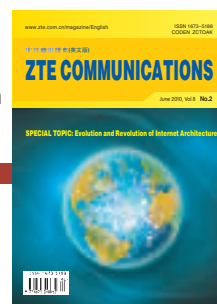


# Contents

Http://www.zte.com.cn/magazine/English  
Email: magazine@zte.com.cn



## Editorial Committee

**Chairman:** Zhong Yixin  
**Vice Chairmen:** Hou Weigui,  
Mi Zhengkun

## Members (in Alphabetical Order):

Ai Bo, Cao Shumin, Chang Jinyun,  
Chen Changjia, Chen Jianping,  
Chen Jie, Chen Xisheng,  
Cheng Shiduan, Cheng Shixin,  
Gao Wen, Gong Shuangjin,  
Gu Yongcheng, Gu Wanyi,  
Guo Yunfei, Hou Weigui, He Shiyong,  
Hong Bo, Ji Yuefeng, Jiang Hua,

Jiang Lintao, Lei Zhenzhou,  
Li Hongbin, Li Jiandong, Li Lemin,  
Li Shaoqian, Li Xing, Meng Luoming,  
Mi Zhengkun, Ni Qin, Sun Zhengze,  
Tan Zhenhui, Tian Wenguo,  
Wang Xiaoming, Wang Xiaoyun,  
Wang Yumin, Wei Leping, Wei Guo,  
Xie Daxiong, Xie Xiren, Xu Anshi,

Xu Heyuan, Yang Yixian, Yang Zhen,  
Yin Yimin, You Xiaohu,  
Yue Guangxin, Zhang Tongxu,  
Zhang Zhijiang, Zhao Houlin,  
Zhao Huiling, Zhao Xianming,  
Zhong Yixin, Zhou Susu,  
Zhu Jinkang

ZTE COMMUNICATIONS  
Vol. 8 No.2 (Issue 26)  
Quarterly  
First Issue Published in 2003

## Supervised by:

Anhui Science and Technology  
Department

## Sponsored by:

ZTE Corporation and Anhui Science  
and Technology Information  
Research Institute

## Staff Members:

Editor-in-chief: Xie Daxiong  
Deputy Editor-in-chief: Deng Xin  
Executive Deputy  
Editor-in-chief: Huang Xinming  
Editor in Charge: Zhu Li  
Editors: Paul Sleswick, Yang Qinyi, Lu Dan  
Producer: Yu Gang  
Circulation Executive: Wang Pingping

## Editorial Correspondence:

Add: 450 Rongshida Avenue,  
Hefei 230041, P. R. China  
Tel: +86-551-5533356  
Fax: +86-551-5850139  
Email: magazine@zte.com.cn

## Published and Circulated (Home and Abroad) by:

Editorial Board of  
ZTE COMMUNICATIONS

## Printed by:

Hefei Zhongjian Color Printing Company

**Publication Date:** June 25, 2010

## Publication Licenses:

ISSN 1673-5188  
CN 34-1294/TN

## Advertising License:

皖合工商广字0058号

## Annual Subscription Rate:

USD\$20

Responsibility for the contents rests  
upon authors of signed articles and  
not upon the editorial board of  
ZTE COMMUNICATIONS or its sponsors.  
All rights reserved.

## SPECIAL TOPIC: Evolution and Revolution of Internet Architecture

- 1 Hierarchically Switched Networks
- 7 Evolvable Internet Architecture (EIA)
- 12 Bearer Network of the Future Internet
- 16 Architecture of Ubiquitous Mobile Internet
- 21 Future Architecture and Mechanisms of the Self-Managing Internet
- 26 Services and Key Technologies of the Internet of Things
- 30 A Study on the Standardization of Future Internet Architecture

## RESEARCH PAPERS

- 33 MAC Protocols for Distributed Cooperative Communication Networks
- 37 Optimization of One-Plane Packet Loss in IP Bearer Networks
- 40 Routing in Cognitive Networks

## DEVELOPMENT FIELD

- 43 Impacts of GPS Synchronization Loss on TD-SCDMA Network Performance
- 48 Full-Service Operation and IMS Network Management

## OPERATIONAL APPLICATIONS

- 51 Integrated Network Management System for CSL
- 55 Using OBSAI to Build the Baseband-RF Interface of Multi-Mode Base Stations

## LECTURE SERIES

- 59 Cloud Computing (2)

## ROUNDUP

- 11 ZTE and Vivo Unveil World's First Low-Cost Handset with Digital TV in Brazil
- 24 ZTE to Build IMS Core Network for China Mobile
- 47 ZTE Sells World's Fastest HSPA+ 28.8M Data Card with Greece's COSMOTE
- 54 ZTE and Innofidei Achieve Industry's First Field IOT on Multiple TD-LTE USB Dongles in a Mobile Network Cell
- 62 ZTE Hosts IEEE 10G-EPON Interoperability Showcase

## DEPARTMENTS

- 36 Ad Index
- 63 Abbreviation Index

# Hierarchically Switched Networks

*Qian Hualin, E Yuepeng*

(Computer Network Information Center of Chinese Academy of Sciences, Beijing 100190, P. R. China)

## Abstract:

The Internet of today is facing serious challenges including lack of routing system scalability, unpredictable network behavior, uncertainty of data packet paths, poor control and manageability, unachieved Quality of Service (QoS), vulnerability of network facilities to Distributed Denial-of-Service (DDOS) attacks, core router complexity, costliness, and high power consumption. All of these defects have their root causes in the routing system. This paper first proposes a new network architecture which combines network typology with addressing. It then highlights that reliability of the tree structure is guaranteed by the concepts of logical node and logical link. Furthermore, shortcut link technology makes tree topology more flexible, and IP routing can be replaced with IP switching. As a result, all flaws in the current Internet architecture can be overcome.

## 1 Challenges Facing the Internet

The Internet is one of the most influential inventions of the twentieth century. It provides people with new means of communicating, exchanging, and acquiring information. Indeed, it has dramatically accelerated the progress towards more connected information societies. More than 3 billion people worldwide use the Internet, and it should not escape mention that in populous countries such as China and India, over three quarters of the population are still unable to surf online. The reason why the Internet has developed so rapidly is that it sates the demands for an information society, and adopts concise packet switching protocols and flexible routing methods.

Unlike traditional circuit switching, packet switching requires complete routing technology. It takes advantage of computer intelligence to periodically

exchange information among routers and then form a routing table. Based on the destination address (written on the surface of the data packet) and the saved routing table, each router transfers a data packet to the next hop until the packet reaches its destination. Forwarding operations and updating of the table are performed automatically by the routers without any manual intervention. Because routers automatically adapt to the network structure, people can construct networks as they like, and network architecture can have random connections. Where the reliability of network components, especially communication lines, is very low, a network structure with random connections and automatic routing capability is very effective. Indeed, routing technology is the very core of the Internet.

In the early stages of development, the Internet excelled other network architectures with its simple network protocol, packet switching technology, and routing technology. However, as technologies developed and advanced applications were introduced, and as the size of the Internet grew far beyond what its designers originally imagined,

the advantages of the Internet were gradually undermined. Some of the features that made the early Internet so effective are now not advantageous at all, and some have even become obstacles in the Internet's development.

As the network scale has enlarged and demand for real-time communication increased, the Internet has encountered a series of problems. These include:

(1) Huge-sized routing tables due to the large-scale network. This prevents quick and effective forwarding of data packets.

(2) Local network behaviors (such as partial change of network topology, failure and recovery of links or devices, and configuration or operation mistakes of network administrators) are being treated as global behaviors and are being broadcasted worldwide. This requires all routing information to be changed. As a result, the burden on backbone network routers becomes unbearable, and after a network event, the convergence time of routing information exceeds one minute. This causes a large number of data packets to circulate in the network.

(3) Routers are becoming

**This work was funded by the National High Technology Research and Development Program of China ("863" Program) under Grant No. 2007AA01Z214.**

increasingly complex, and their costs and power-consumption have increased accordingly.

(4) Network protocols are becoming more complicated due to the addition of virtual circuit switching technology. Virtual circuit switching technology draws on the strengths of circuit switching technology in order to overcome some of the shortcomings of packet switching technology.

(5) The advantages of randomly-connected network architecture are being offset against the high reliability of optical communication lines.

(6) Full and reasonable use of network channel resources is difficult to achieve. Network designers cannot assign a suitable bandwidth for each channel because the exact route of a data packet cannot be determined manually, and the data packet is likely to be detoured via other channels.

(7) Carrier-class Quality of Service (QoS) is difficult to achieve due to a slow end-to-end recovery approach, and lack of self-healing capabilities.

(8) Effective management and control is difficult to implement due to the uncertainty of network behaviors.

(9) Backbone network devices are vulnerable to fatal security threats. The network address space is not strictly distinguished from the user address space, and backbone signaling is completely integrated with user network signaling.

(10) Malicious network behaviors cannot be effectively detected and controlled because the network source address can be easily forged.

All these problems are fatal. Moreover, because early designers underestimated the scale of the Internet, the IPv4 address space will be used up in one to two years. Many private addresses are currently being used, but this weakens end-to-end communication capability. If IPv6 protocol is adopted, and the number of address spaces dramatically expanded without consideration of the network hierarchy, routing tables will also be dramatically increased. Routers will become more complex, and more serious bottlenecks will appear in the

network. To date, there have been many improvement measures, but these cannot solve the problems completely while they increase the complexity of network protocols. Therefore, there is a pressing need for significant reform of the Internet.

To deal with the Internet's tough challenges, this paper proposes a new network architecture: an hierarchically switched network. This architecture is designed to:

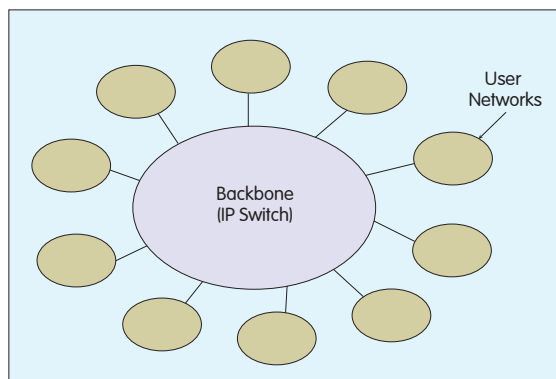
- Completely exclude routers from the network;
- Reintroduce the principle of simplicity into the network;
- Make the data packet path predictable in order to reasonably utilize the network's channel resources;
- Localize events such as topology change, failure and recovery of devices or communication lines, and mis operations of network administrators;
- Make the quick self-healing capability of a network independent of other complicated networks, such as Synchronous Digital Hierarchy (SDH)/Synchronous Optical Network (SONET);
- Enable the natural formation of a multicast tree;
- Separate the backbone address space from user address space;
- Allow malicious behaviors to be easily traced.

No matter which reform or new technology is applied to the Internet, it should be fully compatible with existing Internet protocols; otherwise, it will be unfeasible.

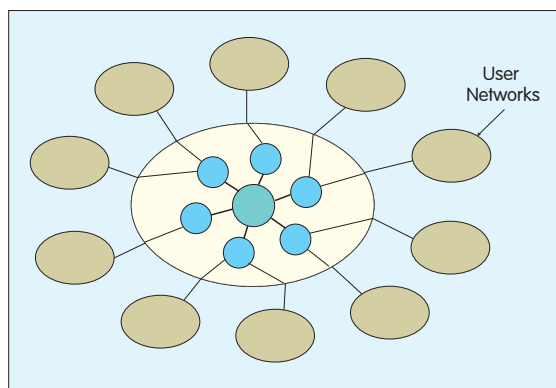
## 2 Basic Structure of Hierarchically Switched Networks

In the early design of the Internet, reliability was a core principle. At the time, this principle was warranted because both channel failure rate and bit error rate were very high, and designers also hoped the Internet would survive wars and natural disasters. But few could have predicted how this network would apply to real-time multimedia services such as voice and video. Even the number of network users today would have been

beyond their imagination; had they been able to predict this, they would have planned more carefully for address space. Taking reliability as a core principle, early designers adopted a dispersed, distributed, and non-centric approach to their designs. Ethernet is a typical example of such architecture. It consists of many computers that are interconnected with thick or thin cables. All computers are peers without any controller or coordinator, and the failure of one computer does not adversely impact another. The topology of the Internet is a mesh with random connections. There is no center or hierarchy in the Internet. Each node can randomly connect to other nodes. As long as each switching device has two or more channels, the network is regarded as highly reliable. The assignment of IP addresses is based on the network identity as well as the host number in the network. And the network identity, which plays a decisive role in the routing algorithm, is flat rather than hierarchical. When the number of such flat IP addresses becomes exceedingly large, it is impossible to develop an efficient switching algorithm for routing information. Nor is it possible to develop a quick routing table lookup algorithm. This is the exact sticking point of Internet routing. The randomly-connected structure and flat address space does not conform to the current thinking of human beings, and does not meet the efficient processing requirement of computers. Moreover, they are of poor scalability and can only be applied in very small systems. In fact, all organizations and address spaces of human society are hierarchical: a nation, a school, an enterprise, an army, postal address space, subject categories and cataloguing of books. A traditional telephone system is a manageable, controllable, scalable system that guarantees communication quality, and is also hierarchical. The domain name system of the Internet was originally flat, but it had to adopt hierarchical structure because it became infeasible once more than several hundred computers were connected. As for the



▲ Figure 1. Two-layer structure of the Internet.



▲ Figure 2. Tree structure of a backbone network.

Ethernet architecture, buses have become extinct from use. People now use hubs or switches. When ports are not sufficient, or the distance is extensive, several switches are cascaded to form a typical star or tree structure. In short, the hierarchical structure is present everywhere. From a management perspective, the hierarchical structure itself represents a kind of dispersal or distribution. Upper level management cannot and does not concern itself excessively about things that should be done at a lower level; an upper level manager may not be aware of changes made by a lower level manager within their jurisdiction. This enables the network system to be fully scalable. Reference [1] proposed the first hierarchical structure. However, this hierarchical structure has been largely ignored because its addressing method, still affected by the routing approach, is not flexible enough. Researchers have come to realize that when the scale of a network becomes exceedingly large, the scalability of its

routing system is the first thing to be challenged. Hence, attention has been focused on hierarchy, and methods such as landmark hierarchy<sup>[2]</sup>, geographical hierarchy, and Internet Service Provider (ISP)-rooted hierarchy<sup>[3]</sup>, have been proposed.

The hierarchically switched network proposed in this paper simply and clearly divides the network into two parts: backbone and user networks (as shown in Figure 1).

In Figure 1, all communication entities come from user networks. That is to say, communication is required only within a user network, or between hosts of two user networks (e.g. PCs, servers, or any wireless or wired terminals that can access the network for communication). No user can request to communicate with devices in the backbone. The function of the backbone is

very simple: it forwards data packets from one user network to another. Therefore, the backbone can be considered as a large IP switch. In a large-scale system, however, it is impossible to make such a switch that can connect all user networks in the world. This virtual large switch can be physically implemented with a simple tree structure. Figure 2 illustrates a two-layer tree; but in reality, the tree can be many layers, just like in a telephone network.

The fatal flaw of the tree structure is that failure of any node or channel will cause all subtrees under the node to disconnect. This defect can be overcome with logic nodes and logic channels, as shown in Figure 3.

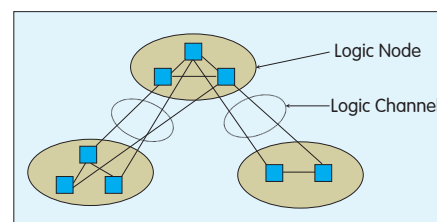
Figure 3 illustrates a basic tree. Regardless of its level, a node may have many lower level nodes under it. In Figure 3, the blue boxes represent IP switches. Two or more switches make a logic node. The switches in a logic node are interconnected with high speed channels, and with the control

software of the logic node, they are known as a single node to other nodes. Between the two levels of logic nodes there is a set of physical channels that are used to connect the IP switches of the nodes. This forms a logic channel (circled with broken lines in Figure 3) through the control software of logic nodes. Such a structure is tree-like in design, but physically, it has complicated connections that solve the problem of single point failure.

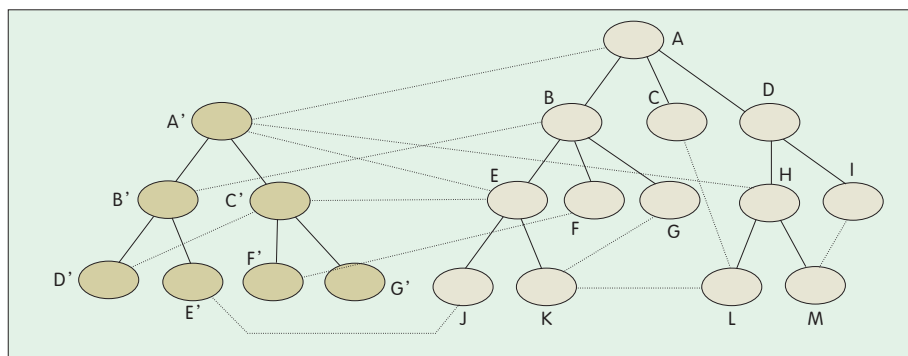
### 3 Expansion of the Tree Structure

Despite its advantages, the tree structure is less flexible than the mesh structure (which allows random connections) of the existing Internet. For example, when transmitting a data packet between two user networks on the leaves of a tree, the packet must go upward from the source user network to the root of the subtree of the two user networks. It then goes downward to the destination user network. In reality, the two user networks may be very close to each other. Supposing two ISPs deliver access services in City A at the same time, there will be two trees extending to the city, but the meeting point of the two trees might be in City B. When two communicating user networks, both in City A and close to each other, are connected to different ISP trees, data packets must first go along the ISP's tree to the meeting point in City B, then go down the tree of the other ISP to the target user network of the other ISP in City A. If there are interconnection channels between the two ISP trees in City A, the detour to City B can be avoided. Figure 4 illustrates a network structure that meets such requirements.

If we treat equally the channels represented by broken lines and solid lines in Figure 4, and allow more



▲ Figure 3. Logic nodes and logic channels.



