Web-based Configuration Management Architecture for Router Networks

Hosoon Ku, Jan Forslow and Joon-gil Park

Ericsson Inc.
Datacom Networks and IP Services
1555 Adams Dr. Menlo Park CA. 94025
Tel: 650-463-6988, Fax: 650-463-6755
E-mail: {hosoon.ku, jan.forslow, joon-gil.park} @ericsson.com

Abstract

As networks grow in size, speed and complexity, the role of network management becomes increasingly important. Network management is the ability to monitor and manage all network elements, ensuring availability, optimal performance, and reliability. A high level of automation in network configuration and management is a critical issue in today's rapidly growing IP networks.

In this paper we describe a web-based secure configuration management architecture for Internet backbone router networks and discuss on the implementation. A framework for web-based configuration management is suggested by using secure protocols and a centralized database. It provides a simple and powerful way of configuring backbone router networks, which is accessible from any platform by combining Web and Java technology. The suggested architecture achieves a high level of security, and reduces complexity in network configuration without adding any functions on the managed entity. Semi-automation of network configuration is accomplished by using pre-defined configuration templates and by intelligent validation of the router networks.

Keywords

Web-based Network Management, Configuration Management, Network Validation, Gigabit Router Networks, Protocol View

1. INTRODUCTION

The current Internet is a collection of Internet Service Providers (ISP) which have connection points called Point of Presence (POP) over many regions. Normally, an ISP is considered as one Autonomous System (AS). ISPs are exist in many shapes and sizes, sometimes defined in terms of 'tiers' or 'level' depending upon whether they are backbone service providers for other ISPs, or whether they deploy customer Internet connections directly to customer premises. To enable customers of one provider to reach customers of another provider, a Network Access Point (NAP) is defined as

interconnection point. Today, the experimental four-node network connected via 56 kbps circuits which started 30 years ago, has been enormously expanded and grown to thousands of networks composed of OC3/OC12 links connected via high-speed ATM switches or Internet backbone routers. [1, 2]

Gigabit routers are one of the core equipment connecting different networks in the Internet. The routers are traditionally configured and maintained manually with Command Line Interface (CLI) via a *telnet* session. The configuration results often remains at the device itself and configuring several routers at the same time without any graphical tool is a time consuming and complicated process. Configuration management involves initializing, maintaining and shutting down individual network devices in the core network. The configuration management is also responsible for monitoring the configuration and making changes according to request. The main functions of configuration management can be identified as follows:

- define the configuration information, in our case the specification of the backbone router
- set and modify the configuration information
- define and modify the association between link and router
- initialize and terminate the operation of network devices

The Configuration Management (CM) is generally highly cost, element specific, error prone and can cause serious performance problem even on a simple mis-configuration. The motivation and main goal of this project is to design management architecture and a tool that provide an easy and fast, yet secure and reliable way of configuring Internet backbone router networks.

2. MANAGEMENT FUNCTIONS FOR A GIGABIT ROUTER

Figure 1 shows the overall router management functionality, which needs to be considered for the complete management suite. The complete management system consists of a Network Resource Manager (NRM), a Service Level Manager (SLM) and optional external systems. In this paper, we will focus on the configuration management covering Config display, multi-protocol topology, validation and import/export, which are main components of the NRM.

The NRM interacts with the routers using Secure Shell (SSH) in order to import and export configuration files. The Network Resource Manager is also providing an interface to Service Ordering System such as Customer Care Billing System or Virtual Private Network management solution etc. The NRM provides four components for network configuration:

- The *Config* Displays provides an Explorer-like GUI to all configuration information.
- The Validation makes it possible to do integrity checks on the network configuration.
- The Multi-protocol Topology is used to display the proposed configuration in detailed subviews related to individual routing protocols.

