. The Data Link Layer has two types of sublayer, a MAC sublayer for each physical device type and a Logical Link Control sublayer.

[0432] DSL: digital subscriber loop

[0433] DTV: Digital TV

[0434] EMS: element management system

[0435] FTTH: Fibre to the Home

[0436] HFC: Hybrid Fibre Coaxial network for carrying broadband (video, data and voice). The CATV company installs fibre from the Cable Head End (distribution centre) to serving nodes near the uses, then coaxial cable to the customer premises.

[0437] HSD: high speed data

[0438] Hub (See Regional networks and Hubs below) data can come in/go out in many directions. Usually includes a router, bridge or switch. May include modem cards for dial-in users, a gateway card to a LAN, and a line connection.

[0439] HTTP: HyperText Transfer Protocol

[0440] IDS: Intrusion Detection System

[0441] IDSL: Integrated Digital Subscriber Line. Can be flat rate without usage charges. It bypasses the voice network by plugging into a special router at the phone company end.

[0442] IEMS: Intelligent Element Management System

[0443] MAP: Internet Message Access Protocol. For accessing e/mail from a local server. The user can decide when and what should be downloaded. Cf POP3 (Post Office Protocol) in which everything is downloaded at once.

[0444] IP: Internet Protocol

[0445] ISM: Internet Service Monitor by Netcool

[0446] KMS: knowledge management system

[0447] LDAP: Lightweight Directory Access Protocol. Enables anyone to locate organisations, files, devices etc in a network.

[0448] MAC address: Media Access Control address. The unique hardware number of a device. In an Ethernet, it is the Ethernet address. In the Internet, a correspondence table relates the IP (Internet Protocol) address to a physical device address on a LAN.

[0449] MOM: Manager of Managers

[0450] MRTG: Multi Router Traffic Grapher. A tool which monitors traffic load on network links. It generates live representation by means of HTML pages containing GIF images. Available under GNU public licence.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 086

[0451] NHE: Network Head End

[0452] PCS: Personal Communications Services

[0453] Regional networks and Hubs: these can carry digital multiplexes of entertainment video, high speed connections with the Internet and local servers via cable modems, commercial enterprise LANs/WANs, PCS over cable and telemetry, as well as traditional analogue TV. Typical architecture is the head end, where all the signal sources are collected and processed, distributing over a backbone to primary hubs which in turn distribute to secondary hubs which in turn distribute to fibre nodes. Everything between the head end and the fibre node is carried on fibre. The fibre nodes convert to RF and send signals onto coaxial cable to the users. The head ends and hubs will also distribute to their local vicinities.

[0454] Scope: in DHCP, a pool of IP addresses which the DHCP server can assign or lease to clients.

[0455] Segmentation: a network design approach using routers, switches and bridges to keep traffic levels down in a network. A router, switch or bridge provides an access point controlling traffic into and out of a segment of network. Traffic is only sent into the segment containing the destination of the traffic and won't be sent out of a segment if it is already in the segment containing its destination. Broadcast traffic may be blocked from a segment as a default behaviour of a router unless the router has for instance explicit instruction to pass broadcast traffic into the segment. Traffic in practice tends to be locally addressed. With segmentation, less traffic goes out onto the backbone and thus collisions are reduced. Segmentation reduces the number of users sharing the bandwidth since, within a segment, all users share the bandwidth and the smaller the segment the fewer the users sharing. It therefore increases available bandwidth to each user. It can also extend Ethernet cabling distances because the beginning point for the maximum cabling distance is reestablished.

[0456] SMTP: Simple Mail Transfer Protocol

[0457] STB: Set Top Box

[0458] Telnet: user command and underlying TCP/IP protocol for accessing remote computers with permission. HTTP and FTP can be used to request files but not to logon. With Telnet, a user can log on like a regular user with privileges of the relevant application and data on that computer.

[0459] UBR: unspecified bit rate? For efficient, shared use of capacity.

[0460] VOD: Video on Demand

[0461] WLL: Wireless Local Loop

[0462] Referring to **FIG. 26**, a cable network operator may use several different access networks **2702** to support multiple services **2704** for delivery to multiple types of Customer Premises Equipment (CPE) **2706**. To do that, it is necessary to manage behaviour of the components of the network, particularly to monitor for alarms, and it is known to run an Element Management System (EMS) **2708** to do that, such as Hewlett Packard's OpenView or BMC Patrol. At this level, it is also known to run an intrusion detection system and a network performance monitoring system such as Multi Router Traffic Grapher, available under GNU public licence.

[0463] All the data output from the EMS is collected for processing by a Manager of Managers (MOM) **2710** such as Micromuse Netcool and aspects of the processed data may be made available to various users of the system who may be in the Network Operations Centre **2712** or the Customer Operations Centre **2714**. There will usually be two types of user in the Customer Operations Centre **2714**, a service operator and a customer service manager. Hence overall, aspects of the processed data may be required for presentation at three different Graphical User Interfaces (GUIs), a network operator GUI **2716**, a service operator GUT **2718** and a customer services GUT **2720**.

[0464] Importantly in embodiments of die present invention there is also an Intelligent Element Management System (IEMS) **2722** and it is this which provides a fully integrated management system which has powerful analysis capabilities across all levels of service provision to the end user, for use at three different levels, the network, the services and the customer interface. That is, the IEMS **2722** provides in a unique package the complete set of functionalities which are needed to manage a full network.

[0465] Referring to **FIGS. 26 and 27**, the IEMS **2722** provides the following aspects:

[0466] fault processing based on the services **2704** supported so that subscribed services can be kept up and running

[0467] subscriber oriented information processing and provision, which is obviously important since subscriber satisfaction is always a major priority of the service provider

[0468] all-in-one product supporting the complete set of functionalities which are needed to manage a full network

[0469] an integrated and powerful knowledge management system **2706**, which can be provided with a complete set of relevant content

[0470] a multi-use/multi-purpose GUI, remotely accessible over low bandwidth links and offering relevant views for the Network Operator Console **2716**, the Service Operator Console **2718** and the Customer Operator Console **2720**

[0471] powerful correlation which can be used to analyse service failure to provide an impacted subscribers list and details, information on the network components involved in the failure and, due to a second level of correlation, to extract the root component alarm(s)

[0472] a complete set of tools **2802**, adapted to user type and including service, customer and network related tools

[0473] adaptation to multiple services **2704** and multiple access networks **2702**

[0474] The example of an embodiment of the present invention described below is designed particularly to support high speed data services on a HFC network. For the

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 087

cable operator, this means providing always-on connection with performance parameters to meet the contractual aspects signed with the subscriber. Because of the always-on connection, it is also particularly important to prevent fraud, such as a non-subscriber trying to get a free connection, and security violations such as hacking. It is intended in embodiments of the present invention to support the cable operator to do at least one and preferably all of the following in the event of a problem:

[0475] Identify the global impact on Service in terms of

[0476] Where (which segment, which hub, which regional head end, . . .)

[0477] Who are the subscribers impacted (list)

[0478] What is the detailed impact (no access, limited performance, . . .)

[0479] Identify the equipment(s) (hardware, software, link) which has generated the service problem (current or predicted)

[0480] Find and validate a solution to the problem

[0481] Log the problem for further analysis

[0482] Referring to **FIG. 28**, the IEMS comprises inputs for network alarm data via a database **2902** and more service-specific monitoring data via service simulation data processing software **2904**, a powerful knowledge management system **2906** for use in generating corrective solutions to problems and a correlation engine **2908** for analysing alarms to the root component level. Supporting these is a database **2910** holding for example the rules for the correlation engine **2908** and data supporting the knowledge management system **2906**. The service simulation data processing software **2904**, receiving service data via probes **2912** in response to service activity triggered by simulators embedded in the equipment being monitored is particularly powerful in that it can be used to test services proactively, and to validate corrective solutions, by simulating instances of services, as a user might trigger in normal use, and detecting service level responses via the probes **2912**. Use of the simulators can also produce network alarm data in the same manner as normal use of the network and services.

[0483] The following description firstly describes a network environment for providing High Speed Data services to an end user, to put embodiments of the present invention into a working context, and then takes the above areas and describes them in more detail.

[0484] Network Environment as Working Context

[0485] Referring to **FIG. 42**, a typical regional network for providing broadband services will comprise a regional head end **4302** which receives services from Internet Service Provider equipment **4304** over a core network **4306**. The regional head end **4302** transmits services in connection with identified locations in its regional network over a collection network **4308** to a plurality of hubs **4310**. These hubs **4310** contain routing devices **4312** which route the services towards the end user equipment **4314**.

[0486] A management network **4316** is provided for monitoring and controlling the network and service platform used to support service provision. The management network **4316** is used in particular to pick up alarms and event data in respect of the network and services and to transport it to an operations centre, in the case shown in **FIG. 42** to the High Speed Data service and network operations centre **4318**. In the operations centre **4318**, it is input to an intelligent management system **4320** where it is processed in the light of network and service data, and in particular with reference to the knowledge management system **2906** and the correlation engine **2908**. Once the alarm and event data has been processed, the results can be stored in a database of the management system **2902** and viewed via Graphical User Interfaces (GUIs) by users of different categories. In particular these GUIs will be dedicated to a network operator **2716**, a service operator **2718** and a customer relations operator **2720**.

[0487] The intelligent management system **4320** primarily comprises the software processes needed to process the incoming alarm and service data. It needs to call on data such as correlation rules for the correlation engine **2908**, and data to support the knowledge management system **2706**. This data can be stored on any accessible database, preferably local, and can conveniently be stored on the network resource database **4322** and/or the provisioning database **4324** of the operation centre **4318**.

[0488] Network Alarm Data

[0489] Referring to **FIG. 28**, looking first at the collection and processing of network alarm data, the Netcool ObjectServer **2902** integrates and consolidates alarms coming from network equipment **2918** via a set of probes **2922**. For each piece of network equipment **2918**, including servers, the tools from the EMS layer **2708** will detect a range of alarms. For the purpose of the IEMS, particular data content of these alarms is appropriate. The probes **2922** are used here effectively as filters which select the types of alarms which are appropriate to the IEMS and input them to the Netcool ObjectServer **2902**.

[0490] At least the following pieces of network equipment **2918** can be monitored:

[0491] CMTS (MC16 card)

[0492] Unspecified Bit Rate (UBR) Router

[0493] Catalyst™ (Cisco router)

[0494] NT Operating System

[0495] Solaris Operating System

[0496] DHCP servers (CNR)

[0497] LDAP servers

[0498] Oracle Database Server

[0499] Back-end Provisioning Server

[0500] The network monitors **2920** are of known type and may comprise for instance the following:

[0501] Hewlett-Packard OpenView: a set of products such as a Network Node Manager which provide event correlation, thresholding and alarming;

[0502] BMC Patrol: a set of products by BMC Software which include for instance a central point of control for applications, computers, LANs, WANs and communications devices;

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 088

[0503] Chetah: a network management tool for HFC networks

[0504] Intrusion Detection Systems: these are systems which run continuously on a network and produce alerts for system and network administrators of potential illegal access to the network or host;

[0505] SATAN and SAINT tools: a Security Administrator's Tool for Analysing Networks and the Security Administrator's Integrated Network Tool which improve the security of a network by trying to break into it, available under a GNU public licence;

[0506] Performance monitoring tools; these measure performance in terms of response times or loading. An example of a performance monitoring tool is the Multi-Router Traffic Grapher, available under a GNU public licence, which monitors traffic load on network links and generates HTML pages containing GIF images to give live representation.

[0507] Alarms detected by the tools **2920** are selected by the probes **2922** for input to the Netcool ObjectServer **2902**. The particular alarm types may be in relation to the following:

[0508] Availability (hardware or software)

[0509] Servers (including operating system processes, application processes and the like)

[0510] Network devices

[0511] Security

[0512] Some critical servers are security hardened so that some services such as Telnet for instance are not available, and alarms arise if security is not maintained

[0513] Access Control Layer (ACL) violation

[0514] Firewall down

[0515] Performance

[0516] Central processing Units (CPU)

[0517] Random Access Memory (RAM)

[0518] Bandwidth and traffic

[0519] Cable Modem Terination System

[0520] Fraud

[0521] The MAC addresses of Customer Premises Equipment (CPE) for invalid (unsubscribed) users are identified. A "diff-file" between LDAP repository and SMS database is built, and an appropriate alarm is generated for invalid Mac-addresses

[0522] Change configuration

[0523] In network equipment

[0524] In servers

[0525] The network alarm data is stored for the IEMS in a database **2902** which does some processing of received alarm data. The database **2902** used in this embodiment is the Micromuse Netcool ObjectServer which maintains an overview of events and processes them to the extent that they can be grouped according to the services they potentially impact.

[0526] Service Monitoring Data

[0527] Referring to **FIGS. 28, 29** and **42**, as well as the collection of network alarm data, service-specific data is collected for each service type. Importantly, service data is picked up by the service simulator probes **2912** in response to activity triggered by service simulators **3002, 4326, 4328** which are installed at relevant sites in a network environment. The data collected is then processed and stored by service simulation data processing software **2904** for the IEMS system.

[0528] To put the use of service simulators **3002, 4326, 4328** and monitors into context, the following describes the collection of data for a High Speed Data (HSD) service run over a regional network as shown in **FIG. 42**.

[0529] There are three types of simulator **3002, 4326, 4328** in the embodiment presently described, installed in different locations of the HSD network.

[0530] A first type of simulator **4326** is provided by the known Internet Service Monitor (ISM) produced by Micromuse Netcool, in the regional head end **4302** to monitor links for the ten most popular Web sites (to be defined in setup), the IMAP and LDAP based services, and POP3/SMTP e-mail services, and in the hub **4310** to monitor DHCP based services.

[0531] A second type of simulator **3002**, the HSD service simulator, is installed using a personal computer (PC) in the hub **4310** to test the "last mile" on all segments of the hub **4310**. This PC is connected on the cable side of a cable modem termination system **3004** in the manner of end user equipment. The PC is operated periodically to check a set of functionalities. The operations carried out by means of this PC include at least:

[0532] Reboot the PC and test provisioning access

[0533] Send an HTTP request to the provisioning server

[0534] Send HTTP requests to some popular Web servers to test access and response times

[0535] Attempt to use Telnet access to hardened servers

[0536] A third type of simulator **4328** is used specifically to test Telnet responses. It will launch Telnet commands to different pieces of service equipment in order to test critical links. For instance, it will "ping" a DHCP server or a Web site from an unspecified bit rate connection. That is, it will issue an echo request. All Internet hosts are required to send echo replies in response to an echo request and this is a simple way of finding out if a host can be reached.

[0537] A powerful aspect of embodiments of the present invention is the link that can be made between alarms detected by the various probes **2922, 2912** and other information such as services and customers affected and root component alarms. The data content of the alarms collected by the probes **2922, 2912** is of course important in this. This data content can be used in conjunction with the knowledge management system **2906** to produce the necessary links.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 089

[0538] EMS Database

[0539] Component Alarm Information Database

[0540] Each alarm generated has the following attributes:

[0541] IP Address

[0542] Equipment/module/port

[0543] Date/time of occurrence

[0544] Location, in particular where physically in the network (NHE, RHE, HUB)

[0545] Detailed description (in an "operator" comprehensive text)

[0546] Severity

[0547] Type of alarm (fault, performance, security, fraud, configuration change, . . .)

[0548] Actions to Lake/recommendations to fix the problem, for instance this might be in the form of a direct link to the right page and the right alarm in the trouble-shooting guide or the right procedure

[0549] Additional links to useful documentation

[0550] Procedures, docs, troubleshooting guide, install ation guide, . . .

[0551] Engineering documentation (technical architecture, detailed design)

[0552] Operational procedures

[0553] Configuration files

[0554] Vendor's documents

[0555] Link to vendor's Web site

[0556] Status, such as new, deleted (TBC)

[0557] Service Alarm Information Database

[0558] Each alarm generated has the following attributes:

[0559] Type of service

[0560] Internet Access

[0561] Service Provisioning

[0562] ISP Services (such as Email . . .)

[0563] Security/fraud

[0564] Performance

[0565] Management (i.e. part of IEMS tool, like ISM, PC Simulator, . . .)

[0566] Location

[0567] Detailed description

[0568] Alarm management

[0569] New, acknowledge, update, close, delete, assign to (whom)

[0570] When the status changes, store and display dale/time, name of the operator and comment

[0571] KMS

[0572] KMS Tool

[0573] KMS tool is a Web-based application allowing operators to:

[0574] Browse content

[0575] Add/Modify/Update content (according to access profile)

[0576] Search documents with a textual search engine

[0577] The KMS tool is accessible from all screens of IEMS, and also directly from a browser by typing the right URL.

[0578] KMS Content

[0579] The content of KMS is as exhaustive as possible; this is one of the major values of the IMS product. The following lists the different sources of information available for all equipment of the HSD network:

[0580] Installation procedure

[0581] Configuration guide/files

[0582] Troubleshooting guide

[0583] Maintenance manual

[0584] User manual

[0585] Operations Manuals

[0586] Engineering documents

[0587] End To End Architecture

[0588] FAQ

[0589] Glossaries

[0590] Contact lists

[0591] Vendor's URL

[0592] GUI

[0593] Functional Role

[0594] As mentioned above, there are different categories of people who are going to use IEMS and who are therefore provided with GUIs, these being users responsible for network, service and customer operations. For each type of user, there are different levels of access defined, such as basic and advanced. For instance, a skilled operator's user should be able to create rules. Navigation within the different screens is designed to be intuitive, in order to minimize the technical skills needed by users.