▲ Figure 4. Shortcut channels.

channels in broken lines to be added, the network topology is almost the same as that of the existing Internet. The detour to upper-level nodes can be reduced or even eliminated and flexibility is enhanced. But such a network structure comes at the cost of the advantages of the tree structure. To ensure both the flexibility of the Internet and the advantages of tree structure, the channels in solid lines and broken lines in Figure 4 should be distinguished as tree channels and shortcut channels (or through channels) respectively. A shortcut channel can be a single physical channel or a logic channel made up of several physical channels. The shortcut channel functions no differently from the tree channel, but in switching user data packets, the shortcut channel is treated as a special case and given high priority.

When connecting via shortcut channels, data packets can be forwarded not only to the opposite end of the shortcut channel, but also to a farther node. For example, in Figure 4, logic node E' can not only forward the data packet to J via the E'–J shortcut channel, but also to remote logic nodes L and M via the E'–J shortcut channel. This forwarding involves direct and indirect shortcut channel technologies. Details about these technologies can be found in Reference [4] and it is not intended to discuss them here.

## 4 Switching Method

After the backbone network in a tree structure is constructed and configured with a certain number of shortcut

channels, any routing protocol can be cancelled, and simple switching of IP data packets can be achieved. Take for example the IPv6 address format. The low 64 bits are used as the interface identifier and cannot be used by the backbone devices, while the high 64 bits are routable addresses used by the backbone devices for forwarding IP packets.

In the IPv6 address structure, the Site Local (SL) part is assigned to users. Because the network topology is a tree, an ISP can divide the addresses it receives into several variable-length fields, which are called Switching Fields (denoted as  $SF_i$ ). Each switching field corresponds to a layer of the tree; a high-ranking switching field corresponds to a high layer of the tree.

User networks are at the edges of the backbone network. A data packet sent from a user network always enters the backbone tree via a leaf node. Supposing this logic leaf node corresponds to switching field  $SF_i$ , the packet switching process is very simple if no shortcut channel is involved:

- (1) The prefix of the IP packet's destination address is compared with the address prefix of the logic node.
- (2) If the two prefixes are not equal, the packet goes upward. In this event, it selects an uplink channel and forwards the packet to an upper-level logic node.
- (3) If the two prefixes are equal, the packet goes downward. In this event, it selects a downlink logic channel according to the value of  $SF_i$  (e.g. if the value of  $SF_i$  is 5, the logical channel 5 should be chosen), and forwards the packet to a lower-level logic node.

When shortcut channels are involved,

packet switching is a little complex. Before the above steps, it must first be determined whether the logic node has any shortcut channel. If there are shortcut channels, each channel will be assigned a shortcut channel table, which contains address prefixes of the direct shortcut logic node of the channel (i.e. the opposite logic node of the shortcut channel). This table also contains remote, indirect shortcut logic nodes of the channel. If the address prefix of the packet is the same as that of any logic node in the table, the packet will be forwarded via the shortcut channel; otherwise, the above steps will be executed to complete packet switching.

In sum, once the address structure is associated with the network topology, packet switching becomes quite simple. It can be done by simply comparing the prefix of the packet's destination address with the value of a related switching field, and routing information that is exchanged globally becomes unnecessary.

## 5 Benefits of an Hierarchically Switched Network

Associating the tree structure with address structure brings a series of benefits to the network.

First, the tree structure is a deterministic structure. Packet flow within the network is predictable, as is network behavior. As a result, the network becomes more controllable and manageable. The ISP can simply divide network management into two layers: logic node and entire network. Logic node management involves monitoring states, flows, performances, and charging information from switches and internal channels in each logic node, as well as from external channels of each logic node (i.e. channels between local logic node and other logic nodes). Management of the entire network is simpler because management information of all logic nodes is integrated to give an overall picture of the network. This information includes network status, external channel load, and charging database,



and can be displayed in appropriate diagrammatic forms. In addition, a network with a tree structure is scalable. Horizontally, logic nodes can be increased easily; while vertically, layers can be added to the tree to enable more users to access the network.

Second, because communication paths are certain, management, assignment, and admission control of path resources can be achieved. Accordingly, QoS guarantee is also possible. For QoS to be guaranteed, resource management, admission control, and output scheduling is necessary. Resource management involves registration and allocation of communication path resources, such as channel capacity and port buffer, ensuring existing communication flows get enough resources. Admission control involves accepting or rejecting new communication requests based on remaining resource information. This information is provided by resources management in order to avoid heavy traffic contending for limited resources. Output scheduling is designed to manage the output queue according to the priorities of communication flows. The existing Internet cannot guarantee QoS. It cannot even determine the path for a data packet. How then can we expect it to reserve resources for the path and implement admission control?

Third, certainty about the communication path enables the communication load to be estimated and channel capacity to be configured well. This avoids low resource use that arises from an unbalanced network load, and which is quite common in existing networks. It also reduces the load from complicated and inefficient Traffic Engineering (TE).

Fourth, by associating network topology with address structure, the tree adopts IP switching instead of IP routing. In this way, it is released from routing-related work such as routing information exchange in the entire network, maintenance, management and update of the routing table, and looking up unwieldy routing or forwarding tables for IP packets. In this structure, IP packet forwarding is quick



and simple, and network performance is enhanced.

Fifth, the tree structure localizes network events. For example, the failure and recovery of any node or channel does not have an impact on remote packet switching algorithms. Also, configuration and management of logic nodes is much simpler than that of a routing system. Network operation and maintenance personnel are unlikely to make mistakes during operations. Even if there is an operational error, it does not have any negative impact on the worldwide network, unlike the routing system. As there are no Border Gateway Protocols (BGP)s, all core routers are free from the heavy burdens of updates and withdrawals of BGP)s.

Sixth, the security of the network itself is greatly enhanced. In existing networks, the port IP address of the core router resides in the same address space as the users' host IP addresses. So any user can carry out a Distributed Denial-of-Service (DDoS) attack on any core router. In hierarchically switched networks, the address space of the backbone network and user networks can be easily separated, so user data packets can transverse the backbone network without interfering with its devices. In addition, in the existing Internet, a user can fake their source address to avoid the network tracing their malicious behavior. In an hierarchically switched network architecture, the address prefix of a user network is the same as that of a device port at the edge of the

backbone network, so any false use of a source address can be immediately detected and reported.

Seventh, logic channel technology brings two benefits: the channel's capacity for self-healing, and additional means of expanding channel capacity. The self-healing capability ensures that if a physical channel fails, the overall capacity of the logical channel is only slightly reduced, but communication of other channels can still proceed. This is a necessary condition for guaranteeing QoS. As for enlarging channel capacity, the logic channel capacity can be expanded by increasing the bandwidth of each physical channel or the number of physical channels.

Eighth, network devices can be greatly improved in terms of complexity, reliability, cost, and power consumption.

## 6 Deployment of Hierarchically Switched Networks

The key to success in the reformative reconstruction of existing systems lies in the deployment of new systems. The new systems should be compatible and easily inter-connectable with existing systems. Due to incompatibility between IPv4 and IPv6, the deployment of IPv6 has been very slow. The hierarchically switched network, on the other hand, does not have any incompatibility problem caused by the coexistence with existing networks, does not require any modification of

those existing networks, and does not involve the application layer. The hierarchically switched network can be deployed in a gradual manner.

With the development of Gigabit Ethernet (GE)—10GE, 100GE, and long-distance high-speed transmission technologies (e.g. 10 Gbit/s, 40 Gbit/s, and even 100 Gbit/s)—the current Internet can easily apply the rates of long-distance backbone network in user access networks. These rates are obviously insufficient for the backbone network, and due to the bottleneck problem caused by routers, the Terabit per second transmission capability of optical fiber cannot be fully exploited. But for user access networks, which serve limited user groups, the demand for voice, video, and data communications can be satisfied even with existing routing technology. Therefore, the issue of solving fatal defects in the Internet is not so pressing in user networks as it is in the backbone network.

In addition to non-real time applications, the backbone network has to process millions of flows of video and voice traffics. The existing routing structure, which is characterized by low efficiency, low rate, slow self-healing, difficult to realize multicast, and lack of effective QoS guarantee, has become a critical obstacle for tri-network convergence (i.e. convergence of telecom networks, radio and television networks, and the Internet). Solving the problems of the backbone network is the most urgent issue for the existing Internet. The Internet industry has devised numerous QoS schemes and methods which all focus on the backbone network. Unfortunately, these methods are extremely complicated, ineffective, and hard to deploy. Even their standards are difficult to make.

In the evolution to the hierarchically switched backbone network, it is proper to do with the ISP's backbone network or part of the backbone network each time. The address structure of the hierarchical network should have enough space to be easily layered. The IPv6 address structure meets such a requirement and can be

directly used in a hierarchically switched network.

The study of topologies of current ISP backbone networks shows that a hierarchical tree structure is adopted in all layers of these networks except the core nodes (often about a dozen) in the topmost layer. These are randomly and fully interconnected into rings or other forms. If these core nodes are organized into one (or a few) logical node(s), the entire network architecture naturally forms a tree. The tree structure is quite common because it is naturally formed based on the geographical location of nodes. However, the adoption of the routing system has changed everything; the advantages of the tree structure are lost, and orderly network architecture is changed into a disorderly system. In nature, there can be found many large chaos systems, but among artificial systems, only the Internet has such an attribute.

Therefore, in reforming the existing backbone network into a hierarchically switched network, existing nodes and channels can be divided into logic nodes and logic channels, and control software for each logical node can be installed without changing the existing network topology.

The hierarchical structure can also be applied in user access networks. With such a structure, user networks can have hierarchically switched logic nodes and Ethernet switches only, or have Ethernet switches only, so that the technologies involved in network management will be considerably simplified.

## 7 Conclusions

The new hierarchically switched network architecture overcomes almost all defects of the existing Internet and proves Rekhter's Law<sup>[5]</sup> correct. Prototype system and sampling switches with hierarchically switched network architecture as discussed in this paper have been developed and tested on a test platform. Moreover, these systems have long been used in office networks, offering access to IPv6 and IPv4 networks. Experimental results demonstrate that this architecture is

feasible, simple to implement, and performs satisfactorily.

## References

- [1] KLEINROCK L, KAMOUN F. Hierarchical Routing for Large Networks: Performance Evaluation and Optimization [J]. *Computer Networks*, 1977, 1(3): 155–174.
- [2] TSUCHIYA F. The Landmark Hierarchy: A New Hierarchy for Routing in Very Large Networks [C]// *Proceedings of Symposium on Communication Architectures and Protocols (SIGCOMM'88)*, Aug 16–18, 1988, Stanford, CA, USA. New York, NY, USA: ACM, 1988: 35–42.
- [3] FRANCIS P. Comparison of Geographical and Provider-Rooted Internet Addressing [J]. *Computer Networks and ISDN Systems*, 1994, 27(3): 437–448.
- [4] 钱华林, 葛敬国, 李俊. 层次交换网络体系结构[M]. 北京: 清华大学出版社, 2008.  
QIAN Hualin, GE Jingguo, LI Jun. Hierarchically Switched Network Architecture [M]. Beijing: Tsinghua University Press, 2008.
- [5] MEYER D, ZHANG L, FALL K. Report from the IAB Workshop on Routing and Addressing [R]. IETF RFC 4984. 2007.

## Biographies

### Qian Hualin



Qian Hualin is chief scientist, researcher, and doctoral tutor at the Computer Network Information Center of the Chinese Academy of Sciences. He is mainly engaged in researching network architecture, routing systems, and network security. He is also a subject consulting expert and China

Next Generation Internet (CNGI) expert in the National Basic Research Program of China (also called "973" Program). Qian Hualin has held successive positions in several international Internet organizations including the Internet Corporation for Assigned Names and Numbers (ICANN), Asia-Pacific Network Information Centre (APNIC), Asia Pacific Top Level Domain Association (APTL), and Chinese Domain Name Consortium (CDNC). He has presided over and participated in several major network projects, and is the first person to introduce the Internet into China and to construct the Chinese domain name system. He has won over 10 national and ministerial Science and Technology Progress Awards, and has published over 100 academic papers.

### E Yuepeng



E Yuepeng is a doctoral candidate at the Computer Network Information Center of the Chinese Academy of Sciences. He is mainly engaged in researching network architecture and transport layer congestion control.

# Evolvable Internet Architecture (EIA)

*Bi Jun, Lin Pingping, Hu Hongyu*

(Network Research Center of Tsinghua University, Beijing 100084, P. R. China)

## Abstract:

The end-to-end attribute of the Internet enables easy modification and deployment of applications running at the host. Competition among these applications promotes the development of the Internet. However, new protocols related to the core layer, and network routers and switches are often hard to successfully implement. This paper proposes an Evolvable Internet Architecture (EIA). It suggests that new network architectures can be plugged into network equipment or into a host through interfaces provided by EIA for network experimentation or actual network deployment. Users can independently select network architectures, and use one or some of these architectures at the same time. The diversity provided by EIA will promote the evolution of the Internet.

After more than 30 years development, the Internet has achieved unprecedented prosperity and has become an essential infrastructure in our daily work and lives. However, the Transfer Control Protocol (TCP)/Internet Protocol (IP)-based architecture of the Internet was born with defects. The best-effort forwarding strategy, for example, cannot provide users with required Quality of Service (QoS); network management is hard to implement; network security vulnerabilities are increasingly exposed; IP address resources are almost exhausted; access devices are ubiquitously mobile and heterogeneous; and routing in a large-scale network suffers poor scalability.

Efforts to reform TCP/IP-based architecture have been unceasing, with new protocols and algorithms being introduced one after another. The end-to-end attribute of the Internet enables application layer protocols at

the host end to be easily modified and deployed, and through competition between all applications (both old and new), development of the Internet is driven forward. However, this attribute limits innovation in the core part of the Internet. In order to deploy new protocols designed for the Internet core or core network devices, global deployment or modifications on all network devices is necessary. In reality, however, network operators and device vendors are often disinclined to make such large-scale deployments or modifications due to lack of incentive mechanisms. Also, because new protocols have often not been thoroughly tested in a real network environment, they fail to win the trust and support from network operators. This hinders the protocols from maturing in their implementation, and affects operators' decision-making on deployment. As a result, new protocols have not been applied on a large scale and the evolution of Internet core technology has come to a standstill.

To overcome the defects of TCP/IP-based architecture, network researchers have put forward new

architectures including Role-Based Architecture (RBA)<sup>[1]</sup>, Recursive Network Architecture (RNA)<sup>[2]</sup>, and architecture for Services Integration, Control, and Optimization (SILO)<sup>[3]</sup>. Each of these architectures provides a solution to certain problems with existing architectures, but due to the following reasons none of them come close to meeting all requirements of the future Internet.

(1) Multiple architectures are needed at the same time in order to solve the different aspects of network problems, and to meet the demands of future applications. Network problems can be solved by using multiple architectures together rather than by improving existing TCP/IP-based architecture. Employing one architecture to satisfy all demands is something akin to seeking the optimal solution within multiple constraints. Where there are contradictory constraints, there cannot be an optimal solution. Hence, a single, standalone architecture is insufficient to meet the demands of future applications. Multiple architectures can deliver services in a complementary or competitive way so as to drive the

**This work was funded by the Research Fund for the Doctoral Program of Higher Education of the Ministry of Education of China under Grant No. 200800030034.**



development of the Internet.

(2) Network architecture is always enhanced and optimized. It is difficult to predict demands of the future Internet because such demands change with time. The need for new functionality may give rise to new protocol stacks (or network architectures), and a new mechanism is required to allow these protocol stacks to coexist with the old architecture. Conversely, an old protocol stack may be completely abandoned if it has not been used for a long time.

(3) Experimental network traffic should be tested in a real network and coexist there with user traffic. Issues such as competition, strategy, and incentive do not arise in any test bed with no user traffic. Therefore, a prototype system that has been proven successful in a test bed is not sure to work well in the real Internet. Researchers should conduct experiments in real networks rather than in test beds. In this way, when a new protocol is accepted by users, it can be directly put into practical use, avoiding the transplant from experimental network to real network.

This paper proposes an Evolvable Internet Architecture (EIA) that supports the coexistence of multiple architectures. EIA is a structure that is able to contain several network architectures and that allows new architectures to join. It functions as a “dock” or “socket” for these architectures, enabling them to plug in. Existing TCP/IP stack is one of these plugged in architectures. Architectures using the EIA can supplement each other to solve different problems, or can contend to solve a same problem—like the relationship between Skype, QQ, MSN and Gtalk in real-time communications. Users can randomly select different architectures, and use one or some network architectures simultaneously.

## 1 Evolvable Internet Architecture

### 1.1 Evolution Strategy of EIA

There are two main approaches to the

evolution of the Internet: involution and evolution.

The projects that adopt the involution approach include Global Environment for Network Innovations (GENI), Future Internet Design (FIND) and Future Internet Research and Experimentation (FIRE).

The evolution approaches attempt to mend the existing Internet.

Taking the involution approach involves reconstructing an experimental network, and this inevitably leads to high costs. And forecasting to the future can also be erroneous. Only continuous reform to the current Internet is possible. Therefore, EIA takes the evolution approach, which enables researchers to implement and deploy new protocols within existing networks.

The evolution approach used for EIA differs from existing ones.

Existing approaches mend the current TCP/IP-based architecture, find new problems, solve the problems, and then mend it again. However, a certain mend may not be compatible with future mends. Moreover, these approaches, including Network Address Translation (NAT), focus on short-term return but may cause long-term damage.

EIA is different. It supports the coexistence of multiple architectures, and TCP/IP-based architecture is just one of them. Through competition, the best solutions survive and develop.

### 1.2 Objectives of EIA

The main objectives of EIA are as follows:

Researchers can develop and test new protocols on real network devices. Experimental data flow and normal flow run parallel in the real network and do not affect each other.

EIA is able to accommodate a variety of architectures. EIA works as a platform enabling competition among these architectures; they can contend for solving the same problem or supplement each other to solve different problems. They can also share their hardware resources with each other.

Various network architectures have been proposed, each of which has its

own special design. However, EIA enables the most suitable architectures to survive and develop by means of competition. As an inclusive network platform to the upper architectures, EIA must take the following issues into account:

Each architecture may cover a part of the Internet only.

