<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>China’s national financial network design : an information systems engineering prospective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Kozik, Eugene</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>1999</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/1888">http://hdl.handle.net/10220/1888</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td></td>
</tr>
</tbody>
</table>
Paper No. 40
CHINA’S NATIONAL FINANCIAL NETWORK DESIGN:
AN INFORMATION SYSTEMS ENGINEERING PROSPECTIVE

INFORMATION POOR TO INFORMATION RICH STRATEGIES
FOR THE 21ST CENTURY CONFERENCE 1 – 3 JULY 1999,
CHENNAI (MADRAS), INDIA

Eugene Kozik
Penn State University
School of Graduate Professional Studies
Malvern PA 19355
Phone: (610) 648-3219
Fax: (610) 889-1334
Email: exk6@psu.edu
# Table of Contents

<table>
<thead>
<tr>
<th>Section I. Executive Summary</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 The problem/Analysis</td>
<td>5</td>
</tr>
<tr>
<td>1.2 CNFN Constraints</td>
<td>5</td>
</tr>
<tr>
<td>1.3 Design Indicator and Summary</td>
<td>6</td>
</tr>
<tr>
<td>1.3 Design Indicator and Summary</td>
<td>7</td>
</tr>
<tr>
<td>Section II. Background of the Problem</td>
<td>8</td>
</tr>
<tr>
<td>2.1 Scenario of the Problem</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Infrastructure</td>
<td>11</td>
</tr>
<tr>
<td>2.3 Objective Tree</td>
<td>14</td>
</tr>
<tr>
<td>2.4 State of the Arts</td>
<td>16</td>
</tr>
<tr>
<td>2.4.1 Structured Network</td>
<td>16</td>
</tr>
<tr>
<td>2.4.2 Quality of Service (QoS)</td>
<td>17</td>
</tr>
<tr>
<td>Section III. Requirement Analysis and Conceptual Design</td>
<td>19</td>
</tr>
<tr>
<td>3.1 Requirement Summary</td>
<td>19</td>
</tr>
<tr>
<td>3.1.1 Payment System</td>
<td>20</td>
</tr>
<tr>
<td>3.1.2 Statistics Information Systems</td>
<td>23</td>
</tr>
<tr>
<td>3.1.3 Information Monitoring system</td>
<td>24</td>
</tr>
<tr>
<td>3.2 Financial Information System Strategy</td>
<td>24</td>
</tr>
<tr>
<td>3.3 Conceptual Modeling</td>
<td>34</td>
</tr>
<tr>
<td>3.4 Spiral Model</td>
<td>35</td>
</tr>
<tr>
<td>3.5 Concept of Operations</td>
<td>35</td>
</tr>
<tr>
<td>3.5.1 Thin Thread Analysis</td>
<td>37</td>
</tr>
<tr>
<td>Section VI. System Design (Case Study)</td>
<td>39</td>
</tr>
<tr>
<td>4.1 System Configuration Overview</td>
<td>39</td>
</tr>
<tr>
<td>4.2 Regional Network Center</td>
<td>42</td>
</tr>
<tr>
<td>4.3 Network Functional Module</td>
<td>45</td>
</tr>
<tr>
<td>4.3.1 Interface with Customers</td>
<td>48</td>
</tr>
<tr>
<td>4.3.2 Function of Transaction Message Protocol</td>
<td>49</td>
</tr>
<tr>
<td>4.4 Flow Control and Network Management</td>
<td>51</td>
</tr>
<tr>
<td>4.4.1 Network Manager</td>
<td>52</td>
</tr>
<tr>
<td>4.4.2 System Status Monitor</td>
<td>52</td>
</tr>
<tr>
<td>4.5 Security</td>
<td>54</td>
</tr>
<tr>
<td>4.6 Data Dictionary</td>
<td>56</td>
</tr>
<tr>
<td>Section V. Conclusions</td>
<td>57</td>
</tr>
</tbody>
</table>

Appendix

Bibliography
Acronyms:

ATM Asynchronous Transfer Mode
CPU Central Processing Unit
CSMA/CD Carrier-Sense Multiple Access with Collision Detection
CSU Channel Service Unit
DDS Data phone Digital Service
DSU Digital Service Unit
FDDI Fiber Distributed Data Interface
IP Internet Protocol
IS Information Science
ISDN Integrated Service Digital Network
ISP Internet Service Provider
LAN Local Area Network
MAU Medium Access Unit
MIS Management of Information Systems
NIC Network Interface Card
NOS Network Operating System
RMON Remote Monitoring
SQL Structured Query Language
VLAN Virtual Local Area Network
VMS Virtual Memory System
WAN Wide Area Network
Section I. Executive Summary

This report is to design a comprehensive nationwide financial network system for People's Republic of China. This network must be capable of supporting many new generations of financial services. The design of this network needs to meet the China's current financial information demands, and yet be flexible enough to meet the financial information technology integration requirements of the 21th century.

1.1 The problem / Analysis

China is currently going through a historical change. The high rate of economical growth in the past ten years has led China to a critical and historical juncture. Its central planning economy is gradually transforming into market economy. The economical reform has reached a point where information technology will play a vital role. The essence of a market economy is its ability to allocating resource efficiently. To allocate resources efficiently, it must have low cost, timely and accurate economic and financial information.

The banking system of China is at the beginning of reform. There have been some considerable achievements. The Central Bank Law passed in March 1995 has given the People's Bank of China (PBOC) greater autonomy in conducting monetary policy and in national banking supervision generally. As China starts to revamp its banking systems and other financial institutions, an advanced Information system is becoming necessary. Fully realizing the importance of the Internet Information technology, in April of 1997, the central government sponsored China's first National Information Technology conference. A long-term strategy for developing China's Internet technology was developed. The strategy can be summarized into following: unified planning, centralized leadership, uniformed standards, joined development, open
interface, and share resources. This need has placed information technology into national conscious.

In the 21st century, Internet will provide a powerful media for people to exchange information, conduct work, and doing business. The network will not only provide data communications, but more importantly it will also guarantees the qualities of the many network services. The applications of future will very different from those of today. Distributed computing promises to deliver data process at much large system scale. The numerous programs for a financial information network including data collection, economy monitoring and forecasting, and financial transaction processing will be implemented over a geographically distributed system. Success of deploying those applications will be depend on a network infrastructure that will provide reliable data transfer, deterministic propagation delay, privacy and a variety of data capacities.

The future success of such network is depended on its design. Because of its size and complexity, the construction of such network must be a joint effort among academia, industry and government. The role of the government is to provide necessary guidance and financial support at beginning stage of the development. When the network reaches its critical mass and become a viable business environment, industry will provide necessary funding to sustain its growth. Academia also plays an important role. The network must demonstrate its commercial value. In order for the network to be useful, the necessary information technologies to provide commercial services must be researched and developed.

1.2 CNFN Constrains

People’s Bank of China must balance its operating goals and available resources. The implementation and maintenance of CNFN are constrained by available telecommunication devices, skilled manpower and available money.

One of the main constraints of the CNFN project is to have access to existing
network services. However, Ministry of Information Industries (MII) owns most of the nation's network infrastructure. Constructing CNFN must interface with ChinaNet, a proposed nationwide network backbone. To do so, PBOC needs to work closely with MII who owns ChinaNet and other network owners and piggyback on existing systems.

The needed distributed financial applications and network components are highly advanced technologies. They require the availability of skilled manpower before the system can be available for commercial use. Therefore, the success of the project will depend on partnerships among universities, the private sector and government research communities. To ensure the network to function successfully, a large number of technical personnel will be needed to design, implement and to maintain the network at Regional Network Control Centers (RNCC), which are the access points that are necessary to interface with ChinaNet. Designing and manning the system will be the great challenge for the project.

The budget constrain is existed for almost every project. The CNFN is a long-term project. It needs investments in hardware, application and maintenance. How to best allocate limited resource is a great challenge for the project.

1.3 Design Indicator and Summary

The use of proper financial functional application software can provide important services to a diverse collection of financial institutions. Well-designed software can interface with multiple disparate system provide uniform services without major alteration. Interface resolution and application modularization is essential for successful operations within a large-scale system.

Network fabric provides the connections between the end users and network resources. Among the remote connecting points, the wide area network must support differentiated QoS as well as highly reliable, high-capacity transport. QoS includes important network parameters such as latency time, capacity and loss rate.
The design of CNFN is based on Regional Network Control Centers (RNCC) and ATM switches. The RNCCs are high capacity and state-of-the-art interconnection points. Within those centers, the next generation network protocols are implemented. Through those protocols, CNFN should offer guaranteed Quality of Service (QoS). Between those centers, high-speed lines connected with ATM switches capable of carrying large quantities of data. In order to provide an uniformed service for everyone, financial transaction message standards and network interface protocol should be defined and implemented at each participating institution. The function of the message standard is to provide uniform network interfaces to dissimilar hardware platforms and databases. PBOC must design, publish and maintain a set of communication protocols as well as a set of application and network interface standards. These standards are necessary for integrated cost-effective operations.