[0595] Service Operations GUI **2718**

[0596] This GUI is fully Web-based and should be accessible through a low bandwidth link (typically 56 kbs). It shows:

[0597] Service status per service type/per location

[0598] Service outage list with % of users impacted/type of users impacted

[0599] Statistics of service outage per location/per type of service/per type of user

[0600] Planning (network bandwidth, IP Scope, System resources, . . .)

[0601] KMS: service related information

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 090

[0602] Information on location: postal address, manager's name/phone/email

[0603] Customer Operations GUI

[0604] Referring to **FIGS. 30 and 31**, the information that embodiments of the present invention can make available to a user in a customer operations centre **2714** clearly links problems arising at the network level with the impact on customers. Further, it links service alarms with component alarms in relation to the same part of the network. **FIG. 30** shows a screen available to a service operator in the customer operations centre **2714** and **FIG. 31** shows a screen available to a customer operator. **FIG. 31** is simpler and has been taken first in the description below.

[0605] **FIG. 31** shows a menu of potential service alarms **3202** together with indicators **3204** as to whether there is an alarm of that type ongoing. The potential service alarms **3202** include five categories of service alarm which are being monitored:

[0606] Internet access

[0607] Provisioning

[0608] ISP

[0609] Security

[0610] Management

[0611] An indicator **3204** for the provisioning service alarm is darkened, indicating a current provisioning service alarm. A user has clicked on the "Provisioning" box which has had the effect of drilling down to location information in respect of the ongoing alarm. The location information shows that there is a problem in the Manchester region of the Bromley NHE. Clicking on the Manchester region has opened up the Baguley regional head end and the Baguley hub locations as having problems in provisioning. The user has selected the Baguley regional head end in order to get further information.

[0612] Below the Service Alarms **3202** section of the screen, there is a Component Alarms section. This shows the user has drilled down to expose two component alarms **3208** relevant to the Baguley provisioning problem in the regional head end, and gives the diagnosis that the LDAP server and database are down.

[0613] The main portion **3210** of the screen is given to a "Service Alarms" screen showing management information in respect of the alarm in the Baguley regional head end for which the user has selected to drill down to the component alarms. This management information shows date, location, description, status and user impact. Importantly, the status data shows how the problem is being dealt with (it has been assigned to James Reid) and the user impact data shows what category of customer is hit by the problem. In this case 10% of gold customers, 22% of silver customers and 43% of bronze customers are affected.

[0614] Referring to **FIG. 30**, the service operator has access to much more detailed information by pulling in data using the KMS **2906**. Here, the user has selected an "Alarm Detail" screen in place of the "Service Alarms" screen. This has three sections. Firstly, in a "Service"**3102** section of the screen, there is similar information to that shown to the customer operator on the "Service Alarms" screen described above, except that there is also now an estimated correction time of 25 minutes. Secondly, in a "Description"**3104** section of the screen, there is information about the impact and importance of the problem. In the example in **FIG. 30**, customers are unable to do any provisioning and the problem is said to be critical with immediate action required. Thirdly and importantly, in an "Action"**3106** section of the screen, the identified component alarms likely to be causing the problem are offered as links to a search engine for searching for information using the knowledge management system **2906** about these component alarms.

[0615] It can be seen from the right hand section **3108** of this screen, dedicated to the KMS **2906**, that the search engine has already been launched in respect of the component alarms listed in the "Action"**3106** section of the screen to offer five sources of information relevant to correcting the problems, from the provisioning detailed design through to the Baguley Hub Rack layout. This is a powerful aspect of embodiments of the present invention in that targeted data from so many sources can be accessed.

[0616] This GUI is Web-based and therefore accessible through a low bandwidth link.

[0617] The primary types of information given which are accessible via the Customer Operations Centre **2714** are:

[0618] Service status per service type/per location

[0619] Service outage list with % of users impacted/type of users impacted

[0620] Statistics of service outage per location/per type of service/per type of user

[0621] KMS with custom operations information, such as FAQ, etc.

[0622] CPE manager (see "Tools")

[0623] Network Operations GUI **2716**

[0624] Referring to **FIGS. 32, 33** and **34**, a network operator, usually working in the network operations centre **2712**, has access to the full set of functionalities described above in relation to **FIGS. 30 and 31** together with additional capabilities. These are accessible via the following:

[0625] Location explorer

[0626] Alarm explorer

[0627] Full KMS access (service and component related information)

[0628] Full set of tools

[0629] Rules editor

[0630] This GUI **2716** is not necessarily fully Web-based.

[0631] **FIGS. 32 and 33** show two screens in particular giving the network operator information on equipment at two different levels. **FIG. 32** shows the Location Explorer screen for equipment located at the Baguley regional head end and **FIG. 33** shows the Equipment Explorer screen for a route connecting London to Newcastle. **FIG. 34** shows the overall layout of the Location and Equipment screens. This is that the user has a selectable list **3302** of Locations and/or Equipment to the left, a central view of the relevant geographic or architectural layout **3304** of network equipment and KMS access **3306** to the right. A way the user can

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 091

interact with these views is via a set of pulldown menus **3308** at the top and further detail of these pulldown menus is as follows:

[**0632**] Menu detail:

[**0633**] File

[**0634**] Login

[**0635**] Logout

[**0636**] Quit

[**0637**] View

[**0638**] Alarm Explorer

[**0639**] KMS (y/n)

[**0640**] Location

[**0641**] All

[**0642**] Regional

[**0643**] Report

[**0644**] Summary

[**0645**] By location

[**0646**] By service

[**0647**] By users

[**0648**] Tools

[**0649**] Telnet

[**0650**] MRTG

[**0651**] KMS

[**0652**] IP Address management

[**0653**] IP provisioning query

[**0654**] DHCP LOG

[**0655**] BMC Patrol

[**0656**] HP OpenView

[**0657**] Settings

[**0658**] KMS setup

[**0659**] Inventory setup

[**0660**] Correlation setup

[**0661**] Graphics setup

[**0662**] Select Mode

[**0663**] Create Link Mode

[**0664**] Save Geometry

[**0665**] Help

[**0666**] About

[**0667**] Location Explorer Help

[**0668**] The Alarm Explorer screens available to service and customer operatoins in the Customer Operations Centre **2714** are described with reference to **FIGS. 30 and 31** above. However, the Alarm Explorer screens available to the network operator in the Network Operations Centre **2712** and their associated navigation menus give access to different content.

[**0669**] **FIG. 35** shows an alarm list for a user selection from a list of all alarm types **3602**. The user has selected to get further information on ongoing alarms associated with the Baguley hub and status information **3604** is shown for two alarms affecting the hub, "LDAP server down" and "LDAP database down". The status information is that both of these have been assigned.

[**0670**] **FIG. 36** shows the Alarm Explorer screen for tracing component alarms **3702** relevant to ongoing service alarms **3704**. In this case, the network operator has selected the Baguley regional head end and the service alarm associated with the Baguley regional head end is shown to be related-to the same two component alarms as the Baguley hub, "LDAP server down" and "IDAP database down". The network operator has selected one of these, "LDAP server down", for Alarm Detail. In a manner equivalent to the Alarm Explorer capability for the service operator, shown in **FIG. 30**, the Alarm Detail section **3706** has brought up comments on the component involved, a description of the problem and action to take. A search has been run using the KMS **2906** to bring up related documentation in the KMS portion **3708** of the screen.

[**0671**] **FIG. 37** shows the overall layout of the Alarm screens of **FIGS. 35 and 36**. This is that the user has a selectable list of Service Alarms **3802** and a selectable list of Component Alarms **3804** to the left, a central view of the relevant Alarm List or Alarm Detail **3806** and KMS access **3808** to the right. A way the user can interact with these views is again via a set of pulldown menus **3810** at the top and further detail of these pulldown menus is as follows:

[**0672**] Menu detail:

[**0673**] File

[**0674**] Login

[**0675**] Logout

[**0676**] Quit

[**0677**] View

[**0678**] Location Explorer

[**0679**] KMS (y/n)

[**0680**] Sort alarm list

[**0681**] By nb user impacted

[**0682**] By service impacted

[**0683**] By location

[**0684**] Correlate

[**0685**] Find root alarms

[**0686**] Tools

[**0687**] Telnet

[**0688**] MRTG

[**0689**] KMS

[**0690**] Re-segmentation

[**0691**] IP Address management

[**0692**] IP provisioning query

[**0693**] DHCP LOG

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 092

[0694] BMC Patrol

[0695] HP OpenView

[0696] Settings

[0697] KMS setup

[0698] Inventory setup

[0699] Correlation setup

[0700] Others

[0701] Help

[0702] About

[0703] Alarm Explorer Help

[0704] In the above, correlation and sorting mechanisms are mentioned. These are both further discussed below.

[0705] It is possible for a user to run the KMS **2906** directly to locate information in the documentation available to the KMS. FIGS. **38** to **41** show example screens and the content of the navigation menus in this respect.

[0706] Menu detail:

[0707] Documentation

[0708] Vendor manual

[0709] Engineering documents

[0710] Platform Administration

[0711] Procedures

[0712] Configuration files

[0713] Equipment

[0714] Inventory

[0715] Equipment types

[0716] Links

[0717] Software

[0718] Inventory

[0719] Software types

[0720] Links

[0721] Fault Monitoring

[0722] Component alarm classes

[0723] Service alarm classes

[0724] Services

[0725] Impact

[0726] Contacts

[0727] People

[0728] Sites

[0729] Companies

[0730] KMS Administration

[0731] Users administration

[0732] Other tables

[0733] SQL requests

[0734] HELP

[0735] About

[0736] KMS Help

[0737] Correlation and Sorting

[0738] From the Alarm Explorer screen, and referring back to **FIG. 28**, a user can launch a correlation engine **2908** by choosing an appropriate menu. The goals of correlation in embodiments of the present invention are (depending on the user) to link a service alarm or a location either to impacted subscribers or to associated components. Linking to impacted subscribers can be used to give a measure of the importance of the problem and linking it to associated components can be used to put the problem right. The identification of impacted subscribers might be done in more than one way. Three examples are to:

[0739] select all subscribers associated with a location by reviewing a list of customer premises equipment MAC addresses mapped to the location

[0740] select some of the above subscribers according to a further selection criterion

[0741] run an IP address management application which provides details on subscribers impacted

[0742] The identification of associated components might also be done in more than one way. Two examples are to:

[0743] generate a full list

[0744] use correlation rules to find and display only root component alarms

[0745] Once the impacted subscribers and the associated components have been identified, it is possible to sort them in various ways. For instance, the type of service affected can be sorted against location, against the number of subscribers impacted or against the type of subscribers impacted. For instance the types of subscribers might be coded as VIP, gold and the like.

[0746] Defining Rules

[0747] The rules for reporting are preferably stored in a database and preferably viewable and modifiable by means of a graphical user interface. A conventional expert system may be employed to manage and update the rules. Some rules may be general rules and others may be tailored to a particular environment.

[0748] Trouble Reporter

[0749] Referring again to **FIG. 28**, another Web-based application which can be provided in embodiments of the present invention, and will be accessible to users via the network operations GUI **2716** and the service operations GUI **2718**, is a trouble reporter **2916**. This can provide service-related statistics for use for example in managing service level agreements. Useful data in this respect can be accumulated by day, week or month on the following:

[0750] service impacted

[0751] number of alarms

[0752] localisation

[0753] severity

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 093

[0754] subscribers impacted in terms of number and/or type

[0755] start/end date/time

[0756] Other statistics which might be desirable via the trouble reporter **2916** are the identification of recurring failures, mean time to repair, percentage availability and the like.

[0757] A series of tools **2802** may be supplied in embodiments of the present invention which can be run separately by means of the GUIs but which might also support the main functions concerned with alarm and service analysis. These tools can provide a very rounded and flexible approach to service management in a complex network environment.

[0758] A first of these tools **2802** for instance might be an IP address management tool which allows a number of address aspects to be reviewed as follows:

[0759] Checking an IP address by selecting a subscriber's IP address and then—

[0760] the MAC address of the subscriber's device

[0761] MAC address and IP address of associated cable modem (if MAC address is different)

[0762] Associated DHCP server IP address

[0763] Associated CMTS IP address

[0764] Associated LDAP IP address

[0765] Subscriber's details (i.e., name, address, credit status . . .)

[0766] List of services used (HSD Gold, . . .)

[0767] Checking an IP address by selecting an infrastructure IP address and then—

[0768] Equipment name

[0769] Equipment location

[0770] List of software running on it (if appropriate)

[0771] (Optional) Details of software (e.g., login, password, . . .)

[0772] (Optional) List of related equipments (if appropriate—e.g., CMTS-uBR)

[0773] Additionally, this tool can be used to return statistics on the utilisation of IP address scopes on a DHCP server basis. For each server the application returns the list of managed scopes. For each scope the application returns:

[0774] Scope name

[0775] Scope range

[0776] Private/public

[0777] Scope utilisation

[0778] Associated DHCP server IP address

[0779] Associated CMTS IP address

[0780] Time of last update (i.e., the last time the statistics were gathered)

[0781] Lastly, this tool can be used to display a list of equipment, in terms of name, type and IP address, sorted by location.

[0782] Another of the tools **2802** might be used to launch a Telnet session with specified equipment.

[0783] A DHCP server tool can be arranged to parse the DHCP log file from CNR servers in order to extract useful information such as failure of a cable modem provisioning process, and/or to automate a progressive re-provisioning process in case of outage of a complete part of the network in order to avoid flooding the DHCP servers.

[0784] A CPE manager tool can be dedicated to address a specific subscriber or end-user request:

[0785] Find out the status of a cable modem, from an IP address or a subscriber ID (in relation with the IP Provisioning Database)

[0786] Check status of the associated HSD Service Simulator (same HUB/same segment as the subscriber), and compare it to the subscriber's problem

[0787] Associate subscriber with a current service outage

[0788] Reboot subscriber's cable modem, change/update service class (gold/Silver/Bronze), IP filters

[0789] Monitor performance

[0790] A maintenance forecast tool can be dedicated to send messages/postal mails/ . . . to customers when a forecasted maintenance operation will have an impact on a specific service impacting them.

[0791] A resegmentation tool can process performance warnings (e.g. available bandwidth in a CMTS card) to propose resegmentation options.

[0792] In **FIG. 42** described above, an embodiment of the present invention is shown for the environment in which a global infrastructure provider controls the end to end network, up to the Internet Service Provider's platform. In **FIG. 43**, the equivalent arrangement is shown where the service provider uses an embodiment of the present invention to control the ISP part of network, but is also able to use the HSD simulator **4402** installed within the hubs of the infrastructure provider.

[0793] In summary, the communications network management system is herein disclosed which can assist identification and rectification of faults on a network, particularly a broadband access network, leading to more effective service provision.

[0794] Further Details of a Knowledge Management System

[0795] As discussed above, the CNMS may be implemented in conjunction with a Knowledge Management System (KMS). Further details of one embodiment of a KMS which may be implemented in conjunction with the methods and systems described herein, or as an independent entity, are outlined below. This embodiment is described by way of example only and is not intended to be limiting in any way.

[0796] The KMS tool may be implemented as a web-based application that allows you to instantly access a variety of documents pertaining to your network equipment and to retrieve context sensitive help relating to component and service alarms.

[0797] The Knowledge Management System **4802** can be integrated with Imagine Service Emulation Agent (ISEA) modules, such as the Cable Modem Manager **4804** and Set Top Box Manager **4806**, embodiments of which are described in more detail below, in a distributed system to simulate a subscriber access to Internet Service as shown in **FIG. 47**.

[0798] The following are non-limiting examples of functions and associated method steps which may be performed using a KMS application:

[0799] The Knowledge Management System may display a list of documents based on user input. This may be implemented as described below:

[0800] After selecting the type of document from the available options, for example vendor manual, engineering documents or procedures, a Document Selection display mode allows a user input corresponding to that type of document. Search criteria to apply can be chosen by selecting items from list boxes. If it is not desired to specify a particular type of equipment, type of software, or company name, then "All" can be chosen from the menu. This choice indicates that no specific selection has been made and provides a view of all documents corresponding to the remaining search criteria for all available types of equipment, software and company names. If the exact reference for the document required is not known, it is possible to look for information according to subject. The following common information fields may be used:

[0801] Title

[0802] Author

[0803] Description

[0804] Equipment Type

[0805] Software Type

[0806] Company

[0807] The KMS screen may display a list of candidate documents from which a user can select.

[0808] The Knowledge Management System may also display detailed information for a selected document. Detailed information about all the documents found that correspond to inputted search criteria may be displayed. Each document may be viewed in turn. Details may include the author of the document, a description of the document, file format, version, and the document URL

[0809] The Knowledge Management System further allows the management of documents according to user rights. User rights may be used to define what actions a user will be able to take within the KMS tool. Possible actions include:

[0810] Adding a new document.

[0811] Updating the detailed information for a document

[0812] Deleting a document.

[0813] The KMS may further allow the contents of a document to be viewed. It may be possible to view the contents of a document from the Document Details display mode by clicking on the document URL.

[0814] The KMS may be operated via a Graphical User Interface architecture as shown in **FIG. 48**.

[0815] An Imagine Service Emulation Agent (ISEA)

[0816] The principles and methods described herein may be implemented in conjunction with a Imagine Service Emulation Agent (ISEA). An ISEA for a High Speed Data (HSD) service system may be implemented as a standalone system and may be dedicated to monitor end-user High Speed Data Services, enabling remote diagnosis and reducing lead-time for problem resolution. This application is described by way of example only and is not intended to be limiting in any way.

[0817] According to the present embodiment, the ISEA is located on the "last-mile" access network (typically one agent per HUB). Features provided may include some or all of the following:

[0818] Sophisticated, permanently-running scenarios to simulate extensive HSD end user activity:

[0819] Provisioning process

[0820] Internet access

[0821] ISP access

[0822] Security checks

[0823] Configuration of scenarios through scripting language (e.g. XML).