Terminal users may use one or several architectures, but not all the architectures, in a similar way that some Internet users use QQ and Gtalk, but not MSN, in real-time communications.

### 1.3 Makeup of EIA

The EIA is made up of two parts:

- Normal hosts with EIA software to support multi-architecture;
- EIA supported network devices (switches or routers).

#### 1.3.1 EIA Host

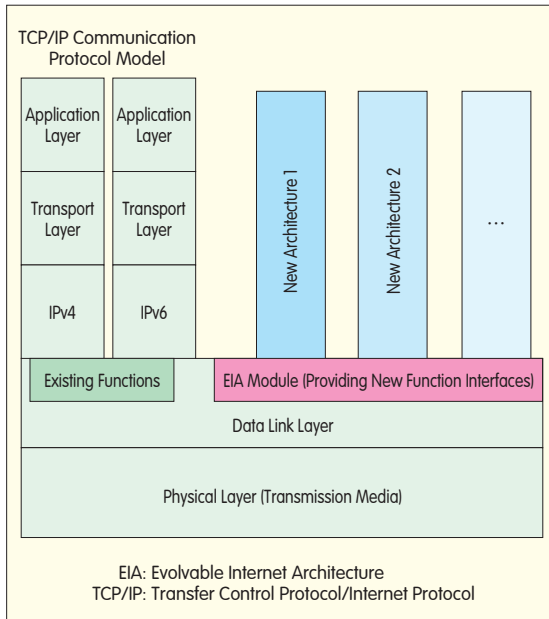
##### (1) Basic Mode

Figure 1 shows the multiple protocol stacks of an EIA host. From this figure, it can be seen that the EIA module is at the data link layer, and provides some function interfaces to support multiple architectures. In existing architecture, the host has to be configured with the EIA module in order to enable the coexistence of several architectures. Some architectures may use existing function interfaces rather than those provided by the EIA module to meet service requirements.

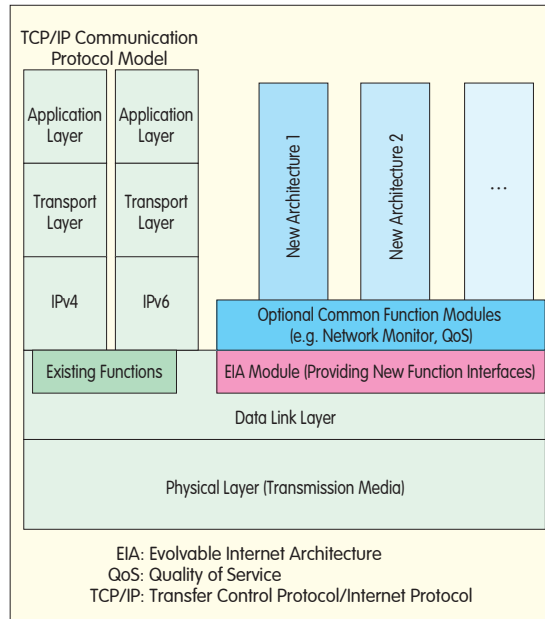
The EIA module transfers data packets to different architectures based on their architecture ID (defined as architecture protocol numbers). The existing TCP/IP communication protocol model acts as a special architecture and coexists with other architectures.

After the EIA module is added, the data link layer works as follows:

- Upon receiving a packet from the lower layer, the data link layer deframes the packet and uploads it (according to the protocol ID) to a related protocol stack (i.e. architecture) above.
- When it receives a packet from the upper architectures, the data link layer forwards the packet to a port or calls related hardware resources to process the packet, depending on the task



▲ Figure 1. Multiple protocol stacks of the EIA host.



▲ Figure 2. EIA with common functional modules added.

virtualization of Personal Computer (PC), acts as the primitive operation to directly operate hardware resources. The packet action interface layer—also called the network virtualization layer—encapsulates the instructions of the lower layers as a packet-level interface, and provides it to the upper layer architectures for forwarding, discarding, rewriting and other functions.

The packet action interface has the

assigned by the upper protocols.

Compared with the existing Open System Interconnection (OSI) model, the EIA model moves the socket interface down to the physical layer. The architectures above the data link layer are arranged vertically and in parallel.

#### (2) Advanced Mode

In the basic model, the data link layer is mostly responsible for deframing packets and encapsulating frames. To enable the easy development of new architecture, advanced EIA abstracts the common functional modules of new architectures, such as network monitor and QoS, and provides them to the developer as optional. Figure 2 illustrates EIA with common modules added.

#### (3) Storage Location of Architecture ID

Architecture ID can be stored in one of the following ways:

- In the frame head of data link layer—as the packet format differs from one architecture to another.
- In a field after the frame head. All architectures can negotiate on a common data field or location used to save the architecture codes. This is similar to the location of the version number in IPv4/IPv6 dual-stack structure. When the data link layer

receives a data packet, it splits the packet and checks the packet head. If the first field of the packet head includes 4 (meaning the version number of the IP packet is 4), this packet will be processed by IPv4 stack; if the first field is 6, the packet will be processed by IPv6 stack. This working mode is similar to that of an IPv4/IPv6 dual-stack node.

#### 1.3.2 Network Device Supporting EIA

##### (1) Principle

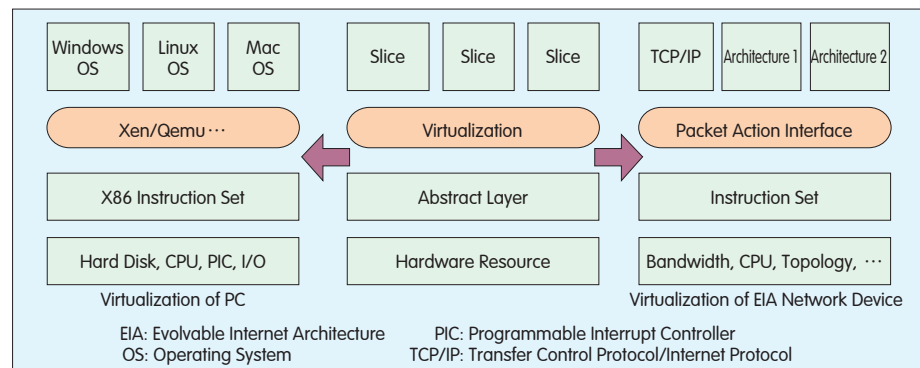
The coexistence of several architectures, supported by EIA, requires the underlying hardware resources to be shared.

As shown in Figure 3, the instruction set in virtualization of EIA network device, similar to x86 instructions in

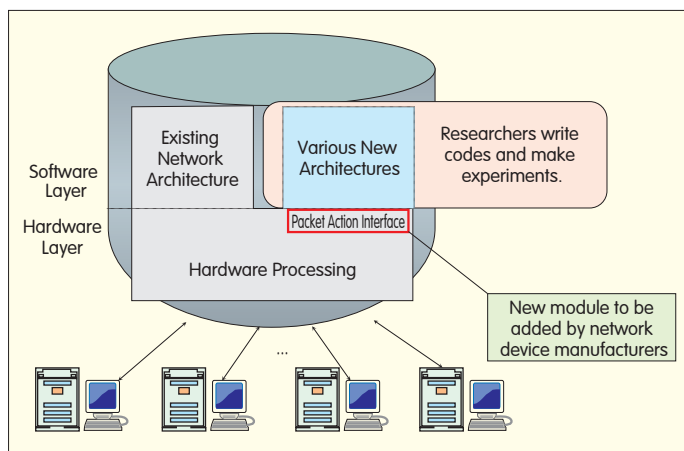
following two tasks:

- To receive data packets from a port and upload them to related protocol stacks according to protocol numbers.
- To accept tasks from upper layer protocols and then call the instruction set to perform corresponding operations on the data packets (e.g. to forward data packets to related network device interfaces). The operations on data packets are defined and processed by each protocol, while the virtualization layer only forwards data packets and calls functions to execute lower-layer primitive functions.

Above the packet action interface, each architecture runs independently and has no impact on the other. Therefore, each protocol sees a



▲ Figure 3. PC virtualization vs. virtualization of EIA network device.



◀Figure 4.  
Enabling network  
devices to support EIA.

different network view or network topology from others. In addition, the communication between architectures can be further defined.

#### (2) Enabling Commercial Network Devices to Support EIA

On condition that developers promise not to perform any operation affecting normal data flows (for instance restarting or shutting down a network device), network device manufacturers can open some interfaces to developers without exposing details of their devices. In Figure 4, these interfaces refer to packet action interfaces, which are the modules to be added by the manufacturers. The relationship between a network operator and the developers is similar to the relationship between the super administrator and common users in Linux Operating System. Once such interfaces are provided, users can write codes and test them directly on network devices.

When the primitives of a network device are not enough for a new protocol—for example, some special encryption algorithms are needed for hardware implementation—the developer can perform the new function by adding a hardware module with solidified software to interconnect with the packet action interface. Developers can make independent and creative experiments, or even directly run a new architecture or protocol to deliver services, once the programmable platform of EIA is set up and opened to the public. And they can do this without the assistance of network device

manufacturers and network infrastructure operators.

## 2 Compatibility of EIA with Existing Architecture

Adopting the evolution strategy, EIA treats TCP/IP protocol stack as a special case among its several architectures to facilitate compatibility with existing networks. That is to say, existing IP and hierarchies still work in the network, but only act as one of the competitors. EIA does not add new protocol layers to existing architecture, as does Shim6<sup>[4]</sup>, but adds some interfaces. Hence, it is not necessary to change the old TCP/IP-based architecture. Compared with layer-adding methods, this approach can be more quickly implemented with existing devices, making the transition easier.

In the era of IP/IPX, several protocol stacks are already supported by the host. Current IPv4/IPv6 dual-stack structures can upload the data packets to a specified protocol stack by identifying the version number, and the original socket can receive the entire data frame. All these show that it is feasible for the host to support EIA. To enable their network devices to support EIA, manufacturers need only add interfaces for the developers of new architectures without changing the existing network.

Once network device manufacturers accept and support EIA, experimenters can program on Internet devices. As existing architectures and protocols

take different processing procedures from the newly-added modules, such experiments will not have an impact on the running of other protocols. Once a new architecture or protocol proves successful, it can be put directly into actual use, and the deployment of the new architecture or protocol will be quite smooth.

## 3 Comparison with Current Works

Among evolution approaches, the most typical is OpenFlow<sup>[5]</sup>. OpenFlow provides Internet researchers with experiment methods for processing real flows. It adopts the structure of OpenFlow controller plus OpenFlow switches, where controller software instructs devices to perform related operations. This technology can be used in software defined networks. At present, OpenFlow can only run in local networks and can only support IPv4. That is, the flow table can only process IPv4 packet format and does not support any new protocol. The operations on the flow table are limited to flow-based forwarding, discarding, forwarding packets to the controller, and common forwarding, and the statistics function of the table is quite rough. New protocols may require more detailed statistics. As for packet processing, OpenFlow forwards the packets to specific external hardware for processing. This method is passable for trial networks, but for real networks (e.g. software defined networks), it suffers forwarding bottleneck and has poor scalability. Before it can be used in real networks, problems such as the scalability and redundancy of the controller, and the secure channel bottleneck (similar to the internal channel bottleneck of a router), must be solved. In contrast, EIA allows different protocol stacks to be installed in the devices as pluggable software modules. If the basic primitives are not enough, the hardware module with solidified software can be plugged. So EIA can be more easily applied in real networks than OpenFlow, which consists of remote controller and external hardware.

In OpenFlow, other operations, such as adding a flow table onto existing switches, and looking up each data packet in the table, are involved. EIA is free from the burden of table lookup and only forwards the packet to a related protocol stack based on the protocol ID. OpenFlow contains devices such as controller and NetFPGA, whereas EIA does not require any additional devices. EIA also provides developers with a real, programmable network; therefore, it is more likely to facilitate the smooth transition of the Internet than OpenFlow.

## 4 Conclusions

Currently, difficulty in implementing and applying new protocols in the core network layer and in network devices (e.g. switches and routers) hinders the development of core Internet technologies. Although researchers have proposed diversified Internet architectures, so far there has not arisen an architecture that can be widely applied to the existing Internet. This paper proposes EIA as a carrier of all network architectures. Adopting a special structure, EIA provides an ideal experimental platform for researchers of new architectures. It allows several architectures to be smoothly applied and to coexist in the future Internet. Thus, it promotes the continuous

evolution of core Internet technologies. EIA ends the situation where only one architecture is used for all networks, and lays a solid foundation for the graceful evolution of Internet.

On the programmable platform EIA, Internet researchers can experiment with their research results. As a result, EIA can better solve the existing problems of Internet, which in turn will speed up the evolution of the Internet and enable the Internet to become increasingly powerful. In the future, the study of EIA will mainly focus on clarifying the actions of the network device virtualization layer so as to determine the interfaces that should be provided by network device manufacturers.

### References

- [1] BRADEN R, FABER T, HANDLEY M. From protocol stack to protocol heap: role-based architecture [J]. Computer Communication Review, 2003, 33(1): 17–22.
- [2] TOUCH J D, WANG Y S, PINGALI V. A recursive network architecture [R]. ISI-TR-2006-626. Marina del Rey, CA, USA: ISI, 2006.
- [3] DUTTA R, ROUSKAS G N, BALDINE I, et al. The SILO architecture for services integration, control, and optimization of the future Internet [C]// Proceedings of IEEE International Conference on Communications (ICC '07), Jun 24–28, 2007, Glasgow, UK. Piscataway, NJ, USA: IEEE, 2007: 1899–1904.
- [4] NORDMARK E, BAGNULO M. Shim6: Level 3 multihoming shim protocol for IPv6 [R]. IETF RFC 5533. 2009.
- [5] The OpenFlow switch consortium [EB/OL]. [2009-01-31]. <http://openflowswitch.org>.

## Biographies

### Bi Jun



Bi Jun is a professor and director of the Network Architecture & IPv6 Division, Network Research Center of Tsinghua University. His research interests include network architecture and protocol, and next generation Internet. He has led over several national scientific research projects and was once awarded the second prize of National Science and Technology Achievement Prizes. He has published over 70 academic papers and has applied for 15 national patents of invention.

### Lin Pingping



Lin Pingping is a doctoral candidate at the Network Research Center of Tsinghua University. She is mainly engaged in researching network architecture and protocol, and next generation Internet. She has published 15 academic papers.

### Hu Hongyu



Hu Hongyu is a postdoctoral researcher at the Network Research Center of Tsinghua University. She is mainly engaged in research on network architecture and protocol, and next generation Internet. She has published 20 academic papers.

## Roundup

### ZTE and Vivo Unveil World's First Low-Cost Handset with Digital TV in Brazil

ZTE Corporation, a leading global provider of telecommunications equipment and network solutions, announced the Brazilian launch of N290, a low-cost cell phone with digital TV in Brazil on April 21, 2010.

Available exclusively through Vivo, the mobile phone are available in Rio de Janeiro and São Paulo, priced at BRL 399 for the pre-paid version and BRL 199 for the post-paid plan. It will be available in other Brazilian cities in coming weeks where Digital TV

signals are just available.

The ZTE N290 incorporates an MF645 3G modem for Digital TV reception, and supports Vivo's strategy to bring mobile Digital TV to its customers in time for the World Cup in South Africa in June.

With a 3.2 inch widescreen, the handset works with the Brazilian TV digital system ISBD-T which allows the access to all digital open channels at no cost. The new handset also features a 2.0 MP camera and

supports a Maxim 8G TF card.

Importantly, Digital TV services are free of charge. This means that once a handset is purchased, there is no need for a monthly subscription to access Brazil's broadcast TV.

According to Eliandro Avila, ZTE's President in Brazil, the manufacturer's goal is to offer an innovative and low-cost device in a market that, until very recently, only had expensive deals to offer with Digital TV.

(ZTE Corporation)



# Bearer Network of the Future Internet

*Jiang Lintao*

(China Academy of Telecommunication Research of the Ministry of Industry and Information Technology of the People's Republic of China, Beijing 100191, P. R. China)

## Abstract:

The future Internet needs to support broadband services, fixed services, mobile services and a combination of these. Such a wide range of services and multi-processes between users demands flexible and effective network-wide resource scheduling and support. Two approaches are currently being studied: reformative method and revolutionary method. The reformative method, based on existing technology, uses various techniques to achieve improvement. Revolutionary method seeks to address future business demands by completely re-designing the network, and overcoming problems that cannot be solved by current IP networks.

## 1 Mainstream Network Technologies

For a long time, the issue of mainstream networking technology has been scarcely discussed. The communications industry has firmly believed that data packet technology will be the dominant technology of future networks, and academia has been persistently studying various new technologies and publishing research results in academic papers. With the rapid development of communication technologies—especially transmission and switching technologies—it is no longer difficult to achieve a terabit per second transmission rate over an optical fiber, and a terabit per second switching or routing capability on a single device. And such devices can be mass-produced. Moreover, transmission resources are becoming increasingly inexpensive and powerful. On the other hand, data packet technology, which is based on

statistical multiplexing theory, faces some problems. Issues such as security, and Quality of Service (QoS) greatly perplex the communications industry. In seeking solutions to these problems, the communications industry has considered timeslot switching-based network technology, and the number of voices now espousing this as dominant technology has increased. As a result, conjecture has also arisen as to whether or not data packet technology or timeslot switching-based network technology should be used in future networks.

In the Internet environment, the network needs to support narrowband services, broadband services, fixed services, mobile services, and any combination of these. The future network should adapt to the following application scenarios: where users access narrowband services (which may be real-time voice services, non real-time data services, or a combination of these), the network should be capable of matching all narrowband services or service combinations and providing variable bandwidths to meet the demands of simultaneous real-time and non real-time services. Where users

access broadband services, the network should be capable of providing a bandwidth that matches those services. Where users access a combination of above services, the network needs to provide rapid, flexible, and on-demand transmission resources within the entire network. Timeslot switching-based technology has difficulty meeting such requirements in fixed communications let alone in a mobile communications environment where network resources need to be scheduled dynamically. The problem in the above scenarios demonstrates only one side of the matter, and it can be solved by providing resources according to the maximum demand of all services; that is, 40 Mbit/s per user. But this solution leads to a great waste of social resources, and it is generally unacceptable for both operators and consumers. It is also inadvisable from the perspective of energy saving and reasonable use of resources.