- Import/Export are used for transport of the configuration and data conversion

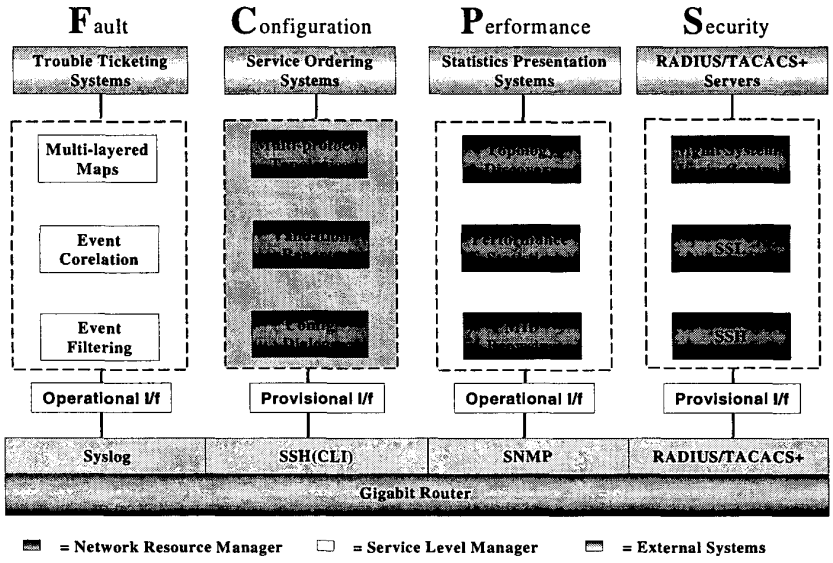

Figure 1. Router Management Functional Diagram

Security is enforced at every level. Secure Shell is used as a transport mechanism between a router and the network management server, while Secure Socket Layer (SSL) is applied between the management server and a client's Graphical User Interface (GUI) applet. The intuitive explorer-like graphical interface simplifies the entire process of router configuration. The *login* keys on each router can be administered through an external Remote Authentication Dial-In User Service (RADIUS) and Terminal Controller Access Control System Plus (TACACS+) server. [3]

The Management Server uses the router's Command Line Interface (CLI) to load and commit new configuration files. A special module for storing template and neighbor configuration files exists on the management server, which is utilized for validation of devices on several Routers in order to verify the configuration of the router. The Management Server allows the operator to test configurations and changes off-line before committing them to the live network. To summarize, the provisioning part of the Management Server provides:

- Explorer-like user friendly Configuration Displays.
- Protocol-sensitive Topologies.
- Configuration Syntax Checking.

- Network Integrity Checking (Validation).
- Audit Configuration Changes.
- Export/Import of Configurations via SSH.

The Web-based Enterprise Management (WBEM) initiative is an effort driven by Distributed Management Task Force (DMTF) [12] to help organizing distributed computing systems based on industry standards. The goal of WBEM is to provide a simple, scalable, platform independent and cost-effective way of accessing management data by using WEB technology as a common base for systems management. On top of existing management standards and protocols, WBEM proposed new set of standard for object data model called Common Information Model (CIM) Schema and communication protocols designed to run over HTTP etc. [13, 14]. Since WBEM initiative had been started many researches have been done and several Web based NMS tools are available today [16, 17, 18]. Nevertheless most of the Web-based NMS are focusing on SNMP based performance monitoring, trap oriented event correlation, trouble ticket and customer care systems and Web-based configuration management tools are hard to find in the industry [15].

Most of the existing Web-based management systems provide element management to configure and monitor devices by embedded Web server. In our proposal, the Web server is separated from the devices and 3-tier architecture is used to focus on the "network" management not on the element specific management.

3. MANAGEMENT SYSTEM ARCHITECTURE

The configuration management architecture is based on a stand-alone Management Server system. Such management architecture avoids porting a Web Server and Java Virtual Machine (JVM) to the target Routers, thus shortening the time to delivery and reducing the complexity of the network elements. The Management server uses the SSH protocol for secure access the routers for importing and exporting the configuration files. SSL encryption is be applied between the browser and the Management server as long as the web server provides the service. Each user of the Management server is authenticated with userID and password. Message Digest (MD5) algorithm is used for password encryption. The administrator can assign different levels of privileges to each user.

This architecture has the advantage of allowing certain level of network management activities in the standalone management system, such as validation of proposed configuration file, import of configuration data from same interface type on several routers, calculating and displaying subnets/routing areas before export into networks, etc. The Management Server is a Java-enabled platform equipped with a Web server and GUI applets that can be downloaded and executed from any browser. The Management Server system is scalable and capable to configure and monitor up to hundreds of network elements.

Figure 2 shows a simplified interaction scheme between the Browser GUI (Configuration applet), Management Server and the Router. The core of the Management

Server consists of a Web server, servlets, Database engine, Topology server, Validation engine and Import/Export component.