[0824] Logging of service outages to local files.

[0825] Integrated Web Server for Service Alarms Monitoring.

[0826] Specific check on request (Dynamic Check), to provide help on failure diagnostics.

[0827] SNMP interface to an external SNMP manager (for example, HP OV, or Spectrum)

[0828] Reporting of Service Alarms to Service Manager, part of Service Assurance Product Suite.

[0829] The emulation of services may be used to test the provisioning and quality of a number of services offered over the Communications network. Emulated services may include some or all of those listed below:

[0830] Emulation of the provisioning process may allow a number of the following features to be assessed:

[0831] Response time to get a new IP Address

[0832] DHCP renew

[0833] Alarm on timeout

[0834] Emulation of Internet access may test:

[0835] Response time to access some (e.g. 20) popular web sites

[0836] Alarm on timeout

[0837] ISP Access (E-mail, Chat, News, etc.) simulation may also be provided to test:

[0838] Simulation of Mail Send and Receive

[0839] POP/SMTP protocols

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 095

[0840] Chat/news simulation (IRC or equivalent protocols)

[0841] Response time

[0842] Alarm on timeout

[0843] Security Check

[0844] Simulation of hacker attacks may be used to test security holes, for instance:

[0845] Ping on secured servers

[0846] Open UDP/TCP sockets on secured server ports

[0847] Alarm if successful

[0848] The ISEA may perform permanent monitoring and/or may implement dynamic checks on request, for example by activation through an integrated web-server.

[0849] A scenario may be defined by a number of different parameters and conditions. These may include the scenario name and/or the different locations and services with which the scenario is concerned. **FIG. 55** illustrates one embodiment of scenario organization.

[0850] The ISEA may be implemented as a Java application designed to run on a Linux box. Other equivalent scripting or programming languages may also be used and may be implemented within other operating environments. In term of hardware, in this embodiment, the box must have at least 2 NIC cards, the first one dedicated to the management (eth0) and the second one (eth1) dedicated to perform all the required tests as shown in **FIG. 56**.

[0851] The ISEA Architecture of the present embodiment is composed of six key components, as shown in **FIG. 57**:

[0852] The Imagine Service Emulator Agent Engine **5702**

[0853] The Configuration **5704**

[0854] The Connectivity **5706**

[0855] The Protocol **5708**

[0856] The Alarm Handler **5710**

[0857] Communication **5712**

[0858] Each of these components may be configured in two files:

[0859] The Agent file that contains:

[0860] The Agent Configuration

[0861] The Communication Configuration

[0862] The Connectivity Configuration

[0863] The Scheduler Manager Configuration

[0864] The scheduler manager file that contains:

[0865] The Alarm Handler Configuration

[0866] The Protocols Configuration

[0867] The Service Configuration

[0868] The Scenarios Configuration

[0869] The Scheduler Configuration

[0870] Configuration of the Agent may be provided by a number of modular commands, and these are typically in the form of an activation script. Preferably this script is a markup language, and more preferably XML (extensible markup language) is used. A number of XML configuration sections are shown by way of example in FIGS. **49** to **54**.

[0871] With reference to **FIG. 51**, it should be recognized that often the protocols section must only contain protocols that will be used. It is however possible to add protocols by concatenation of the protocol section into one XML file.

[0872] A Hybrid Fiber-Coax Manager

[0873] The systems and methods described above may further be implemented in conjunction with a Hybrid Fiber-Coax Manager, a description of one embodiment of which follows below. This application is described by way of example only and is not intended to be limiting in any way.

[0874] The Imagine HFC Manager (HFC-MGR) tool may be used to provide the customer service operator with different views of the HFC network to enable remote diagnosis and to reduce lead-time for problem resolution. The resulting remote operations may increase call centre efficiency and reduce manual transfers and interventions. The Imagine HFC Manager tool may be used to help customer service operators and network operators by offering visibility of various aspects of the platform from allocation of the bandwidth and packet loss, monitoring of network interfaces such as HUB and CMTS CARD, and HFC segmentation.

[0875] **FIG. 44** shows a sample HFC manager deployment. In this embodiment, the HFC manager **4502** is installed in a national data centre near a Provisioning Database. Only infrastructure elements relative to HFC Manager are shown

[0876] According to one embodiment, the HFC Manager application can be broken down into four main functional areas:

[0877] Location/Equipment tree.

[0878] CMTS Router Management.

[0879] CMTS Card Management.

[0880] Segmentation Management.

[0881] **FIG. 45** illustrates CMTS router **4604** and CMTS card **4602** relationships.

[0882] According to the present embodiment, the HFC Manager may provide the user with the following views, accessible through a drill-down geographical tree:

[0883] A global National view, showing Regions information

[0884] A Regional view (National/Regional Head-End (NHE, RHF), Hubs), showing nodes information

[0885] A node view, detailing HFC segments information

[0886] **FIG. 46** shows a user interface overview.

[0887] According to one embodiment of the user interface, a user may drill-down through Countries, Regions or Equipments, or obtain open detailed information about CMTS

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 096

router or CMTS cards. This may be done by a user, for example, by clicking on appropriate text or icons in a user interface display.

[0888] The main window of the HFC_MGR user interface may be divided into two main parts. A "Location/Equipment Panel" may be used to display the different levels of the location tree and related equipment An "Information Panel" may allow the display of information about HFC equipment. The system may be configured so that only HPC equipment relevant to the selection in the Location/Equipment Panel is displayed.

[0889] The "Location/Equipment Panel" may display information according to the following structure:

[0890] All Locations may be attached to the country with a hierarchical tree: Region, NHE, RHE and attached HUB All Equipment attached to any Location. For instance all CMTS Router attached to a HUB, then all CMTS cards attached to a CMTS Router.

[0891] If a Country, region, NHE or RHE is selected in the first (location) environment, a second (display) environment, the "Location Information Panel", may be used to display the list of all available locations. The fields may include some or all of the following:

[0892] Location: depending on the selection in the first environment, the "Location/Equipment Panel":

[0893] If a Country is selected, a list of regions within the country maybe displayed.

[0894] If a Region is selected, a list of Regional Head Ends (RHEs), National Head Ends (NHEs) and HUBs may be displayed.

[0895] Total HP: number of "Home passed". A "Home passed" represents the number of Cable Modems or Set-Top Boxes we can potentially connect.

[0896] Total CM-STB: number of Cable Modems or Set-Top Boxes actually connected.

[0897] Penetration: Total CM-STB as a percentage of /Total HP

[0898] Bronze: number of Cable Modem or Set-Top Boxes with Bronze Quality of Service

[0899] Silver: number of Cable Modem or Set-Top Box with Silver Quality of Service

[0900] Gold: number of Cable Modem or Set-Top Box with Gold Quality of Service

[0901] If a HUB is selected in the first environment, the "Location/Equipment Panel", the second environment, the "Location Information Panel", may further display information on the Signal-to-Noise Ratio (SNR), downstream/upstream bandwidth, and CM for all CMTS cards in this CMTS Router. The fields may include some or all of the following:

[0902] CMTS: CMTS card identification e.g. "Cable3/0"

[0903] CMTS Router: CMTS Router path e.g. "ubr01 soph.ib.sophia.com"

[0904] SNR min: in db, Signal to Noise Ratio. Minimal Signal/Noise ratio as perceived from this CMTS card.

[0905] SNR max: in db, Signal to Noise Ratio. Maximal Signal/Noise ratio as perceived from this CMTS card.

[0906] Downstream bandwidth: in bits, the bandwidth of this downstream channel.

[0907] Upstream bandwidth: in bits, the bandwidth of this upstream channel.

[0908] CM number

[0909] Registered CM number

[0910] If a CMTS Router is selected, for example on the "Location/Equipment Panel" or the "Location Information Panel", detailed information for this CMTS Router can be displayed. In this embodiment, information is displayed in two main sections; one for CMTS Router detailed information and the other for CMTS downstream/upstream data.

[0911] The information displayed in the CMTS Router Information Panel may include some or all of the following:

[0912] System Description: a text description of the entity. This value may include the full name and version identification of the system's hardware type, software operating system, and networking software.

[0913] System Up Time

[0914] Memory Daily Graph: graph of memory utilisation.

[0915] Overall CPU 0 Load: The Current Load or a Daily Graph may be displayed.

[0916] Interface FastEthernet 0/0: The current Status (e.g. UP/DOWN) may be displayed in addition to or in place of a Daily Graph of the FastEthernet 0/0 traffic.

[0917] Interface FastEthernet 1/0: The current Status (e.g. UP/DOWN) may be displayed in addition to or in place of a Daily Graph of the FastEthernet I/O traffic.

[0918] For all CMTS cards, downstream and upstream information can be displayed in the "CMTS Card Upstream/Downstream section".

[0919] CMTS CARD information may also be displayed in a "CMTS Card Information Panel", which may incorporate sonic or all of the following CMTS card information:

[0920] General Information may Include:

[0921] Number of Cable Modems

[0922] Number of Cable Modems registered (online)

[0923] Number of Flapping Modems

[0924] Check Segmentation

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 097

[0925] CMTS CARD Downstream information, such as that below may also be displayed:

[0926] Total bytes OUT

[0927] Total discard OUT

[0928] Traffic Analysis/Daily Graph

[0929] CMTS CARD Upstream information, such as that below may also be displayed:

[0930] Codewords received without errors

[0931] Codewords received without correctable errors

[0932] Codewords received without uncorrectable errors

[0933] Current SNR in dB

[0934] Signal Noise Ratio Analysis/Daily Graph

[0935] Traffic Analysis/Daily Graph

[0936] Total bytes IN in Mb

[0937] Total discard IN in packets

[0938] According to one embodiment, it may also be possible to perform a segmentation audit using the HFC-_MGR. The user may edit segmentation parameters and the process display shows if segmentation is needed or not. According to the present embodiment, the segmentation process uses three methods that provide three different results.

[0939] Method 1: If the total number of Cable Modems (CMs) registered on the network is greater than the edited Number Max of CM/Seg parameter, then segmentation is needed.

[0940] Method 2: If the total number of CM registered on the network, multiplied by the Bandwidth min parameter is greater than the Bandwidth parameter, then segmentation is needed. This means that given the available bandwidth, the pre-defined minimum QoS is not guaranteed for all the CMs.

[0941] Method 3: If the total number of CMs registered on the network, multiplied by their maximum bandwidth (defined in their configuration file) and multiplied by the Contention parameter, is greater than the Bandwidth parameter, then the segmentation is needed since, given the available bandwidth and the contention, the QoS is not guaranteed for all the CMs.

[0942] Parameters used in segmentation, some or all of which may be displayed in a "Segmentation Parameter Panel" include:

[0943] Bandwidth in Mb:: available bandwidth.

[0944] In this embodiment, there are two possible values:

[0945] 24 Mbps for USDOCSIS

[0946] 34 Mbps for EURODOCSIS

[0947] Number Max of CM/Seg: maximum number of CM (used for Method 1)

[0948] Bandwidth min in Kb/s: minimum bandwidth available for all the CMs, without regard to their QoS. (Used for Method 2)

[0949] Contention in percentage: 100% means that the bandwidth is shared between all the CMs, at the same time. (Used for Method 3).

[0950] The three results of the segmentation process can be displayed. For each of these three results, the value can be "segmentation needed" or "segmentation not needed".

[0951] "NB CM=": result of Method 1

[0952] "MIN=": result of Method 2

[0953] "MAX=": result of Method 3

[0954] A Cable Modem Manager

[0955] The system may also be implemented in conjunction with a Cable Modem Manager. An embodiment of the Cable Modem Manager, or Cable Modem Manager Application (CM_MGR) is described in more detail below. The CM_MGR may be implemented as part of the system described herein or may be provided independently. The features of the system described herein may be provided in combinations other than those outlined here and may be provided independently unless otherwise stated. This embodiment of the Cable Modem Manager application is described by way of example only and is not intended to be limiting in any way. Potential users of the system may be described as customers or subscribers in the following description.

[0956] The Cable Modem Manager may be implemented as a distributed web based application, and can be deployed centrally or be distributed. **FIG. 23** shows an embodiment of the CM-MGR **2302** with a distributed solution incorporated into a network environment for provisioning apparatus. Other elements of the provisioning apparatus, such as the Set Top Box Manager **2304** and the Knowledge Manager **2306**, are described herein and may be implemented alongside the CM_MGR **2302**. In an alternative embodiment, features of the other elements may be incorporated into the CM_MGR.

[0957] The Cable Modem Manager can be integrated with Imagine Service Emulation Agent (ISEA) modules to simulate a subscriber access to Internet Service.

[0958] **FIG. 24** shows the CM-MGR technical architecture overview, and how, in this embodiment, the CM-MGR application **2402** can retrieve and display information from sources including.

[0959] The ISA Database **2404**, which may be used to retrieve subscriber, provisioning and services data.

[0960] The Dynamic Host Configuration Protocol (DHCP) servers **2406**, which may be used to retrieve cable modem IP addresses.

[0961] The Cable Modem Termination System (CMTS) **2408** and cable modem, which may allow retrieval of cable modem data.

[0962] The ISEA **2410** (when ISEA integration is employed), which may be used to obtain detailed information concerning subscriber services.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 098

[0963] According to the present embodiment, the Cable Modem Manager application can perform some or all of the following main functional features:

[0964] Subscriber information searching, wherein information about individual subscribers may be obtained by inputting criteria such as first name, last name, PID, MAC or IP address into a search panel. The application displays a list of subscribers that match the search criteria in a Results list.

[0965] Status Monitoring, wherein by inputting the details of a selected subscriber, the application displays detailed information about that selected subscriber. Such detailed information may include:

[0966] Subscriber Information: PID, name, address and e-mail address.

[0967] Cable modem status from the ISA database: MAC address, CMTS name, UBR name, Location and Region.

[0968] Cable modem status from the Cable Modem Termination System (CMTS): includes downstream and upstream channel information, online state, timing offset, received power, and Quality of Service (QoS) profile.

[0969] Cable modem status directly from the cable modem: serial number, software and hardware versions, and operating system.

[0970] Performance MoniLoring (Polling), wherein by inputting the details of a selected subscriber and polling characteristics, the application can monitor and display performance inforination such as the start date, MAC address, PID and status.

[0971] Service status monitoring, whereby if ISEA Integration is employed, status of ISP, Internet, and performance can be displayed

[0972] In this way the CM-MGR can be used as a tool to solve a number of technical problems in the field of communications networks. For example, if a subscriber has recently upgraded to a premium subscription service, but complains that service is no faster than before, then by taking the subscriber's details, the status of the subscriber's modem can be displayed at a remote location, and if necessary that modem can be remotely rebooted.

[0973] In an example where ISEA integration is employed, if a subscriber makes a complaint because of being unable to access their e-mail service, and by taking the subscriber's details and analyzing the status of the subscriber's modem the cause of the subscriber's issue is not identified, then ISEA connection can be activated and the availability of the email service to the user account can be displayed.

[0974] It will be appreciated that such an application can be used to monitor a wide variety of information associated with a communications network. Examples of status information which the present application may be used to monitor are given below. The status information may be displayed on a control terminal or apparatus to allow monitoring of the system and resolution of faults which may arise. The system may be arranged so that selected items of information may be displayed in a "Standard View" and further details may be obtained by entering a "Advanced View" for each of the frames below.

[0975] Subscriber information including the following details may be displayed in a "Subscriber Information Frame":

[0976] Personal ID (PID)

[0977] First and Last Name

[0978] Address: street, city, zip code

[0979] E-mail

[0980] A "Cable Modem Information from Database Frame" may display inforination retrieved from the ISA database, including:

[0981] CM MAC address

[0982] CMTS name

[0983] UBR name

[0984] Location and Region

[0985] A "Cable Modem Status from the CMTS Frame" may display information retrieved from the Cable Modem Temination System, including:

[0986] Downstream Channel:

[0987] Identification. The Cable Modem Termination System (CMTS) identification of the downstream channel.

[0988] Frequency. The frequency of this downstream channel.

[0989] Bandwidth. The bandwidth of this downstream channel. Modulation. The modulation type associated with this downstream channel.

[0990] Interleave. The Forward Error Correction (FEC) interleaving used for this downstream channel.

[0991] Power. At the CMTS, the operational transmit power. At the CM, the received power level.

[0992] Upstream Channel:

[0993] Identification: this may comprise a unique value, greater than zero, for each interface. In one embodiment, values could be assigned incrementally starting from one.

[0994] Frequency. The centre of the frequency band associated with this upstream channel may be displayed. "0" may be shown for an unknown or an undefined frequency. Minimum permitted upstream frequency is 5 MHz for current technology.

[0995] Bandwidth. The bandwidth of this upstream channel may be displayed. "0" may be shown for an unknown or an undefined frequency. Minimum permitted channel width is 200 kHz currently.

[0996] Transmit timing offset. A measure of the current round trip time at the CM, or the maximum round trip time seen by the CMTS may be displayed.

[0997] Slot size. The number of 6.25 microsecond ticks in each upstream mini-slot may be displayed.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 099

[0998] Ranging backoff start. The initial random backoff window to use when retrying Ranging Requests.

[0999] The value may be expressed as a power of 2. A value of 16 at the CMTS may be used to indicate that a proprietary adaptive retry mechanism is to be used.

[1000] Ranging backoff end. The final random backoff window to use when retrying Ranging Requests.

[1001] The value may be expressed as a power of 2. A value of 16 at the CMTS may be used to indicate that a proprietary adaptive retry mechanism is to be used.

[1002] Transmit backoff start. The initial random backoff window to use when retrying transmissions. The value may be expressed as a power of 2. A value of 16 at the CMTS may be used to indicate that a proprietary adaptive retry mechanism is to be used.