Communication between users is no longer simply point-to-point; users no longer do only one thing at a time. A common scenario might be a person is calling while surfing the Internet; or in a family, one person is surfing the Internet

This work was funded by the National High Technology Research and Development Program ("863" Program) of China under Grant No. 2008AA01A301

while another is calling, a third is watching IPTV, and yet a fourth might be downloading large-size video files using a Peer-to-Peer (P2P) system. This means current communications often involve several connections. These include point-to-point, point-to-multipoint, and multipoint-to-multipoint. In such application scenarios, it is impossible for timeslot switching-based networking technologies to dynamically schedule network resources and set up connections.

In the above scenarios, the services are of variable rate, and this requires the network to be capable of scheduling all its resources in a flexible and efficient way. Communications between users is multi-process; that is, in any given period, communication connections are of different kinds. This requires the network to be capable of point-to-point, point-to-multipoint, and multipoint-to-multipoint communications. At present, these scenarios cannot be handled with timeslot switching-based networking technology, but can only be realized with data packet technology.

## 2 Transport Layer Technologies

The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) has spent eight years (two study periods) researching Next Generation Networks (NGN) and has determined the core technology and architecture for NGN. This core technology comprises packet data technology because only it can deliver variable-rate multimedia services and meet diverse service requirements. NGN architecture consists of service layer, transport layer, and the support systems of these. One characteristic of NGN is that the service network is separate from the transport layer, and develops independently from the bearer network. Such architecture provides a broad space for service development and an open environment for delivering services to users. There are two functional modules—Network

Attachment Control Functions (NACF), and Resource and Admission Control Functions (RACF)—between the service layer and transport layer. These two modules are used to connect the two layers, allowing transport layer resources to be controlled by the service layer while the two layers work independently. This lays a good technical foundation for future operational services.

As for the question of whether the transport layer comprises one or two layers, opinions differ. People who regard the transport layer as one argue that it is completely flat, and the transport network of a communication network provides end-to-end communication capability. Those who regard the transport layer as two hold the idea that the transport layer consists of two networks: packet data network and transport network. The former provides end-to-end data packet communication capability, while the latter provides point-to-point connection (dedicated line) for packet data network devices.

It should be noted that the layers here are logic rather than physical devices. The functions of different logical layers can be integrated into one physical device. Existing transport networks mainly include optical transport networks (which are based on optical mux/demux and optical wavelength switching technologies), and Synchronous Digital Hierarchy (SDH) transport networks (which are based on SDH virtual container mux/demux, and SDH cross connection technologies). These transport networks are not capable of forwarding or switching packet data, and only provide dedicated lines for point-to-point connection between packet data network devices. Since the concept of "transport network" was coined, it has never been treated as a network but as a dedicated line of different granularities or different dimensions. Theoretically, the transport network can become a real network after the signaling system is added. But in reality, due to various dimensions of granularities, this can hardly be realized. To form a network, a unified

granularity dimension has to be used. Even if the packet is used as the unified dimension of granularity, the nodes in existing transport networks cannot process data packets with current technologies. Therefore, the transport network, including SDH and Wavelength Division Multiplexing (WDM), and the packet data network will not be converged into one network in the near future.

ITU-T's research into NGN architecture provides useful references for the design of the future Internet.

## 3 Packet Data Network

There have been many packet data networks constructed on different technologies including X.25, Frame Relay (FR), Asynchronous Transfer Mode (ATM), Ethernet, and IP network. Most of these technologies were put into widespread commercial use and some are still being used in commercial networks today. In light of new demands brought about by service development and development trends in networking technologies, IP networking is now recognized as the dominant direction of future networks and will be an important part of national information infrastructure in the future. However, IP networking is not without its flaws. It must contend with two architectural bottlenecks: one is the shortage of address space (as the existing IPv4 address system cannot meet the increasing demands), the other involves network problems in security, trustworthiness, controllability, manageability, and QoS, all of which cannot be solved with existing architecture.

The shortage of IPv4 addresses can be alleviated with dynamic address translation technology, but this solution brings with it problems with security trace, application development, and sunk costs. One feasible solution lies in IPv6. IPv6 is a widely recognized address solution for the next generation Internet. Adopting a 128-bit address coding method, the address space of IPv6 is 296 x that of IPv4. The number of address spaces is almost infinite. But the deployment of IPv6 cannot create

directly unique services and market opportunities; on the contrary, it requires huge investment. Hence, industry insiders are not commercially motivated enough to deploy IPv6. The decision of one or even several participants to deploy is not really enough to initiate the market. In the past few years, all countries and participants have shown great interest, but have taken a wait-and-see attitude to IPv6. Moreover, the IPv6 international standards have almost been completed. According to its protocol and standards, IPv6 is basically an upgrade version of IPv4 except that its fundamental protocol is incompatible with IPv4. An IPv6 network, adopting the same architecture and core technologies as an IPv4 network, is also an upgrade of an IPv4 network. Indeed, IPv6 expands the address space and solves the shortage of address space forever, but its performance and other functions do not radically change when compared with IPv4. More importantly, it cannot solve security, trustworthiness, controllability, manageability, and QoS problems of the Internet.

Because IPv6 can only solve the shortage of address space, other ways must be determined to overcome the second bottleneck. The study of next generation Internet shows two technical methods are available for Internet evolution: reformative and revolutionary. In the reformative method, the architecture of existing IP networks is not changed but improved with various technologies. With certain enhancements added to meet the bearer network's demand, existing technologies gradually evolve into next generation networking technologies.

Using on the revolutionary method, a new network is designed based on future Internet technologies and future service application demands. This new network solves all problems that cannot be solved in existing IP networks and meets demands for future information and communications services.

As for the controllability, manageability, operability, QoS, and security problems inherent in existing IP networks, experts favoring the reformative strategy try to amend the IP

network with various technologies, and let the network meet the demands of future networks. Representatives of these technologies are Multi-Protocol Label Switching (MPLS) and its derivatives, such as Transport MPLS (T-MPLS), and Virtual Private LAN Service (VPLS), and Provider Backbone Transport (PBT) and related technologies, such as Media Access Control (MAC) in MAC. Although these technologies can partially solve the manageability, controllability, and security problems of the IP network under certain conditions, they have their own limitations. For example, the core idea of MPLS is to implement control and security similar to an ATM network, to deliver Virtual Private Network (VPN) services, and to guarantee QoS via the connections it establishes on the IP network. But being connection-oriented, MPLS suffers poor scalability as network scale and services continue to grow.

MPLS is applicable to small networks and some VPNs. It cannot be used in a large network, especially a nationwide or worldwide network. The setup of MPLS Label Switching Path (LSP) and the distribution of labels both depend on routing protocols. On the one hand, existing and extended routing protocols simplify the implementation of MPLS; on the other, they cause problems such as convergence, loop, and network overhead. These problems cannot be neglected. In addition, to provide QoS and traffic engineering, the routing selection protocol has to provide a QoS-based routing selection function or constraint-based routing selection function, which complicates the routing selection protocol further.

The network core also becomes much more complicated with MPLS. First, the generation, allocation, query, and mapping of labels requires the participation of the core node. Second, in order to provide MPLS services, all network devices have to support MPLS. The core node in particular has to implement complicated routing protocols and MPLS protocol in addition to high speed packet switching. The larger the network, the more complicated the processing.

Third, with an increase of VPN users, the information maintained by Provider Edge (PE) routers increases accordingly, and the Border Gateway Protocol (BGP) routing table, operated and maintained by telecom operators, will become more complicated.

MPLS, T-MPLS, and VPLS suffer serious scalability problems but do not basically solve QoS, security, and other problems. MPLS has a 12 year history and every means have been tried to enhance its functions. It is unlikely that any breakthrough will be forthcoming. If the functions of existing IP networks were continually enhanced and their defects amended, the consequence would be that the IP networks, which were originally simple and efficient, become more complicated. Their efficiencies would decrease gradually and they would not be able to solve the root problems. Surely, the reformative approach will continue but it is unknown whether this approach can escape its current difficult situation.

The revolutionary method completely solves the problems inherent in existing IP networks and meets demands for future information communication. It does this by innovatively redesigning a new packet data network based on future Internet technologies and service demands. To redesign such a new network, one key problem is to clarify technical requirements and work out topmost layer for the network. The new packet data network should provide solutions to problems involving work mode of the network, network control, QoS guarantee, performance management, and security.

## 4 New Packet Data Network

ITU-T's Focus Group on NGN (FG NGN) has clearly specified the position of Future Packet Based Network (FPBN) in NGN architecture and has conducted research into the following: problem description, general requirements, topmost layer design, and candidate technologies. At present, the first three have been completed under the leadership of Chinese researchers and two recommendations have been given:

Y.2601—General requirements of Future Packet Based Networks, and Y.2611—High level architecture of Future Packet Based Networks. These recommendations have laid a solid foundation for future research<sup>[1-2]</sup>. Now, research on specific network implementation schemes for FPBN requirements and top design (i.e. candidate technologies) has passed to Study Group 13 of ITU-T (ITU-T SG13) under the Packet Data Network (PDN). So far, China has offered a candidate scheme: Public Telecom Packet Data Network (PTDN).

PTDN takes the non-connection-oriented transport mode as its main work mode. Theories and practice indicate that this mode offers good openness and scalability. Non-connection-oriented mode plays a critical role in the success of IP networks and is their most important feature. PTDN inherits this mode, which ensures excellent scalability. By introducing the features of communication networks, PTDN achieves predictability, controllability, and manageability of the network. PTDN also supports connection-oriented transport mode to satisfy special scenarios.

PTDN adopts a hierarchical network architecture, dual address mapping-based address system, ordered address structure (where addresses are assigned by region), node potential-based routing technology, and automatic multi-routing technology. All these enable PTDN to offer carrier-class protection and changeover capabilities.

To ensure trustworthiness and security of the network, PTDN takes a series of technical measures in the data, control, and management planes. First, it divides the data plane into two areas: trustable and suspect. In the trustable area, information is transferred in a transparent way, enabling network interception, while in the suspect area, user information is transferred in a non-transparent way, guaranteeing security and integrity of user information. Second, in the control plane, Service Node Interface (SNI), User Network Interface (UNI), and

Network Node Interface (NNI) are separated to secure the control plane in the network node. Third, the user in the management plane is unreachable, ensuring the node security.

In order to implement hierarchical management and control of the network, as well as to support multiple services, PTDN adopts multiple data plane technology. PTDN supports multiple data planes, but the information in all data planes is strictly isolated and the resources of the planes are used independently. As a result, even in extreme scenarios, the resources are independent and secure. Each data plane independently performs Operation, Administration and Maintenance (OAM) to ensure its own performance. Each data plane also has a complete signaling system.

To ensure the reasonable use of resources, adherence to green, energy-saving principles, to guarantee QoS, and to support feasible business models, PTDN should have a complete resource management system. It should combine resource management technologies such as fair algorithm, threshold-based alarm, and overload discard to achieve precise control over network resources, and to reach the QoS class required by the service network. PTDN should also feature decentralized resource management (to ensure scalability, and to ensure its resources are configurable, predictable, and measurable), and the capability of emergency communication.

To meet the requirements of quality broadcast services, PTDN should adopt resource ensuring technology for controllable multicast. In addition, the information among multicast groups should be strictly isolated, resources of different multicast groups should be independent, delicate management should be used for multicast resources, and these multicast resources should be predictable, manageable and controllable.

## 5 Conclusions

With a history of over 30 years, IP networking is a kind of packet data

networking that bears Internet services.

The Internet is one of the most influential inventions of the twentieth century, and since the 1990s, it has undergone rapid development. It now interacts with globalization and has profound influence on production, daily life, scientific innovations, social services, and cultural propagation. The Internet is a driving force behind world development and change, and the transformation of human society into an information society<sup>[3]</sup>. With the worldwide popularization of the Internet, problems such as address shortage and poor security control have become increasingly serious. Therefore, the Internet's sustainable development is greatly constrained. The Internet is now at a crossroads and is seeking a significant breakthrough to evolve into the next generation. Such a breakthrough will be born from the bearer network; that is, a new packet data network.

## References

- [1] ITU-T Y.2601-2006. Fundamental Characteristics and Requirements of Future Ppacket Based Networks Study Group [S]. 2006.
- [2] ITU-T Y.2611-2006. High-Level Architecture of Future Packet Based Networks [S]. 2006.
- [3] 蒋林涛. 电信转型和下一代网的若干问题研究 [J]. 电信工程技术与标准化, 2006, 19(1): 1-5.  
JIANG Lintao. Research some questions on transformation and next generation network [J]. Telecom Engineering Technics and Standardization, 2006, 19(1): 1-5.

## Biography

### Jiang Lintao



Jiang Lintao is chief engineer at the China Academy of Telecommunication Research, the Ministry of Industry and Information Technology of China. He also serves as chairman of the IP & Multimedia Standard Working Group of China Communications Standardization Association, vice chairman of ITU-T SG 13, and member of the 1st, 2nd and 3rd sessions of Multimedia Expert Group of Communication Technology Area of the National High Technology Research and Development Program ("863" Program). He has been engaged in R&D and standardization of multimedia, digital communications, and IP technologies for many years. He has received a special government allowance since 1992, and was awarded "Youth Science & Technology Expert with Significant Contributions" by the Chinese government in 1996.



# Architecture of Ubiquitous Mobile Internet

*Su Wei, Zhang Hongke*

(National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, Beijing 100044, P. R. China)

## Abstract:

With shortcomings in its original design, the Internet is limited in its capacity to meet increasing demands from ubiquitous mobile users. This paper discusses a new architecture for ubiquitous mobile Internet as well as the models and theories of its two layers. The infrastructure layer allows users to access the Internet anywhere, anytime, and by any means, while the pervasive service layer supports a variety of services. This paper proposes a mobility management mechanism under the new architecture. Experimental results show that this new network architecture overcomes the shortcomings of the existing Internet, satisfying demand for ubiquitous mobile service.

Due to technological advances, the amount of information available within societies is ever increasing. The Internet has become a strong driving force of economic and social development, and such development requires the Internet to provide pervasive services anywhere, anytime, and in numerous ways. However, defects in the Internet's original design hamper it from fulfilling these requirements. First, by employing fixed and wired connections, the Internet cannot meet user demands in a wireless mobile environment<sup>[1]</sup> (let alone provide network services for users anywhere, anytime, and in numerous ways). Next, the Internet was originally designed for data services, and is not satisfactory for voice and image transmission. It is insufficient for diverse networks, and cannot support diverse and pervasive services. Finally, as a scale-free network with a power-law structural topology<sup>[2]</sup>, the Internet is poorly secured, and quite vulnerable to attack

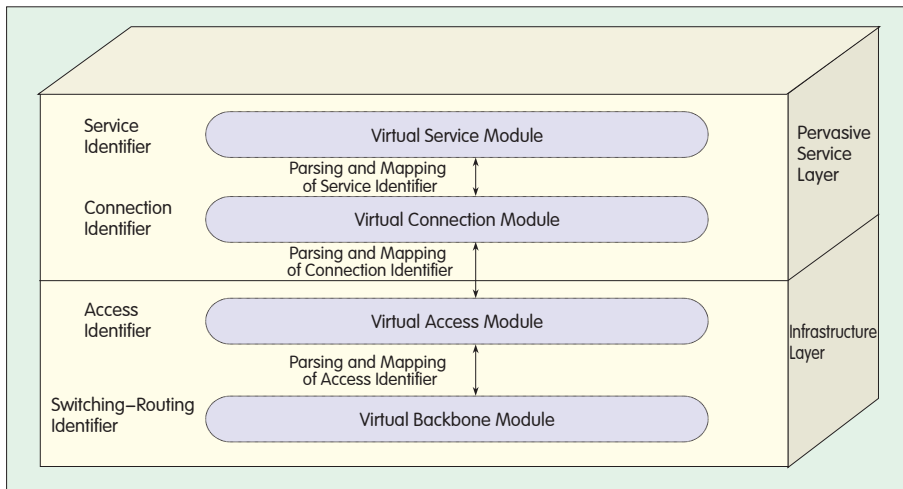
or deception. In sum, the existing Internet is not only incapable of satisfying current application demands for ubiquity and mobility, but is also hindering the further development of information networks. A new network architecture with breakthrough design is needed to solve the Internet's serious shortcomings.

In recent years, many countries have begun to carry out research into new Internet architecture. The US National Science Foundation (NSF) launched a 100x100 Clean Slate Project<sup>[3]</sup> in 2003, and in August 2005, sponsored the well-known Global Environment for Network Innovations (GENI) project<sup>[4]</sup>. Later in December 2005, the NSF also proposed the Future Internet Design (FIND) program<sup>[5]</sup>. In 2004, British Telecom announced their 21st Century Network (21CN) project<sup>[6]</sup>, and in 2007, the European Union approved the Seventh Framework Programme for Research and Technological Development (FP7). This programme attracted 930 million euros for research into information and communication technologies; in particular, the design of future network and service architecture. It aimed to spark a revolution in the information industry by

creating a new architecture. Also in 2007, the EU established a next generation network research group and started the Future Internet Research and Experimentation (FIRE) Initiative<sup>[7]</sup>. Forty million euros were invested into this initiative. Meanwhile, countries such as Japan and South Korea also began researching theories of future Internet architecture. By redesigning a next generation information network, these abovementioned projects, especially GENI and FIND, have attempted to remedy serious defects in Internet mobility, security, sensing, and support for pervasive services. However, projects such as GENI are still in their infancy and are at the stage of planning the research of next generation information networks. They have yet to work out clear schemes for theoretical research. Other projects have studied only a single or several aspects of future Internet but lack a comprehensive and systematic approach to new network architecture, its key theories and technologies.

The National Engineering Laboratory for Next Generation Internet Interconnection Devices (Beijing Jiaotong University) has used the "Fundamental Research on the

**This work was funded by the National Basic Research Program of China ("973" Program) under Grant No. 2007CB307101 and the National Natural Science Foundation of China under Grant No. 60833002 and 60903150.**



▲ Figure 1. Model of ubiquitous mobile Internet architecture.