Section II: Background of the Problem

2.1 Scenario of the Problem

China National Financial Network (CNFN) project was defined by People’s Bank of China (PBC) in 1995. The goal of the project is to construct a nation wide financial network that can offer cost effective and advanced financial services. The network not only will address the country’s problem of lacking an advanced financial network but also will serve as Central Bank’s decision making and regulatory tools.

China’s banks are among the largest in the world in terms of assets. People’s Bank of China is the Central Bank of China, which is the main financial regulator body in China. Its main function is maintaining and fostering a safe and sound financial system. To meet those responsibilities, the Bank performs a wide range of activities relating to payment system, gathering and distribution of financial information and encouraging the usage of new financial technologies. It is also empowered to set national monetary polices as well as regulate and supervise the business of financial institutions. Differ form its western counter part, the Central Bank of China is also responsible for solvency
of many state-owned enterprises. Periodically, it funnels politically based funding through commercial banks or direct lending institutions. As the country moves more and more closely to a market economy, its role of fostering country's new financial industry is becoming ever more important. This includes creating new financial markets, developing new financial services, and encouraging technology innovations in financial area.

Four specialized commercial banks: Agriculture Bank, Industry and Commerce Bank, Construction Bank, and Bank of China serve as the extensions of the Central Bank. The bank reforms of 1994 converted those four banks into true commercial banks. Those four specialized banks are responsible for 70% of the country's lending. To relieve their political leading pressures, PBC set up three new policy banks to channel political based lending. Currently, although foreign bank access to the local markets are very limited, their presence will only grow. Other institutions, which provide financial services, include Postal Offices, credit card companies, and various cooperatives. China currently has a currency exchange market, bond market, futures market, and stock market. Currency exchange market is dominated by Bank of China. Bond market is small and illiquid. The common problems those markets facing are their credibility. Public and regulators lack timely financial information.

Financial Institutions need a financial information system to serve a wide range of business applications. The end users of the CNFN are divided into financial institutions and regulatory bodies. Financial institutions are commercial bank, investment companies, insurance companies, and several exchange markets. The regulators are the central and local government agencies that regulate financial institutions. They formulate financial regulations and oversee financial activities.

The recent Asian financial crisis has brought China's financial system into spotlight. Although, China was relatively unaffected by the crisis, the government recognized possible crisis in developing. The mass economic reforms that were proposed at National People Congress are to solve those problems. The most urgent task of the reform is to clean up the banking system and to build a healthy financial system. The
The government has decided to inject a large amount of capital into its four main commercial banks. This addresses China's banking system's short-term problem. In the longer term, China needs a more modern banking system than its current antiquated information system. Commercial banks and other financial institutions need a nationwide database for information such as the risk nature of business, credit worth and history of a company; and economical related data for its daily operations. The government agencies need to monitor country's financial activities closely to prevent financial crisis. To anticipate possible problems and regulate financial activities, the regulators need an information system that will collect, process and analyze the nation's daily financial activities.

China's banks are among the largest in the world in terms of assets. The economic growth in China for the last 10 years has been breathtaking. It is growing from a central planning economy into a mostly market-based economy. The gross nation outputs changed from mostly agriculture goods to high percentage industry products. Those changes have dramatically altered the country's financial landscape. Its banking system changed into a system with multiple financial and commodity exchange market hundreds of large and small banks, and various other non-banking financial institutions. To regulate this system is a formidable task. Currently, China does not have a system to monitor the assets of state banks. Without timely and complete financial information, regulating would be impossible.

The problems of current financial information system can be summarized into following:

1) Lacking adequate and timely financial information. Financial information is scarce and expensive. Information gathering techniques used are mostly antiquated. Investor as well as financial regulators lack effective means to collect necessary financial data.

2) Information delivery system is costly and time consuming. The country lacks a low cost and timely financial information delivery system. The efficient financial markets require a highly efficient financial information delivery system.
3) Financial transactions are slow and costly. This would leave its banks at competitive disadvantages when they compete with international banks.

4) Lacking a sophisticated financial network hinders developments and growth of many new financial services. New financial service industry is one the brightest sector for the country in the coming decade.

2.2 Infrastructure

Internet started late in China. However, it was selected as one of the national focus projects. Central and regional governments, as well as academic community have allocated substantial funds and resources to develop and implement a nationwide network in the last ten years. As part of the National Information Infrastructure (NTI) project, the former Ministry of Posts and Telecommunications decided at the beginning of the 1990s to build within 10 years a nationwide fiber-optic telecommunications network. The network is composed of eight (8) east-west and eight (8) north-south main trunk lines.

The eight east-west trunk lines include: Tianjin-Hohhot-Lanzhou, Qingdao-Shijiazhuang-Yinchuan, Lianyungang-Urumqi-Yining, Shanghai-Nanjing-Xi'an, Hangzhou-Changsha-Chengdu, Shanghai-Wuhan-Chongqing Guangzhou-Nanning-Kunming, Shanghai-Guangzhou-Kunming. The eight north-south trunk lines are: Mudanjiang-Shanghai-Guangzhou, Qiqihar-Beijing-Sanya, Hohhot-Taiyuan-Beihai, Harbin-Tianjin-Shanghai, Beijing-Jiujiang-Guangzhou, Hohhot-Xi'an-Kunming, Lanzhou-Xining-Lasa, Lanzhou-Guiyang-Nanning. The completed project is composed of 50 fiber optic lines, totaling 80,000 kilometers (49,712 miles), and connecting all provincial capitals and 70% of all large cities.

Fueled by government supports and business demands, Internet growth in China is very impressive. Currently, there are four major nation wide networks that are authorized to connect with Internet – ChinaNet, Gbnet, CERNet and CASNet. Internet developments in China can be divided into three stages.
First stage: (1987-1994). This stage is characterized by low speed and low quality services. Mostly, the Internet was used for Email. All the connections are limited to low speed dial-ups. The first international connection was a 64kps satellites lease line between (MP) Institute of High Energy Physics and Stanford Linear Accelerator Lab. It was not until 18 month later, a dedicated lease line and Cisco routers were put in place running TCP/IP. This network evolved later into CSTnet (China Science and Technology Net).

Second stage (1994 -1995). This stage is development of national education networks. During this stage, TCP/IP was selected as the standard communication protocol. All Internet functions are supported during this stage of implementations. Early in 1995, IHEP established permanent connection to Japan use undersea optical fiber. At the same time, Academy of Science, Beijing University and Tsinghua University jointly established the National Computing and Networking Facility of China (NCFC). It uses high-speed optical fibers and routers to connect for all the backbone connections. Soon after that CERNET (China Education and Research Network) is formal established. Using one 128 Kbps line to US, and one 64 Kbps line to Japan, CERNET truly became part of Internet community. In May 1995, MPT (Ministry of Posts and Telecommunications) started its own version of public networks (ChinaNet). It is intended to providing Internet services to the public.

The separation of China Postal Service and China Telecom began in April 1998. The two services were operated jointly under China’s former Ministry of Posts and Telecommunications until July 1998, when China Telecom was subsumed by the Ministry of Information Industry. By January 1999, all postal services in China’s 31 provinces, autonomous regions and municipalities have been separated from China Telecom. Now the China Postal Service and China Telecom are two different establishments with separate management. China’s Ministry of Information Industry has also announced the plan for the break-up of its highly profitable telecom monopoly, China Telecom. China Telecom will be split into separate nationwide pager, cell phone and landline companies.
Third Stage (1995 and Since). This stage is the commercialization of Internet in China. Business community accepted Internet with a vengeance. ChinaNet installed two Internet connecting points. One is in Shanghai and the second one is in Beijing. In the end 1996, Ministry of Electronics started fourth nationwide network China GBNet (China Golden Bridge Net). The primary objective of the Network is to provide financial and business information and services. The last segment of the Guangzhou-Beijing-Kunming-Chengdu fiber-optic cable trunk line was completed at the end of 1998, marking the completion of China’s first nationwide fiber optic telecommunications network.

Currently, in China the Internet landscape is highly fragmented. There are four nationwide networks – ChinaNet, Gbnet, CERNet and CASNet. There are some inherent faults in this structure. One problem is lack of leadership, which is critical for a forward-looking system such as the CNFN. CNFN is large and complex project. Its success requires a long time investment in technology. When a system is designed for tomorrow rather than today, there are many risky technical investments and discussions must be made. Without a powerful national committee oversee its design, development and implementation, it will be very hard to success. The second problem is it is wasteful. There are many duplicated efforts in each network. Third, when resources are distributed among four or more Internet technology organizations, none of those organizations will have the critical mass to adopt any standards or new technologies. Each organization can only take what technology is available from the PTB. The decision by the PTB may not always be in the best interests for the Internet community.