[1003] Transmit backoff end. The final random backoff window to use when retrying transmissions. The value may be expressed as a power of 2. A value of 16 at the CMTS may be used to indicate that a proprietary adaptive retry mechanism is to be used.

[1004] Other information, such as that listed below, may also be displayed in the "Cable Modem Status from the CMTS Frame". For any unknown value, a value of "0" may be displayed:

[1005] Max number of CPEs. The maximum number of permitted CPEs connecting to the modem.

[1006] IP address. IP address of this cable modem. If no JP address has been assigned, or for an unknown IP address, a value of 0.0.0.0 may be displayed. If the cable modem has multiple IP addresses, the IP address associated with the cable interface may be displayed.

[1007] Received power. The received power as perceived for upstream data from this cable modem.

[1008] Timing offset. A measure of the current round trip time at the CM, or the maximum round trip time seen by the CMTS. This may be used for the timing of CM upstream transmissions to ensure synchronised arrivals at the CTMS. In this embodiment, units are in terms of (6.25 microseconds/64).

[1009] DOCSIS status. Status code for this cable modem as defined in the RF Interface Specification. In this embodiment, the Status code comprises a single character indicating error groups, followed by a two or three digit number indicating the status condition.

[1010] Unerrored. Codewords received without error from this cable modem.

[1011] Collected. Codewords received without error from this cable modem.

[1012] Uncorrectable. Codewords received with uncorrectable errors from this cable modem.

[1013] Signal to Noise Ratio. Signal/Noise ratio as perceived for upstream data from this cable modem.

[1014] Micro reflections (dbmV): A rough indication of the total microreflections including in-channel response as perceived on this interface. This may be measured in dBc below the signal level.

[1015] Connectivity state. Current cable modem connectivity state.

[1016] Online times. The percentage of time that the modem stays online during the time period starting with the modem's first ranging message received by the CMTS until now.

[1017] Minimum online time. The minimum period of time the modem stayed online during the time period starting with the modem's first ranging message received by the CMTS until now.

[1018] Average online time. The average period of time the modern stayed online during the time period from the modem's first ranging message received by the CMTS until now.

[1019] Maximum online time. The maximum period of time the modem stayed online during the time period from the modem's first ranging message received by the CMTS until now.

[1020] Minimum offline time. The minimum period of time the modem stayed offline during the time period from the modem's first ranging message received by CMTS until now.

[1021] Average offline time. The average period of time the modem stayed offline during the time period from the modem's first ranging message received by the CMTS until now.

[1022] Maximum offline time. The maximum period of time the modem stayed offline during the time period from the modem's first ranging message received by the CMTS until now.

[1023] Admin status

[1024] Quality of service. This may be a group number, for example a QoS profile of 9 may mean that the maximum downstream data rate is 128 kb/s, corresponding to a bronze QoS.

[1025] In Octets (MB). The total number of octets received on the interface, including framing characters.

[1026] In Packets

[1027] Create time

[1028] SID. Service ID

[1029] A "Cable Modem Status Directly from Modem Frame" may display information that has been retrieved from the cable modem itself, including some or all of:

[1030] Description. A text description of the entity. This value may include the full name and version identification of the system's hardware type, software operating system, and networking software.

[1031] System uptime. Time the system has been up for, since last reboot.

[1032] CMTS MAC address. MAC address of this cable modem. For a cable modem with multiple MAC addresses, the MAC address associated with the cable interface may be displayed.

[1033] Ranging response waiting time. Waiting time for a Ranging Response packet.

[1034] Ranging waiting time. Waiting time for a Ranging packet.

[1035] Upstream transmit power. The operational transmit power for the attached upstream channel.

[1036] Resets. Number of times the cable modem reset or initialised this interface.

[1037] Lost syncs. Number of times the cable modem lost synchronisation with the downstream channel.

[1038] Status code. In this embodiment, this may consist of a single character indicating error groups, followed by a two or three digit number indicating the status condition.

[1039] Invalid MAP. Number of times the cable modem received invalid MAP messages.

[1040] Invalid UCD. Number of times the cable modem received invalid UCD messages.

[1041] Invalid ranging. Number of times the cable modern received invalid ranging response messages. Invalid registration. Number of times the cable modem received invalid registration response messages.

[1042] Counter T1, T2, T3 or T4 expired. Number of times counter T1, T2, T3 or T4 respectively expired in the cable modem.

[1043] Down channel frequency. The frequency band associated with this upstream channel.

[1044] Up channel frequency. The centre of the frequency band associated with this upstream channel. Minimum permitted upstream frequency is 5,000, 000 Hz for current technology.

[1045] Up channel transmit timing offset. A measure of the upstream transmissions.

[1046] Relative priority [0-7]. A relative priority may be assigned to this service when allocating bandwidth. (0) may be used to indicate lowest priority; and (7) may be used to indicate highest priority. Interpretation of priority is device-specific.

[1047] Maximum upstream bandwidth (kbps). The maximum upstream bandwidth, in bits per second, allowed for a service with this service class.

[1048] Guaranteed upstream bandwidth (kbps). Minimum guaranteed upstream bandwidth, in bits per second, allowed for a service with this service class.

[1049] Maximum downstream bandwidth (kbps). The maximum downstream bandwidth, in bits per second, allowed for a service with this service class.

[1050] Transmit burst. The maximum number of minislots that may be requested for a single upstream transmission.

[1051] Profile status.

[1052] Downstream signal to noise ratio: describes the Signal/Noise of the downstream channel.

[1053] Micro reflections: A rough indication of the total microreflections including in-channel response as perceived on this interface, measured in dBc below the signal level.

[1054] Examples of performance information which the present application may be used to monitor include:

[1055] Current In: current number of octets received on the CM, in Bytes/seconds

[1056] Current Out: current number of octets transmitted by the CM, in Bytes/seconds

[1057] Average In: average number of octets received on the CM, in Bytes/seconds

[1058] Average Out: average number of octets transmitted by the CM, in Bytes/seconds

[1059] Maximum In: maximum number of octets received on the CM, in Bytes/seconds

[1060] Maximum Out: maximum number of octets transmitted by the CM, in Bytes/seconds

[1061] Current SNR: current Signal/Noise ratio as perceived for upstream data from the CM., in dB

[1062] Average SNR: average Signal/Noise ratio as perceived for upstream data from the CM., in dB

[1063] Maximum SNR: maximum Signal/Noise ratio as perceived for upstream data from the CM., in dB

[1064] These data may be displayed either graphically as shown in **FIG. 25**, or in tabular form.

[1065] A Set Top Box Manager

[1066] The provisioning system described above and the communications network management system, which will be described in more detail below may be implemented in conjunction with a Set-Top Box Manager, an embodiment of which is described below.

[1067] To implement fault resolution in provisioned communications systems, it is often necessary to have direct access to the user equipment. It may be possible to resolve faults by instructing a user to implement changes in the user equipment. However, for more complicated faults, it may be necessary for a system engineer to attend the user's site. This may mean that there is a significant delay between fault detection and resolution.

[1068] The set-top box manager (STB-MGR) is a tool which may allow customer service operators and network operators to interact directly with user devices, such as a Set-Top Box or DOCSIS-compliant (Data Over Cable Systems Interface Specification compliant) cable modems. The STB_MGR may allow a service provider to reduce the lead-time for problem resolution.

[1069] The STB-MGR tool may be provided as part of the system described herein, or it may be provided in depen-

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 101

dently. By way of example, one embodiment of the STB-MGR will now be described in more detail. The features of the system described herein may be provided in combinations other than those outlined here and may be provided independently unless otherwise stated. The following description is not intended to be limiting in any way. Potential users of the system may be described as customers or subscribers in the following description.

[**1070**] As stated above, the STB-MGR tool may be used to provide the customer service operator with a means of interacting directly with a user's Set-Top Box to reduce lead-time for problem resolution.

[**1071**] **FIG. 11** provides an outline of how one embodiment of the STB-MGR **1102** may be incorporated into a network environment for provisioning apparatus. Other elements of the provisioning apparatus, such as the Cable Modem Manager **1104** and the knowledge Manager **1106**, are described herein and may be implemented alongside the STB_MGR. In an alternative embodiment, features of the other elements maybe incorporated into the STB_MGR.

[**1072**] The STB_MGR tool may perform some or all of the functions outlined below. Features of the STB_MGR functionality may be provided independently, or may be provided by elements other than the STB-MGR within the system.

[**1073**] By way of Example, the functions of the STB-MGR may include at least one of:

[**1074**] Displaying a list of users based on the identity of their Set-Top Box. For example, based on the user's PID, MAC address or IP address. More details of this functionality are provided below.

[**1075**] Managing Installation parameters. This button may be configured to run the query with the content of the selection fields and is also described in more detail below.

[**1076**] The type of window used by the STB_MGR tool to display user details may depend on the number of users for which details have been retrieved. For example, if the details of many users are retrieved in response to a particular query, a "matched subscribers list" may be displayed. If the details of only one user is retrieved, the "'Install' Results List Panel" for this user may be displayed. By way of example, the 'Install' Results List Panel may provide information such as the About Installation parameters, hardware and code release version, MPEG and PCM attenuation level and the MAC Address. It may be possible to update some Installation parameters within the 'Install' Results List Panel, for example: the Network ID, QAM (Quadiature Amplitude Modulation) rs: Default frequency and symbol rate.

[**1077**] Detailed information from the Set-Top Box of a selected user may also be displayed. This information may include, for example, the About Forward Path or the About Return Path for a particular user. According to a further example, a list of events/status with time stamps may be displayed.

[**1078**] A user interface may also be provided. The user interface may be divided into a number of different types of windows. For example, three types of windows may be: a selection panel to edit, for example, the user name, PID, IP or MAC address for a particular user, a results list window to show user details that match a particular selection and a details window to show all the Set-Top Box information. More details of one embodiment of a STB_MGR user interface are provided below.

[**1079**] Use of one embodiment of the STB-MGR tool will now be described in more detail. A number of user issues and problems that may be overcome by use of the STB_MGR will be described to illustrate use of the STB-MGR tool, but these issues are not limiting and are provided by way of example only.

[**1080**] According to the first example scenario, a user makes a complaint that the can not gain access to a regional channel. By way of example, this complaint may be dealt with using the steps outlined below.

[**1081**] A typical screen display which may be viewed by the STB_MGR tool operator whilst dealing with this problem is shown in **FIG. 12**.

[**1082**] Step 1: Display Subscribers Set-Top Box Installation parameters

[**1083**] Ask the caller for their name or PID and input this information into the relevant PID **1202** or Name **1204** fields.

[**1084**] Click on the Search button **1206** to view the Set-Top Box-Manager screen display.

[**1085**] In this example, the correct Set-Top Box is identified and the detailed Set-Top Box information, for example the Default Frequency **1208**, is automatically displayed.

[**1086**] Step 2: Analyze the Data

[**1087**] In this example, the value of 'Network ID'**1210** does not match the region of the subscriber (this may occur due to a moving for instance). In this example, the problem may be cured by updating the Set-Top Box installation to reload the right Set-Top Box configuration file, as outlined in Step 3.

[**1088**] Step 3: Update Set-Top Box configuration

[**1089**] In this embodiment, the Set-Top Box configuration file may be updated by editing the right Network ID **1210** and clicking on the Update button **1212** to display the Set-Top Box-Manager tool screen

[**1090**] In a second scenario, a user makes a complaint that he can't access a pay-per-view service. By way of example, this problem may be solved, with reference to **FIGS. 12 and 13**, using the following numbered steps:

[**1091**] Step 1: Check Installation parameter

[**1092**] In this example, this may be done in the same way as in Step 1 of the previous scenario, but, in this case, the initialization parameters are correct.

[**1093**] Step 2: Display Subscriber's Set-Top Box Forward parameters

[**1094**] Ask the caller for their name or PID and input this information into the relevant fields **1202**, **1204**.

[**1095**] Click on the 'Search' button **1206** to view the Set-Top Box-Manager screen display, as illustrated in **FIG. 12**.

[1096] Click on 'Forward Path'**1214** menu to view the Set-Top Box-Manager screen display shown in **FIG. 13**.

[1097] Step 3: Analyze the Data

[1098] In this example, the value of 'Credit'**1308** shows that the user does not need to carry a sum to his credit. The status of the smardcard **1310** may show that the Credit Card is out of order. In analysing the data, the STB_MGR operator may be able to identify problems with the user's system which may be preventing the user from accessing the pay-per-view service. The user may then be able to rectify, for example. problems resulting from his credit card.

[1099] In a third scenario, the subscriber makes a complaint that his Set-Top Box often reboots. This problem may be solved, by way of example, according to the following numbered steps.

[1100] Step 1: Check Installation Parameters

[1101] In this example, Step 1 may be implemented in the same way as in Step 1 of the previous scenario, but, in this case, the initialization parameters are correct.

[1102] Step 2: Display Audit information

[1103] With reference to **FIG. 12**, click on the Audit menu **1216** to view the Set-Top Box-Manager screen display shown in **FIG. 14**. The event log **1402** is displayed.

[1104] Step 3: Analyze the Data

[1105] This may allow the operator to see if the number of reboots announced by the subscriber is correct and abnormal. Further action may then be taken to rectify any problems detected in the event log.

[1106] Further details of a preferred embodiment of a user interface for the STB-MGR tool are outlined below. Features may be provided independently or in alternative combinations. Features of the following components of the STB-MGR tool user interface are outlined: the Connection Window, the Main Window and the Top-bar. Features described herein may be applied to other components of the STB-MGR tool.

[1107] **FIG. 15** illustrates a screen shot of an embodiment of the Connection Window. According to a preferred embodiment, the Set-Top Box-Manager tool may be accessed by an operator by entering the correct URL in the browser bar. According to a further, optional feature, the Set-Top Box-Manager can be accessed directly either from a Customer Operations Dashboard application, for example, by clicking on 'STB-MGR' in the top bar or from a Network Operations Dashboard application, from either the Alarm Explorer or the Location Explorer. The Customer Operations Dashboard application and the Network Operations Dashboard application may comprise applications via which system or network operators may access a number of different tools, such as the STB_MGR tool, to help in fault detection or resolution.

[1108] A login window may be provided for the Communications Window, as shown in **FIG. 15**, at which a valid username **1502** and password **1504** are required. Text entered in the Password field may be obscured with asterisk (*) characters. If connection fails due to an incorrect username or password, a connection error dialog box may be displayed.

[1109] A screen display of one embodiment of the Main Window is shown in **FIG. 16**. According to one embodiment, the Main Window may be used to retrieve details from the Set-Top Box Manager (STB-MGR) based on either user information, IP Address or MAC Address or to check the status of a user's Set-Top Box.

[1110] Preferably, a Select Panel **1602** may be provided as part of the Main Window and may be used to search within any combination of selection fields such as the Last name **1604** or First Name **1606** of a user, a user's PED **1608**, an IP address **1610** or a MAC Address **1612**.

[1111] Preferably, at least one field must be completed to run the query and avoid an error message. A cancel button **1614** may be provided to clear the content in the selection fields. A Search Button **1616** may be used to run the query with the content of the selection fields.

[1112] As described above, the window displayed may depend on the number of users for whom details are retrieved:

[1113] If many user details are retrieved, the "matched subscribers list" may be displayed.

[1114] If the details of only one user is retrieved, the 'Install' Rcsults List Panel for this user may be displayed.

[1115] In this embodiment, the 'Install' Results List Panel is displayed and shows the results of the query matching the selection. A screen shot of this panel is shown in **FIG. 16**.

[1116] The 'Installation' parameters that may be displayed for a particular user include:

[1117] Default frequency **1618**: Frequency in Hz of the Home Transport Stream

[1118] Default symbol rate **1620**: Rate at which the data leaves the modulator. In one embodiment, the symbol rate may be calculated as outlined below:

[1119] symbol rate=input rate rate (Mbps)*framing overhead*1/RS-rate*1/FECrate modulation factor

[1120] QAM **1622**: Type of Quadrature Amplitude Modulation (for example, QAM64 or QAM256)

[1121] PIN **1624**: The user's Personal Identification Number

[1122] Network ID **1626**: Identifies the network segment (in DVB terms) to which the STB is attached. If a subscriber moves from one region to another, he typically needs another STB ID

[1123] Hardware version 1628: Version of the hardware platform

[1124] Code release version 1630: Release number of the software platform

[1125] Build date **1632**: Download date of the software platform

[1126] MPEG attenuation level **1634**

[1127] PCM attenuation level **1636**: Pulse Code Modulation attenuation level

[1128] Attenuation **1638**

[1129] MAC address **1640**: MAC address of the integrated cable modem

[1130] Update Button

[1131] In a preferred embodiment, the user can use an 'Update' button **1642** to modify only information displayed in **FIG. 16** with a white background, by edition or predefined value selection. The parameters which it is possible to modify may include some of all of the following:

[1132] Default frequency **1618**

[1133] Default symbol rate **1620**

[1134] QAM **1622**

[1135] PIN **1624**

[1136] Network ID **1626**

[1137] The Update button **1642** preferably displays a confirmation box.

[1138] A further feature may be the 'Forward Path' Results List Panel, an example of a screen display of which is shown in **FIG. 17**, which may display parameters such as those outlined below:

[1139] SNR estimate **1702**: Signal/Noise estimate. Should be high if there is little noise

[1140] Pre RS Error rate **1704**: Number of errors per 500 ms before Reed-Solomon error correction

[1141] Post RS Error rate **1706**: Number of errors per 500 ms after Reed-Solomon error correction

[1142] Lock status **1708**: Indicates whether the STB is successfully tuned to a transport stream (i.e. locked to a RF carrier).