Architecture of Universal Trustable Network and Pervasive Services" project of the National Basic Research Program of China ("973" Program) as a platform for actively exploring new architectures. It has produced a series of research results<sup>[8-10]</sup>. Drawing on these results, this paper proposes an architecture for ubiquitous mobile Internet, enabling the Internet to provide pervasive services at any place, at any time, and by any means.

## 1 The Overall Architecture of Ubiquitous Mobile Internet

Reference [8] proposes an overall universal network architecture and defines a number of basic concepts, such as parsing and mapping of access identifier, parsing and mapping of service identifier, and parsing and mapping of connection identifier, that are used herein. This paper introduces an Internet architecture based on that architecture, and which encompasses the demands and features of ubiquitous mobile Internet.

As shown in Figure 1, the overall architecture of ubiquitous mobile Internet can be divided into two layers: infrastructure layer and pervasive service layer.

The functions of the infrastructure layer include providing unified network access for ubiquitous wireless and mobile terminals, implementing mobility

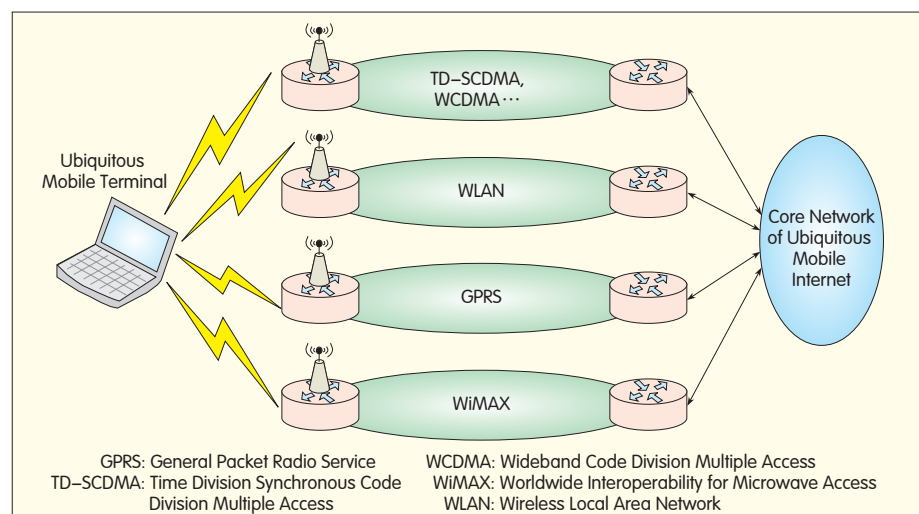
management of ubiquitous mobile Internet, and performing data switching and routing. In the infrastructure layer, a virtual access module, virtual backbone module, and parsing and mapping of access identifier are introduced. Using access identifiers, the virtual access module supports identification and access of ubiquitous mobile terminals. The virtual backbone module provides switching–routing identifiers for various types of access; these indicate the locations of ubiquitous mobile terminals and are used in switching and routing in the core network. The parsing and mapping function of an access identifier maps an access identifier onto a switching–routing identifier, thus enabling user identities to be separated

from and combined with their locations.

To control and manage diverse services, the pervasive service layer uses concepts such as virtual service module, virtual connection module, parsing and mapping of service identifier, and parsing and mapping of connection identifier. The virtual service module uses a service identifier to describe and represent various services; the virtual connection module provides several connections for each service; the parsing and mapping of the service identifier maps a service object onto several service connections (to support diverse services); while the parsing and mapping of the connection identifier maps a service connection onto several connections in the infrastructure layer. This embodies the idea that one service can correspond to several connections and paths, thus making service more reliable.

## 2 Architecture and Theory of the Infrastructure Layer

Unified network access is necessary for various types of mobile terminals in the ubiquitous mobile Internet (as shown in Figure 2). The terminal can be a specific type—for instance, a Wireless Local Area Network (WLAN) terminal that accesses the core network via a corresponding access network—or it can be a reconfigurable terminal that uses Software–Defined Radio (SDR) technology to dynamically and



▲ Figure 2. Ubiquitous mobile access.

intelligently select an access network before accessing the core network.

To enable unified access of ubiquitous mobile terminals, the virtual access module introduces an access identifier mechanism. The module not only allows users to enjoy optimal access and communication anytime, any place, and with widely pervasive services, but also ensures interconnection and close cooperation among heterogeneous networks. The module enables coordinated configuration of services and resources via the core network; that is, traffic sharing among networks and spectral resource sharing. To facilitate route selection of the core network, the virtual backbone module employs a switching–routing identifier for generalized switching and routing in the core network.

As shown in Figure 1, a core function of the infrastructure layer is parsing and mapping of the access identifier. The parsing and mapping function of the access identifier is responsible for mapping an access identifier into a switching–routing identifier, achieving separation of user identifier from its location. Specifically, its main functions include:

(1) Ensuring the mobility of various access networks and users. When one access network relocates, only its switching–routing identifier and the mapping relation between the switching–routing and access identifiers (representing user identities), needs to change. The access identifiers need not change. In this way, a user can enjoy various services without experiencing an interrupted connection.

(2) Enabling unified access of ubiquitous mobile networks and terminals, such as WLAN, Code Division Multiple Access (CDMA), Worldwide Interoperability for Microwave Access (WiMAX) and sensor networks, in the infrastructure layer. This expands the range of network services.

(3) Guaranteeing user security and privacy. The access identifier is the identity of the whole network, whereas the switching–routing identifier is only

used for switching and routing in the core network. When separated from the switching–routing identifier, the access identifier will not be broadcast in the core network. Other users cannot therefore intercept user information for malicious purposes because such information is effectively secured. Nor can they intercept core network information for the purpose of analyzing another user's identity. User privacy is protected.

(4) Allowing the network to be controllable and manageable. When a ubiquitous mobile access network applies for its access identifier, the network administrator must execute access control by giving authentication according to subscription information. Based on the authentication result, the administrator decides whether to accept a connection request, and determines the Quality of Service (QoS) class to be provided.

In short, the infrastructure layer offers sound, network–level support to the ubiquitous mobile Internet.

### 3 Architecture and Theory of the Pervasive Service Layer

The goal of the pervasive service layer is to provide diversified, pervasive services for the ubiquitous mobile Internet. To this end, the pervasive service layer employs a virtual service module, a virtual connection module, parsing and mapping of service identifier, and parsing and mapping of connection identifier.

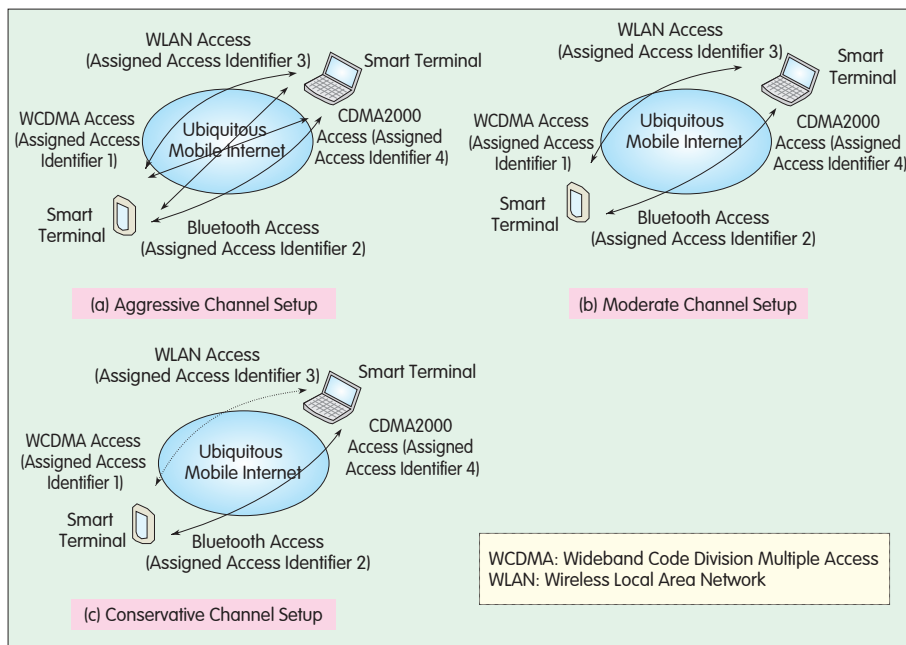
The virtual service module is the basis for delivering pervasive services. It is used to describe various services in a unified way, and to control and manage these services. It uses a service identifier to uniformly distinguish and describe diversified services, conveying the idea of pervasive services. The parsing and mapping done by the service identifier associates the virtual service module with the virtual connection module, thereby mapping the service identifier into the connection identifier and setting up connections for various services.

The virtual connection module employs a connection identifier for identifying a service connection and a user. It offers mobility and security to a connection and guarantees a certain QoS class. The parsing and mapping done by the connection identifier, maps a connection identifier into an access identifier of the infrastructure layer.

Here, the primary focus of explanation lies on the mapping mechanism from a connection identifier into an access identifier—as this is central to ubiquitous mobile support.

Traditional network design does not take into account the coexistence of multiple accesses, and in most cases communication parties can only use one path for data transmission. When the path fails or performs poorly, the sender can do nothing but wait. With the continuous development of wireless technology, an increasing number of network access technologies have been put into commercial use. As a result, it is now possible for the communication parties to establish active and standby paths for data transmission. When one path fails or does not perform well, the sender can use the other to transmit data. Moreover, the introduction of multiple access modes creates conditions for concurrent transmission via multiple paths. Concurrent transmission implies the simultaneous transmission of data via multiple paths. A transmission method of this kind can improve both reliability and security of data transmission. Where one path only is involved, an eavesdropper can easily intercept the communication by monitoring the path. Multipath concurrent transmission, however, prevents this from happening because an eavesdropper is unlikely to attempt monitoring data packets on multiple paths at the same time. A higher level of data transmission security is therefore realized.

In the ubiquitous mobile Internet, multipath concurrent transmission is closely related to the mapping from the connection identifier to the access identifier. After a connection identifier has been generated, the question of setting up a corresponding data



▲ Figure 3. Three channel setup methods.

transmission channel must be addressed. This setup process entails the mapping from the connection identifier to the access identifier. Upon generating a connection identifier, the two communication parties should establish a suitable path according to the requirements of services they wish to obtain. When they procure these services, they may adjust the path based on the network status (as the Internet is time variant). Therefore, the mapping process should be dynamic and in real-time.

A simple example can explain the process of dynamically selecting a suitable channel setup. Suppose both A and B can access the Internet via two modes: WLAN and 3G. They can establish an aggressive channel setup method (four data transmission channels), a moderate setup (two transmission channels), or a conservative setup (only one transmission channel). These three methods are shown in Figure 3. The channel should be specifically set up according to each connection identifier.

## 4 Mobility Management Mechanism

In the ubiquitous mobile Internet with

access identifiers and switching-routing identifiers, the two communication parties use an access identifier to initiate communication. Because the access identifier visible to users does not include location information such as network prefix, the two parties do not know the location of each other until the communication has been set up. Therefore, a complete location management scheme is necessary to enable the router accessed by the user to obtain the location of the other user according to the access identifier. Otherwise, the communication cannot be set up. This paper proposes a location management system to facilitate this connection. A location management system stores the access identifiers of various terminals in the local network, and also the mapping relations of current switching-routing identifiers. It accepts queries for switching-routing identifiers to match access identifiers. When the location of a terminal changes, its information in the system is updated to avoid any communication failure due to location information error.

For effective management of identities and terminal location information, two functional entities are needed: access switching router and

mapping server. The access switching router assigns access identifiers and switching-routing identifiers for users. During communication, it replaces the user's data packet identifiers, enabling the packets to be transmitted between the core network and access network. This router stores the location information of the local access terminal as well as that of the opposite terminal. A local buffer approach enhances efficiency in querying. When an identifier cannot be found in the router's storage table, the query then turns to the mapping server. For the most part, this server maintains the mapping relations between access identifiers and switching-routing identifiers in the network, and provides a query service for access switching routers and other mapping servers. It is the most important storage component in the whole location management system. In designing the storage system for a mapping server, a centralized storage approach by region can be adopted.

Mobility management predominately involves mobility detection, location registration, and location update.

### (1) Mobility Detection

Mobility detection combines active and passive detection methods. In passive mobility detection, a mobile node passively monitors the access router notifications or messages broadcast or multicast on the links after the link layer has been switched over. According to the contents of these notifications or messages, the node judges whether movement has taken place. In active mobility detection, a mobile terminal actively scans surrounding networks when the quality of the radio link (e.g. signal strength) of the local network cannot meet normal communication requirements. The mobile terminal determines whether there is any access switching router that can meet the communication requirements. On detecting such a router, the terminal initiates authentication and access to that router.

### (2) Location Registration

Location registration is the basis of terminal management in the network. It is implemented by the access



switching router and mapping server, and is designed to create storage units within the mapping server for the terminals (which are used for query during communication setup).

When a user accesses the network via an access switching router, the router takes an idle switching-routing identifier from the local identifier pool, assigns it to the user, and initiates the location registration process for the user terminal. If the terminal moves to a new region, the location registration process is also performed and the location update function triggered.

When a new terminal appears, the access switching router checks the local switching-routing identifier pool. If there are idle identifiers, the router assigns one switching-routing identifier to the terminal. Upon assignment, the router sets up a new storage unit in the local user mapping table, records the access identifier/switching-routing identifier mapping pair of the terminal, and sets a related timer for this storage unit. Then the router reports the mapping relation to the local mapping server as the terminal cannot initiate communication until it is registered with the local mapping server.

After the mapping server processes the reported mapping relation, it returns a response message to the access switching router, where the registration result is included. If the registration fails, the router can obtain related error information from the response message and re-initiate the location registration following error correction. If the registration is successful, the location registration process ends.

The location registration process described above begins with the assignment of a switching-routing identifier by the access switching router and ends with a successful registration message returned by the mapping server. This process is designed to set up a storage unit for a new terminal (or a terminal arriving from elsewhere) in both the access switching router and mapping server. If the terminal's storage units already exist, the location information will be updated.

### (3) Location Update

The number and types of mobile

terminals in the network are continuously increasing, and new services are demanding more in terms of mobility support. One critical issue in mobility management is the timely update of mobile terminal locations. During communication, a terminal may frequently change its access points. At each change, the location management system needs to update the terminal's location information to ensure uninterrupted communication.

In a local network, access for all types of terminals is unified and the locations of all terminals are centrally managed by region. The location update process is as follows: when a terminal changes location, all entities holding the old mapping information are informed by the network of the terminal's new switching-routing identifier. Upon receiving the new identifier, all entities update their mapping information or delete the old storage unit of the terminal. The update process is performed via message interaction between mapping servers and access switching routers. The goal of location update is to ensure all entities holding location information can update or delete old information in a timely manner in order to avoid errors when setting up a new communication.

## 5 Conclusions

To remedy serious defects in the Internet, this paper proposes a new architecture for ubiquitous mobile Internet and discusses the models and theories of its two layers: the infrastructure layer, and the pervasive service layer. The former allows users to access the Internet at any place, at any time and by any means; and the latter can support pervasive services.

Although some encouraging advances have been made, the architecture presented in this paper is still in the conceptual design stage. Deeper research needs to be undertaken into the theories and key technologies.

### References

- [1] 张宏科. 移动互联网技术的现状与未来 [J]. 电信科学, 2004, 20(10): 5-7.  
ZHANG Hongke. Mobile IP Technology: Present

- and Future Directions [J]. Telecommunications Science, 2004, 20(10): 5-7.
- [2] WATTS D J, STROGATZ S H. Collective Dynamics of Small-world Networks [J]. Nature, 1998, 393(6684): 440-442.
- [3] 100x100 Clean Slate Project [EB/OL]. [2009-08-19]. <http://100x100network.org/>.
- [4] DEMPSEY H P. GENI: Global Environment for Network Innovations [EB/OL]. [2006-11-15]. <http://www.geni.net>.
- [5] FIND: Future Internet Network Design [EB/OL]. [2008-08-19]. <http://find.isi.edu>.
- [6] 21CN Project [EB/OL]. [2008-07-17]. [http://www.btglobalservices.com/business/global/news/2005/edition\\_1/21CN.html](http://www.btglobalservices.com/business/global/news/2005/edition_1/21CN.html).
- [7] FIRE: Future Internet Research and Experimentation [EB/OL]. [2008-08-20]. <http://cordis.europa.eu/fp7/ict/fire/>.
- [8] 张宏科, 苏伟. 新网络体系基础研究——体化网络与普适服务 [J]. 电子学报, 2007, 35(4): 593-598.  
ZHANG Hongke, SU Wei. Fundamental Research on the Architecture of New Network —Universal Network and Pervasive Services [J]. Chinese Journal of Electronics, 2007, 35(4): 593-598.
- [9] 董平, 秦雅娟, 张宏科. 支持普适服务的一体化网络研究 [J]. 电子学报, 2007, 35(4): 599-606.  
DONG Ping, QING Yajuan, ZHANG Hongke. Research on Universal Network Supporting Pervasive Services [J]. Chinese Journal of Electronics, 2007, 35(4): 599-606.
- [10] 杨冬, 周华春, 张宏科. 基于一体化网络的普适服务研究. 电子学报 [J]. 2007, 35(4): 607-613.  
YANG Dong, ZHOU Huachun, ZHANG Hongke. Research on Pervasive Services Based on Universal Network [J]. Chinese Journal of Electronics, 2007, 35(4): 607-613.

## Biographies

### Su Wei



Dr. Su Wei is a lecturer at the National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University. He is mainly engaged in researching key theories and technologies for the next generation Internet. He currently presides over the research project

"Fundamental Research on Cognitive Services and Routing of Future Internet", a project funded by the National Natural Science Foundation of China.

### Zhang Hongke



Zhang Hongke is the executive dean of the Institute of Network Technologies, Beijing University of Posts and Telecommunications. He is also the director of the National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University. His research interests include key

theories and technologies for next generation information networks. He holds the position of chief scientist presiding over the "Fundamental Research on Architecture of Universal Trustworthy Network and Pervasive Services" project of the National Basic Research Program of China ("973" Program).