The implementation of CNFN (China National Financial network) was designated by PBC (People's Bank of China) as major nationwide financial modernization project. The network is partitioned into three levels. The top level is national financial backbone. It will connect all the city wide network centers across the country. There are two national data processing centers and one remote application center. The second level is the regional network centers. Those network centers are located at one of the major cities.
of the region. They are to provide service accesses to banks and financial institutions of the region. The lowest level is the local network centers. They are subnets of the regional network. Regional networks are connected to national backbone via network centers.

The CNFN will be a financial information network for China. The network will deliver financial transactions, distribute financial information and collection vital national economic statistics. Within the country, CNFN will connect all the commercial banks, security markets, and financial institutions. To outside the country, CNFN will be the country's financial information system gateway to the global financial system.

For the financial institutions, CNFN will provide a media for low cost financial transactions and access to valuable financial information. For the Central Bank of China, it will be an instrument to collect important financial and economic statistics. As China moves into deeper into market economy, Central bank's role of macro-managing economy will become crucial for the nations financial well being. To do so, there are most be adequate timely financial data available to generate meaningful economic forecasts. Currently, The central bank is still relying on forecasting model inherited from its past centrally planned economy. Lately, China financial regulators have under strong pressure from central government to improve the quality of data. Therefore, one of the main system requirements will be constructing a information gathering system. This system will automatically gather relevant financial statistics from all the financial institutions and forward them to a central repository.

2.3 Objective Tree

The ultimate goal of the CNFN system project is to construct a national financial information system that will serve all the financial companies and regulator agencies in the country. The scope of the project is so large that it can not be undertaken by PBC alone. It should be a part of NTI (National Information Infrastructure) project. The objectives are as follows:
Primary Goal

The primary objective is to design a state-of-art financial information system that will service China's financial community. At this stage, many new applications have to be developed and implemented. Without good financial applications such as advanced payment system, and rich information resources on the net, CNFN will not achieve its intended objectives. This includes design and implementing robust financial applications build on advanced information technologies and services.

Secondary Goal

The intermediate range goal of CNFN project is to develop and evaluate advanced network services and comprehensive network security that are necessary for national banking financial applications. The components include specifying the network architecture and protocol standards that offer good QoS, data security and system performance. The goal is to run realistic trials base on prototypes built using new architectures and associated services. Establishing standards that provide uniform interfaces for all the software developers.

Tertiary Goal

The short-range goal is to build a baseline network infrastructure using available communication links. At the initial stage of the project, it is important to define a CNFN model of operations. RNCC will be the corner stone of such a nationwide backbone. Designing and constructing an information network that covers the entire country is the focus of this report.
2.4 The State of the Art

The following section some of the technologies that are pertaining to our project will be discussed. Some of those technologies are currently widely in use commercially; some of the others are close to be commercialized; and others are purely experimental.

2.4.1 Structured Network

The structured network design philosophy is to use a high hierarchical star approach. The physical star topology provides increased manageability, control and configuration flexibility. This design scheme aligns perfectly with network center idea. To group servers, switches and other communication equipment to a centralized location can improve the management, control and security protection over the networks.

Virtual backbone

Many new financial applications will use distributed technologies. This design allows software components to process information located far away. Implementing those applications requires a high performance information network. The network must meet certain minimal performance, security standards. The main challenge is to design and implement a high performance and secure network backbone without creating a costly dedicated nation wide infrastructure. The proposed China National Financial Network will be a virtual network backbone. The network will structured such way that data traffic will be separated from other commercial networks such as CERNET, GBNet, China Net and CASTNet. But it shares the costly underlying commercial ATM communication infrastructure. The virtual backbone will allow CNFN to operate independent of bandwidth requirements from other commercial networks. Within the CNFN domain, it needs to allocate network resources according to the application requirements as well as each financial institution's need. The mechanisms to deliver differentiated QoS require care consideration and investigation.

Network Centers

Network Centers are the physical access points for lower level networks. Below the National Network Infrastructure are Metropolitan Networks that cover citywide areas,
and many regional subnets that cover the rest of rural regions. The data communications
among the different network regions are handled through the network centers. The
network centers are collections of advanced network communication equipment,
monitoring devices, security mechanisms and some advanced application servers. Within
the centers, many advanced information technologies such as protocols that support
differentiated QoS, data encryption and bandwidth control are implemented. The
network centers are ideal places for advanced nation wide application servers. The
design goals of the network centers are to allow them to deliver network services that are
rich in feature, high in performance and low in cost.

2.4.2 Quality of Service (QoS)

Different applications need different service qualities. Some the network QoS
parameters are bandwidth latency and lost rates. The advanced network-based financial
applications are emerging. Those applications will greatly enrich our financial activities.
However, the impediment to realization of those applications is the QoS of current
network services such as current commodity Internet. Because in the large network, the
interconnection is very complex and dynamic, the QoS guarantees are very difficult.
Service quality can be classified into following:

- Best-effort (no QoS)
- Stochastic guarantees (for 99% of all packets the delay will <5 ms)
- Deterministic guarantees (no possible)

The goal of the network system is to provide high level of the stochastic guarantees. The
components in the network are listed below.

Router and Bridge

Routers and Bridges are basic building blocks of the WAN (wide area network) and
the Internet. The function of routers and bridges are to forward the packets on the
networks to their appropriate destinations. Routers and bridges do so by exam the
destination address of the packet and compare it with its routing table. If the address is
an unknown destination the router or bridge will send out a routing discover call.
Because they use shared media, the QoS is difficult to control. As new set of application
software is becoming available, the network traffic pattern is shifting dramatically. Unlike before, the function of the network is to deliver data, now many mission critical applications demand high level of QoS.

**Switch**

Switching is a new technology trend in networking. Unlike traditional broadcast-based shared-media hubs, switch provides an end to end dedicated link. The two forms of switching are frame switching and cells switching. Frame switching forwards traditional network packet frames, while cell switching, commonly known as ATM (Asynchronous Transfer Mode) switches forwards 5 3 byte cells instead of variable-length frames. The fixed length allows ATM to operate at much higher speed 155 to 622 Mbps.

Total demand for switches in is expected to be 165 million units by 2000. This means that 40 million additional switches are needed by 2000. It is likely that China will exceed this target, installing a total of 180 million switches by 2000. The total demand for switches through July 1998 was 120 million units. Demand is increasing at an average of 1.1 million units per month. According to estimates, the total cumulative demand for switches will be 126 million units by the end of 1998. Demand this year for lines for computerized switchboards is estimated at 23 million lines, including network connections and 3 million dedicated lines. By the end of 1997, China had about 24 million mobile switches and planned to install 10 million additional switches in 1998. By 2000, a total of 56 million mobile switches are planned. Total demand for 1999 is estimated at 10 million units.

**Internet**

Internet is the largest world wide public network. The networks was designed and built around 1980s using packet-switching based technologies. The internetwork covers very country on the earth. It provides low cost and high availability electronic services to many people around the world. Although Internet currently provides valuable services and low cost services to many people around the world, it also has many inherent short
comings for emerging network based applications especially for those financial applications. Some of the most glaring problems are low QoS and lacking of adequate data security on the Net.

Database

Database is an integral part of business. Financial services are information intensive processes. Business requires heavy number crunching such as banks largely use index sequence database such as IBM IMS system. SFN cuts across a wide range of businesses. There is a large variety of database systems currently in use by financial institutions in Shanghai. Other financial institutions might favor SQL based database from Oracle, Microsoft, Informix, and Sybase. The network system not only needs to connect those dissimilar hardware platforms and databases together, but more importantly also have to provide a common standard for all companies to communicate with each other.

ODBC is the standard database protocol of the industry. However, many older database systems do not have native ODBC support. In those cases, an emulation or proxy server needs to be implemented. The proxy server will stand in as the translator for ODBC message and the legacy systems.

The above discussion defines the context of the problem in terms of current state of information technology in China, the objective to be achieved and constraints. This leads to the requirement analysis.

Section III: Requirement Analysis and Conceptual Design

3.1 Requirement Summary

This proposal will focus on three different areas of requirements for CNFN. They are application requirements, network service requirements and network infrastructure requirements. The applications are the most important part of the network. Application requirements are defined by the functional requirements of the system. Network
applications use services provided by the network to accomplish their tasks. Advanced applications demand network services to meet a set of minimal standards. With the current Internet the major impediments to the realization of advanced network applications is its lack of advanced network services. Although the Internet provides low cost and convenient network solutions for many businesses, the Internet lacks many desirable characteristics that are demanded by next generation software. The CNFN seeks to enable those technologies. It can do so by developing common standards in communications, network interfacing, and network messaging that is required by future financial applications. The advanced network services are delivered by a collection of communication hardware. To support advanced network services, there must be a nationwide high performance and secure communication environment. This network fabric will be large and robust enough to support nation wide real time application software.