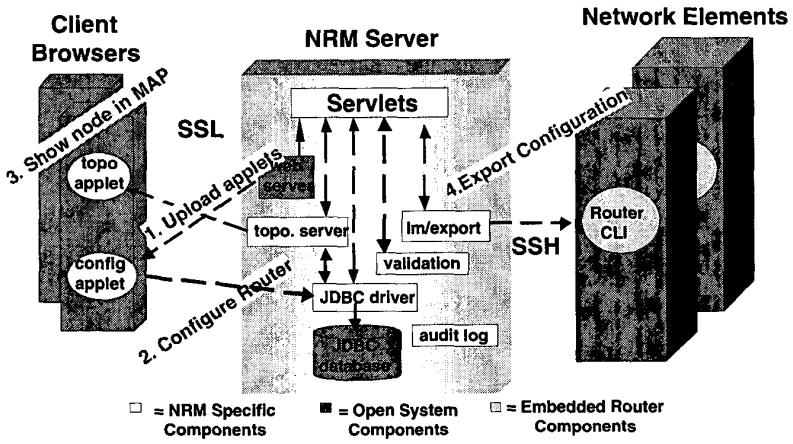

Figure 2. Management Server Interaction Diagram

Routers are configured using the *Config* applet GUI in the browser, which is accessible from any Java-enabled browser. The applet GUI displays and saves the configuration information into the database residing on the Management Server. Multiple browsers can be logged on to the management server at the same time. In this case, database locking is applied to control synchronization among users and only one client can have a write access on a router. Locking is marked as an icon on the applet GUI. For database, any JDBC-compliant database can be used.

User can preview the topology of the proposed configuration to verify the configuration by using the Topology server. The Topology server can provide protocol-sensitive view on OSPF, BGP, IS-IS and MPLS etc. This feature is unique in the NRM and very helpful on configuration checking. When user decide to export the configuration to routers, SSH/SCP session is established with the router for configuration transferring. The information in the database is parsed and reformatted to a router configuration file for exporting before transfer. The following chapter describes detailed description on each subsystems of the NRM server.

4. SUBSYSTEM DESCRIPTIONS

4.1 Configuration GUI Applet

Figure 3 shows a snap shot of Configuration applet GUI. It consists of three major components: a navigational panel, a context-sensitive panel and menu item. Navigational pane has one or more icons that can be initiated using the Palette display. Copy and paste

of configurations is provided by icon level between routers. This allows a user to quickly create multiple router configurations, normally a very labor-intensive process. Context-sensitive pane holds Palette and Properties panel. Palette displays available templates or icons that can be instantiated and Properties panel displays the entries and help texts. Menu items are consists of following icons:

- Read DB-Make a connection and retrieve configuration information from the Database
- Copy-Copy a selected icon from navigation pane
- Paste-Paste copied icon under selected item
- Delete-Delete selected icon from Database
- Refresh- Reload the database
- Validate- Network integrity check and syntax error check
- Import- Import configurations directly from the device or from the TFTP server. Option to schedule import
- Export- Export configurations directly to the device or to the TFTP server. Option to include only modified values. Option to schedule export, and send notification message
- Topology- Set of physical/logical views for the network and its protocols
- Log-View server log message
- Revert-Undo one level Database action