# Future Architecture and Mechanisms of the Self-Managing Internet

*Li Yühong, Cheng Shiduan*

(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, P. R. China)

## Abstract:

This article introduces the architecture and mechanisms of the self-managing future Internet currently being developed by the European Union Seventh Framework Programme (FP7) project EFIPSANS. In this architecture, network functions are divided into four planes: decision, dissemination, discovery, and data. Decision Elements (DEs), managed entities, and other information collecting entities at different planes comprise control loops of four layers: the protocol layer, the function layer, the node layer, and the network layer. DEs and their related control loops contribute to network self-management and self-maintenance. This greatly reduces the need for intervention in the network, thus reducing costs and improving user experience. The European Telecommunications Standards Institute (ETSI) has now established a new Industry Specification Group to standardize the self-managing Internet.

In current Internet research, the design objective, architecture, implementation and features of the future Internet are being discussed, and experts generally hold different views<sup>[1-5]</sup>. Experts within the European Union Seventh Framework Programme (FP7) EFIPSANS (Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services) believe self-management will be one of the main features of the future Internet. The service flexibility, network reliability and availability of a network can be markedly improved by self-management, and the operational and maintenance costs can be significantly reduced.

The main purpose of EFIPSANS is to

propose a new architecture for the Internet, describing its behavioral features and how they might be implemented. A number of research institutes, universities and companies participate in the project, including the Fraunhofer FOKUS in Germany, the Waterford Institute of Technology (TSSG) in Ireland, the National Technical University of Athens, the Warsaw University of Technology, the University of Luxembourg, Ericsson in Sweden, Alcatel-Lucent in France, and Telefónica in Spain. The Beijing University of Posts and Telecommunications (BUPT) is the only non-EU member of project.

## 1 Autonomic Computing, Autonomic Communications and Control Loop

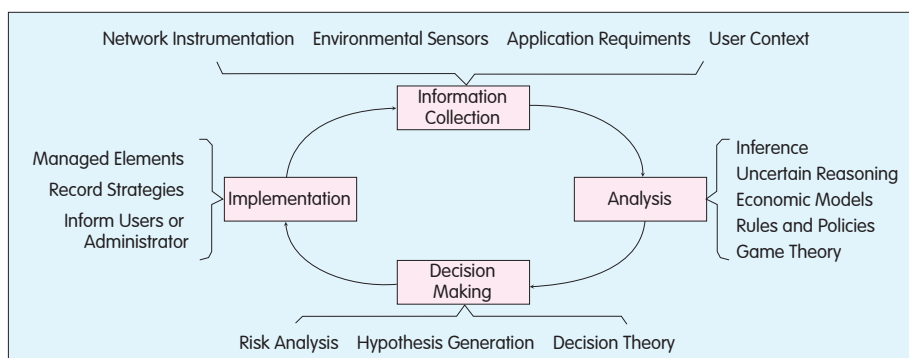
The self-managing future Internet is based on autonomic communications technology. The technology is derived from control theory—the main objective of which is to manage and optimize devices and components dynamically

at run time. Control theory can describe a closed system with clear architecture, but it is less able to describe open systems with uncertain information, and systems that are discrete and vary with time. Therefore it cannot be used unmodified.

Autonomic technology is based on and expands upon control theory. It can integrate and optimize the use of various resources quickly and dynamically in an open environment. An autonomic system comprises one or more autonomic units. Each unit provides some functions and interacts with other units in a dynamic environment. An autonomic unit consists of an autonomic managing entity, and one or more managed entities. The managing entity controls the configurations, input, and output of the managed entities, which implement all system functions.

An autonomic system can form a feedback control loop<sup>[6]</sup>, as shown in Figure 1. It collects information from network measurement, environmental sensing, users and applications' contexts. The information is then

This work was funded by EFIPSANS under Grant No. INF50-ICT-215549, National Basic Research Program of China ("973" Program) under Grant No. 2009CB320504, National Natural Science Foundation of China under Grant No. 60672086, and Sino-Swedish Strategic Cooperative Program on Next Generation Networks under Grant No. 2008DFA12110.



▲ Figure 1. Control loop in an autonomic system.

analysed using uncertain inference, game theory, or economic modeling, and decisions are made accordingly. Finally, these decisions are acted on by the managed entities.

Considering the increased complexity that communications and distributed systems now have, it becomes evident that the research objective of autonomic communications should be to enable a network (and its devices and services) to operate unattended with self-configuration, self-detection, self-adjustment and self-healing attributes.

Autonomic communication technology allows the network to adjust its behavior dynamically according to user requirements. This improves network performance and resource utilization, and greatly reduces the cost of network maintenance and operation.

Research into autonomic communications has been undertaken in areas such as Foundation, Observation, Comparison, Action, and Learning Environment (FOCALE)<sup>[7-8]</sup>, Autonomic Network Architecture (ANA), and Complexity Oblivious Network Management (CONMan)<sup>[9]</sup>. However, none of these provide a general, overall autonomic network architecture. The EFIPSANS project is based precisely on autonomic communications theory. It draws on the existing research in this field to propose a new architecture and implementation mechanism.

## 2 Self-Managing Network Architecture and Mechanism

The EFIPSANS project explains the

future self-managing network as follows<sup>[10]</sup>.

The basic functions of network management (such as configuration management, performance management, fault management, security management, and billing management), and basic network functions (such as routing, transfer, monitoring, and administration), can all participate in the control loop by interacting with each other automatically. This allows the network to operate and maintain itself without external intervention, and thus become a self-managing network<sup>[11]</sup>.

This definition is based on the following two assumptions<sup>[12]</sup>:

- (1) Some of the network function planes require re-construction and even integration.
- (2) In terms of network function

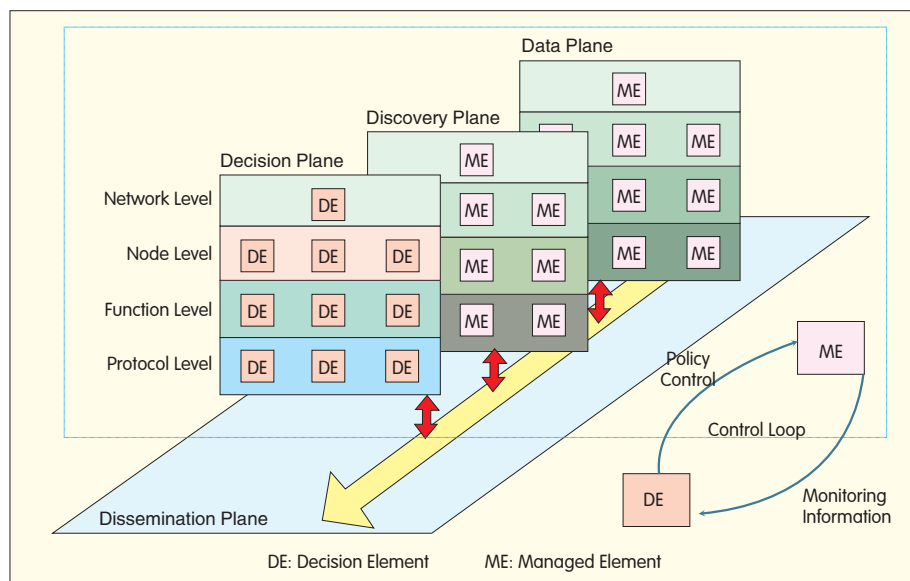
descriptions on the nodes and devices at different levels, new concepts, function entities, and relevant framework design principles are required for implementing a self-managing network.

Therefore, the EFIPSANS project proposes General Autonomic Network Architecture (GANA) and uses it as the basis for designing and achieving the self-managing future Internet.

### 2.1 General Autonomic Network Architecture

Figure 2 illustrates GANA architecture. GANA is generally designed in cubic architecture that comprises different function planes, each of which contains different levels of functional entities. In terms of functions, GANA uses the concept of 4 functional planes in 4D<sup>[13]</sup> architecture, which divides the network into decision, dissemination, discovery, and data planes. However, GANA provides specific definitions and descriptions of the functions and architecture of each plane. The architecture also defines the relationships between the planes according to the characteristics and requirements of the autonomic network.

The decision plane controls all decisions related to network behavior including admission control, load balance, network configuration, routing, Quality of Service (QoS) and security. It



▲ Figure 2. General Autonomic Network Architecture (GANA).

also makes decisions according to network topology, flow, time, user context, network objective/policy, nodes within a specific network domain, device capability, and resource restriction changes. Thus, it controls the behavior of all the managed entities.

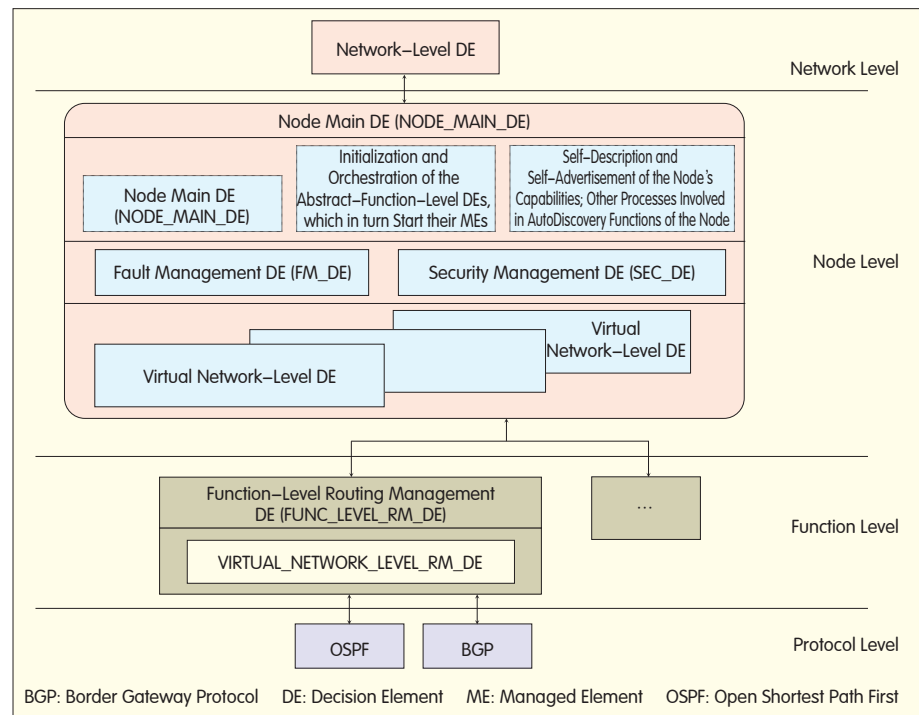
The decision plane comprises different Decision Elements (DE), and together these are key components for providing autonomic properties of a self-managing network.

The discovery plane consists of protocols or mechanisms responsible for discovering entities that make up the network or service. It is also responsible for creating logical identities to represent those entities. The discovery plane defines the scope and persistence of the identities, and carries out management accordingly. For example, it can discover how many interfaces and how many Forwarding Information Bases (FIB) a node has. It can also discover neighborhoods.

The discovery plane is responsible for discovering node capabilities, networks, and services. The core of this plane consists of self-describing, self-advertising protocols or mechanisms. In a self-managing network, these protocols or mechanisms are automatically configured by the DEs on the decision plane, and are called Managed Elements (ME).

The data plane consists of protocols and mechanisms that handle individual packets such as IP forwarding and Layer-2 switching. This handling depends on the state that is output by the decision plane; that is, information such as FIB settings, packet filtering policy, link scheduling weight, queue management parameters, and the mapping between tunnels and network addresses. Similar to the discovery plane, the data plane also comprises multiple managed entities.

The dissemination plane provides a reliable and efficient communication method for exchanging control information and non-user data within a node and between different node entities (such as DE and ME). There are two types of information exchange:



▲ Figure 3. Hierarchical DE.

passive acquisition (through Push) and active query (through Pull). The dissemination plane transmits signalling information, monitoring data (including status information changes), and other control information transmitted between DEs (such as fault, error, failure, and alarm information). ICMPv6, MLD, DHCPv6, SNMP, IPFIX, NetFlow and IPC all belong to this plane. The dissemination plane is also made up of multiple MEs.

In GANA architecture, the four planes are only partially independent of each other. Some elements of the discovery plane, for example, may use data plane service and also functions provided by the dissemination plane. However, the dissemination plane may not necessarily use the data plane service. These can be independent of each other. DEs of the decision plane communicate with other through service provided by the dissemination plane.

It should also be noted that a control loop, which is necessary for forming an autonomic system, is established between DEs and MEs on different planes. These DEs and MEs can be located on the same or different

network nodes.

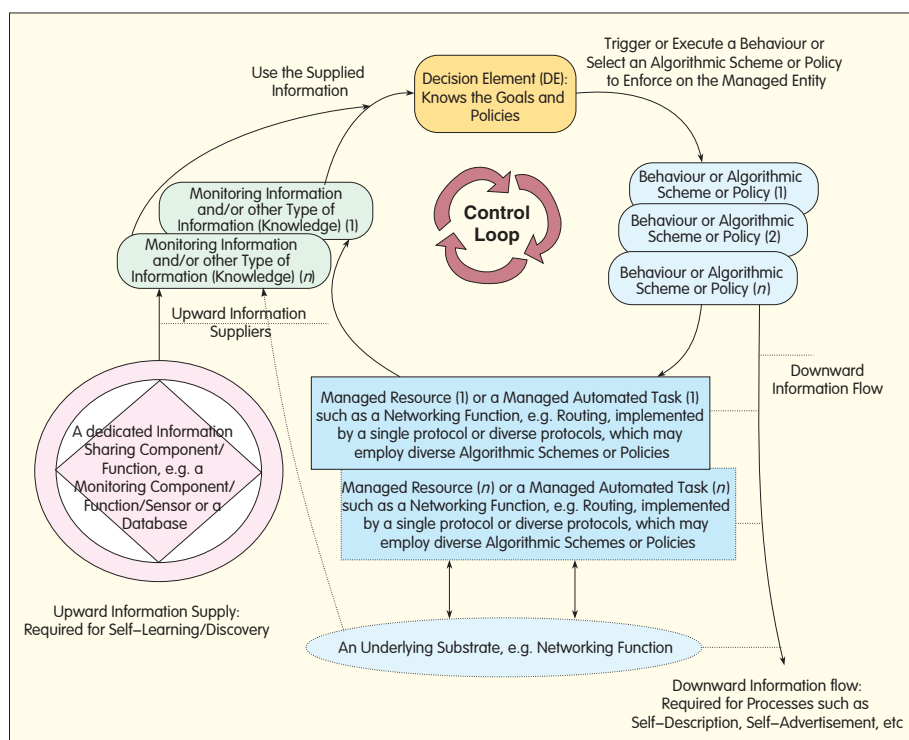
## 2.2 Decision Elements and Hierarchical Control Loop

DEs are key to GANA achieving autonomic functions and network self-management. Network functions are complex, so it is generally necessary for a node to use multiple DEs for different decision processes. In this way it can control and manage different network entities.

As shown in Figure 3, DEs are organized hierarchically in GANA architecture. All DEs are divided according to protocol level, function level, node level, and network level. The protocol level is the lowest, involving specific protocols such as Open Shortest Path First (OSPF) and Transmission Control Protocol (TCP). Protocol-level DEs allow relevant protocols to have autonomic characteristics.

Function-level DEs reside on the second layer. These are DEs for designing and realizing network functions. Function-level DEs abstract some specific network functions (such as routing and portability management) and the related algorithms. Node-level





▲ Figure 4. Control loop in the GANA.

DEs are on the third layer. These DEs contain all the information of a network node and can affect all DEs of the node directly or indirectly. For example, the

main DE of a node adjusts the node behaviors in the network by managing different DEs.

Network-level DEs are on the highest

layer. These DEs contain some of the information of other nodes in the network. They can use this information to control and affect the main DE of the local node. In addition, network-level DEs are responsible for cooperating with network-level DEs of other nodes and exchanging information with them. Thus, self-management of the entire network is realized.

DEs in GANA architecture may have the following relationships:

- Hierarchical: a relationship between DEs on different layers within the same node;
- Peer: a relationship between DEs on the same layer between different nodes;
- Sibling: a relationship between different DEs on the same layer within the same node.

Different relationships directly affect the communication mechanisms between DEs. In the GANA four-plane architecture, in order to achieve all autonomic functions, DEs on the Decision Plane and MEs on each plane form a control loop according to the principle illustrated in Figure 1. As shown in Figure 4, DEs and MEs of the nodes in GANA architecture are

## Roundup

### ZTE to Build IMS Core Network for China Mobile

ZTE Corporation, a leading global provider of telecommunications equipment and network solutions, announced on April 26, 2010 that it has been chosen by China Mobile to deliver its IMS core network in key Chinese provinces. The China Mobile's commercial IMS network will boast 1.4 million lines when it is completed in three months. According to the comprehensive evaluation process by China Mobile, ZTE was ranked among the tier one IMS supplier group for the project this time.

Based on ZTE's full package of IMS core network products, the network will enable China Mobile to quickly launch the various fixed/mobile

convergence services such as Converged Centrex, Converged One Number, Multimedia CRBT and Converged Conferencing, further enhancing the user experience.

China Mobile is one of the leading operators in China, boasting the largest mobile network and subscriber base in the world. After the re-organization of China's telecom industry, China Mobile has become a full-service operator. Deploying an IMS-based network will allow China Mobile to deliver fixed voice and multimedia services to individual and enterprise users over IMS, and finally, to build an IMS-based FMC network.

As one of the leading IMS providers

worldwide, ZTE provides end-to-end IMS product portfolio covering IMS core network, service platform, access, terminal, and OSS/BSS. The IMS solution is a fully converged solution, supporting fixed & mobile convergence, IT & CT convergence, and telecom & cable convergence. It provides complete voice and multimedia solution for LTE network evolution, helping operator to achieve various business models and scenarios, including enterprise, home, and individual users.

With innovative technologies and rich deployment experience, ZTE has established extensive references in IMS field. (ZTE Corporation)

organized hierarchically to form a Hierarchical Control Loop (HCL).