The overall application design goal of CNFN is three fold. First the network will become a financial information system delivering vital statistical and informational data to the Peoples Bank of China (PBC). Using the network, PBC can gather broad, accurate and timely data from banks and various financial institutions in the country to provide an accurate and timely picture of the country's economical activities. Second, the network will also function as an information distribution system for banks and financial institutions. Finally, the network will provide an infrastructure that will support electronic commerce. Several on-line business services as well as personal financial transaction services will be made available by providing a secure, reliable, comprehensive and easily accessible infrastructure for making payments and offering banking products to consumers and corporate customers. Three main application subsystems will be designed to implement these requirements.

3.1.1 Payment System

Commercial banks provide various payment services to their customers. Commonly provided services are issuing cashiers check and credit cards; withdrawal and transfer service based on demand deposits, inter-bank fund transfers, etc. Recent
financial innovations and customer demand for better financial services have led to the provision of new payment services such as on-line corporate banking and home-banking services. Because the transaction amounts and transaction time requirements are very different it is necessary to design more than one independent payment systems.

Requirements for the payment system depend on services that commercial banks provide to their customers. Payment services allow fund transfer between banks without the exchange of cash or checks. Two types of payment systems are required. One service, the Inter-Bank Electronic Payment System, can be used for small amount transactions such as: collecting monthly fees for public service and utility companies. This system would eliminate loss or misappropriation of funds associated with direct cash payment. Another service, the Large Amount Payment Transfer System, can offer large amount real time money transfers between banks. Requirements of the two transaction systems can be very different. For the Large Amount Payment Transfer System, timing is the most critical requirement. Large amount transfers require real time settlements. On the other hand, the Inter-Bank Electronic Payment System requires a low cost approach. With the cost it incurs, real time settlements should never be used for small amount transactions. The following is the discussion of the different payment systems.

**Inter-Bank Electronic Payment System**

One of the financial network requirements is a small amount payment system. This system will provide small amount fund transfers between banks. The services include payment services for saving accounts, currency exchange and public services, clearing house service and automated banking services.

Automatic Response Service System (ARS) and Automatic Teller Machine (ATM) are automated services that allow banks or financial institutions to offer their clients on-line corporate banking and home banking. On-line banking is required to respond to the rapid advances in information and telecommunication technologies and diversification of customers' financial needs. The services are provided through a nationwide network such as CNFN. CNFN will handle financial transactions for homes.
and banks using host computers, personal computers, telephones, facsimile machines and ATM terminals. The service typically covers financial and accounting information services, fund transfers, and financial and economic information services. Using the ARS system, a customer can obtain information by telephone. The ATM system provides customers with services such as cash withdrawal and fund transfers through cash dispensers and automatic teller machines located at any bank. As China’s communication system continues to improve ATM machines could be put anywhere making banking services more accessible to the population.

Currently, the data for those three systems are delivered manually via paper or diskette. CNFN clearing facility will provide an automated small value payment system, providing automatic transmission and account reconciliation. Timing is not critical since most of transactions will be small. Low transaction costs is the primary design goal. Therefore, the large amount real time payment system can not be used for these services.

**Large Amount Real Time Payment System**

The Large Amount Real Time Payment System must support real time large amount payment transactions. For that reason, this system should be separate from the small amount payment system. The connections should avoid network intermediate connections and use high-speed lines. The clearance and payment transactions should be done in real time.

PBC currently uses a centralized collecting and net settlement method to settle fund transfers among the banks. As the number of banks and services increase, this method is becoming inadequate. The new central bank clearing system should connect PBC to the computer systems of each commercial bank via PBC-wire. This system will facilitate large value fund transfers between banks that can be executed electronically and settled on gross basis across each bank’s current account with PBC.
3.1.2 Statistics Information System

PBC is responsible for the well being of nation's financial system. As the importance of financial markets grow in China's economic system, they are attracting ever more attention from regulators and central government. PBC needs to monitor each exchange's daily activities as well as collect data for policy making purposes. Three subsystems are required.

*Foreign Currency Management System*

To improve international trade, CNFN needs foreign currency management system. The system will use The Peoples Bank of China to collect all foreign trade related information and forward it to the Currency Management Bureau. This system will provide reliable international payment data. This data will enable PBC to intelligently formulate new national currency policies.
Equity and Bond Registration System

A national equity and bond registration system is needed to improve storage and transfer of securities, to provide better control of government bond market information, and to establish a national macro monetary policy. This system will use CNFN to collect data from each commercial bank. Summarized data will be encrypted and transmitted via point to point connections to the database a system located at one central location.

3.1.3 Information Monitoring System

Financial Market Monitoring System

For better anticipation any financial market changes, the Financial Market Monitoring will collect and process daily trading data and economic information. At the same time, any new currency and market policies will be delivered to each financial institution via this system.

3.2 Financial Information System Strategy

One of the major functions of the CNFN will be to provide financial information to China's banks, financial institutions, and general population. The Financial Information System will provide real-time financial data and information. The system will supply any financial related information to users on demand. The system will provide large quantities of business and commercial data at low costs.

3.2.1 Design strategy

The design strategy starts with forming a National Internet Governing body. This body will draw talented people from various interest and organizations - MPT, Academy of science, Department of Electronics and etc. The function of the governing body is to oversee technological developments and to maintain a set of common standards for China's Internet. In addition to maintaining Internet standards, it should also forester and encourage new innovations.
The design of the physical network will stress the qualities of services to be delivered. The new network will be based on MPT's existing hardware. However, new communication technologies should be explored in the interests of feature growth.

After the network infrastructure is defined, the design will address integration issues. The CNFN will connect thousands financial institutions together. Sharing data with different hardware platforms and databases will be major task for the designers. To minimize the over-all costs of integration, open standards on the network will be established for each financial institution to interface. The network should maintain a set of network standards for all financial institutions to follow. The standards should include new protocols that will deliver advanced network services. However, it will be the responsibility of each financial institution to determine their own best solution.

Finally, the design will address the interface with the Internet. Security is the main concern here. Due to proposed infrastructure design, connections to Internet will be concentrated at network centers. This design facilitates administering a centralized security policy. Network centers will implement a set of stringent security policies.

3.2.2 Organization Strategy

Currently, there are several major players and interested parties in the Internet business in China. One of the major players in the Internet business is MPT. MPT maintains its own nation wide network - China Net. But more importantly, it supplies communication links for all the nation wide networks. Its technology investment decisions will impact the long-term technology landscape of Internet in China. Other players include Academy of Science, Ministry of Education, Ministry of Electronics, and PBC. Their roles in the Internet are limited to maintain their special purpose nation wide networks. Although their network objectives can vary widely, it is in their common interest to adopt set of national Internet standards. Based on those facts, a National Internet Governing Body (NIGB) should be formed by joint forces from MPT, Academy of Science, Ministry of Education, Ministry of Electronics, PBC and other interested parties. An organization chart is shown as follows:
The Ministry of Information will be the Executive Committee of the body. The top leaders form each organization will be responsible for defining long term direction and commit necessary resources from each organization for long term projects. Under the Executive Committee are the technical committees. They are the Infrastructure Committee, Standard Committee and Security Committee. The Infrastructure Committee is responsible for overseeing current and long term infrastructure design, testing and implementation. It presents recommendations to MPT for any new Internet related technologies.

The Standards Committee defines set of Internet standards, oversees their development and testing, and finally provides technical specifications and certifications to the users. The Standards Committee can be further divided into sub-committees by the subtasks. For example, there should be a sub-committee on financial transaction standards. On top of the already defined Transmission Communication Protocol / Internet Protocol (TCP/IP), financial institutions need another layer of the protocol to conduct financial transactions. Other sub-committees can be formed to define network file transfer protocols, directory service protocols, multimedia protocols and etc.

The Security Committee monitors and maintains all the nation wide networks. It is responsible for all the connections to the world wide Internet, as well as the security of
CNFN. The Security Committee should go beyond defining network security policies. It needs to participate actively in day to day security operations, which include but are not limited to monitoring data coming into the country from overseas, detecting unauthorized breaks-ins and eavesdropping on the national network, safeguarding the integrity of CNFN and provide disaster recovery services.

3.2.3 Network strategy

One of the important CNFN indicators is that the financial network must guarantee high quality of the service (QoS). Some of those qualities are transmission speed, bounded delay and delay variance, throughput transmission reliability and data security. Meeting those requirements are designing challenges.

