IMPLEMENTATION OF PUBLIC AGENCIES NIT

*D. Jaiani *, K. Demetrashvili**, Z. Chaganava***, N. Napetvaridze*****

**I. Vekua Institute of Applied Mathematics,
Iv.Javakhishvili Tbilisi State University
** Department "Automation of Production Engineering",
Georgian Technical University
*** UNDP Georgia Projects' Consultant in IT
**** UNDP Georgia Projects' Consultant in ICT*

Key words: LAN, switch, firewall, NIT

2000 MR Subject classification 68M10

The LAN of the Ministry of Finance of Georgia is one of the most modern, large, expandable, properly configured and simple in use for its users Local Area Network in Georgia at a present time. The LAN is installed in whole building of the Ministry of Finance. Number of LAN points on the each floor varies depending on number of rooms and working places on the each floor. The total number of points installed is 260 (see Figure1). The topology of the LAN is so called Star, the most convenient and reliable topology in case of the Ministry of Finance, which considers cabling from each workstation until the switch.

In the process of network planning and building the following was considered: the used material and physical elements had to fulfill the last norms imposed by the international standard organizations that apply to the sphere of Local Area Networks and investment in cabling system had to meet future demands for data networks. The existing power system in the building of the Ministry of Georgia was in a poor condition; power cabling had been redesigned several times and as a result power cables were almost everywhere in the walls and were lied in a random order; besides, power cabling system for heating purposes with high electromagnetic fields existed in the building. As it is generally known, standards require that in case of UTP cable using the distance between data and power cables should be 200mm and crossing should be at 90 degree; it was impossible to follow these requirements in the most cases. Considering all above mentioned, it was decided that using of FTP CAT5e cable for horizontal cabling was the best solution to ensure avoiding of interferences between power and data cabling systems. Using of UTP cable for backbone could cause the galvanic discharge between the floors and using of copper as a media was not considered as best suitable for inter-floor connections. Finally it was decided to use fiber optic 1000 Base-SX MMF cable for backbone connections (see Figure 2).

It is well known that maximum distance for all types of twisted pair cable types is 100 meters without repeater. This fact was reason for dividing whole ministry building into A, B and C blocks. In each block Access Layer switches (SuperStack 3 Switch 4400 with 1000BASE-SX module) were installed and each switch itself was connected to the Core switch (SuperStack 3 Switch 4900SX).

Core and Access Layer switches used are of high quality and ensure Gigabit backbone connection and high performance in the process of data interchange. The equipment allows its configuration, monitoring and administration as from the serial interface, so from the central point of the LAN with the help of specialized administration software (LAN devices management software).

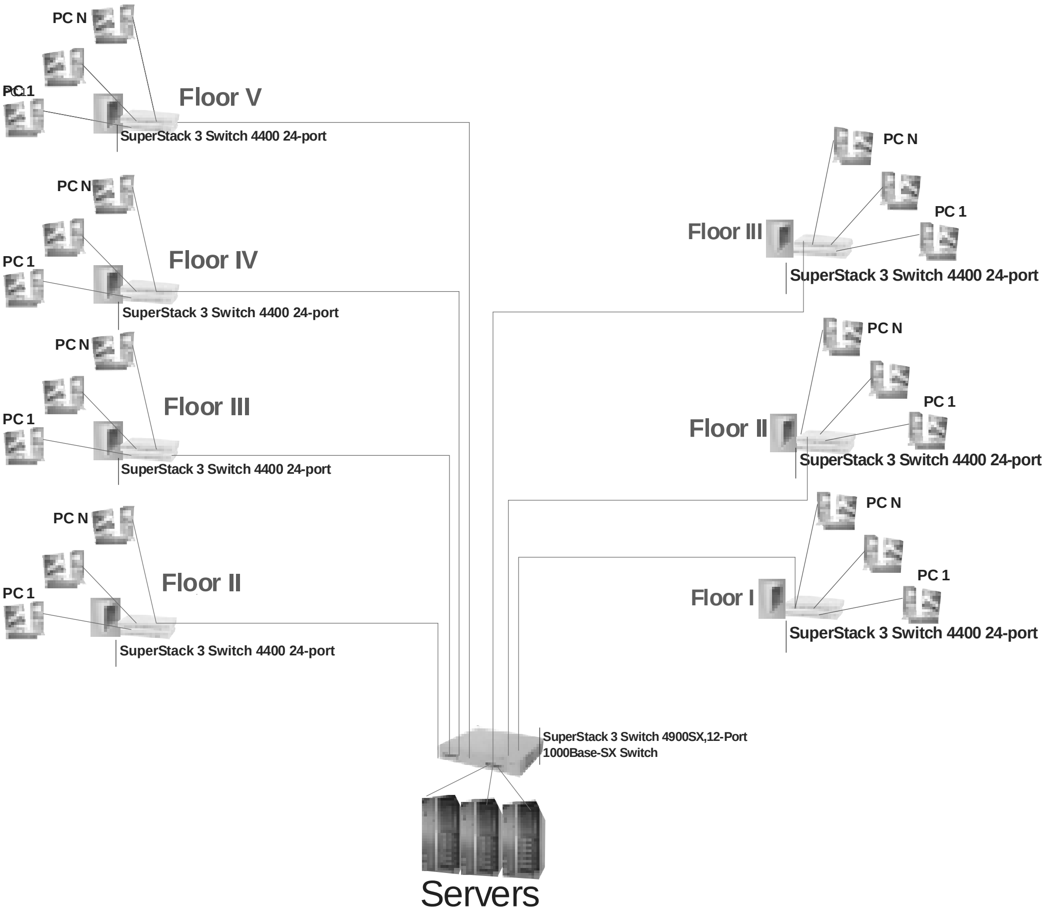
PC N
PC 1
Floor V
SuperStack 3 Switch 4400 24-port
PC N
PC 1
Floor IV
SuperStack 3 Switch 4400 24-port
PC N
PC 1
Floor III
SuperStack 3 Switch 4400 24-port
PC N
PC 1
Floor II
SuperStack 3 Switch 4400 24-port
PC N
PC 1
Floor III
SuperStack 3 Switch 4400 24-port
PC N
PC 1
Floor II
SuperStack 3 Switch 4400 24-port
PC N
PC 1
Floor I
SuperStack 3 Switch 4400 24-port
SuperStack 3 Switch 4900SX,12-Port
1000Base-SX Switch
Servers