### 2.3 Engineering Design and Standardization Considerations

GANA is actually a reference model for the self management of nodes/devices and network architecture. It uses standardized and structural function entities, as well as specifications to ensure interoperability.

In GANA architecture, the behavior triggered by a DE after it collects and analyzes information is called autonomic behavior. Autonomic behaviors, such as self-configuration, self-description, self-advertisement, self-healing and self-optimization, are those used to manage or reconfigure relevant MEs. They are also related to specific DEs; they may be bound to the information-providing parts of the control loop (where the DEs are located) or bound to each ME controlled by the DEs. Therefore, the autonomic behavior descriptions/specifications are formal, and describe the GANA architecture and DE functions.

In addition, EFIPSANS researchers are designing models and tools for engineering DEs and the related control loops. These include meta-model, information model, system model, data model, policy model, configuration file, knowledge base, and a tool chain.

ETSI has now established an industry specification group called Autonomic Network Engineering for the Self-Managing Future Internet (AFI-ISG)<sup>[14]</sup> for the standardization of the self-managing Internet. AFI-ISG is researching autonomic network engineering, and in particular, one of its sub-project groups is focused on GANA standardization. Another sub-project group is focused on applying the meta-model to GANA. Its objective is to determine a GANA model and to engineer control loop through formalized descriptions and designs.

## 3 Conclusions

Self-management will be a major feature of the future Internet. It will

implement autonomic functions, including device and network self-discovery, self-configuration, resource self-provision and virtualization (without human intervention), service composition, application self-awareness, and self-monitoring. Basic network functions such as routing, forwarding, mobility management, and QoS management will also become autonomic.

This article introduces GANA, developed by the EFIPSANS Project as a means of achieving self-management of the future Internet. In GANA, all autonomic functions of the network are implemented by DEs and their control loops on different planes and different layers. The next stage is to standardize and engineer GANA, which will require the description of autonomic behaviors. Research into the stability, complexity, and expandability of self-managing networks based on GANA is well underway.

### References

- [1] GENI Net Global Environment for Network Innovations [EB/OL]. [2009-09-30]. <http://www.geni.net/>.
- [2] NSF NeTS FIND Initiative [EB/OL]. [2009-07-25]. <http://www.nets-find.net/>.
- [3] European IST FP6 ANA (Autonomic Network Architecture) Project [EB/OL]. [2009-08-20]. <http://www.ana-project.org/>.
- [4] GREENBERG A, HJALMTYSSON G, MALTZ D A, et al. A Clean-slate 4D Approach to Network Control and Management [J]. Computer Communication Review, 2005, 35(5): 41-54.
- [5] EC funded - FP7 - EFIPSANS project [EB/OL]. [2009-09-30]. <http://efipsans.org/>.
- [6] DOBSON S, DENAZIS S, FERNANDEZ A, et al. A Survey of Autonomic Communications [J]. ACM Transactions on Autonomous and Adaptive Systems, 2006, 1(2): 223-259.
- [7] BELL J. IBM article: Understanding the Autonomic Manager Concept [EB/OL]. [2009-09-10]. <http://www-128.ibm.com/developerworks/library/ac-amconcept/>.
- [8] JENNINGS B, van der MEER S, BALASUBRANIAN S, et al. Towards Autonomic Management of Communications Networks [J]. IEEE Communications Magazine, 2007, 45(10): 112-121.
- [9] STRASSNER J C, AGOULMINE N, LEHTIHET E. FOCAL: A Novel Autonomic Networking Architecture [C]//Proceedings of the 1st IEEE Latin American Autonomic Computing Symposium (LAACS'06), Jul 18-19, 2006, Campo Grande, Brazil. Piscataway, NJ, USA: IEEE, 2006.
- [10] BALLANI H, FRANCIS P. CONMan: A Step Towards Network Manageability [C]//Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'07), Aug 27-31, 2007, Kyoto, Japan. New York, NY, USA: ACM, 2007: 205-216.
- [11] CHAPARADZA R, PAPAVALASSIOU S, ARISTOMENOPOULOS G, et al. First draft of Autonomic Behavior Specifications (ABs) for Selected Diverse Networking Environments [R]. EFIPSANS Project Deliverable D1.1v1. 2008.
- [12] ITU-T Rec. M. 3400. TMN Management Functions [S]. 2006.
- [13] CHAPARADZA R. The Self-managing Future Internet Powered by Current IPv6 and Extensions to IPv6 Towards IPv6++ and EFIPSANS Initiated IETF drafts [C]//Proceedings of Global Mobile Internet and IPv6: Next Generation Internet Summit 2009, Apr 15-16, 2009, Beijing, China. 2009.
- [14] AFI ISG: Autonomic Network Engineering for the Self-managing Future Internet (AFI) [EB/OL]. [2009-05-30]. <http://portal.etsi.org/afi/>.

### Biographies

#### Li Yühong



Li Yühong received her doctoral degree from the Technical University of Braunschweig, Germany. She is an associate professor at the Institute of Networking Technology, Beijing University of Posts and Telecommunications (BUPT). She has led and participated in many projects funded by

the National High Technology Research and Development Program of China ("863" Program), National Natural Science Foundation of China, Sixth Framework Programme (FP6) of the EU, Seventh Framework Programme (FP7) of the EU, and national and international enterprises. She has published over 50 articles, 30 of which are indexed by Science Citation Index (SCI) and Engineering Index (EI). Her research interests include Internet architecture, self-organizing network technology, and wireless mobile network technology and applications.

#### Cheng Shidian



Cheng Shidian is a professor and doctoral advisor at the State Key Laboratory of Networking and Switching Technology, BUPT. She has been involved in communications and computer network research and development for many years. She was formerly the leader of the Networking and

Switching Expert Group of the National "863" Communication Subjects, and director of the State Key Laboratory of Networking and Switching Technology, BUPT (1992-1999). Cheng Shidian is now a council member of the Beijing Institute of Communications (BIC), and a commissioner of the China Communications Standards Association. Her current research interests include new-generation Internet architecture, and performance optimization technology.

# Services and Key Technologies of the Internet of Things

*Xing Xiaojiang, Wang Jianli, Li Mingdong*

(ZTE Corporation, Shenzhen 518004, P. R. China)

## Abstract:

This article introduces the services and development of the Internet of Things, and analyzes the driving forces and obstacles behind such development. Looking at application types and the different development stages of the Internet of Things, this article categorizes its services into four types: identity related services, information aggregation services, collaborative-aware services, and ubiquitous services. For the first two types of services, applications and system framework are discussed; for the last two types, development trends are discussed. Services provided by the Internet of Things will gradually be integrated into human life and society; with the development of the Internet of Things, applications will evolve from relatively simple identity-related and information aggregation-related applications, to collaboratively-aware, and finally ubiquitous applications. It will then be possible for the Internet of Things to be fully integrated with Internet and telecommunications networks.

## 1 Development of the Internet of Things

The concept “Internet of Things” was coined by Kevin Ashton of Massachusetts Institute of Technology (MIT) in 1999, and is defined as follows: all things are connected to the Internet via sensing devices such as Radio Frequency Identification (RFID) to achieve intelligent identification and management. Early in 1995, the book *The Power to Predict*<sup>[1]</sup> first described application scenarios of the Internet of Things.

In recent times, the Internet of Things has developed rapidly and globally due to increasing government and enterprise investment in projects in regions such as the USA, Europe, Japan, and South Korea. IBM’s Smarter Planet initiative will see an

investment of 3 million dollars made in smart grid and digital healthcare projects. The EU has proposed an i2010 policy framework that aims to enhance economic efficiency and promote the development of Information and Communication Technologies (ICT) through widespread use of these technologies. In Japan, the i-Japan strategy is based on E-Japan and U-Japan. South Korea has also proposed a new project for the Internet of Things. In China, Prime Minister Wen Jiabo presented the concept of “Experiencing China” in August 2009. Driven by the Chinese Government, the Internet of Things industry has developed rapidly in China.

### 1.1 Driving Forces for Development of the Internet of Things

First, the development of the Internet of Things conforms to the trend of using information technologies to better serve society. On the one hand, modern society suffers development bottlenecks in the fields of energy, transport, logistics and financing. On

the other, people have direct demands in health, and medical treatment and services. With a general belief that information technologies make for smarter terminals, wider networks, and better services than other technologies, they are naturally chosen to solve problems encountered in social and economic development as well as to enhance standards of living.

Second, the Internet of Things is regarded as a new source of economic growth by many governments. The Information Superhighway Plan implemented by the Clinton administration brought 10 years of rapid economic development to the USA. Now, the Obama administration has put forward “Smarter Earth,” which probably has relations with the Information Superhighway Plan. In China, the Internet of Things is regarded as the practice of using information technologies to promote industrialization. In regions such as Europe, Japan, and South Korea, government plays an important role in Internet of Things planning.

This work was funded by the National S&T Major Project of China under Grant No. 2009ZX03004-002.

Third, with its businesses reaching saturation point, the telecom industry also regards the Internet of Things as a new breakthrough. In many European countries, mobile phone penetration rate has reached 100%. As a result, person-to-thing and thing-to-thing communication has been placed high on the agenda. The Internet of Things therefore represents a new stage in the development of the telecom industry.

### 1.2 Factors Affecting the Development of the Internet of Things

Despite these strong driving forces, the Internet of Things faces challenges.

First, inter-industry barriers are an important factor affecting the development of the Internet of Things. Currently, telecom service providers are the main promoters of the Internet of Things, and have made (or are making) ambitious plans for its development. However, there are technical barriers among industries, and different industries have their own industry chains, which are sometimes difficult to penetrate.

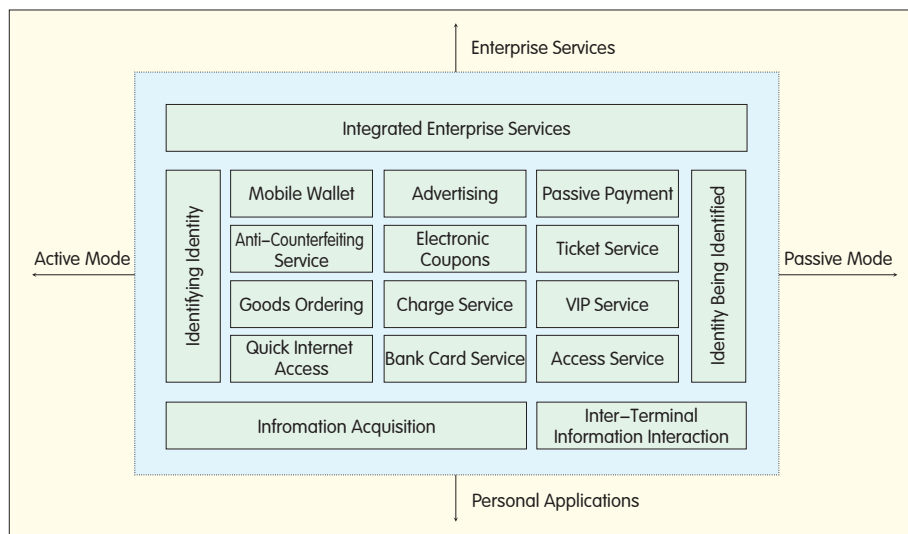
Second, several technological issues are difficult to overcome. Vast differences in applications make it difficult to work out a uniform service provision platform. Terminals and services vary dramatically in relation to industries and applications.

Third, the question still remains whether the scale of the Internet of Things industry can support the entire industry chain. At present, interest from industries that may benefit from Internet of Things service is far from strong.

## 2 Services of the Internet of Things

There are a large number of applications that can be included as Internet of Things services, and these can be classified according to different criteria. According to technical features, Internet of Things services can be divided into 4 types: identity-related services<sup>[2]</sup>, information aggregation services, collaborative-aware services, and ubiquitous services<sup>[3]</sup>.

It is generally agreed that an inevitable trend for the Internet of



▲ Figure 1. Applications of identity-related services.

Things will be its development from information aggregation to collaborative awareness and ubiquitous convergence, and that not all services of the Internet of Things will develop to the stage of ubiquitous convergence. Many applications and services only require information aggregation, and are not intended for ubiquitous convergence as the information is closed, confidential, and applicable only to a small group.

### 2.1 Identity-Related Services

Identity-related services adopt identity technologies such as RFID, two-dimensional code, and barcode. Figure 1 lists some identity-related services.

According to the identification mode of the terminal, identity-related services can be divided into two categories: active and passive. They can also be classified by served objects (enterprise or individual): personal applications or enterprise services.

The implementation of different applications may vary. Figure 2 illustrates the basic principle of tag-based information acquisition services. The general procedure for such services is as follows: first, an RFID tag is attached to a thing. Then, a read device accesses the information in the RFID tag (including the identity information of the thing), and makes a

request to the name resolution server of the Internet of Things. In this way, it may obtain the Uniform Resource Identifier (URI) of the thing. Finally, the read device obtains further information from the URI.

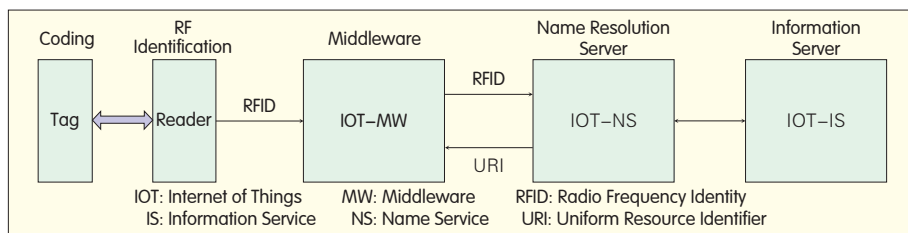
### 2.2 Information Aggregation Services

With such services, a terminal collects and processes data, and reports it via the communication network to the platform. The platform further processes the data and implements unified management of the terminals, data, applications, and services as well as third parties. Specific service applications include automatic meter reading, elevator management, logistics, and traffic management.

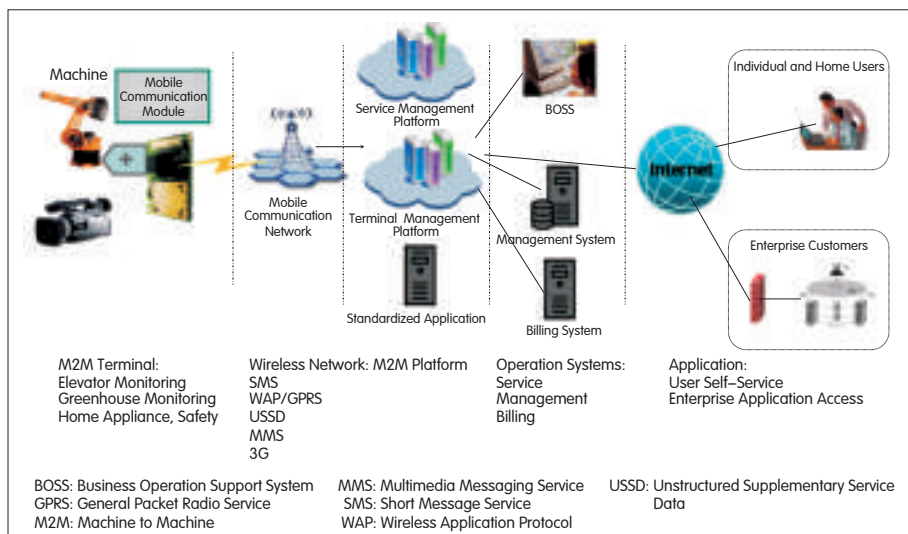
Figure 3 illustrates the framework of information aggregation services<sup>[4]</sup>. In the Figure, the entire system is made up of Machine-to-Machine (M2M) terminals, a communication network, platforms, applications, and operation systems. The mobile communication network acts as an information transmission carrier, transmitting data in several ways. In fact, a fixed network can also be used as the data transmission channel.

Access gateway devices and application gateway devices can be added to the framework in Figure 3 in order to meet the demands of different networks, and to enable more terminals to access or provide services to





▲ Figure 2. Principle of tag-based information acquisition services.



▲ Figure 3. Information aggregation services.

enterprise customers.

The access gateway device supports aggregation of terminals, and supports different networks, especially Network Address Translation (NAT) traversal. The application gateway device provides enterprises with services or service interfaces by means of a gateway similar to an SMS gateway device.

Figure 4 shows a detailed function platform and its functions<sup>[4]</sup>.

### 2.3 Collaborative-Aware Services

The development of the Internet of Things should bring about the delivery of more important and complicated services. Such services often require terminal-to-terminal and terminal-to-person communication. Moreover, these communication capabilities impose higher requirements on reliability and delay, and require terminals to be smarter. Only in this way, can collaborative processing be done.

To date, scenarios, demands,

framework and communication protocols of such services have not been studied in depth. But in the long term, collaborative-aware services will be a trend in the development of the

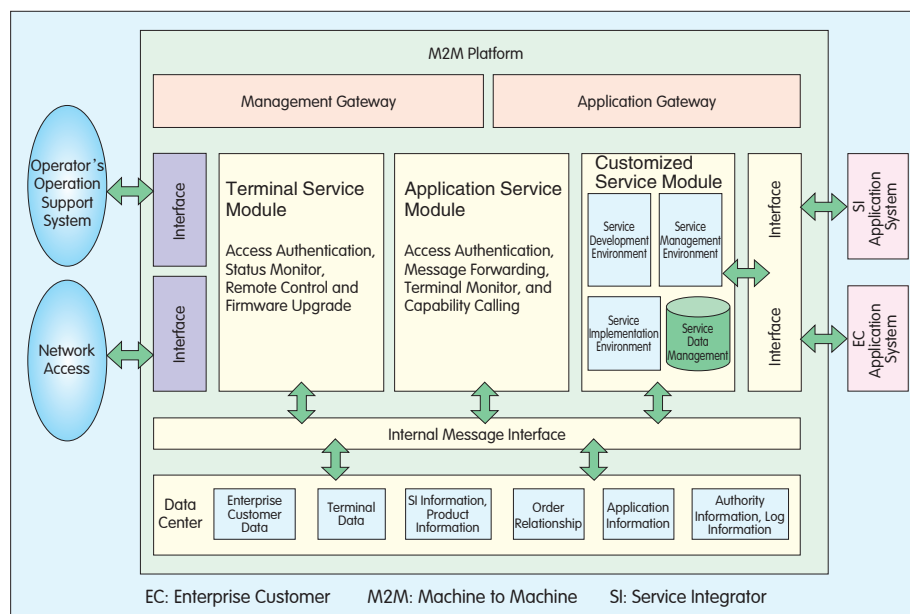
Internet of Things.