The financial network will be a competitive production network, not a network research experiment. A key guiding principle is to use off-the-shelf technology wherever possible. Nevertheless, in implementing NFN, some research questions must be pursued. The research questions should relate to network itself as opposed to specific application areas. They can include following areas:

- Network service requirements. What are the QoS requirements for the set of most demanding applications?
- Protocols for delivering different QoS levels. How much state information must be maintained in network devices to deliver high-quality differentiated service?
- Cost Allocation: How should cost be fairly allocated to multiple levels of QoS.

Beyond these technologies, The financial network must also provide cost effective services. The networks should provide an infrastructure that allows its end users to choose services and manage the costs. The funding for network maintenance and future upgrades will be generated from its server fees. The acceptance by the financial community is critical for the networks long-term survival. One way to entice financial institutions to adopt this vision is to lower the entry costs to the network. Under the
principle of not impeding future developments, design should use as much existing technology as possible.

There are two important network design goals for CNFN. One is to integrate all the existing nation wide networks into a nation wide backbone that will be dedicated for Internet traffic. The second one is to prepare it for new generations of distributed financial applications.

Currently, there are four nation wide Internet systems exist in China. Each of them is dedicated for a specific mission, and is run independently. This poses a great challenge for forecasting technology innovations that need large investments for the underlying technology. The goal is to consolidate all the Internet connections into one nation wide backbone. This will require all the networks to share common network equipment and the backbone. But they can be separated logically. Logical separation of networks will allow each network to maintain its own security policies and bandwidth allocations. The aggregation of network equipment can decrease each network's investment costs for the new technologies, and the maintenance costs of operations.

Networks exist to move application data. As applications become more and more network centric and rely more on network data. The traditional way of network design has to be evaluated, in the early phase of network evolution, building connectivity and creating basic interoperability among major groups of systems were the primary goals. Now, Information technology is taken on new challenges by deploying mission critical applications on the distributed networks. Deploying application software on current distributed networks is enormously difficult. Network architectures lack necessary capacities and characteristics for distributed applications. As the result, network designs are more and more focusing on network performance as one of the design goals. One well-designed network system can not only move data among different groups of the system; it must also guarantee some levels of QoS.
One solution to address those design goals is to create a network center at a major city within a network area. The network centers provide the access points to the regional networks they cover. All network maintenance and security monitoring will be done at the network centers. Between network centers are high-speed ATM switches providing high-speed data throughput and logical partitioning. Network center configuration provides several benefits. Structured, hierarchical ATM based network centers and centralized network access points are the two essential steps to achieve standardization and security network environment. This switching technology offers guaranteed quality for network services. It is important for the future mission-critical client/server applications, that require a reliable, high performance and secure network infrastructure. The network centers also make network administration and security monitoring easier. Centralized connection allows repair and trouble shooting communication equipment much easier than they are dispersed. The network security also is improved when the network interfaces with the world wide Internet can be well defined and monitored. Because those interfaces use standard equipment, the security policies will be greatly simplified.

3.2.4 Integration strategy

Integration is the most difficult problem in designing CNFN. Network design faces a complex problem of absorbing and supporting a large number of disparate core systems, which are result of many years of internal development. There is little or no easy means of communicating between those systems. The challenge is to allow financial institutions to access and deliver diverse information across disparate systems to provide all financial institutions a single view of their relationship with the whole network of financial institutions.

The lacking of standards in interfacing with financial institutions discourages new software development. Within the financial institutions’ information systems, there is a wealth of information. New software is needed to unlock those data. One of the objectives for CNFN is to create a financial information center to collect and store those
valuable data. Developing unique interfaces for each information system is too costly for any software company to bear. A solution to this problem is to define an open, cross platform standard messaging interface. This interface will provide secure information exchange among financial institutions, regulatory agencies and the central bank. The existence a communication interface standard will decrease software development costs for software companies. Therefore, it will encourage new developments and innovations in software development.

The financial information system in China is multi-server, multi-service, multi-vendor and multi-network. CNFN is a network that encompasses a large network of dissimilar servers and databases. The goal of CNFN is not only to connect those systems together, but also to create an environment such that distributed computing will be possible. Integrating a multi-vendor large-scale network is a major challenge. To support a multi-vendor platform and database system, one solution is to separate the application from the database. Applications will process transactions across the network. The applications are made of a collection of objects and interface with a set of well defined network protocols. Because the data that the application software needs are stored in the systems of different financial institutions, those object components will be distributed across the network.

The information system allows network objects to access the database by implementing a 3-tier architecture. 3-tier architecture partitions an information system into 3 layers: application layer, middleware and database server. The middleware makes the database and hardware system transparent to the application software. In the center of CNFN design is a middleware layer. Middleware creates a common view of all the services on the network. In order for client/server computing to carry out mission critical financial operations, it will require high quality QoS and well defined middleware features such as transaction message protocol, network security, remote protocol and directory service.
Another task is to create a financial transaction message standard. The objective is to create an open, cross-platform standard messaging interface that will be employed by banking transactions within the CNFN. This message standard is to enable financial institutions and their allied application developers to utilize and explore the power of network based applications. This message standard should be independent of operating system, programming language and the communication/messaging software. The message should not carry any platform dependent information. Intelligent middle-ware on both host and client system will wrap the message in the envelope or carrier frame of the underling system. The design principle of the message should follow some general guidelines:

- Provide a flexible way to define data that is both unambiguous and concise.
- Support both client/server and client-server-host models of computing.
- The message standard should be independent of the underlying client/server technologies. This includes user interfaces and network transport mechanisms.
• The message standard should be portable across major hardware and operating system platforms - client server and mainframe.
• The message standard should have build-in security mechanisms such as PIN and encryption.
• The message standard should provide an easy programming environment. This would require it to interface with common programming languages.
• The message standard should be flexible enough for future expansion and technical innovations.
• The message standard should be compatible with international message standards. In the long term, CNFN will become part of the global financial network.

3.2.5 Security strategy

Security is an important aspect of the CNFN. The network is designed to carry a large amount of public and private financial information and transactions. Information such as monetary policies and directives from the central bank are highly sensitive. Any information leaks due to eavesdropping on the network can damage the confidentiality of the investment community. Furthermore, there will be hundreds of thousands of financial transactions cross the network. Many of those transactions will be nation wide or even international. Any network failures due to attacks will cause panic in the financial markets. This means that network security is very important. One conclusion from this analysis is that CNFN should be a semi-private network. It should be dedicated to financial usage only. That will require that the network be logically separated from other commercial networks. On the other hand, at network centers, NIGB will define and execute a set comprehensive security policies and sophisticated monitoring systems.

Network security is one of the major concerns of the CNFN. It will carry a large amount of sensitive financial information and connect to every bank’s production system. A secure network allows authorized users to access the network resources unhindered,
but prevents access to network resources and private information by any unauthorized users.

Network security mechanisms include security policies, technologies, education and implementation of the policies. An comprehensive security policy must include published security guidelines regarding client responsibility, well defined operation policies on the network and service access, user authentication, data encryption, virus protection and client education. A network and service access security system involves setting up a protected premise for network resources. This is often accomplished using firewalls. A firewall sets up a barrier between network resources and the public. The firewalls are usually placed at centralized network access points. At those points, all incoming and outgoing data are filtered. The goal is to keep hackers, crackers, vandals and spies out of the protected network. Security is very complex issue. It warrants a detailed and comprehensive analysis. Below, some minimal guidelines for designing a firewall are be discussed.

To select a Firewall, there are several questions must be answered.

1) What is the security philosophy of the network?
   There are two stances on network security philosophy. The first one is that all the traffic that is not specifically permitted is denied. This means that only carefully selected services are granted permission to access the network. The second one is all the traffic that is not specifically denied is allowed.

2) What is the security policy of the organization?
   In order to design an effective overall policy, the network administrators must know what data are to be protected and what is the premise of the defense. In a large scope network such as CNFN, there are a large number of resources on the network. Those network resources have different security requirements. One solution is not going fit all.
3) What are the components of the firewall system?
All firewalls consist of three basic components.

1) Packet filtering router
Packet filter Firewall makes the simple decision of forward/deny for each packet. The decision is depended on the EP source and destination addresses. It is determined by comparing EP addresses with the security rules in the routing table.

2) Application level gateway
An application level gateway offers tighter security controls. It allows only permitted application service requests.

3) Circuit-level gateway
A circuit level gateway relays TCP connections. Doing that effectively hides the internal network from outside world.

3.3 Conceptual Modeling
The financial information system is an aggregation of servers, databases, applications, network connections and security policies. The value of the network is its ability to collect, process and distribute valuable information, perform financial transactions on-line and generate vital financial and economic statistics.