Figure 1

For distribution, control and interconnection of the cables there are used cabinets (racks) with keys of security and patch panels in each cable center. The LAN equipment and UPS-es also are placed in the cabinets.

The network was elaborated with the view of further extension. LAN of the Ministry of Finance is connected to State Treasury, Tax Department and Customs LANs. In 1999-2000 Tbilisi State Agencies MAN (20 agencies are connected) was implemented under our guidance; connection to this MAN is intended in the nearest future. All users (about 210) are connected to the Internet. Future connections will not incur too many expenses in regard of installation of additional expensive equipment.

There are three main servers in the LAN, which function as local domain controllers, file and print servers, database servers, mail, ftp and proxy servers. Microsoft Windows 2000 Advanced Server with Active Directories installed is used as a local domain controller. As a new approach LAN users are provided with

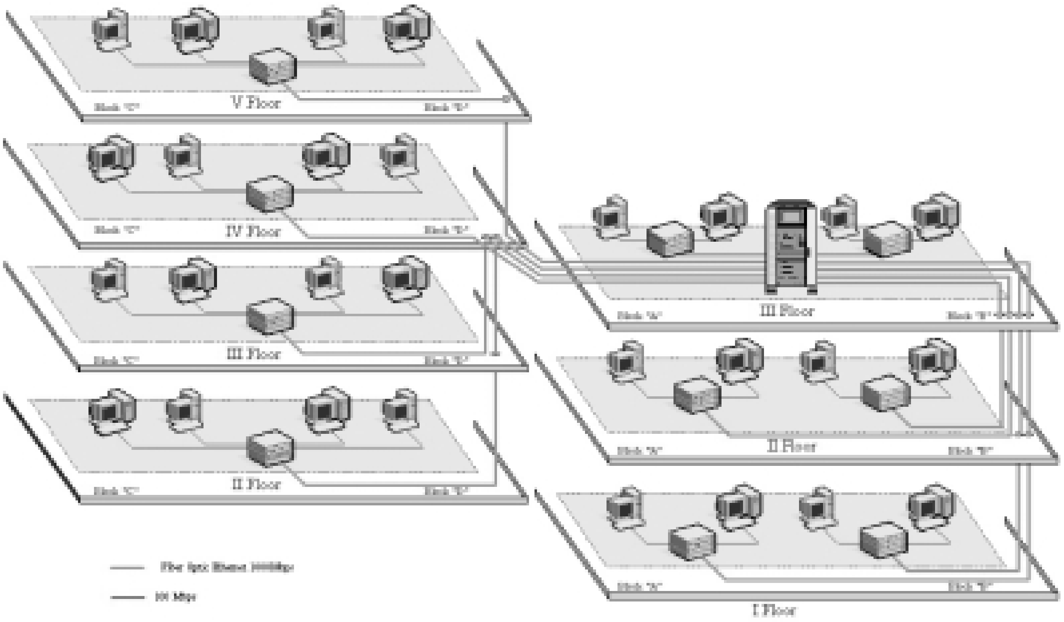

Figure 2

special logon scripts that enable them to work with network shared resources more efficiently; client protection antiviral software is updated via special scripts too. In order to reduce user time expenditure and increase user's work efficiency, several useful folders are deployed on the fileservers: each user has a dedicated folder with the exclusive access rights, where one can store private essential files and information; other folders are deployed for departmental users to exchange common information with each other and to store the information which is necessary for the whole department; information folder for data interchange through the whole Ministry is deployed too, where everybody has right to write or modify data. To prevent information loss all the data on the fileservers is backed up once a week on the special backup devices. Microsoft SQL 2000 Server is used as database server software. At the moment about ten databases are in use, including databases of Institutional Corporate Management Information System, Personnel Management System, Monitoring Tasks Implementation and etc. Red Hat Linux is used for Internet access purposes. The following vital services are running on that server: proxy server, mail server, FTP server, Network Address Translator (NAT) and etc. A special software (squid guard) filters internet connections and denies access to the prohibited web requests (adult sites, ads, chats); users are not allowed to download files greater than 2048 KB. As a result internet traffic is reduced and efficiency is increased. Special software (MRTG) monitors users' activity in the internet and graphically shows how much traffic is used, it also makes available daily, weekly, monthly and yearly statistics.

To ensure highest level of protection against external intrusion and to achieve fastest speed of data transfer over the internet, two firewalls are set up: dynamic firewall on the Cisco router and static router on the Internet Access (IA) server. The following static firewall rules are configured on the Internet access server:

Source	Destination	Action
Internet	LAN IP range	Reject
255.255.255.255	IA Server	Reject
Internet	IA Server TCP Port 25	Accept*
Internet	IA Server TCP Ports 1:1024	Reject
Internet	IA Server TCP Port 3128	Reject
Internet	IA Server UDP Ports 1:1024	Reject
LAN	ICQ server IP Addresses	Reject

* As mentioned above, IA Server is running mail server and it needs incoming connection on TCP port 25 from other mail servers.