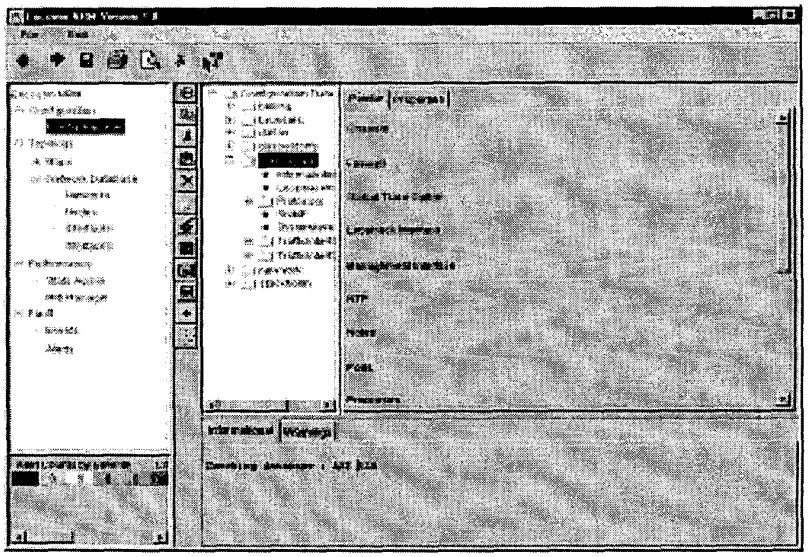

Figure 3. Configuration GUI Applet view

4.2 Import/Export

The user shall be able to request from the configuration GUI applet that the configuration shall be exported to, imported from the corresponding routers. The GUI applet will call a *port* servlet for this service. In case of an *export* request, the servlet will fetch the corresponding objects and attributes from the database and parse the information into create a configuration file. The *port* servlet will in turn call the SSH client to send the configuration file to the router along with simple Command Line Interface (CLI) interaction. The *port* servlet will receive a response from the router via the SSH client to acknowledge success or failure of the export action. In case of failure, the *port* servlet will interpret the failure message and request the GUI applet to display the failure message in the informational part of the panel as well as highlight the specific entries of interest. In case of success, the configuration GUI applet is informed and can display the message in the informational part of the panel. The *export* procedure uses SSH command to copy the configuration file from the management server to the router by set of commands.

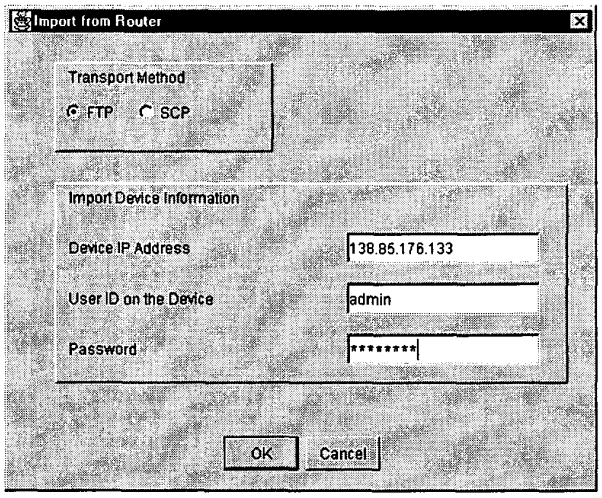

Figure 4. Import/Export GUI view

The *import* function is handled in a similar way as the *export* function but in reverse order. The *port* servlet fetches the configuration file from a router through the SSH client. The *port* servlet parses the data into the information model and stores it in the database. Every *import* writes to a clean sheet in the database with new IDs. Import can supports unidentified keywords from deivces and save it under user-defiend value. This will be used as part of s/w version handling and adaptation to changes such as addition of

new protocols etc.

Above Figure 4 represents the Import/Export pop-up window. Transport method is the application that should be used to rtansfer the configuration between the network device and the NRM server. One can use FTP if the network device has been configured for FTP support, or select Secure Copy (SCP) protocol if the device supports SCP and you have installed Secure Shell on the router device. Device Ip adress is the network device's IP address that you want to import/export from. User ID and password are valid login ID and password on therouter. Import/Export runs the connectivity test (eg. ping) before initilize the process.

4.3 Validation

The validation function provides an extensive network integrity check detecting common yet hard-to-isolate pre-defined configuration problems by systematically diagnose the entire router networks. For network integrity check more than 100 rules (problem types) are defined mainly in Protocols related parameters.

Ericsson developed proprietary high-level script language is used for easy handling of the validation process. The main purpose of this script language is to simplify coding of the rules, define complex problem types efficiently, easy to use in mapping and retrieving database information etc. As an alternative choice of this script language, UML Object Constraint Language (OCL) [11] was considered. OCL was originally designed to formally define the semantics of the Unified Modeling Language (UML) which was not efficient to handle non-object constraints.

Validation rules are mainly focused on Protocols area such as BGP, OSPF, MPLS, ISIS, RIP, PIM, RSVP, and IP address consistency in subnet, OSPF area homogeneity, etc. Some of the example problem types are

1. BGP Type of group mismatch
2. IBGP Internal not fully meshed
3. Unique Name for LSP etc.

The following Figure 5 shows the example of validation rule definition for Unique Name for LSP. In this rule, the name of a label-switched-path must be unique within the ingress router. Validation rules can be applied on multiple network elements at user's choice.