[1143] Last PAT **1710**: Last time/date when a Program Association Table was received

[1144] Last CAT **1712**: Last time/date when a Conditional Access Table was received

[1145] Channel table **1714**: Status of the channel table capture process, for example: "Looking for UPDATES" means that the STB is receiving DVB SI tables under normal conditions. If the status remains "Looking for NIT", it means the STB can not receive the Network Information Table

[1146] Number of transport streams **1716**: Number of Transport Streams available received by the STB (i.e. Transport Streams available to the configured Network ID)

[1147] Number of services **1718**: Number of video services (digital channels) available received by the STB (i.e. DVB services available to the configured Network ID).

[1148] AGC combined **1720**: Combined Audio/Video gain currently applied to the forward Path signal.

[1149] AGC stands for Automatic Gain Control.

[1150] Current TSD: Transport Stream ID to which the STB is currently tuned.

[1151] Current Service ID: Service ID (i.e. digital channel) to which the STB is currently tuned.

[1152] In a preferred embodiment, at least some of the following information may also be provided in the "Forward Path Results" List Panel:

[1153] Nagra serial number **1722**: CAS (Conditional Access Smartcard) serial number.

[1154] Smartcard status **1724**: Shows the status of the Conditional Access smartcard

[1155] IPPV status **1726**: Status of theJImpulse Pay-Per-View service provision

[1156] Credit **1728**: Current credit available for Impulse Pay-Per-View

[1157] Smartcard Version **1730**: version of the Conditional Access smartcard

[1158] Smartcard Revision **1732**: Revision of the Conditional Access smartcard

[1159] CA Version **1734**: Version of the CAS software kernel

[1160] CA Revision **1736**: Revision of the CAS software kernel

[1161] Smartcard zipcode **1738**: Zipcode of the smartcard owner

[1162] Smartcard serial number **1740**: Serial number of the Conditional Access smartcard

[1163] Set Top Box serial number **1742**: Serial number of the Set-Top-Box

[1164] Last EMM received: Dale when the last EMM was received

[1165] The information displayed may be used for fault detection and resolution for systems, such as Set-Top Boxes of users.

[1166] The 'Return Path' Results List Panel may display a number of 'Return Path' parameters. An example of a screen display of the 'Return Path' Results List Panel is shown in **FIG. 18**. In a preferred embodiment, the parameters displayed may include:

[1167] MCNS (Multimedia Cable Network System) IP addressing

[1168] MAC address **1802**: Set-Top-Box integrated cable modem physical address

[1169] STB IP **1804**: Configured Set-Top-Box IP address

[1170] DNS Server IP **1806**: Configured domain name server IP address

[1171] Subnet mask IP **1808**: Configured subnet mask

[1172] Default gateway IP **1810**: Configured default gateway IP address

[1173] Quality of service **1812**: Current cable modem configuration file (which may be used to define the Quality of Service allocated to the STB)

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 104

[1174] Liberate proxy **1814**: IP address of the Liberate Proxy server (alternative types of Proxy servers may be used in some implementations)

[1175] Liberate security proxy **1816**: IP address of the Liberate Security Proxy server (alternative types of Security Proxy servers may be used in some implementations)

[1176] First URL **1818**: URL opened upon start-up of the browser. The browser used may depend oil the user equipment used to implement the system, for example the Liberate Browser may be used as a software platform for browsing from a television.

[1177] MCNS Downstream

[1178] Channel frequency **1820**: Frequency of the used return path downstream channel

[1179] Symbol rate **1822**: Rate at which the data leaves the return path modulator. According to one embodiment, the symbol rate may be calculated as outlined below:

[1180] symbol rate=input rate rate (Mbps)*framing overhead*1/RS-rate*1/FECrate modulation factor

[1181] SNR estimate **1824**: Signal/Noise estimate. Should be high if there is little noise

[1182] Pre RS Error rate **1826**: Number of errors per 500 ms before Reed-Solomon error correction

[1183] Post RS Error rate **1828**: Number of errors per 500 ms after Reed-Solomon error correction

[1184] Lock status **1830**: Indicates whether the STB is successfully tuned to a transport stream (i.e. locked to a RF carrier).

[1185] Power level **1832**: Radio Frequency power level

[1186] Assigned SID **1834**: Assigned DOCSIS channel identifier (Service Identifier)

[1187] A further feature of a preferred embodiment may be the 'Resources' Results List Panel, an example screen display of which is shown in **FIG. 19**, which may display information such as:

[1188] Available flash **1902**: Free Flash memory currently available

[1189] Total flash **1904**: Total Flash memory available on the STB hardware

[1190] Available RAM **1906**: Free volatile memory currently available

[1191] Total RAM **1908**: Total volatile memory available on the STB hardware

[1192] Available NVRAM **1910**: Free non-volatile memory currently available

[1193] Total NVRAM **1912**: Total non-volatile memory available on the STB hardware

[1194] A screen shot of the 'Audit' Results List Panel according to one embodiment is shown in **FIG. 20**. This panel may be used to display the list of the last status logged by the STB. In this example, the information may be formatted in 3 parts:

[1195] Date of the action in MM-DD-YYYY IIH-MM (AM/PM)

[1196] Code

[1197] Messages to describe the status.

[1198] For instance:

[1199] STBMGR_LOG_REBOOT

[1200] STBMGR_LOG_CM_OPERATIONAL

[1201] STBMGR_LOG_TUNING_PARAMETERS_CORRUPT

[1202] STBMGR_LOG_PERIODIC_RANGING-_FAIL

[1203] STBMGR_LOG_TIMEOUT_ON_RECEIVING_PAT

[1204] Further messages may also be provided to describe the status of the STB.

[1205] The STB-MGR TopBar may contain buttons which control the overall functionality of the system. An example screen display of a Sct-Top Box Manager Top Bar is shown in **FIG. 21**. The buttons on the Top Bar may include:

[1206] The 'Install' Button **2102** may be used to run a query relative to the Installation information of the Set-Top Box. The selection criteria may be set in the Select Panel (as described above) and the information may be displayed. This button **2102** may run the query with the content of the selection fields. As described above, the window displayed may depend on the number of users for whom data is retrieved:

[1207] If data for many users is retrieved, the matched subscribers list is displayed.

[1208] If data for only one user is retrieved, the 'Install' Results List Panel for this subscriber may be displayed, as described earlier with reference to **FIG. 16**.

[1209] The 'Forw. Path' Button **2104** may be used to run a query relative to the Forward Path information of the Set-Top Box. The selection criteria may be set in the Select Panel (described earlier) and the information may be displayed in the 'Forward Path' Results List Panel (described earlier with reference to **FIG. 17**).

[1210] The 'Ret. Path' Button **2106** may be used to run a query relative to the Return Path information of the Set-Top Box. The selection criteria may be set in the Select Panel and the information may be displayed in the 'Return Path' Results List Panel (described earlier with reference to **FIG. 18**).

[1211] The 'Resources' Button **2108** may be used to run a query relative to the Resources information of the Set-Top Box. The selection criteria may be set in the Select Panel and the information may be displayed in the 'Resources' Results List Panel (described earlier with reference to **FIG. 19**).

[1212] The 'Audit' Button **2110** may be used to run a query relative to the Audit information of the Set-Top Box. The selection criteria may be set in the Select Panel and the information may be displayed in the 'Audit' Results List Panel (described earlier with reference to **FIG. 20**).

[1213] The 'Log Out' Button **2112** this may be used to close the current STB-MGR session and open a new Connection Window.

[1214] A summary of the functionality of one embodiment of the STB-MGR is provided below:

[1215] The STB-MGR may be used to increase call centre efficiency by facilitating remote operations and reducing manual transfers and interventions. The functionality of a preferred embodiment of the Set-Top-Box Manager may include:

[1216] Monitoring the status of a particular Set-Top-Box by sending a request to the STB directly with any of the following being used as input criteria: STB MAC address, STB IP address or subscriber name/PID. As described above, the following sets of data may be retrieved from the STB:

[1217] Installation parameters

[1218] Forward path parameters

[1219] Return path parameters

[1220] Resources information

[1221] Audit information.

[1222] Polling a set of selected Set-Top-Boxes for a given period of time in order to gather history of STB utilisation.

[1223] Selected STB may be polled at a regular interval for a defined duration (customisable)

[1224] The polling feature may be limited to a configurable number of simultaneous STB to be polled.

[1225] The data generated by this polling may be stored for a configurable time period in a separate database or until extra space is needed to store more recent data.

[1226] A web-based application may allow operators to view, over the polled time period, utilisation of:

[1227] STB Memory

[1228] Channels

[1229] Transport Stream ID

[1230] Service ID

[1231] In a preferred embodiment, the managed information may include:

[1232] Installation parameters

[1233] Default frequency*

[1234] Default Symbol Rate*

[1235] Modulation type*

[1236] PIN*

[1237] Network ID*

[1238] Hardware version

[1239] Code Release version

[1240] Build date

[1241] MPEG Attenuation

[1242] PCM Attenuation

[1243] Attenuation*

[1244] Mac Address

[1245] Forward path parameters

[1246] Conditional Access Status

[1247] Nagra Serial Number

[1248] Smart card Status

[1249] IPPV Status

[1250] Credit

[1251] Smart card Version

[1252] Smart card Revision

[1253] Conditional Access Version

[1254] Conditional Access Revision

[1255] Smart card Zip Code

[1256] Smart card Serial number

[1257] Set-Top-Box Serial Number

[1258] Last EMM received: Date when the last EMM was received

[1259] DVB Demodulator Status

[1260] SNR Estimate

[1261] Pre-RS Error Rate

[1262] Post-RS Error Rate

[1263] Lock Status

[1264] Last PAT

[1265] Last CAT

[1266] Channel Table

[1267] Number of Transport Streams

[1268] AGC Combined

[1269] Return path parameters

[1270] MCNS IP Addressing

[1271] Mac Address

[1272] STB IP Address

[1273] DNS Server IP Address

[1274] Subnet Mask IP Address

[1275] Default Gateway IP Address

[1276] Quality of Service

[1277] Liberate Proxy

[1278] Liberate Security Proxy

[1279] First URL

[1280] MCNS Downstream

[1281] Channel Frequency

[1282] Symbol Rate

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 106

[1283] SNR Estimate

[1284] Pre-RS Error Rate

[1285] Post-RS Error Rate

[1286] Lock Status

[1287] Power level

[1288] Assigned SID

[1289] STB Resources information

[1290] Available flash memory

[1291] Total flash memory

[1292] Available RAM

[1293] Total RAM

[1294] Available NVRam

[1295] Total NVRam

[1296] Audit information

[1297] Log of the last STB operations (Date/Code/Operation . . .)

[1298] (Preferably, appropriate installation parameters (*) can be updated directly from the STB Manager front-end (reload of the right Set-Top Box configuration file).)

[1299] The Architecture of a preferred embodiment can be summarised as follows with reference to **FIG. 22**: The STB manager is preferably implemented as a distributed web based application. It may be deployed centrally for a small amount of STBs to poll but could be distributed as the number of polled cable modems increases. The preferred STB manager may be implemented in conjunction with its own database to store historical data polled from cable modems.

[1300] **FIG. 22** shows one embodiment of an STB manager with a distributed solution. This may provide the advantage that the number of STB that can be polled by this solution is greater than in a centralised solution. Only infrastructure elements relative to the STB Manager are shown in **FIG. 22**.

[1301] Any convenient hardware and software platform may be used. Purely by way of example, a Unix platform may be used, and this may be conveniently based on readily available components. Hardware and software resources required are not excessive and, for example, a commercial deployment may be implemented readily using the hardware and software below (or equivalents).

[1302] Hardware for STB manager:

[1303] Sun E420

[1304] 1×450 MHzCPU

[1305] 1 Gb RAM

[1306] 2×17 Gb disk

[1307] Additional software required for STB manager

[1308] Apache 1.3.19

[1309] Tomcat 3.2.1

[1310] JVM 1.3.1

[1311] Solaris 7 or 8

[1312] Database: Oracle or any SQL-compliant database

[1313] A further feature of one embodiment of the present system may be the Digital Subscriber Line modem manager. The DSL modem manger may allow an operator to view the status of each VPN subscriber's DSL line and modem. For example, when an ADSL CE router is provisioned in the database, a DSLAM port must be assigned for the customer and using DSL modem manager it may then be possible to gather information. Examples of the information which may be gathered may include one or more of: the customer name, the port on the DSLAM, the port status, the modem SNR US/DS, a 5 minutes average input/output rate and bytes input and output. The invention independently provides a method comprising gathering status data from a DSJ modem connected to a broadband comprising communicating with the modem or an agent associated with the modem over the network.

[1314] A further feature of the system described above may be the VPN MPLS network manager. Using the network view of MPLS network manager, it may be possible to browse, for example: PAD (PACA), POP (Antibes), PE router (PE4).

[1315] The network view of the network manager may also be used to show the VPN logical view functionality that displays, for example, VPNs from the OSS database and VRFs that are auto-discovered from the PE.

[1316] The network view of the network manager may also be used to show, for example the PE router's:

[1317] CPU (MRTG)

[1318] Memory (MRTG)

[1319] Interface bandwidth utilization per physical interface. Show the button that can be used to define target max aggregate bandwidth for the physical interface

[1320] Number of sub-interfaces per physical interface. Show the button that can be used to define target max number of sub-interfaces per interface

[1321] Total number of VRFs (target max VRFs can be edited by clicking on a button)

[1322] CEF statistics (show ip cef summary)

[1323] The customer view of MPLS network manager may be used to browse, for example: Customers (B), VPNs (VPN B), PE routers and CE routers.

[1324] When on the PE router level one can view the same data in the customer view as in the network view, an example of which is provided above.

[1325] All of the above features are advantageously provided in an exemplary network manager; however, features may be omitted in a simplified embodiment.

[1326] A further feature of the present embodiment may be the ISM VPN, which may advantageously be implemented using one or a number of agents. Each agent may monitor the network for, for example: VPN connectivity, VPN Performance, Centralized services, Management VPN and Audit & accounting.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 107

[1327] In a preferred arrangement, which may be independently provided, at least one agent is provided, the agent comprising means for accessing a service and means for signalling an alarm in the event of detection of a fault condition. By providing an agent which accesses a service, potential or actual faults may be more reliably or rapidly identified as compared to detection of a hardware failure and subsequent determination of affected services.

[1328] For each alarm that may be generated by ISEA VPN, each ISEA may be able to detect connectivity, performance, management, audit and centralised service problems independently. Five different scenarios that simulate each type of problem will now be described by way of example.

[1329] VPN Connectivity Alarm

[1330] A VPN connectivity alarm may be generated by making a CE router unavailable. This may occur if, for example, the CE router's Ethernet connector is physically unplugged. In this situation, ISM may be configured to generate a VPN connectivity alarm.

[1331] Performance Monitoring

[1332] A performance alarm may be triggered, for example, when the data is beyond "acceptable" levels, for example, the system may be set up to trigger a performance alarm when data is being processed at a slower rate than it is being received. Rate limiting may be disabled from the VPN to make performance acceptable. Preferably, the disabling of rate limiting may allow the alarm state to be overcome within 1 minute.

[1333] VPN Central Services Monitoring

[1334] A central services alarm may be generated in the ISM in certain situations, for example, if the ISEA is continuously monitoring central services (email and www) offered from the operator's central services site and the central services www server is shut down, a central services alarm may be generated. Preferably, when the www server is resumed ISM central services monitoring should return to green status in less than 1 minute.

[1335] Management Network Monitoring

[1336] The ISEA may include management VPN monitoring that can check on the status of the management VPN by continuously pinging the management network central router. A management services alarm may be triggered if, for example, the IP address of the management router is deconfigured. If the management services router is subsequently re-configured, ISM central services monitoring preferably returns to green status in less than 1 minute.

[1337] Audit & Accounting

[1338] Using ISEA MPLS, examples of statistics that may be gathered for each VPN include:

[1339] Total uploads/downloads for each CE router using Netflow

[1340] Analysis of traffic patterns using netflow.

[1341] A further feature of an embodiment may be the Imagine Component Fault Manager (ICFM). An ICFM view may show an inventory with a map of the network of the system. The ICFM may be implemented as a client of the inventory manager that is described in more detail later.

[1342] A Knowledge Management System (KMS) may be implemented as part of the ICFM, it may be possible to right click on "documentation" for a given PE router to show the documentation associated with the device. Further, a component alarm may be generated by shutting down the PE-PE core link on PE3. This alarm, and the documentation associated with the alarm may be shown within the ICFM. The documentation linked to the alarm may also be modified within the ICFM.

[1343] A link to a configuration manager may also be provided for each PE router, for example it may be possible, for a given PE router, to click on "Configuration manager" to be taken to the "Configuration Manager" application and to view the configuration file of the PE router. A link to an inventory manager in the ICFM, outlined in more detail below, may also be provided and may be used to be taken to the inventory manager application

[1344] An inventory manager may further be provided in which it may be possible, for example, to add a new PE router (for example, PE **5** of type Cisco **3662**) to the Sophia Antipolis POP. Equipment can be auto-discovered by, for example, running an auto-discovery script. A file may be generated to populate the database.

[1345] As part of the resource management of the inventory manager, it may be possible to define a pool of IP addresses by adding a new pool of IP addresses. Utilization statistics on the pools of IP addresses and the pools of RTs, RDs, VLANs, ASN numbers may be viewed.

[1346] A further feature of one embodiment of the present invention may be a Configuration Manager, which may allow the use of template configuration files. New template files may be added to the template manager.

[1347] Further, the configuration file may allow the display of configuration files of routers in the system and may allow the version history of configurations on routers to be displayed.