In the dynamic firewall only TCP 25 port is open from the Internet side. Firewall listens to http, TCP, UDP, ftp connections and only returning requests are allowed to enter back, else it checks validity of each request (i.e. if http request is really http, not any kind of chat using any http port or so).

Maintaining internal security is not less vital and dangerous than external intrusions. As usually not all points of the LAN are used, to prevent unauthorized network connections unused switch ports are disabled, i.e. it's impossible to use this connection in any way, as if there was no cabling at all. Apart from this the used switches give availability many opportunities to make the LAN fast, reliable, secure and managed. For the best outcomes the following main capabilities are used by the LAN administration: *Auto-negotiation* allows ports to auto-negotiate port speed, duplex-mode (only at 10 Mbps and 100 Mbps) and flow control. When auto-negotiation is enabled a port “advertises” its maximum capabilities — these capabilities are by default the parameters that provide the highest performance supported by the port; *Port security* guards against unauthorized users connecting devices to the network. The port security feature, *Disconnect Unauthorized Device (DUD)*, disables a port if an unauthorized device transmits data on it; *resilient link* feature enables to protect critical links and prevent network downtime should those links fail. Setting up resilient links ensures that if a main communication link fails, a standby duplicate link automatically takes over the task of the main link. Each main and standby link pair is referred to as a resilient link pair. This option is mainly used regarding servers; *Traffic prioritization* allows time-sensitive and system-critical data, such as digital video and network-control signals, to be transferred smoothly and with minimal delay over the network. This data is assigned a high priority by the transmitting end station and traffic prioritization allows high priority data to be forwarded through the Switch without being delayed by lower priority data; *Remote Monitoring (RMON)* is an industry standard feature for traffic monitoring and collecting network statistics. The Switch software continually collects statistics about the LAN segments connected to the Switch; *Broadcast Storm Control* is a system that monitors the level of broadcast traffic on that port. If the broadcast traffic level rises to a pre-defined number of frames per second (threshold), the broadcast traffic on the port is blocked until the broadcast traffic level drops below the threshold. This system prevents the overwhelming broadcast traffic that can result from network equipment which is faulty or configured incorrectly; *Virtual LAN (VLAN)* is a flexible group of devices that can be located anywhere in a network, but which communicate as if they are on the same physical segment. With VLANs, one can segment a network without being restricted by physical connections — a limitation of traditional network design.

The above implemention was carried out using [1-7].

References

[1] Computer Networks. Microsoft Press 2002 (in Russian)
[2] Windows 2000 server. Microsoft Press 2002 (in Russian)
[3] TCP/IP Networks. Microsoft Press 2001 (in Russian)
[4] 3com SuperStack« 3 Switch Implementation Guide 2002
[5] Sportac M., Sportac F., Computer Networks and Network Technologies. Diasoft Press, 2002
[6] Peterson R., Linux: The Complete Reference, Fourth Edition, Osborne/McGraw-Hill Press 2002
[7] Negas Ch., Red Hat Linux 7.2 Bible, 2001

Received September 5, 2003; accepted November 14, 2003.