Because CNFN is very long-term project, its design must address technological as well as organization issues. The current state of the Internets' organizational structure is not suited for quick adaptation to new technological innovations. Currently, four networks compete for limited resources at the time when technology leadership and corporation are required. Without leadership, there will not be innovation. To ensure the success of the CNFN, there must be a powerful technical body to define, implement and maintain a series of standards. This body must also be able to influence future directions of Internet technologies in China. With the current segmented Internet landscape, this is not possible. Developing new state of art Internet technologies require large investments in technologies and people. Many highly talented engineers and scientists must to work
together to develop a state of the art Internet. None of the four current national networks has the resources to undertake those tasks. Furthermore, network management should be centralized. Currently, the four networks do not have full control of network traffic and security policy.

3.4 Spiral Model

Designing CNFN system is a large and complex engineering endeavor. The design process is necessarily an iterative one. For this reason the spiral model should be used during all phases of the project. There should be two main design groups researching and developing the project. They are the network architecture group and the application development group. The two activities are to be conducted simultaneously. The design and development of such a large scale network will face many difficulties. The primary difficulty is the absence of system requirements. To successfully design and implement the network requires researchers to take many iterative steps. Each development cycle produces a base line product that provides a necessary starting point for the next stage. Each successive stage starts with a better understanding of the problems that need to be solved and generates a new set of objectives designed to solve those problems. With a better understanding of the desired applications, new network services can be considered. This continues a feedback and feedforward loop between the designers and results in identifying required network services and applications. This cycle is repeated until the final network design is approved. This design model results in lower overall cost and minimal risk.

The goals of the system design encompass a wide range of application, technical, and economic objectives. It will take long-term improvements and refinement rather than a quantum jump to achieve the ultimate objectives. This is why this method of design is the best choice for this project.

3.5 Concept of Operations

The concept of operations is based on the overall design strategy. The CNFN will use the advanced communication equipment provided by MPT. Centralized network
access points are located at network centers. CNFN will also implement and maintain a
collection of application servers to provide a wide range of services to the financial
community. Those application servers will be responsible for financial transactions,
information processing and statistics gathering. The financial transactions will require a
message standard. This message can be based on well-established financial transaction
protocols such as the Gold standard used by Globalnet. The message defines the required
message fields that are necessary for financial transactions. Underneath the message
standards are set of interface standards including network transport, database driver and
communication access standards.

Applications will generally consist of 3 layers: user interface (UI), middleware
(application servers) and backend (database servers). User interfaces are the presentation
of the data to the end users. They will be created according to each financial institution's
needs. UI's communicate with the databases through application servers. Application
servers are collections of business objects and network service objects. Those objects
carry out important business transactions and network services. Because the application
servers can be distributed, applications will be highly scaleable. One such application is
the financial settlement system. The application accesses database and uses database
interface protocols. Database servers are generally located at secure locations at each
financial institution and centralized data center of CNFN. A database driver is
implemented for each database system. Application objects communicate with database
objects through those database drivers.

All application servers, network centers and financial institution's internal
networks on the network will be protected by firewalls. Application level firewalls
should be used between the application servers and the network. The national network
will also provide connection to world wide Internet. The connection to Internet will be
established at network centers. At those connecting points, firewalls will be constructed.
Because the main purpose of those firewalls is to block unwanted traffic from the outside,
a packet filter router can be used.
The concept of operation can be illustrated by a payment transaction process.

3.5.1 Thin Thread Analysis

A client at Bank initiates a payment transaction request. The beneficial bank (Bank A) requests a payment from a remitter bank (Bank B). A Bank sends a transaction request to the clearing house that provides financial settlement services. At the heart of the clearing house are the application servers that are responsible for the nations' financial settlements. The first request from Bank A is a transfer request. The financial transfer message contains well-defined structure. At transaction centers, the firewalls examine incoming packets. Often the transaction related requests are allowed to pass. After the application server intercepts and parses the message, it requests a transaction service by creating an object for the request. The object sends out an authorization request to the remitter bank (Bank B). If the message passes the challenges of firewall at Bank B, it is forwarded to the main system of the bank. The database driver implemented on the host system parses the message and translates them into database's native commands. Using the commands and business rules implemented at Bank B’s host system, a reply of the request is generated and forwarded to clearing house. The application server at the transaction center processes the transaction according to the message from Bank B. If Bank B accepts the transaction, the application server will send out confirmations to both banks. At the same time, a transaction journal is created at the center. The clearing-house settles all the outstanding transactions between banks via PBC-wire daily. An application level diagram is shown as below.
Fig. 6 Application Architecture
Section IV: Systems Design (Case Study)

4.1 System Configuration Overview

The CNFN needs an advanced nationwide backbone to deliver its information services. There are two very important goals in designing this backbone. The first goal is that the network must provide advanced network services for the new generation of financial software applications. Those applications require high QoS include guaranteed bounded delay, low data loss and high capacity. The second goal is provide affordable network connections to the most regions of the country. Currently, there are vast area lacking modern telecommunication services. In order to reach those remote places, CNFN must utilize satellite base communication system. VSAT technology can provide a quick solution to large area in short period of time.

A number of technical and practical considerations underlie the over all architecture of the CNFN. One is the network hardware design and the level of QoS that can be delivered by the network. Another consideration is the integration of the network. A third consideration is the security of the system.

The overall architecture of CNFN is shown in Fig. 7. The key to our design is network centers and distributed application architecture. Those network centers are high capacity and state-of-the-art interconnection points. Within those centers, the next generation network protocols are implemented. Through those protocols, CNFN can offer high quality guaranteed services. Between those centers, high-speed lines carry large quantities of data daily. In order to provide a uniform service for everyone, an abstraction layer is installed at each participating institution. The function of abstraction layer is to provide uniform network interfaces to dissimilar hardware platforms and databases. PBC will design, maintain and publish a set of financial protocols and network interface standards.
Connecting to the financial network are advanced application servers. Those application servers handle two functional requirements of the financial network. They are the Payment System and the Statistics and Information Monitoring system.

The payment system supports two different payment methods. They are small amount payment system, large amount payment system. The payment system should be effective and capable of handling all the payment needs in a cost-effective way.

Statistics Information system collects information on financial activities from financial institutions. Policy makers can use information to aid their decision-making process.
The Information Monitoring system collects financial information and information on financial activities from financial institutions. Advanced distributed applications process and store the data received from financial institutions in a centralized data storage location. Financial news agencies can also use this system to distribute news and information. Currently, The most widely used information delivery format is an open standard. It can transmit multimedia data on the net. The end users can view the information using a browser.

The design of the information system must meet the following characteristics:

1) Timely: It is necessary for the information system to provide results within short period of time. This property becomes more critical when the information is financial related.

2) Trusted: The network should guarantee the integrity of the data.

3) Affordable: The definition of affordable varies according to the services requested. In an advanced society, information should be so inexpensive that anyone can afford.

4) Accessible: Definition of the network access standards and 3-tier architecture will ensure that secure and dependable, efficient and cost effective interfaces between the CNFN and the systems of any financial institution. The abstraction layer will be implemented between the financial network and each institution.

5) Scaleable: The quality of network services varies greatly form one application to another. To be cost effective, QoS should be scaleable.

6) Commercial banks and financial institutions located in the same geographic area will join together to acquire a variety of network services form a regional center. Among the centers, the wide area interconnect service supports differentiated Quality of Service as well as highly secure, highly reliable, and high capacity transport. The regional center network has four technical components:

- Protocols and equipment that require advanced communications services.
- Application servers between the commercial banks or financial institutions and the network centers.
- Network managers consolidating and managing traffic from its clients.
- Security mechanism in the network centers.

4.2 Network centers

The heart of the CNFN design is the RNCCS. The RNCCs are centralized locations for switching local net transactions to the CNFN backbone. It has two important functions: delivering banking services and connecting various communication links; and providing network maintenance and security monitoring. RNCC is located at a major city within the region. Each center is designed to service one region of the country. It provides data communication among the financial institutions within the region. Communication to the outside of the region is handled through the ChinaNet backbone that connects each RNCC. Among the RNCC, the wide area interconnects service supports differentiated QoS as well as secure, reliable, and capacity transport. At the RNCC, differentiated QoS is offered to network and to the centers that support applications and data storage. Through those RNCCS, CNFN can provide advance financial services to the financial community in China.

A Network center is a regional network interconnect point providing access to the Inter-center network. Organizationally, one center is implemented to cover one region of the country. Physically, a network center is a secure and environmentally conditioned location that houses a collection of communication equipment and support hardware. Among the hardware in the network centers are ATM switches firewalls and advanced application servers.