Rule 7: Unique Name for LSP

The name of a label-switched-path must be unique within the ingress router.

```
rule "Rule 7: Unique Name for LSP " {
message "The name of a label-switched-path must be unique "+
        "within the ingress router.";
type "Rule 7";
protocol MPLS;
severity High;
```

```
find SystemlevelIP { // go through all routers
   set @lspName = [];
   set $addr = .RouterId;
       for all DynamicLSP {
         if (.LSPName in @lspName) {
           report;
         }
         @lspName << .LSPName;
       }
    }
}
```

Figure 5. Example of a Validation rule - Unique Name for LSP

As shown is Figure 6, validation is then used with the configuration GUI to find and fix the configuration problems. Selected rules can be applied to selected set of router devices. It also Generate problem reports with List of router, and detailed description of the problem.

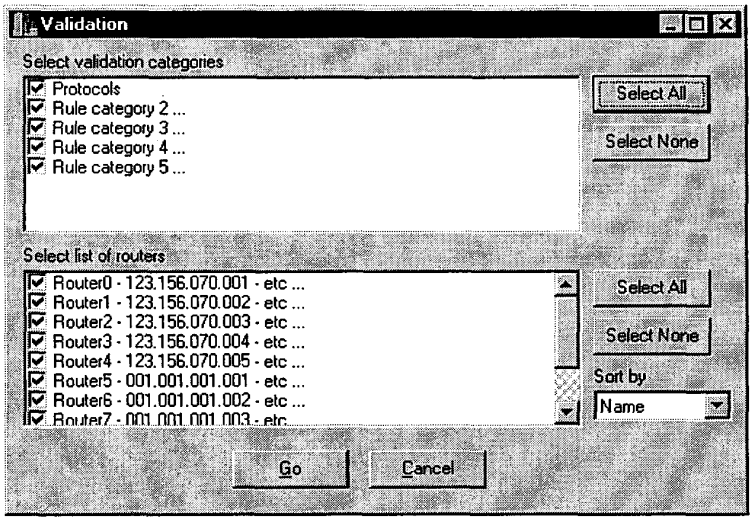

Figure 6. Validation Window

The element validation is executed as a pre-process of the *export* function or independent validation process. These two executions are identical in its function with the following exception: the independent validation action does not request export of the configuration to the router. The network validation checks variables relating to network

rather than node consistency, such as IP address consistency in subnets, OSPF area homogeneity, etc. The validation subsystem searches the database for retrieval of relevant information field.

4.4 Topology Subview

The topology subview option shows the physical layout and/or the logical display of a network and its protocols as shown in Figure 7. Upon user request, it retrieves the corresponding data from the management server database, and draws the selected map. Topology views can be used for analyzing protocol specific areas partitioning information and optionally for updating the configuration.

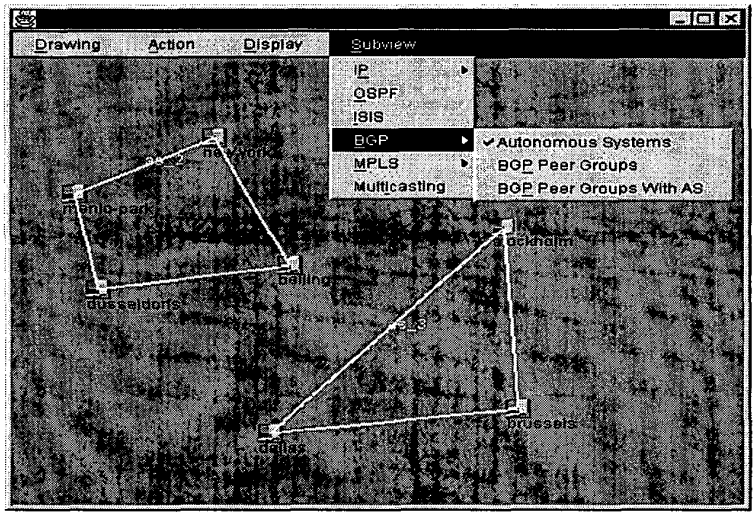

Figure 7. Topology subview window

The Protocol-sensitive topologies provide views for the physical topology and each routing protocol. Consequently, the topology is shown as configured, not as discovered. Proposed configurations can be displayed before exporting them to the router network. Visual queries can be made in each view. For example, when the user clicks on a set of routers in the MPLS interface subview, the utilization ratio of each interface is presented. Visual configuration changes can be made through tables on each router in the graph.