[1348] HSD Agent

[1349] One embodiment of an agent that may be used in conjunction with the system and methods described herein is a High Speed Data (SD) agent. The HSD agent may be implemented as a standalone system, or may be implemented alongside other aspects of the system described herein. The HSD agent preferably allows a HSD network operator to monitor services as they are delivered to the service user, i.e. in the "last mile". In particular, the agent may provide remote visibility of all critical parameters involved in the High-Speed Data service.

[1350] According to one embodiment, the agent is physically located as one agent per HUB. The agent may provide sophisticated, permanently-running scenarios to simulate extensive HSD end user activity. The simulated user activity may include simulating some or all of the following:

[1351] Provisioning process

[1352] Internet access

[1353] ISP access

[1354] Security checks

[1355] The agent may further provide:

[1356] Easy configuration of scenarios in XML language

[1357] Logging of service outages to local files

[1358] Integrated Web Server for Service Monitoring

[1359] Specific check on request

[1360] Failure diagnostics.

[1361] Interface to any external SNMP manager (e.g. HP OV, or Spectrum)

[1362] The architecture of the HSD agent preferably allows the agent to operate as close to the customer as possible. A scheduler may be used to supervise the launching of the Service Emulation scenarios. According to one embodiment, these scenarios test parameters involved in the nature of the service; regardless at this point to the access technologies or the state of the network components involved in the transport. **FIG. 58** illustrates one embodiment of a scenario organisation for a HSD agent, controlled by a scheduler manager.

[1363] The HSD agent may be implemented on a number of different hardware and software systems. Typical implementations may run on, for example Linux Red Hat 7.1, Java JDK 1.3.1, Apache 1.3.20, Tomcat 3.2.1, NetSaint plug-in. According to one embodiment, hardware requirements may include 2×17 GB Disk, Pentium 3 750 Mhz processor, 256 Mo RAM, 10 GB and 2 Linux compliant Ethernet Cards.

[1364] The IP Address Manager

[1365] A further aspect of the systems and methods described herein is the IP address manager. The address manager may allow a service provider to optimise resource allocation within the network, wherein the network may be a multimillion address network. The IP Address Manager may be implemented as part of a suite of Network Management Tools or may be implemented as a stand-alone, vendor agnostic produce. The address manager may allow a service provider to track the use of every single IP address and to centrally manage entire scopes of IP addresses in a single operation. According to a preferred embodiment, the Address Manager satisfies both legal requirements and security procedures requiring a detailed monitoring of suspected access to restricted resources on the network.

[1366] The IP Address Manager is preferably implemented with at least one of the following management functionalities:

[1367] Identity Management may enable instant access to the name, type, location, domain name of every single IP address currently in use in the network, as well as providing an history of the usage of any IP address.

[1368] Scope Management may provide a series of tools that enable the service provider to analyse the allocation of ranges of IP addresses. The IP Manager may display the percentage of IP addresses

[1369] allocated per DHCP server, which may enable proactive balancing steps to be taken before service failure. Scope Manager may also enable a provider to edit, remove and add any fraction of the IP range anytime and anywhere, providing full control of, for example CMTS, access servers, DHCPs, UBRs and DSLAMs.

[1370] According to one embodiment, Domain Name Server Management is constituted of a series of functionalities which may be used to verify the integrity and the reversibility of the association of an IP address to a domain name.

[1371] Preferably, the IP manager may be implemented with reporting capabilities, including graphic and statistic features and may also interface with third-party reporting software.

[1372] The IP Address Manager may be implemented as part of a suite of service assurance tools and so is preferably implemented with a modular architecture. The integration of the IP address manager into a service assurance suite according to a preferred embodiment is illustrated in **FIG. 59**. The IP Address Manager is preferably located in the Network Operation Centre since the ability of the tool to manage a multimillion address network makes it a centrally based application. The IP Address Manager is preferably implemented with a Graphical Interface, which may allow context-sensitive help to be provided to the network engineers at each step. Examples of the information provided in the context sensitive help may include: the exact page containing the relevant hardware vendor documentation, in-house recovery procedures and reminders of the technical and business rules.

[1373] Operational Integration with BSS Modules

[1374] Integration with BSS elements may allow the IP Address manager to manage multiple logical groups of users, which may be used to allow usage-based billing for dedicated services. Usage-based billing may be provided to a user by collecting and tracking IP address assignments and linking each address to a billing location or group. This seamless integration may allow the service provider to manage large-enterprise customers, offering them differentiated services through organization-based IP address management capabilities. Multi-group membership for a single customer may be implemented to allow customised services for individual users.

[1375] Scope Management

[1376] Analysis tools may be provided by the IP Address Manager to enable pro-active balancing of the network resources and to anticipate potential service disruption. The scope management function may be used to collect statistics about utilisation per DHCP, RADTUS servers. The administrator can set thresholds on IP address scope to generate alarms within a Component Fault Management tool (ICFM). Based on these statistics, the network administrator may reserve and assign IP address across networks, domains and subnets. The scope management feature may allow the service provider to edit, cut and add IP address ranges, or fractions of ranges, and update the scope of IP addresses on the DHCP and RADIUS servers from a central location.

[1377] Inventory Capabilities

[1378] In order to cope with the proliferation of 1P addresses and equipment in the broadband environment, the IP Address Manager preferably provides a view of a large proportion of the IP infrastructure. The IP Address Manager may allow views by subnet, and may support Variable

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 109

Length Subnet Masks (VLSM) to handle subnets in the most flexible and effective way. "Per location" and "per type of equipment" views may also be provided in addition to or instead of the per subnet view. The module may further allow the management of all component IP addresses and subnets with detailed component configuration from a given IP address (name, type, and location). This granularity and flexibility in the views may allow cost effective resource management capabilities. IP Address Manager can reserve and assign subnets. IP address management may also allow quick and easy re-arrangement of the subnets, reflecting the frequent changes in the network organization.

[1379] Policy and Class-of-Service Management

[1380] The IP Address Manager may interfacing to DHCP and Radius Servers to offer the capability to create Classes-of-Services and Policies. Policies may be used to create consistent subnet addressing schemes within multiple sublets, helping to ensure efficient network management and simplified administration. Sub-addresses ranges can be dedicated to different types of cable modems or tiered client classes. Policies creation or modification may be reflected in the service provider billing elements.

[1381] DNS Management

[1382] The DNS Management functionality may allow the service provider to check the availability of an IP address in the DNS server, which may allow the service provider to identify potential causes of service disruption. According to one embodiment, Incognito's IP Commander DNS solution may be used with IP Address Manager interfaces for DNS Management. The IP Address Manager may allow reverse/forward query matching in order to check the IP/Domain association. As a logical complement to its subnet capabilities, the IP Address Manager may also be used to manage DNS Zone and Domain allowing the necessary granularity to differentiate services.

[1383] Typical hardware requirements which may be used to implement the IP Address Manager system may include: Sun E420, 1×450 MHz CPU, 1 Gb RAM and 2×17 Gb disk. Software Requirements for a typical embodiment nay include: Apache 1.3.19, Tomcat 3.2.1, JVM 1.3.1 or Solaris 7 or 8.

[1384] An outline of further features that may be provided as part of the IP address manager system is provided below. Some or all of these features may be provided in some embodiments of the system.

[1385] Included or Supported servers/services may include: DNS/DDNS BIND 8.x compliant, DHCP, RADIUS and SNMP.

[1386] Data storage may take the form of relational database support (e.g. Sybase, Oracle or another relational database) or a directory service (LDAP Support) (e.g. NDS, Netscape, University of Michigan or another directory service)

[1387] Data may be imported using, for example DNS zone files, Unix/etc/host files, BOOTP, User-defined/program-defined system. Similarly, data may be exported using DNS zone files, BOOTP/DHCP, Unix/etc/host files, a user-defined text-based format or a program-defined custom format.

[1388] DHCP services may include: multiple subnets/segment, dynamic DNS update, ping testing before assignment, assign based on MAC address, global templates, template per subnet/by logical group, view active lease information, variable length subnet masks (VLSM), user-to-address mapping, failover DHCP Services, static IP @ assignment & reservation, assignment of PC IP addresses based on CM (i.e. access portal) rights, IETF Draft Standard lease query & inverse lease query, support of source verify DHCP to prevent IP @ spoofing.

[1389] DNS services may include dynamic DNS, incremental DNS updates, direct DHCP integration, GUI management, BIND forwarder/zone updates, integration of infrastructure db with DNS.

[1390] Management may take place over: web management, Java management tool, native NT management tool, native UNIX management tool, SNMP MIB, Reporting/Reporting Tools.

[1391] Reporting features may include: IP Address by device/object, Reserved objects, Dynamically allocated objects, DHCP server status, By administrator, By domain, By subnet, Audit, User-customizable, Service take-up/churn rate per service per location, IP address statistics per location, IP address statistics history per location, Fault impact analysis with impacted subscribers, CMTS management (flap list, segmentation), Security audit, Automatic TTS creation.

[1392] Remote access may also provided via, for example, Windows 95/98/NT/W2K clients, HTMUServlet w XML/XSL, Java applet, Telnet, X-Window,

[1393] Other features of the IP Address manager may include: Centralised IP @ mgt for infrastructure components, Centralised IP address inventory for subscriber address pools, Command line interfaces, Application programming interfaces, Full E2E service monitoring, IP address by subscriber ID (real time), IP address history by subscriber ID, CSR can view real time service status per location, CM management.

[1394] VPN Service Assurance

[1395] A further tool which may be implemented in conjunction with the systems and methods described herein is the Service Assurance (ISA) suite for Virtual Private Networks (VPNs)

[1396] The ISA suite is preferably arranged to monitor the VPN service that is supplied to a user. This service may comprise a number of different VPN technologies, such as Layer 3 MPLS (Multi-Protocol Label Switching), IPSec (IP Security) and Layer 2 MPLS (Martini and Kompelia). This may allow the ISA to be integrated easily into existing systems and to work with existing technologies. The service is preferably monitored by monitoring a series of key indicators of the health of the service which is delivered to the user. This may be advantageous over the disjointed prior art systems which use a series of technical alarms generated by numerous network management systems to monitor the systems. The ISA suite may also be used to simulate complex scenarios relating to the delivery of the VPN services and so test VPN service delivery.

[1397] The service assurance aspect may be provided independently or may be integrated with other system com-

ponents disclosed herein, for example, the ISA may be integrated with a system provisioning too.

[1398] The architecture of the ISA is preferably modular so that the ISA may be based on a series of modular elements that may work together for the monitoring of the end-to-end performance of VPN services. An overview of one embodiment of the architecture is shown in **FIG. 60** in which Customer Edge (CE) Router Managers offer full access to VPN elements, Service Agents monitor VPN services' key features, and the Service Fault Management platform correlates the different OSS elements to simplify the outage resolution from universal graphical frontends.

[1399] A further aspect of the VPN monitoring ISA suite may be I-SEA stand-alone systems (or Agents). The agents are preferably located in the network provider Point-of-Presence (POP) and may be used to test and monitor the VPN services and their provisioning.

[1400] According to one embodiment, the I-SEA redundant principle is based on "round robin" sophisticated scenarios where the features of the created VPN link may be tested and where end-user activity may be simulated.

[1401] According to a preferred embodiment, the agent can test, for example Provider Edge (PE) and CE links, IPSec tunnels, security, QoS, performance by Class-of-Service and central services (mail, internet access, VoIP, etc). The agent may also be used to monitor management links and services. The agent may also monitor a user's IP service within a VPN and within a wide range of protocols (for example, HTTP, ICMP, SMTP and POP). Agents may be implemented for MPLS and IPSec-based VPNs as well as Layer 2 MPLS (Martini and Kompella). Agents are preferably implemented to run on standard PCs running, for example, a Linux operating system.

[1402] According to a preferred embodiment, network providers can create scenarios based on the Class-of-Services (DiffServ) that the used in the network or that are required by the user.

[1403] The agent may be implemented to monitor that the VPN user has access to the service or services that they are entitled to. Hence the agent may be implemented in a flexible manner. Use of the agents may provide the advantage that Service Level Agreement (SLA) metrics associated with the offered VPN can closely match the proposed services whatever the standardized technology in the network.

[1404] An agent may implement test scenarios in order to test the VPN network and service provision in the network. Preferably, an agent can execute up to 10 scenarios per minute. A web interface may further be provided to offer direct access to manage and create the scenarios.

[1405] As discussed above, the agents may he integrated into existing networks (such as IIP VPN (Itinerant Internet Protocol VPN) networks) and may be added to existing service assurance suites to enhance network monitoring and reporting capabilities.

[1406] According to a preferred implementation of the system, once the MPLS PE-CE link or the IPSec tunnel is provisioned by IIP VPN, the operator can automatically activate its monitoring with the agent. One embodiment of the operation of this process is illustrated in **FIG. 61** in which the agent is asked to monitor a new PE-CE link, which allows a Fault Management module to monitor the VPN enhanced by this new link.

[1407] The IIP VPN module may use a template scenario in relation to the provisioning (Class-of-Service, central services etc). In this case, the activation of the agent may be performed in the same seamless workflow. A single agent may be used to monitor multiple VRFs (VPN Routing/Forwarding instances) on a PE. The switch from one VRF to another may be implemented immediately and, preferably no configuration manipulation on the PE is required.

[1408] According to a further preferable embodiment, for the purpose of local maintenance the reports are accessible from a local web-based interface, the CPE Router Manager or from a third party system such HP OpenView or Spectrum via SNMP.

[1409] The agents are preferably integrated within the ISA Suite for VPN to allow the alarms to be remotely collected by a Service Fault Manager (ISFM), which is described in more detail below. The ISFM may be used to compile the results from all agents and may provide audit and accounting reports for example, by VPN domain, by customer, or by site.

[1410] While agents may be used to monitor the performance of the PE and CE links, a centralised module may also be implemented as part of the system to monitor the VPN service as a whole. A key role of the Service Fault Manager's (ISFM) is to manage the agents and to compile results from all

[1411] Service Emulation Agents (I-SEA) and deliver a consistent view of the VPN service performance for various purposes. In the VPN services context, ISFM is preferably located centrally and may be used to monitor, for example:

[1412] VPN connectivity, coordinating tests of each PE-CE link to ensure VPN connectivity. ISFM preferably supports full-mesh, hub-and-spoke or mixed topologies.

[1413] VPN network performance, coordinating tests of each of PE-CE link (for example delay, packet loss, jitter)

[1414] access to central services like internet access, mail, VoIP gateways etc.

[1415] access to management services

[1416] The ISFM's functions may include:

[1417] View of the VPN service outages, for immediate maintenance actions.

[1418] View of VPN service alarm details (e.g. time, date, subscribers). ISFM may also enable the creation of alarm severity thresholds based on percentage of impacted subscribers, the percentage of impacted gold subscribers, etc.

[1419] Access to alarm specific documentation, e.g. linking up to a Knowledge Management System (KMS). From a service outage, die ISFM may list all the suspected network elements (physical or logical). The KMS, as described herein, links the platform components to relevant documentations (for example, vendor manuals, URL, procedures, test

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 111

cases/results, engineering documents). It may also be used to link service alarms to the database which preferably provides a full description of each service alarm, a list of recommended actions to be taken by the user (operator, corporate client), and a list of documents related to the service alarm (URL, procedures, engineering documents). Finally, the ISFM may link the component alarms to the database which preferably provides a full description of each component alarm, a list of recommended actions to be

[1420] taken by the user (operator, corporate client) and a list of documents related to the service alarm (URL, procedures, engineering documents etc).

[1421] Performance of audit and report on daily, weekly or monthly periods for SLA per VPN domain, per customer or customer site.

[1422] Display of the list of the inpacted subscribers when interfaced with the IP database (or an external database), with details about their Class-of-Service (CoS) and the service they should be granted. This may allow pro-active customer care and prioritized resource allocation.

[1423] When interfaced with Imagine Component Fault Manager (iCFM), ISFM may perform conelation with Component Alarms to identify and short-list the suspected cause of the service outage.

[1424] In one embodiment, ISFM can be interfaced with a Trouble Ticketing system (i.e. Clarify) for the automatic creation of trouble tickets based on the severity of the service alarms.

[1425] The monitoring results are preferably accessible from two types of web-based presentation modules:

[1426] Service Operation Dashboard (SOPs) for the Network or Service provider

[1427] Customer Operation Dashboard (COPs) that may be offered by the network provider to the end user as an enhanced SLA feature. COPs may be implemented to offer direct access to some service assurance reports.

[1428] According to a preferred embodiment, both SOP and COP offer drill-down and graphical views of the VPN and sites, identifying the failing links and elements, for example by colours.

[1429] For full automation of the VPN service provisioning process, the JSFM may be interfaced to IIP VPN. When a PE-CE link is provisioned in IIP, IIP may generate the necessary instruction for the proper I-SEA agent to monitor the new PE-CE link with the right scenario and for ISFM to compile the results of this monitoring in the proper VPN.

[1430] When Service Fault Manager (ISFM) identifies a deterioration or an outage in the VPN services, ISFM may use a Component Fault Manager (ICFM) to shortlist the components potentially involved in the event. The ICFM preferably allows operators to collect and manage all platform component alarms from a single point. Correlation Engines may be used to correlate service alarms with component alarms to determine the component responsible for tle failure. ICFM can collect component alarms from any standard industry Element Management Systems (EMS) such as HP OpenView, BMC Patrol, IIP ITO, Micromuse Netcool, Compaq TeMIP, CiscoWorks or OSI NetExpert.

[1431] According to a preferred embodiment, a Java-based Presentation Module provides a sophisticated user interface designed for Network Operators and Administrators (NOPs).

[1432] Types of views available may include:

[1433] Location Explorer View: a graphical view of the platform network.

[1434] Alarm Explorer View: a view that shows the details of VPN services and their component alarms.