The backbone of the network center is a collection of ATM switches and high-speed links. This backbone supports all nation wide Internet traffic. The high-speed 663 OC-12 link is used to connect ATM switches at the network centers.
At the switch, the high-speed link is spliced into lower speed links (155 OC-3). Each down link is capable to supporting all of the network traffic in the region. The subnets are logically separated. Although they all share the same hardware and communication devices, there are no interactions among the subnets. CNFN will be one of the subnets. At the network centers, CNFN will be divided further into metropolitan networks and regional networks. Each metropolitan net covers one large city in the region. Within the metropolitan net are access points to the financial institutions within the city.

Application servers at the network centers run advanced distributed applications. Those servers provide necessary network services such as transaction services, information services. Most of the services are scaleable. It is possible to install the same application at multiple sites. This will increase the execution speed by spreading the load and provide necessary redundancy.
Firewalls enforce access security on the network. Firewalls are placed between servers and the public network. Each server is dedicated for a single application. Moreover, the security requirements on those servers are high. An application level filter firewall can be used. Every request to a server is challenged by that server’s firewall. Use of firewalls is only one part of the overall network security policies. Firewalls only provide adequate security when implemented with other security mechanisms.

Network centers provide the connections to the world wide Internet. The network centers connect to the world wide Internet via a dedicated link. Packet filtering firewall routers are located between the network centers and the world wide Internet. The objective of the firewall is to block unauthorized traffic. The security stance at those points is to allow all traffic that is not specifically denied.
A sketch of the network center is shown in Fig. 10. At the right hand side of the Figure are commercial banks and financial institutions. Each client can have dedicated 10 Mbps point to point connection to the network centers. On the left hand side is the connections with other centers and application servers. Among the network centers, the wide area interconnections must support differentiated QoS as well as highly reliable, high capacity transports.

**Fig. 10 Network Center**

### 4.3 Network Functional Modules

A network center's key function is to exchange traffic with specified bandwidth and other QoS attributes between connected centers. To achieve that, a center must satisfy a variety of specific functional requirements.

**Protocols**

Currently the most commonly used protocol is IP. CNFN will obviously support IP. Ipv4 is the current standard. Ipv6 will be the future standard. So, the networks
should support both Ipv4 and Ipv6. There are other new protocols under development. They should be also considered, but should not be implemented until they become mature technologies.

Speed

Bit rate of connections into a center or between centers will vary widely. Each center has to make sure it has adequate capacity to handle the future traffic load. Switches will provide primary interconnectivity in centers.

Network center

Network center should be managed by MPT. However, CNFN should be responsible for naming national primary process centers, backup process centers and application centers.

Linkage

Linkage between centers will utilize ATM cell switching. Most the centers will be located in the city where MPT has existing digital lines for leasing. However, in areas outside of city, digital lines are not widely available. All of the locations should have analog Telephone lines. Those regions can use remote dialups. Regional aggregation centers can install remote access servers. Banks and financial institutions at remote locations can dial into the regional aggregation center near them. Aggregated network traffic is connected to the Local network center. Digital leased line should be used if it is available. Otherwise, microwave based communication channels can also be utilized.

Regional aggregation

In some regions, the data requirements are not sufficient for a full functional center. Hierarchy of aggregation of exchange points should be encouraged. However, the aggregation levels should be limited to one to two levels. Doing so, not only provides cost effective connectivity for the region, but also maintains consistency throughout the entire network.
Critical properties

CNFN is made of the applications that requires high-level network services; the network centers provide advanced network services; and the advanced network devices interconnecting the network centers. The design addresses the following requirements from the system.

1) The network is designed to provide high speed, reliability and differential QoS of network services.
2) The network software architecture allows easy integration for a diverse choice of hardware platforms, operating systems and databases.
3) The network security mechanisms guarantee reliable, secure and dependable transmissions.

QoS

This network design offers differential levels of QoS, high flexibility, and high manageability. Increase network performance has always been the primary objective of network designs. Because shared access LANs have limited bandwidth, any growing networks can experience bandwidth problems. The traditional solution is micro-segmentation of the network. Network-segmentation, using routers, increases complexity of the network and therefore makes future reconfiguration and upgrades very difficult. Frame and cell switching offer each node its own segment, providing dedicated access to the backbone system. While provide high performance, switching also provides added flexibility. Because it carves the networks into smaller pieces, it makes logical networks possible. In a switched network, the network can be separated into virtual subnetworks. Each network is separated from the others even though they share the same physical devices. This way, CNFN can be separated from other national networks such as Chinanet, Gbnet and etc. Network designs that use virtual networks add security and flexibility to the overall system.

One of the critical requirements for CNFN is reliable network operation. Designing centralized network centers enables easy network management, fast troubleshooting and problem isolation. Because all of the regional communication devices are
housed in one location, network security is also improved. All traffic on each port, in each network center, can be closely monitored. Information gathered from the monitoring can be extremely valuable for trouble-shooting. Centralized network centers also provide ideal locations to implement the security system and other advanced services. All the traffic on the network will have to pass through centralized points. Firewalls at those points are highly effective.

With switching technology, each port receives dedicated bandwidth. So each financial institution is guaranteed to have an allocated bandwidth. This is a critical feature for networks of the future. Unlike traditional shared access media, switching delivers high performance, provides excellent response time, and offers guaranteed capacity. Those are critical properties that are required by next generation application software.

4.3.1 Interface with Customers

In order to protect the customer from making substantial modifications to their back-end system infrastructure, a 3-tier architecture is proposed. Furthermore, a financial message standard will also be defined. Rather than require financial institutions to replace their current processing system, a system abstraction layer will be installed between the CNFN and the their back-end systems.

The abstraction layer hides platform specific information by translating system specific data into system independent transaction messages. The message standard should be robust enough that no native functionality will be lost during the translation. The resulting message is wrapped in an envelope that a carrier frame requires. At the receiving end of the message, the envelope is removed. The message is presented to the application server. The intelligent middleware converts the message into the native platform specific data and presents it to the application.
4.3.2 Function of Transaction Message Protocol

The transaction message is responsible for communication between the application and the database. The middleware and message protocol need to support following functions:

1. Basic payment validation.
   The transaction message protocol should include the means to notify the originator of any possible execution problems before completion of the business transaction.

2. Selection of Payment methods.
   Selection of payment methods will be based upon explicit user request and implicit requirements derived from transmitted payment characteristics. For example, money transfer is used for immediate payment where ATM is unable to handle the transaction. This would be the case if the transfer value were too high (above
$500). The application that handles the transaction will determine the method of the transaction.

ATM: Automatic Teller Machine
SAT: Small Amount Transfer
LAT: Large Amount Transfer
BFT: Inter-Bank Fund Transfer
NIC: National Information Application Center
NSC: National Statistics Application Center

Fig. 12 Middleware-Middleware Communication

   The middleware server will format the message to be passed to the banks’ payment system. Most payment processing including accounting, billing and advising will be carried out by banks’ existing payment system. This portion of the middleware will be developed independently for each bank. However, only layers that handle the lower layer of the physical and logical interfaces will vary from bank to bank. Standardization of all of the common facilities in middleware design should reduce the development work for each bank to a minimum.

   There are several existing transaction message standards that are already under implementation. One of the notable ones is the GOLD message standard, which is supported by IBM and 27 of the largest banks in North America. The GOLD
message standard tries to address many similar issues that are common to CNFN's transaction system. It will be cost effective to adopt the GOLD message standard and make minor changes to the fit the needs of CNFN.

4.4 Flow Control and Network Management

In CNFN, the Regional Network Control Center is the point of flow control, activity monitoring, and network management. Network management is challenged with responding to advances in technology, to the constant increase in users needing connectivity to their networks and to departmental demands while facing increased scrutiny and reductions in information resources management budgets. Managing change and maintaining quality of service are particularly challenging in a network environment.

The NRCC fulfills the functional requirements of flow control and access control. It provides information concerning network performance, disturbances and configuration changes. The Control Center is the place to gather the performance data desired on selected groups of users during peak and non-peak periods. The billing information for all financial network users is gathered and formatted at RNCC.

For flow and access control, RNCC provides direct connection with network backbone switches. On the other end, RNCC provides easy and secured access to a variety of financial information and network configuration or status files. It verifies the users and their access rights. The Control Center also provides historical journals of all network activities and financial transactions.

The smooth operation of CNFN is dependent on Gathering security and operating characteristics about the network's behavior, Acting on this information to solve user technical problems, Making design changes in upgrading and monitoring the security mechanism, equipment, and software.
4.4.1 Network Manager

At each RNCC, a network manager is the person who defines the services known to the system and used in the Security Policy. All network services are screened and controlled, even those that are not defined. A comprehensive set of TCP/IP and network services is pre-defined.