The topology subview consists of following physical/logical views of networks and protocols:

- POP view, Flat view
- OSPF view – OSPF Area, OSPF Metric Cost, OSPF Policy
- IS-IS view – IS-IS Area, IS-IS Metric Cost, IS-IS Policy

- BGP view – AS, BGP Peer Group, BGP Policy
- MPLS view – MPLS path, LSP, Interface
- Multicast view – Connectivity, Administrative scope, Protocol Independent Multicast (PIM)/ Distance Vector Multicast Routing Protocol (DVMRP)

The POP view depicts the rough approximation of the physical layout of the network. The Flat view arranges networks and devices to best display all interconnections without regard to their physical locations. The OSPF view displays the OSPF Area, and includes tables for OSPF Metric Cost and OSPF Policies. It displays the direct and virtual links in the OSPF area and list summary ranges, default routes, export policies and metric cost per interface for shortest path calculation, etc. The IS-IS view is similar to the OSPF view. The BGP view shows the routers in the AS, neighbor relationship among ASs and confederations, and export policies. The BGP peer group view is used to analyze peer relationships in the proposed configuration by displaying peer group routers, and the type of peer group, route reflector, route preference, and export/import policy.

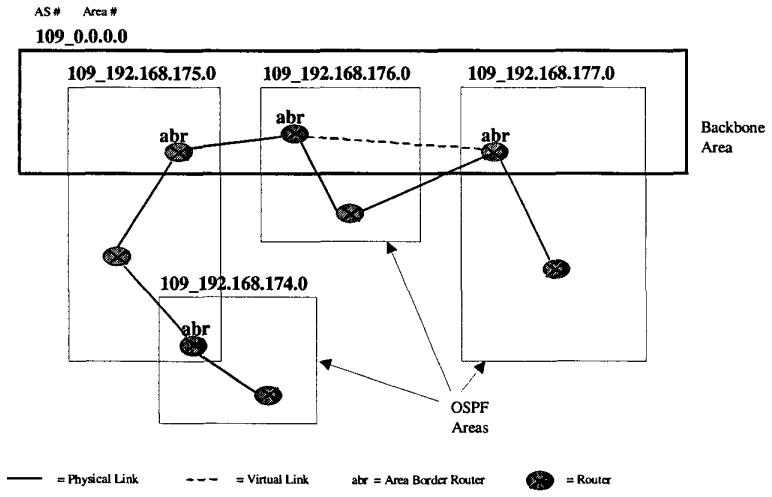

Figure 8. Example Topology subview of OSPF Area

The MPLS Path view is used to analyze connectivity constraints in the configuration. The Path view displays the MPLS traffic trunks, next-hop rules and redundant paths between ingress and egress points and etc. The LSP view is used to analyze topology constraints in the configuration by examining LSPs (MPLS routes) between ingress and egress with CoS and bandwidth, policy filters and preference values, etc. The Multicast view is used to examine the connectivity aspects of the multicast configuration by identifying tunnels (virtual point-to-point links) and direct links between multicast-aware

routers. The Administrative scope view is used to analyze the distribution aspects of the multicast by displaying the router interfaces that are within the administratively scoped boundaries. The PIM/DVMRP view groups the multicast-aware routers that are within the same PIM group range, shows the priorities of a router and highlights the PIM-DVMRP border routers.

Figure 8 shows an example of the OSPF area subview. The OSPF area view displays the OSPF areas as solid boxes, physical links as solid lines and virtual links as dotted lines to the backbone area. It also shows the stub area. Each OSPF Area contains routers belonging to the same OSPF area and using the same autonomous system number. The OSPF Area names have a format of *109_0.0.0.0,* where *109* is an Autonomous System (AS) number and *0.0.0.0* is an OSPF area number. OSPF also allows the definition of virtual links, which can traverse a Transit Area. The Virtual Link is used to connect a backbone area border router, not physically connected to the backbone (*0.0.0.0*), to another backbone area border router that is physically connected to the backbone.

5. PERFORMANCE MEASUREMENT

System performance is measured on the client connection and each subsystem response time in seconds. The testing environment is a 10Mbps Ethernet LAN. NRM server is running on a Windows NT 400MHz box, with 128MB RAM. Client's machine is Window NT 266MHz/64MB. When the client browser connects to the NRM server it starts to download 1.5MB of applet. Client connection time to the server highly depends on the network bandwidth and the traffic. The average client connection time on the tested environment was about 15 seconds which corresponds to 819.2 kb/s.