[1435] ICFM preferably allows reporting of component outage per vendor, equipment type, location or period and the ICFM preferably interfaces with KMS to help fixing the problem.

[1436] A Correlation Engine may further be provided to allow fault and problem management through, for example:

[1437] Correlation from service alarms to component alarms. From a service alarm, die correlation engine may determine the platform components that could be involved in the service outage and get the component alarms of the suspected components from EMS systems.

[1438] Correlation from service alarms to impacted VPN subscribers/users. From a service alarm, the correlation engine may be used to determine the users impacted by the service outage.

[1439] Advanced correlation capabilities, that involve an expert system with its rule set. It allows the operator to view only the component alarms that are relevant for the diagnosis.

[1440] The system may further be implemented alongside a CPE router manager, which may offer full access to remote VPN elements information and full access to the inventory database. The CPE router manager can preferably monitor a large range of equipment namely Cisco, Juniper, Riverstone and Unisphere and Nortel Networks.

[1441] According to a preferable embodiment the CPE router manager monitors the status of CE, PE and P routers of a particular user or VPN providing, for example user and subscription details, traffic history and on-demand polling. The polling function is preferably customizable, for example a group of selected equipment (i.e. serving the same VPN) can be polled at regular intervals for specified durations. The CPE router manager is preferably integrated with the ICFM and may allow remote debugging and fixing of faults, which may significantly reduce the lead time for outage resolution.

[1442] A VPN Network Manager may also be provided to monitor, report and generate alarms for MPLS and IPSec network performances. The VPN Network Manager may operate by polling the groups of physical and logical equipment on customized periods and duration. According to a highly preferable feature, the VPN Network Manager may be integrated with the IIP VPN. When a new PE-CE link is provisioned and activated via IIP VPN, the VPN Network Manager may be automatically updated with this addition. The VPN Network Manager may then poll this new link for

the metrics that have been defined for the VPN. The VPN Network Manager preferably monitors metrics specific to MPLS and IPSec technologies, as well as metrics common to the two, like memory and CPU usage.

[1443] For MPLS VPN services, VPN Network Manager is preferably arranged to poll the performance of the VPN network, for example per network equipment (physical or logical), per CE-PE routes and for the entire VPN. For each of these scopes some or all of the following metrics may be monitored: Jitter, Delay, Packet loss, Throughput, VRF availability. The VNP Network Manager may also monitor Quality-of-Service (QoS) metrics as traffic management, policy and Class-of-Service (CoS) split per equipment or VPN.

[1444] For a given VRF, the VPN Network Manager preferably also monitors traffic shaping and congestion with standards such as Generic Traffic Shaping or Frame Relay Traffic Shaping (providing history for queuing). The VPN Network Manager may also monitor the policy performance based on CAR and D-CAR.

[1445] In order to anticipate outages on the PE-CE links and based on DiffServ standards (RFC 2597 (AF), RFC 2598 (EF), RFC 2474 & **2475** (DSCP) and RFC 791, the VPN Network Manager preferably also provides statistics about the different Class-of-Services. This may be done, for example, per VRF, for reallocation of the workload, per CE, PE, P routers for creation of alternation links, per site, per VPN or per customer.

[1446] The VPN Network Manager may be arranged to monitor the network performance per CoS. The VPN Network Manager is preferably also designed to accommodate customized CoS, in particular those that are based on the DiffServ Standards.

[1447] IPSec MPLS VPN Services may be used in tunnel mode, which may allow the monitoring of metrics such as Jitter, Delay, Packet loss, Throughput and CE availability, for each of the created IPSec tunnels.

[1448] The VPN Network Manager is preferably implemented with a web-based interface with drill-down logical and physical network views for, for example, hourly, daily, monthly and yearly views. The views may be used to show the current situation and history for the provider administrative domain, the POP, the PE routers, the interfaces and the sub-interfaces. Due to its preferable VPN auto-discovery capabilities, the VPN Network Manager may also show the details for the customer VPN.

[1449] According to a further preferable feature, the VPN Network Manager may allow operators to define alarm generating thresholds for each of the monitored metrics. The monitoring reports may then be used by a Configuration Fault Manager for component fault isolations and by a Service Fault Manager for service fault isolation.

[1450] A Service Level Agreement (SLA) Manager may also be implemented as part of the system described above and may be used to measure customizable Key Performance Indicators (KPIs) and compare them with targeted VPN KPIs.

[1451] Major VPN service KPIs include:

[1452] Availability time for each service provided to users within the VPN. These services include Internet Access, mail, access to database or selected extranet sites, chat and Video-conferencing etc.

[1453] The service may be monitored per VPN, per PE-CE link (or IPSec tunnel), per location, per period (month, year).

[1454] The SLA manager may provide details about, for example:

[1455] The occurrence of service outage per service, per location or per period.

[1456] Performance of each VPN service (Response time, Bandwidth, QoS) per location of per period.

[1457] Time to repair after notification from the user, per severity of outage.

[1458] A comparison of the measured KPIs with targeted KPIs may be performed for each customer under a SLA. The SLA Manager preferably monitors and shows the KPI violation, identifies the time to fix a failure before the violation of the SLA and provides details about the remaining 'service non-availability' budget. The SLA Manager preferably orders the Service alarms based on, for example the risk of KPI violation and penalties incurred which may limit the risks of creating unreachable KPIs. According to a further feature, violation of the SLAs can be notified to the customer account manager and the customer by mail or web server notification. SLA reports can be generated for use in Crystal Reports or through a web interface.

[1459] A summary of some advantages of the ISA Suite for VPN is provided below:

[1460] A network operator can access a unique and immediate view of the service delivered to the network user.

[1461] The ISA suite provides seamless integration with pre-existing Provisioning Suites for VPN.

[1462] The ISA suite removes Complexity from the OSS and from VPN service assurance, providing fast access to critical information: impacted customer listings for pro-active customer care actions, service to component correlation for short-listing of the suspected failing elements andl immediate access to the necessary documents.

[1463] ISA Suite for VPN reduces the VPN network complexity with context-sensitive help and views of the service delivered to the user. ISA Suite for VPN interfaces with the most popular OSS and Network Management systems.

[1464] The ISA suite allows fast remote diagnosis since it allows remote access to the PE and CE and P routers in the VPN and also provides a wide range of tools supporting a large range of vendor equipment, protocols, standards and technologies.

[1465] Flexible and Scalable deployment scenarios may be implemented and a suite of stand-alone agents, may be positioned at critical points in the network. The ISFM may further offer customizable Front-Ends for customer self-care, service provider, network provider with granular lights and full integration of legacy systems.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 113

[1466] The Configuration Manager

[1467] The methods and systems described herein may further be implemented in conjunction with a configuration manager, which may be implemented to automate the configuration steps for providing services to users in a broadband network whilst maintaining flexibility in the configuration process and adapting to future evolution in the broadband environment.

[1468] According to a preferred embodiment, the Configuration Manager simplifies all the configuration steps to a command sentence from a Verb/Entity/Attributes (VEA) language. The VEA language provides a grammar which applies a verb on an entity, and qualifies a verb with an attribute. According to a preferred embodiment, the entity is the equipment, the verb is the action and the attribute is the configuration parameter set. Use of the VEA language reduces the risk of configuration errors in the configuration process. The entities, verbs and attributes are preferably dependent on the provider and module in use (i.e. MPLS or IPSec). Each module may be provided with a vocabulary description or dictionary and each backend preferably has a well-defined interface that is coupled with a dictionary. The dictionaries may also be enhanced with new 'entities' (i.e. equipment), new 'verbs' and 'attributes' (i.e. new protocols).

[1469] The configuration manager may also be provided with a template library, which classifies the templates in association with the hardware platform, the software version, the functionalities and the context. The templates can be created from multiple sources, for example MS Excel spreadsheets, manual entry or the IIP VPN module. The template library may allow replication of the configuration to many devices, or to the same device multiple times.

[1470] An example of the operation of one embodiment of the configuration manager is provided below by way of example. When the operator provisions a VPN element, preferably using the VEA syntax, the Configuration Manager automatically selects the correct template from the template library, calls the necessary information about the impacted equipment from an Inventory Manager, creates the proper un-do actions and generates the new configlet. The Configuration Manager may then notify the operator who visualizes the changes and commits the action, requesting the Configuration Manager to deploy the new configuration to the group of devices using various methods like telnet, tftp, ftp, SNMP, and others. The Configuration Manager then preferably audits the deployment and provides a selection of potential remedies when errors are identified. Once deployed, Configuration Manager may save and edit the version of the new configuration. Preferably, the Configuration Manager can be emulated by the IIP VPN scheduler for 'just-in-time' configuration.

[1471] **FIG. 62** illustrates one embodiment of the architecture of the Configuration Manager and the integration of the Configuration Manager into a VPN provisioning network.

[1472] VPN Provisioning

[1473] A further aspect of the provisioning methods and systems disclosed herein may be the provisioning of VPN services. Advantageously, the VPN provisioning system described herein is vendor-agnostic and enables central or distributed end-to-end VPN provisioning from a single front-end.

[1474] The VPN provisioning system (IIP VPN) may be implemented as a stand-alone system, but is preferably implemented with other systems and tools described herein. **FIG. 63** illustrates how the VPN provisioning system may be incorporated into a network according to one embodiment of the systems and methods described herein.

[1475] According to a preferable embodiment, IIP VPN automates the end-to-end process of provisioning customer, service and management MPLS and IPSec VPNs regardless of the routing equipment in the network.

[1476] According to a preferred embodiment, the IIP VPN operates as outlined below: the IIP VPN receives the business service requests from the operator's CRM or from the network provider's IIP VPN front-end. The operator provisions the PE-CE links or tunnels and the associated Quality-of-Service (QoS) level completing assisted fields. It then deploys the configurations that activate the new MPLS and IPSec VPN service.

[1477] Preferably, the IIP VPN can preferably check the CE/PE configuration by executing a static audit. It can also generate an I-SEA agent scenario that will test the full VPN service, for example testing the links, the QoS and the security. 'Just-in-time' activation of the VPN services may be provided by scheduling the download or upload of the configurations to the CE or the PE. A record of the actions is preferably maintained by OSS database, which may allow roll-back or undo of the configurations.

[1478] A Software Development Kit (SDK) may allow the network provider to offer web-based, user-friendly interfaces to service providers or to end users for self-activation. It may also keep direct access to the CLI for batch edition.

[1479] According to a further preferred feature, IIP VPN fully integrates with the network provider's systems for billing and customer management and may further be provided with reporting capabilities, which may include graphical views of the VPN, status and metrics reports which are useful in meeting Service Level Agreement (SLA) targets.

[1480] IIP VPN is preferably built around a modular IIP infrastructure. Some or all of the following elements may be used to enable MPLS and IPSec VPN seamless provisioning:

[1481] The IP VPN SDK

[1482] The IIP VPN SDK allows flexibility in creating automated configlet templates to be used for provisioning, for example PE-CE (Provider Edge—Customer Edge) links and the QoS definition for MPLS VPN, the IPSec tunnel endpoints, the security and authentification methods. The flexibility is achieved by allowing a network operator to independently design the automation of its provisioning workflow and the alteration of PE/CE configlets. This may allow a system in which no re-compilation of the application is necessary unlike in prior alt automated provisioning systems. This may allow The network provider to keep to its current provisioning workflow and to

[1483] independently plan its evolution.

[1484] Templates from OSS and BSS systems are preferably used to limit the number of necessary actions in the provisioning and to automatically complete the maximum number of parameters in the configlet.

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 114

[1485] Three scenarios that may occur while creating a new configlet template are discussed below by way of example.

[1486] 1. The change is made to the configlet template and does not imply any change to the parameters; for example it may be the case for NTP and SNMP. In this case, the network engineer may save the changes in a template library, which allows the IIP VPN to provision these devices with the updated configlets in an automated way. In this scenario, only the network engineer is needed to make the modifications, no additional expertise is required.

[1487] 2. In the second scenario, the network provider can decide:

[1488] to adapt its provision workflow; the network operator may decide to add a QoS provisioning step in the workflow, reflecting an enhancement of its commercial offer.

[1489] to manually modify a parameter in the configlet; it can be a change of the IP address or a new RT.

[1490] As in the previous scenario, the network engineer can modify the configlet template. The IIP VPN administrator may then update the IIP VPN VEA dictionary and the IIP VPN back-end may be stopped and restarted to have the modifications activated for the future automated provisioning. In this case again, the network provider can evolve its configlet library with limited expertise required.

[1491] 3. In the final scenario, the network provider uses parameters that are generated by an algorithm. It can be, for example an IKE hash algorithm for tunnel endpoints authentication for

[1492] IPSec VPN. The network provider may then use the SDK to implement the new "methods" used by the IIP VPN VEA dictionary to automatically retrieve the new parameters. The network engineer may create the new configlet template and the administrator may update the IIP VPN VEA dictionary with the new methods. The IIP VPN back end may then be stopped and restarted to active the changes. The network provider has the capability to independently complete this task using its own Java specialist who has been trained to the IIP VPN SDK.

[1493] As shown in the examples above, the network provider has the independence to evolve its provisioning automation process with very limited dedicated expertise resources, without complexity, and in a very short timeframe.

[1494] The IIP VPN SDK is preferably provided with a template library. Preferably, by means of the IIP VPN SDK, the network provider can independently organize the template library according to the scope of the template's use. The template library may be used as a repository for predefined configlets. According to a preferred embodiment, the library is based on a drill-down tree structure and reflects the following organization:

[1495] Site

[1496] Client

[1497] VPN

[1498] Operator Site

[1499] Operator Network

[1500] All operators

[1501] This structure can preferably be customized to ease the retrieval and use of the configlets for specific deployment purposes.

[1502] A Verb Entity Attributes (VEA) Dictionary may also be deployed as part of the provisioning system. According to a preferred embodiment, the IIP VPN VEA dictionary contains four major functions:

[1503] The Creation function, addresses the MPLS backbone (Traffic Engineering).

[1504] The Provisioning function is usually divided into the following 3 steps but the network provider can create additional steps to reflect its service creation workflow:

[1505] 1. The pre-provisioning of the PE and CE

[1506] 2. The provisioning of the VPN

[1507] 3. The provisioning of the QoS

[1508] For IPSec VPN provisioning, the steps preferably include:

[1509] 1. Traffic flow selection

[1510] 2. Choice of the security parameters

[1511] 3. Choice of the VPN topology and selection of the endpoints authentication methods

[1512] When pre-provisioning a PE or a CE, the right configlets should be used or instantiated for edition of the parameters. When the creation of a new configlet template is necessary because of the evolutions of the VPN service offer or because of the technology, the configlet may then be saved into the VEA dictionary for future use. This process optimizes the automation of the provisioning and gives flexibility to enrich the VEA library with additional configlet templates.

[1513] The Inventory function may provide static views of the VPNs and PE/CE equipments per Customer, per VPN, or per site.

[1514] The Reporting function may provide SLA oriented information about the VPNs, the CE/PE, and the provisioning dates. This reporting function preferably interfaces with the I-SEA Suite for MPLS and with Cisco SAA to report about the VPN service provisioning performance.

[1515] In addition to the IIP VPN Configuration Manager and SDK, other modules may be solicited in the provisioning flow.

[1516] A further element that may be used in MPLS and IPSec provisioning is the EB OSS Database

[1517] The OSS database may be used to modelize the network and systems infrastructure and maintain the configurations of the CPE, the customer and user information and the service details. The database is preferably implemented as a high availability database, may be based on Oracle and preferably follows the JTU M3100 recommendations for redundancy and data integrity. It preferably

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 115

works on an active-active mode and offers a full back-up, recovery for 'instances' and data protection. **FIG. 64** illustrates one embodiment of the OSS database with the high availability cluster in active-active mode.

[1518] Inventory Manager

[1519] IIP VPN preferably uses the inventory capabilities of an Inventory Manager. The Inventory Manager's primary role is to monitor the CE, PE and P routers availability and their configurations, in order to support the link or tunnel creation. The SDK may collect information, such as that outlined below, from the Inventory Manager:

[1520] Physical and logical inventory of the network elements

[1521] Configuration inventory of existing VPNs

[1522] IP Routing used

[1523] Capacity: PE and CE interfaces, VRF capacity per PE.

[1524] Location and topology information

[1525] QoS

[1526] In the context of Layer 2 MPLS VPN, the Inventory Manager preferably collects the PE and the CE endpoints configuration (CE ID, CE range, logical circuits, node colours and role).

[1527] The IIP VPN provisioning system is preferably implemented in conjunction with an IP Address Manager, which is described in more detail herein. IIP .VPN nay use the IP Address Manager to get the PE, CE, P router IP addresses, and the subnets in the network. Specifically for MPLS VPN, the IP Address Manager preferably also provides:

[1528] the Route Distinguishers (RD) and Route Targets (RT) current assignments

[1529] BGP Autonomous Systems Network elements

[1530] The routing context of VPNs

[1531] The VRF routing tables

[1532] For IPSec VPN, the IP Address Manager preferably provides:

[1533] The subnets details for identifying the traffic that will be protected.

[1534] The IP Address of the equipments that will serve as tunnel endpoints.

[1535] The IIP VPN is preferably also implemented in conjunction with a Configuration Manager, which may be used to create, add and edit the configlets per MPLS or IPSec domain. The Configuration Manager may also create the RD and the RT and configure the VRFs. For IPSec VPN provisioning, Configuration Manager preferably leverages a system such as Cisco's IOS to select the traffic flows. It may then edit the security parameters (IPSec and IKE), the VPN topology, the authentication methods (e.g. pre-shared keys or PKI) and apply them to the CEs. All common IPSec and IKE security algorithms are preferably supported by IIP VPN and Configuration Manager preferably negotiates new keys regularly and provides authentication services.