NRCC NETWORK MANAGER’S RESPONSIBILITIES

- HELP DEFINE, PRODUCE AND MAINTAIN OFFICIAL SECURITY POLICY AND DOCUMENTATION.
- MONITOR, AUDIT AND TEST SYSTEMS FOR POSSIBLE SECURITY PROBLEMS.
- MONITOR SECURITY NEWSGROUPS, MAELRNG LISTS, POSTINGS AND RESPOND TO THEM ACCORDINGLY.
- TEST, INSTALL AND MAINTAIN SECURITY PACKAGES AND PRODUCTS,
- TEST AND INSTALL PATCHES AND FIXES FOR SECURITY BUGS IN VENDOR SOFTWARE.
- DEVELOP SECURITY PRODUCTS SPECIFIC TO YOUR SITE.
- STAY CURRENT ON TECHNOLOGY AND POSSIBLE THREATS TO THE ORGANIZATION.
- PROVIDE INVESTIGATION, COORDINATION, REPORTING AND FOLLOW-UP OF COMPUTER NETWORK SECURITY INCIDENTS.
- COMMUNICATE WITH INVESTIGATIVE ORGANIZATIONS AS NECESSARY.
- PROVIDE SECURITY AWARENESS TO MANAGEMENT, SUPPORT STAFF AND USERS AND RAISE SECURITY CONSCIOUSNESS AT ALL LEVELS IN THE ORGANIZATION.

4.4.2 System Status Monitor

The Inspection Module includes robust status, auditing and alerting capabilities. The System Status window displays a snapshot of all the FireWall Modules and
Networks routers at any given time. Status includes FireWall Module status as well as packet statistics (accepted, blocked, logged, etc.).

NRCC provide a mechanism for automatically recording some aspects of user and system activity. This monitoring mechanism, if used regularly, can help to detect evidence of viruses and related threats. Early detection is of great value, because malicious software potentially can cause significant damage within a matter of minutes. Once evidence of an attack has been verified, managers can use contingency procedures to contain and recover from any resultant damage.

Effective monitoring also requires user involvement, and therefore, user education. Users must have some guidelines for what constitutes normal and abnormal system activity. They need to be aware of such items as whether files have been changes in content, date, or by access permissions, whether disk space has become suddenly full, and whether abnormal error messages occur. They need to know whom to contact to report signs of trouble and then the steps to take to contain any damage.

Use the system monitoring/auditing tools that are available. Use tools as available to help read the logs, and determine what level of monitoring is adequate, and cut back on the level of detail as necessary. Be on guard for excessive attempts to access accounts or other resources that are protected. As a further aid to monitoring, use alarm mechanisms found in some access controls. These mechanisms send a message to the audit log whenever an attempt is made to access a resource protected by an access control.

If no system monitoring is available, or if the present mechanism is unwieldy or not sufficient, investigate and purchase other monitoring tools as available. Educate users so that they understand the normal operating aspects of the system. Ensure that they have quick access to an individual or group who can answer their questions and investigate potential virus incidents.
Purchase or build system sweep programs to checksum files at night, and report differences from previous runs. Use a password checker to monitor whether passwords are being used effectively. Always report, log, and investigate security problems, even when the problems appear to be insignificant. Use the log as input into regular security reviews. Use the reviews as a means for evaluating the effectiveness of security policies and procedures. Enforce some form of sanctions against users who consistently violate or attempt to violate security policies and procedures. Use the audit logs as evidence, and bar the users from system use.

4.5 Network Security

Network security is a major concern in a public network. The common practice of network protection is installing firewalls at the connection points to the public network. Today, almost all the firewalls are implemented at routers because routers can access layer 3 and higher of network protocols. However, this kind of firewall design cannot be implemented at ATM network. In an ATM network, once an ATM connection is setup, there is no intermediate process to interpret the data pass that connection. Otherwise, it would violate the nature of ATM switching. Therefore, it is only possible to implement firewall and other security mechanisms at the boundary of the system.

Security is one the most critical properties of the network. However, security cannot be achieved without greatly degrading other services. Because of its importance, this warrants separate research. Here, only a simplified version of the analysis is presented. Two security concerns are addressed here:

Network break-ins.

This is the most common security risk. An unauthorized user logs on to an internal server. The unauthorized accesses can cause irreversible damage to a company’s data. Damages of this kind are very costly to the target companies. Firewalls are a common mechanism used to prevent this kind of unauthorized access. Firewalls are implemented at every centralized access point of a network center.
Firewalls block unauthorized users from gaining access to the internal network or to any of its components. By setting up a cascaded set of security barriers, a firewall can completely hide the internal network from prying eyes. While a firewall sets up barriers to the internal network, it also needs to permit authorized and desirable operation to continue unimpeded. Firewalls that are designed well will also have sophisticated logging and audit trails.

There are several different kinds of firewalls: packet-filtering routers, application level proxy and stateful inspection. In the network centers, an application level proxy will be used to protect the advanced application servers. There are no interconnections at all between the local and the external network except for the proxy server. The firewall “knows” each application that is allowed to pass. This makes the network very hard to invade. On the other hand, connections to the world wide Internet are protect by packet filtering routers. It is set to pass all the data except those specifically denied.

Unauthorized eavesdropping

Because of the large amount of confidential information that will be transmitted by the network, any information leak because of eavesdropping on the net can have unwarranted consequences for national economy and investment community. To prevent unauthorized eavesdropping, all information on the network must be encrypted. The NFN must implement a proper encryption standard that all the financial institutions must follow. Today, the most commonly used encryption method is RSA, a public-key encryption system. It can be used to for privacy and authentication.

RSA Privacy encryption

Suppose A wants to send a message to B. A creates the encrypted text c using the following algorithm: \( c = m^e \mod n \), where e and n are B’s public key. A sends c to B. To decrypt, B uses the same algorithm: \( m = c^d \mod n \); the relationship between e and d ensures that B correctly recovers m. Since only B knows d, only B can decrypt.
RSA authentication

Suppose A wants to send a message m to B in such a way that B is assured that the message is authentic and is form A. A creates a digital signature s by using the following algorithm: $s = m^d \text{ mode } n$, where d and n are A's private key. A sends m and s to B. To verify the signature, B uses the same algorithm: $m = s^e \text{ mode } n$, where e and n are A's public key.

4.6 Data Dictionary (Sample)

Data dictionary definition of terms:

- **Name** – Primary name of data
- **Alias** – Other names used for Name
- **Where used / How used** – Listing of the services that use the data and how it is used
- **Content Description** – A notation for representing content
- **Supplementary Information** – Other information about data: Values, Restrictions or Limitations

Examples:

<table>
<thead>
<tr>
<th>NAME</th>
<th>ALIAS</th>
<th>WHERE/HOW USED</th>
<th>CONTENT DESCRIPTION</th>
<th>SUPPLEMENTARY INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>None</td>
<td>Kept in data store. Unique identifier for each account.</td>
<td>Account = [Bank Code + Account Type Code + Account Number]</td>
<td></td>
</tr>
<tr>
<td>Bank Code</td>
<td>Bank Number</td>
<td>Kept in data store. Unique Identifier for each bank.</td>
<td>Bank Code = any eight number string</td>
<td></td>
</tr>
</tbody>
</table>
Section V. Conclusion

China needs a low cost, secure and differential QoS financial network. This report addresses the challenges to construct a nation wide financial network. The network is designed to support future mission critical financial applications. These applications demand guaranteed quality of services. At the same time, financial network must also be a highly secure environment. Furthermore, it should be also minimize the integration costs if it is to be accepted by the financial community. To balance those conflict objectives is the greatest challenge.

The primary objective, to construct an advanced communication infrastructure is discussed but not fully achieved. A complete communication infrastructure requires more than sophisticated switches. It encompasses all the supporting mechanisms such as centralized information data warehousing and advanced financial applications. This part is discussed in suggested future works.

The secondary objective is achieved. A switch network can deliver differentiated communication services. The design addressed security issues. We discussed those problems in detail and also present solutions for them. Finally, the tertiary objective is also addressed. A detailed discussion on network design was presented.

This design utilizes switched networks center. It will allow CNFN to offer differentiated and guaranteed network services. Most importantly, the future CNFN will be a dedicated network with Internet-like features. By isolating it from commodity Internet and adopting comprehensive security policies, CNFN can really be secure from attacks and break-in. The case study in this report illustrated those network properties.
Appendix

Bibliography


Brett J. Vickers, Jaime Bae Kim, Tatsuya Suda and Duke P. Hong "Congestion Control and Resource Management in Diverse ATM Environments"


Horii, Akinari and Bruce J. Summers, "Large-Value Transfer Systems," in Bruce J.
Summers (ed). The Payment system, Design, Management, and Supervision, 1994, 73-88


Anthony Alles, "ATM Intemetworking" Cisco System Inc. white paper, May 1995

"Integrating ATM Backbones with High-Speed Ethernet at the Edge", 3Com Corporation white paper

"Bulletproofing Networks for High-Availability Computing", 3Com Corporation white paper

"Layer 3 Switching", 3Com Corporation white paper