Observations: All subsystems interact with the database and this is the main cause of the high response time and other delay. To further reduce the subsystem's response time, a single Database Manager routine that will control all database connection and access is necessary. Import/Export subsystem need to access INI files from the server, this also caused significant delay. All INI files will be converted to object class for faster access.

	Response time(sec.)
Client connection time	15
Subsystems	-
Import	5
Export	7
Validation	6
Topology	5

Figure 9. Performance result

6. CONCLUSION AND FUTURE WORKS

In this paper, we presented the design and implementation of web-based secure configuration management architecture for Internet backbone router networks. High level of security in network configuration, synchronous operation and reduced complexity in network management at the managed entity are achieved by using secure protocols and a centralized database. Emi-automation in configuration management is accomplished by using pre-defined configuration templates and intelligent validation of router network.

The suggested web-based configuration management system improves accessibility and interoperability while still providing a secure connection. User friendly navigational GUI provides an easy way to configure very complex high-end Internet backbone Routers. The Network Resource Manager (NRM) provides easy access from any web browser to the configuration data and simplifies the complexity involved in network configuration management. Simulation tests have shown NRM is capable of supporting up to 50,000 network objects, which can translate to between 250 – 500 router nodes from one management server. The simulation tests will be continued for reliability test and better accuracy. Dependency of the s/w on the network device, for example version upgrade/change in hardware, is handled by NRM version handling. Version handling is supported in Configuration GUI by loading different set of entries on each Database item.

NRM, an Ericsson developed web-based Configuration Management System, version 1.0 is released and available today and fully supports AXI520 Gigabit Backbone router. NRM v2.0 is scheduled to be released on 1Q of 2000 with extended supports on different types of routers and functional increments. Further work is necessary in developing resilient database and currently undergoing tasks are Cisco IOS-based router supports, CORBA standard interface, and DEN/LDAP compliant Database schema conversion etc. [9,10]

REFERENCE

[1] Graham Stanhope and Hakan Sessle: "AXI520 Gigabit Router, Technology overview", Ericsson Telecom AB and Ericsson Business Networks AB , 1998

[2] Bassam Halabi: "Internet Routing Architectures", Cisco Press, 1997

[3] Jan Forslow: "Ericsson Gigabit Router Management", Ericsson Inc. Internal Report ETX/DN/WIG-98-0005 Uen, 1998

[4] Prashant Sridharan: "Advanced Java networking", Prentice Hall, 1997

[5] AXI520 Configuration Guide (JUNOS Internet Software Configuration Guide), Juniper Networks Inc., 1999, http://www.juniper.net

[6] AXI540 Configuration Guide, Ericsson Inc. 1999, http://www.torrentnet.com/usernam/v2-0/confg/index.htm

[7] Cisco Inc., Cisco IOS References Library, "Cisco IOS Configuration Fundamentals", 1998

[8] Robert Wright, "IP Routing Configuration Basics", Cisco Press, 1998

[9] John Strassner, "Directory Enabled Networks", Macmillan Technologies Series, 1999

[10] Timothy A. Howes, Mark C. Smith, " LDAP Programming Directory-Enabled Application with Lightweight Directory Access Protocol", Macmillan Technologies Series, 1997
[11] Object Management Group (OMG), "Object Constraint Language Specification", ad/97-08-08 ver. 1.1, September 1999
[12] Distributed Management Task Force, Inc WBEM initiative home page, http://dmtf.org/wbem/index.html
[13] BMC Software, Cisco, Compaq, Intel, Microsoft Inc., "Web-based Enterprise Management Proposal", Revision 0.04, Jul 16 1996
[14] Distributed Management Task Force, Inc. "Common Information Model (CIM) Specification Version 2.2, June 14, 1999
[15] Mary Jander, "Web-based Management: Welcome to the revolution", Data communication, Nov. 21 1996
[16] J. W Hong, J.Y. Kong et al, "Web-based Intranet Services and Network Management", IEEE Communication Magazine, Oct. 1997
[17] J. P. Thomson, "Web-based Enterprise Management Architecture", IEEE Communization Magazine, Mar. 1998
[18] J. Boyle, H. Truong, N. Nour, "Providing a web-based view of your managed network", Proc. of IEEE International Conference on Communication, 1997