[1536] According to a preferred embodiment, the Configuration Manager allows multi-device and multi-vendor configuration in one step, for example Cisco IOS PE and CE, Cisco VPN 3000/5000, Juniper and Nortel PE/CEs. The Configuration Manager preferably uses the VEA (Verb Entity

[1537] Attributes) language, which may be used to simplify the configlet creation. With the VEA, the operator uses a simple syntax for editing the configlet. However, the use of the VEA does not prevent the operator from immediately accessing the Command Line Interface (CLI), which may be useful for editing batches.

[1538] Once created, the configlets can preferably be downloaded to the VPN network elements via multiple technologies, for example TFTP, Telnet or FTP.

[1539] The Configuration Manager preferably provides a scheduler feature which may allow 'just-in-time' provisioning and activation of the VPN and planning capabilities. In the context of Managed Network Services, where the service provider delivers the CE to the customer, the scheduler may allow automatic activation of the service. The scheduler preferably also limits the necessary operator actions when BGP dampening parameters are configured in the CE or the PE.

[1540] According to a further preferable feature, the Configuration Manager may also enable static audits of the configuration. These static audits may be used to check that the configuration of the router has not been modified during the 'instantiation'. The Configuration Manager preferably also provides a repository for the configlets allowing roll-back and undo of the configlets. The roll-back action can be associated to the scheduler.

[1541] The Front-ends of the IIP VPN According to one Embodiment are Described below.

[1542] The web-based front-ends may be built and customized from a front-end SDK and may be connected to one or multiple back-ends.

[1543] Three kinds of front-ends are usually defined:

[1544] A Network Provider front-end

[1545] A Service Provider front-end; when the VPN service is not delivered by the network provider

[1546] A Customer front-end; offering self-provisioning capabilities.

[1547] Each of these front-ends can preferably be customized to allow different levels of access and rights. By means of the SDK, the network provider can preferably develop the screens and the flows, to reflect the rapid changes in the offering or infrastructure. The front-ends are the interfaces for accessing the graphical views of the VPNs, which may include:

[1548] CPE to CPE tunnelsfor.IPSec.VPNs.

[1549] PE and CE views or CE to CE views for MPLS VPNs

[1550] The GUI Command Line Interface is preferably accessible fi-om the front-ends for the creation of batches.

[1551] I-SEA Suite for VPN

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 116

[1552] The IIP VPN is preferably implemented in conjunction with agents, which may be used to test and monitor VPN services. The agents are also described herein in more detail. The I-SEA agent preferably executes a "round robin" scenario where the features of the created VPN may be tested. The agent can preferably test, for example the PE and CE links and tunnels, the security, the QoS, the performance by Class-of-Service and the central services (such as mail, internet access, VoIP, etc). It may also be used to monitor the management links and services. A single I-SEA agent can be used to monitor multiple VRF on a PE. The switch from one VRF to another is preferably immediate and operation on the PE is not required. The I-SEA agent preferably also offers a web interface for direct access and creation of the scenario.

[1553] The alarms may be collected by a Service Fault Manager (also described in more detail herein) which may be used to compile the results from all ISEA agents and provide audit and accounting reports. The reports are preferably accessible from two web-based interfaces for customer operation and service operation.

[1554] The IIP VPN system is preferably implemented in conjunction with a Component Fault Manager for MPLS.

[1555] The Component Fault Manager preferably collects and manages all platform component alarms (for example, Micromuse, HP ITO, Compaq TeMIP, BMC Patrol). The Component Fault Manager is preferably associated with the Service Fault Manager and maybe used to correlate the service and component alarms to identify the failing component. A Java-based presentation module preferably provides a sophisticated user interface designed for Network Operators and Administrators (NOPs).

[1556] MPLS Network Manager

[1557] The MPLS Network Manager, if required, can be used to monitor the traffic engineering of the VPNs.

[1558] One example of an MPLS VPN Provisioning Flow is described in the numbered steps below.

[1559] 1. The network engineer creates a new Business Service Request (BSR) for a customer, describes it and assign it to an operator.

[1560] 2. The operator creates a new site for the customer.

[1561] 3. The operator initiates the PE-CE link provisioning by selecting the parameters from the predocumented fields.

[1562] 4. The operator executes a visual check of the created configlet and saves it.

[1563] 5. The operator selects the L3 parameters, executes a visual check and saves it.

[1564] 6. The new configuration can then be manually submitted.

[1565] 7. Alternatively, the new configuration can be automatically submitted from the GUL

[1566] 8. The operator then runs the static audit of the configuration.

[1567] 9. The operator adds a VPN to the PE-CE link that he has created. He visually checks the new configlet.

[1568] 10. The operator enters the routing parameters, operates a visual check, and saves the parameters.

[1569] 11. The operator enters the QoS parameters, for example traffic marking, congestion avoidance and class-of-service.

[1570] 12. He operates a visual check, submits the configuration to the PE and CE and runs a static audit The VPN is ready.

[1571] 13. The operator can request a report for the new specific VPN. He will access the details of the PE and CE elements which belong to the VPN.

[1572] The IIP VPN is preferably designed to be multi-technology compliant and is preferably based on the well-established IETF standard RFC 2547 Bis for MPLS-based VPN, and the following routing protocols: RIP v2, BGP, Multi-protocol BGP (BGP-MP), Static routing and OSPF. IIP VPN can preferably provision IPSec-based VPN and automate the provisioning of IP-Sec tunnels encapsulation into MPLS VPN, a configuration that is well adapted to LAN-to-LAN VPN services. In addition to ATM and Frame-Relay, IP VPN preferably supports a large range of Layer 2 technologies, such as PPP, DSL, Optical Ethemet and HFC. IIP VPN is preferably designed to be vendor-agnostic. In particular, because of its flexible template edition capabilities, IIP VPN can activate MPLS VPN services on a large range of routing equipments, such as Cisco Systems, Juniper Networks and Riverstone Networks portfolio. This compliance makes IP VPN particularly suitable for use in MPLS VPN service provisioning in heterogeneous networks.

[1573] IIP VPN can preferably be implemented to provision any kind VPN topologies, for example: fullmesh, hub & spoke or partial-mesh VPNs for extranet applications lip VPN may provision one or multiple PE-CE links, managing the attributes of the BGP routing protocol. This may allow, for example, the following connectivity patterns:

[1574] A CE single-homed and non-redundant as connected to one PE interface.

[1575] Two CE dual-homed with HSRP on one PE interface.

[1576] Two physical interfaces on a CE interfacing to two PEs offering partial redundancy.

[1577] Two CE dual-homed with HSRP on two PEs offering full redundancy.

[1578] In addition, IIP VPN may provision ISDN redundancy solutions for single-homed, non-redundant configurations.

[1579] Quality-of-Service Provisioning:

[1580] In order to address the need for tiered VPN links, IIP VPN may further enable the provisioning of QoS features associated to PE-CE links.

[1581] Class-of-Service (CoS):

[1582] In an MPLS environment, the CoS is enforced on both the PE and the CE. IIP preferably uses imported ACL for defining and applying multiple traffic classes per sub-

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 117

scriber or defining QoS profiles with pre-defined CoS allocation. In this case there is preferably one QoS profile per subscriber. With the imported ACLS, IIP VPN may offer a user flexible requirements and preferably complies with DiffServ's CoS standards-RFC 2597 (AF), RFC 2598 (EF); RFC 2474 & **2475** (DSCP) and RFC 791.

[**1583**] Traffic Shaping and Congestion Management:

[**1584**] In order to complement the CoS capabilities, MPLS IIP VPN preferably handles the traffic shaping configurations by configuring the PE or the CE egress interfaces and marking the traffic with D-WRED and Generic Traffic Shaping (GTS). IIP VPN preferably handles Frame Relay Traffic Shaping (FRTS) for Frame-Relay with the associated queue management protocols WQF, CBWQF, customed queuing (CQ), priority queuing (PQ), PQ-CBWFQ (LLQ) and the non-Frame Relay specific Generic Traffic Shaping (GTS) associated with complementary Frame Relay traffic shaping protocols; Forward Explicit Congestion Notification (FECM) and Backward Explicit Congestion Notification (BECN).

[**1585**] Policing:

[**1586**] As for traffic shaping, IIP VPN may configure the PE or the CE egress interface with policing configuration. IIP VPN preferably uses Committed Access Rate (CAR) and Distributed Commintted Access Rate (DCAR) protocols.

[**1587**] As a further feature of a preferred embodiment, the IIP VPN can provision Layer 2 MPLS VPNs following the IETF drafts 'Martini' and 'Kompella'. Leveraging 'Kompella' auto-discoveiy capabilities (BGP-MP) and Inventory Manager, IIP VPN preferably identifies die membership set of the VPN context and processing intended to receive the new VPN information. The Inventory Manager may then collect the topology information; the details related to the endpoints connectivity and the 'reachability' (VPN routes in the VPN space) that may be used by IIP VPN.

[**1588**] IIP VPN uses 'Kompella' CE indexation membership scheme which includes, for example:

[**1589**] The VPN ID

[**1590**] The CE ID

[**1591**] The CE range, the number of CE within the VPN

[**1592**] The Logical Circuits (e.g. DLCI or VLAN)

[**1593**] The node colour that has to be shared for connectivity

[**1594**] The role (Hub or spoke)

[**1595**] The L2 MPLS VPN provisioning preferably follows the L3 MPLS VPN workflow. IIP VPN preferably provisions the logical circuit, the node colour and the role of the CE. These 'connectivity' parameters preferably serve a similar purpose to LDP signalling in L3 MPLS VPN. The colour of the node and the role of the CE parameters preferably permit VPN topologies other than full-meshed. The provisioning workflow is easily adapted to the L2 MPLS VPN provisioning requirements with the IIP VPN SDK.

[**1596**] IPSec VPN

[**1597**] In the context of IPSec VPN provisioning, IIP VPN may be used to provision IPSec services and may be used in particular but not exclusively, to provision services with the following two protocols:

[**1598**] Authentication Header (AH), RFC 2402

[**1599**] Encapsulation Security Payload (ESP), RFC 2406

[**1600**] Using the AH protocol, IIP VPN can provision IPSec VPN using MD5-HMAC and SHA-1-HMAC authentification algorithms. Using the ESP protocol, IIP VPN can provision IPSec VPN using 56-bit DES, 3DES and should support Advanced Encryption Standard (AES). It may also provision authentication configlets using Blowfish.

[**1601**] IIP VPN can preferably Accommodate the Different modes of IPSec:

[**1602**] Tunnel Mode for passing security gateways when the destination host doesn't support IpSec as the IP packet is encapsulated into AH or ESP and then headed with a new IP header.

[**1603**] Transport Mode where the AH or ESP is placed after the IP header.

[**1604**] For authentification and key management, UP VPN preferably allows manual keying or the use of IKE with the following mechanisms:

[**1605**] Pre-shared keys where the operator manually enters the same key on each peer.

[**1606**] Encrypted nonces where the asymmetric key is generated on a peer, collected by IIP VPN and copied to the other peers.

[**1607**] Digital certificates where die key is generated by the certificate authority (CA) and pre-fed into IIP VPN.

[**1608**] IIP VPN preferably also provides the necessary templates for the automation of the IPSec VPN configlet edition.

[**1609**] Some of the benefits and advantages of the IIP MPLS VPN system are outlined briefly below:

[**1610**] End-to-end and Seamless VPN Provisioning from a single Front-End may be provided IIP VPN preferably provisions MPLS and IPSec VPN on multi-technology access and edge from single customizable front-ends. The same tool may be used for, for example, Frame-Relay, xDSL, Cable, Optical customers, for MPLS/BGP VPN, Layer 2 MPLS VPN and IPSec VPN.

[**1611**] Web-based and CLI Front Ends. IIP VPN SDK preferably allows flexible adaptation of the templates, workflow and front-end screens to the network operator situation. The network provider can offer GUI front ends to the service providers and self-activation to the customers. In addition, the network provider can implement VPN service provision through batches generated in the GUI CLI.

[**1612**] The IIP VPN system is both scalable and distributed.

[1613] Flexible SDK-based. According to a preferred embodiment, the network operator can easily evolve the activation modules, the interfaces reflecting the changes in the workflows, infrastructure, service offering.

[1614] The system is preferably operationally integrated with the BSS and OSS modules, which enables timely and precise billing and customer support. Interfaced to CRM systems, IIP VPN allows flexible changes of, for example the QoS, the customer CoS, the service pack, VPN.

[1615] IIP VPN is preferably compliant with multiple-vendors, multiple-routing protocols, multiple-OS and hence facilitates the provisioning of VPN services in a heterogeneous infrastructure.

[1616] It will be appreciated by the skilled person that there have been described herein numerous aspects and preferred features, including independent methods, tools, agents, interfaces, particularly graphical user interfaces, services, data products for use in a variety of communications problems, including without limitation provisioning and related activities, capacity planning, service monitoring, component monitoring, device management and the like. As apparent and as discussed, some of these may combine synergistically with other features and indeed may enable provision of novel services and applications. However, for the avoidance of doubt, unless otherwise stated, all features disclosed herein, whether as aspects, clauses, features explicitly stated to be preferred, claims or simply as individually identifiable preferred features may be provided independently of other features. In particular, whilst many features have application to provisioning of services and can offer significant advantages in combination with a provisioning application or method, it will be appreciated that these may be applied independently. The examples given have included a variety of broadband communications protocols, including cable modem access, DSL, VPN purely by way of example. The features techniques and tools etc disclosed herein may be applied to other hardware configurations or communications modes, if necessary with changes as will be apparent to the skilled person.

[1617] A large number of features have been described and in several places the foregoing has provided numerous lists of preferred or optional features, for example in relation to sample actions or functions that may be performed, data that may be stored, displayed or communicated, parameters that may be monitored or changed, options that may be provided. In all lists of preferred features herein, unless otherwise explicitly stated, whilst provision of the complete set of features as listed may be advantageous, it is specifically intended that any one of the features listed, or any sub combination, may be provided independently of other listed or accompanying features. The advantages of providing any said features independently will be apparent to the skilled person and may not therefore have been stated explicitly in the interests of conciseness. Whilst described and applied to advantage in a broadband context, where problems peculiar to broadband communications may be solved, aspects and features of the invention may be more generally applied.

1-265 (Cancel)

266. A method of providing an assured service to a user via a virtual private connection in a distributed network, the method comprising providing an agent in the network and configuring the agent to monitor the virtual private connection by simulating communication over the connection.

267. A method according to claim 266 wherein the agent is arranged to reside on a node of the network other than the user's end node.

268. A method according to claim 266 wherein the agent is arranged to receive configuration information identifying a connection to monitor.

269. A method according to claim 266 wherein a single agent is arranged to receive configuration information identifying a plurality of independent connections to monitor.

270. A method according to claim 266 wherein the method further comprises configuring the agent to pass a fault report to a remote network monitoring component in the event that a fault is detected in the provisioned virtual private connection.

271. A method according to claim 266 further comprising provisioning a virtual private connection based on provisioning information.

272. A method according to claim 271 wherein configuration information is sent to a pre-existing agent.

273. A method according to claim 271 wherein an agent is launched if no pre-existing agent is available to monitor the provisioned connection.

274. A communications network management system, which system comprises:

a. an input for receiving fault reports in respect of a network and/or one or more services supported by a network,

b. a data store for storing data in respect of said network and/or services,

c. a fault processor for processing fault reports received via the input, using data stored in the data store, to generate corrective solutions, and

d. a simulator for triggering a service provision response by the network wherein the simulator has an output to the network to trigger a service provision response, such that a fault report in respect of said response will be received at the input and processed by the fault processor.

275. A communications network management system according to claim 274 which further comprises means to apply a generated corrective solution to the network and to trigger a service provision response by use of the simulator such as to validate the applied corrective solution.

276. A communications network management system according to claim 274, wherein said input for receiving fault reports is adapted to receive both fault reports in respect of services provided by said network and component alarms from components of said network, and said fault processor comprises a correlation engine for correlating received fault reports in respect of one or more services with received component alarms.

277. A communications network management system according to claim 274 wherein the data store is structured to hold one or more problem descriptions in addition to one or more fault reports and/or one or more component alarms, at least one stored problem description comprising data received in respect of historic component behaviour, said fault processor being adapted to access data received in

Zoho Corp. and Zoho Corp. Pvt., Ltd.
Exhibit 1023 – 119

respect of historic component behaviour for use in processing fault reports to generate one or more corrective solutions.

278. A communications network management system according to claim 274 wherein the data store is further structured to store customer data in relation to services and the fault processor comprises a correlation engine for correlating received fault reports in respect of one or more services with customer data, and wherein the fault processor further comprises sorting apparatus for sorting fault reports in an order determined by correlated customer data.

279. A communications network management system comprising a fault detector and fault processor for detecting faults in the network or services provided over the network, and for analysing detected faults with the purpose of generating solutions to the faults, wherein the system further comprises means for providing context sensitive help for providing information to the user in relation to one or more faults being analysed.

280. A system according to claim 279 wherein said means for providing context sensitive help comprises a knowledge management system having a search engine, the search engine being arranged to run a search on data stored for the knowledge management system, said search being based on the one or more faults being analysed.

281. A system according to claim 279 wherein the system is provided with a data store for storing data in respect of said network and/or services and processes fault reports in the light of stored data to generate corrective solutions to received fault reports, wherein the system is further provided with at least one simulator for requesting service provision over the network such that the network and one or more services can be proactively tested.

282. A system according to claim 281 further comprising means for adjusting at least one service provisioning parameter for at least one user.

283. A system according to claim 281 wherein the simulator simulates user activity.

284. A system according to claim 281 wherein the network is a broadband communications network.

285. A system according to claim 281 wherein the simulator is provided by an agent associated with a network component.

* * * * *