### 2.4 Ubiquitous Services

Characterized by omnipresence, all-inclusiveness, and omnipotency, ubiquitous services aim to deliver smooth communication anytime, anywhere, for anybody, and for everything. They are the acme of communication services, pursued by human society.

It is unknown whether future ubiquitous services will use the Internet as their carrier, but it would represent a significant leap in the development of the Internet of Things, and an important development stage of Internet. Integration of the information of real-world things into the Internet would enable the sharing of things by more users through the Internet. In manageable and controllable telecom networks, things will be included in the unified management system of the network to support thing-to-person and thing-to-thing communication (as well as wide-range information sharing). Hence, the convergence of telecom networks and the Internet of Things is also an important trend.

So far, little research has been carried out into the research of ubiquitous services from the perspective of telecom networks. In September 2009, the



▲ Figure 4. Information aggregation service platform and its functions.

Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) released the draft recommendation Y.2002(Y.NGN-UbiNet)<sup>[5]</sup>, which outlines ubiquitous networks and their visions.

"5C+5Any" are key features of ubiquitous networks. 5C stands for convergence, content, computation, communication, and connection. 5Any represents anytime, anywhere, any service, any network, and any object.

The ubiquitous network is generally defined as a fully connected, reliable, and intelligent network at the sublayer, and containing integrated content technology, micro technology, and bio-technology. Its communication services are extended into fields such as education, intelligent building, supply chain, health care, everyday life, disaster management, safety service, and transport to provide people with better services. The ultimate objective of ubiquitous networks is to allow people to enjoy convenience in information and communication, to better serve their lives, and even to change their lives.

### 3 Key Technologies for the Internet of Things

The above discussion shows that implementation of services in the Internet of Things mainly involves the key technologies of sensor, sensor network, sensor network-related communication, communication network, the Internet of Things platform, and integrated technologies.

The sensor is used to collect information in the Internet of Things; it is the basic part that senses the real world, and offers services and applications. However, due to the diversity of sensors (there are temperature, pressure, speed, humidity, height, video, image, and location sensors), information interfaces provided by these sensors vary widely. This is the greatest challenge for mass production of Internet of Things terminals.

Much research has already been conducted into sensor networks, and a

complete set of specifications have been made for the physical layer, link layer, and network layer. But sensor networks have not been put into application on a large scale<sup>[6]</sup>. Typical sensor network-related communication technologies include Bluetooth, Infrared Data Association (IrDA), Wireless Fidelity (Wi-Fi), ZigBee, RFID, Ultra-Wide Band (UWB), Near Field Communication (NFC), and WirelessHart. Sensor networks will evolve to next generation IP networks (e.g. IPv6 networks), and sensor terminals will tend to become smarter. The intelligence of a sensor network is mainly reflected in its IP technology, low power consumption, small size, bidirectional transfer of information, and non-manual maintenance.

Communication networks provide the data transmission channel for the Internet of Things. Current research into communication networks focuses on how to enhance existing networks to meet the service requirements of the Internet of Things (e.g. low data rate, low mobility).

The Internet of Things platform works with terminals as well as exiting networks and systems to provide the capabilities to various applications. In terms of network architecture, a unified service platform that is suitable for applications of multiple industries is required to support cross-sector, unified information services. In particular, when the Internet of Things develops into the collaborative-aware or even ubiquitous service stages, more effective network framework, name address, routing, and communication protocols have to be worked out.

### 4 Conclusion

The Internet of Things is an inevitable result of social progress and it has bright prospects. It will, however, encounter many challenges—both technical and industry-chain related—in its path of development. To overcome these challenges, focus will need to be given to Internet of Things' business model and key technologies simultaneously.

#### References

- [1] RANADIVE V. 未来之路——预见力：全球化经济大变局下的企业思维革命[M]. 雷恒, 译. 北京: 东方出版社, 2008.  
RANADIVE V. The Power to Predict [M]. Translated by Lei Yanheng. Beijing: Oriental Publishing House, 2008.
- [2] 马华兴. 解惑3G业务: 概念、实现和规划[M]. 北京: 北京邮电大学出版社, 2006.  
MA Huaxing. Understanding 3G Services: Concepts, Implementation and Planning [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2006.
- [3] 中国移动. 物联网演进蓝图[R]. 2009.  
China Mobile. IOT Evolution Blueprint [R]. 2009.
- [4] 中兴通讯. 物联网平台技术白皮书[R]. 2009.  
ZTE Corporation. White Paper of Platform Technology for the Internet of Things [R]. 2009.
- [5] ITU-T Y.2002 (Y.NGN-UbiNet). Overview of Ubiquitous Networking and of its Support in NGN [S]. 2009.
- [6] 李晓维. 无线传感器网络[M]. 北京: 北京理工大学出版社, 2007.  
LI Xiaowei. Wireless Sensor Networks [M]. Beijing: Beijing Institute of Technology Press, 2007.

#### Biographies

##### Xing Xiaojang



Xing Xiaojang is project manager at the Standard Department of ZTE Corporation, and also deputy head of Workgroup 1 of Technical Committee 2 of China Communications Standards Association (CCSA TC2 WG1). He is engaged in the research of service application standards.

##### Wang Jianli



Wang Jianli is supervisor of the Solution Marketing Department of ZTE Corporation. He is mainly engaged in the research of Next Generation communication network architecture and new technologies for mobile Internet.

##### Li Mingdong



Li Mingdong is chief engineer of the Standard Department of ZTE Corporation. He has participated in the successive design, development, and network construction of multimedia, service, and Next Generation Network (NGN) systems. He has also been awarded first prize of the Science and Technology Progress Award of Guangdong Province. He is a Rapporteur of ITU-T SG13 Q13, deputy head of Workgroup 4 of Technical Committee 1 of China Communications Standards Association (CCSA TC1 WG4), and editor of several international standards of ITU-T NGN. His research interests include M2M and cloud computing.

# A Study on the Standardization of Future Internet Architecture

*He Baohong, Zhu Gang*

(China Academy of Telecommunication Research, MIIT of China, Beijing 100191, P. R. China)

## Abstract:

Due to great changes in the application environment of the Internet, current Internet architecture, with "end-to-end transparency" as its principle, is facing challenges such as security, scalability, and Quality of Service (QoS). This paper introduces the design principles and concepts, evolutionary strategies and research status of future Internet architecture. It also analyzes problems and challenges in the process of its standardization, and discusses three evolutionary routes: reformative, integrated, and revolutionary.

## 1 Problems with Existing Internet Architecture

To facilitate the concept of "participation by everyone", the Internet adopts a transparent end-to-end architecture<sup>[1]</sup>. In such an architecture, the intelligence of terminals is used to produce diverse information, while the network simply does its best to transmit this information without any change or control. This design principle, commonly known as "intelligent terminal plus dumb network", aims to simplify network functions and hand complex information processing and control over to the terminal nodes (including servers and users). In this way, users are afforded greater autonomy and more room for innovation, and everybody is able to participate in the development of the Internet.

In the progression from laboratories and research institutes to commercialization, application scenarios of the Internet undergo an enormous change and architecture related problems begin to emerge.

**This work was funded by National High-tech R&D Program of China (863 Program) under Grant No. 2008AA01A301.**

These problems challenge its core end-to-end transparent design. The basic assumption that Internet users are self-disciplined and can trust each other is no longer justified. Instead, the Internet is often a source of attacks, virus spreading, and malicious information propagation. The Internet's role has also changed, from that of a non-commercial trial network used primarily for research, to an important part of the national information infrastructure. It continues to penetrate into every sector of the national economy. The large-scale application of the Internet has brought about security, business model, and Quality of Service (QoS) problems that are bottlenecks to its sustainable and healthy development. Finally, there are no effective benefit allocation and coordination mechanisms for all participants in the industry chain, and this hinders the further development of Internet services.

As application scenarios of the Internet change, the problem of poor controllability in existing Internet architecture becomes increasingly acute. This is reflected in many aspects, including network security, QoS, scalability, and business model. In terms of network security, Internet

architecture enables the separation of end-to-end services from bearer networks. The network provides a unified IP interface for upper-layer applications, leaving all control capabilities and security responsibilities to users at the edge of the network. The network does not sense or limit upper-layer applications nor does it have a reward and penalty mechanism—a condition which leads to uncontrollable user behavior and high trace cost. As for QoS, the Internet lacks necessary resource control and management mechanisms, and can only do its best to deliver services. Improvement in QoS depends largely on an increase of network resources and the self-discipline of users. In fact, the Internet makes no QoS commitments to upper-layer services and applications. Consequently, applications with strict real-time requirements cannot be widely promoted over the Internet. Dynamic routing in the Internet also makes QoS improvement more difficult.

## 2 Concept and Evolution of the Future Internet

The future Internet may change in many ways, but the fundamental concept of

participation by everyone should be maintained and respected. The Internet will otherwise lose its driving force and orientation, and become something else. Sticking to this core principle means not dogmatizing or making absolute the “spirits”, such as freedom, equality, openness and innovation<sup>[2]</sup>, that derive from it.

The future Internet should adopt end-to-end transparent architecture within certain constraints; that is, conditional end-to-end transparency. On the premise that everybody can participate in development and innovation, management and control mechanisms that are transparent to users, and which restrain unruly user behaviors should be embedded into the Internet. These should also balance the duties and interests of all parties in the industry chain. In light of the Internet’s large-scale, and its infinite, interactive, public, and autonomous attributes, the future Internet must provide users with a trustworthy, high QoS, ubiquitous and harmonious virtual experience.

Today, the evolution from existing Internet to future Internet may follow one of three routes: reformative, integrated, or revolutionary.

The “reformative” route takes advantage of the massive amount of information already known about the Internet and employs new technologies to mend what is already existing. Such technologies include address translation, resource control, and security monitor, and these are used to solve existing Internet architecture problems in order to meet the increasing demands for social applications. Persisting with the original transparent end-to-end Internet architecture, IPv6 can be regarded as a representative technology of this route.

Researchers who advocate the revolutionary route believe the existing Internet is unsuitable as a future information infrastructure, and that patchy or systematic mends will only increase the burden on it. Therefore, a new Internet has to be developed for the long term. New Internet architecture has gradually come to the forefront of worldwide research. Various new ideas and technologies have emerged—for

instance, the Forwarding Directive, Association, and Rendezvous Architecture (FARA) model proposed by Massachusetts Institute of Technology; the I3 project of the University of California; and the Global Environment for Network Innovations (GENI) project supported by the US National Science Foundation<sup>[3]</sup>. Yet questions about which technologies will be used, and whether new technologies will need further integration remain unclear.

Researchers favoring the integrative route try to compromise between reformative and revolutionary routes. They tend to think that patchy mends are insufficient for solving existing problems, and that a revolutionary approach will take an excessively long time to implement. The integrative route holds to the principle of mending the Internet in a systematic, large-scale, and overall way. By nature, the Internet is a kind of overlay network. Based on existing Internet architecture, as well as the idea of an overlay network, an intermediate layer can be added between the carrier and application layers. This added layer implements the individual functions of the carrier layer as well as the common functions of the application layer. Hence, the Internet can develop in a healthy and sustainable way on the basis of existing information.

### 3 Research and Standardization of Future Networks

#### 3.1 Typical Research Projects

Future network architecture is faced with several developmental choices; for instance, virtualization network, automatic network, hierarchically switched network, high performance network, trustable network, long-distance low-consumption network, and high-bandwidth long-delay network. Many countries are actively engaged in policy making and investing into these networks, and are trying to take the lead in next generation Internet research. Typical research projects include PlanetLab<sup>[4]</sup> in

the United States, 4WARD in the FP7 frame of the European Union, AKARI<sup>[5]</sup> in Japan, and the Chinese Public Telecom Packet Data Network (PTDN) project.

PlanetLab started in 2002 and is an open testbed for developing, deploying, and accessing global services. Until January 2009, the platform had 474 sites and 950 nodes distributed in over 40 countries. On February 10, 2009, the slice-based architecture was released, which defines interactive interfaces and data types.

Beginning in January 2008, the 4WARD project is a typical network research project of the EU. It employs a strategy of “walking on two legs”: on the one hand, it tries to innovate its way around the shortcomings in current communication network architecture; on the other, it seeks an overall framework that allows interoperability of several network architectures, avoiding pitfalls like the current Internet’s “patch on patch” approach.

The Japanese AKARI Architecture Design Project was launched in 2006. By 2015, it intends to have developed a new network architecture and created a network design based on that architecture. The project team has studied many technical solutions over the past four years, and the design of the architecture diagram is scheduled for completion in 2010.

In 2003, the Chinese Academy of Telecommunication Research proposed the Public Telecom Data Network (PTDN). Research and development into core routing devices, edge routing devices, address mapping system, and address translation system have been undertaken, and interoperation and interconnection with several manufacturers’ devices has been achieved. The PTDN standard has also been submitted to the ITU-T Study Group 13 (SG13) and has been accepted as a candidate solution for Future Packet Based Network (FPBN) in Next Generation Network (NGN) architecture. Moreover, three ITU recommendations have been approved: ITU-T Y.2601, Y.2611,



and Y.2612.

### 3.2 Standardization Efforts of the International Standardization Organization

In the evolution to future Internet, ITU has tended to pursue the revolutionary route. SG13 is the primary group responsible for future network research. Recently, they established a future network team focused on the vision, demand, new technologies, timetable, and standardization of future networks. So far, SG13 has called two meetings which have been attended by research institutes from Europe, China, Japan, South Korea, and other countries. Future networks such as virtualization network, automatic network, and energy-saving network have been discussed. The main work of SG13, however, still rests on collecting design principles, concepts, demands, and technical features of future networks (which are far from having a standard).

In contrast, the Internet Engineering Task Force (IETF) has made a great inroads into the research and standardization of reformative and integrated strategies. It has introduced next generation Internet protocol IPv6 to solve the address scalability problem, studied next generation routing, and addressed the framework to solve the routing scalability problem (where there are two main approaches: ID/Locator<sup>[6-7]</sup> and Map/Encaps<sup>[8-9]</sup>). It has also researched next generation Domain Name System (DNS) for Peer-to-Peer (P2P) distributed domain name services (in order to solve DNS overload and security problems), and has developed Multipath-TCP to achieve high network throughput.

The World Wide Web Consortium (W3C) currently plays a leading role in developing the principles and protocols of semantic web. Semantic-based stack comprises seven layers: identifiers and character set, Extensible Markup Language (XML) syntax, Resource Description Framework (RDF), ontology, unifying logic, proof, and trust from bottom to top. The standards and specifications for the first four layers have been released. At present, W3C is focused on the

research of new RDF-based tools and languages as well as the development of new applications.

In addition to the ITU, IETF, and W3C, other international standardization organizations like ISO have also undertaken research into the standardization of future network architecture.

## 4 Conclusions

Although several international organizations have studied the standardization of future network architecture, the standardization of next generation Internet architecture still faces many challenges. It may take 10 to 20 years to complete the standards of the next generation Internet and put them into practice.

Standardization organizations have tended to go their own way, as opposed to coordinating with each other. The ITU-T favors the revolutionary route, and the development of a new architecture standard. In contrast, the IETF is relatively "realistic" and focused on the short term. It has a preference for improving existing Internet architecture rather than planning long-term solutions, and attempts to work out new standards for existing problems.

Each organization has its own understanding of network architecture. W3C regards semantic web as the next generation Internet, so it understands network architecture more from the perspective of application layer. ITU-T and other organizations understand the architecture from the point of view of bearer network.

Finally, organizations adopt different attitudes to the inheritance of existing technologies. IETF has acknowledged that a fatal flaw in IPv6 is its failure to be backwardly compatible with existing IPv4. The ITU-T, however, argues that it may be unnecessary to take into account compatibility with existing networks in the innovative design of future network architecture. So far, on the critical question of whether (or to what extent) the Internet will be compatible with existing IPv4 and IPv6, and how to learn from IPv6, little study

has been conducted and no consensus has been reached.

### References

- [1] 何宝宏. 互联网“端到端透明”面临挑战 [N]. 人民邮电, 2006-02-13.  
HE Baohong. Challenges Facing "End-to-End Transparency" of the Internet [N]. People's Posts and Telecommunications News, 2006-02-13.
- [2] 信息产业部电信研究院. 互联网技术发展白皮书 第一卷: 发展脉络与体系架构 [J]. 世界电信, 2007, 20(7): 8-13.  
China Academy of Telecommunication Research (CATR) of MII. Internet Technology Development White Paper Volume 1: History of Development and System Framework [J]. World Telecommunications, 2007, 20(7): 8-13.
- [3] Plain Text-GENI: geni-Trac [EB/OL]. [2009-02-13]. <http://svn.planet-lab.org/attachment/wiki/GeniWrapper/sfa.pdf>.
- [4] PlanetLab [EB/OL]. [2009-05-20]. <http://www.planet-lab.org/>.
- [5] AKARI [EB/OL]. [2009-09-30]. <http://akari-project.nict.go.jp/>.
- [6] MOSKOWITZ R, NIKANDER P. Host Identity Protocol (HIP) Architecture [R]. IETF RFC 4423. 2006.
- [7] XU Xiaohu, GUO Dayong. Hierarchical Routing Architecture (HRA) [C]//Proceedings of Next Generation Internet Networks (NGI'08), Apr 28-30, 2008, Krakow, Poland. Piscataway, NJ, USA: IEEE, 2008: 92-99.
- [8] FARINACCI D, ORAN D, FULLER V, et al. Locator/ID Separation Protocol (LISP) [R]. IETF Network Working Group. Internet Draft. draft-farinacci-lisp-10.txt.2008.
- [9] FRANCIS P, XU X, BALLANI H. FIB Suppression with Virtual Aggregation and Default Routes [R]. IETF Network Working Group. Internet Draft. draft-ietf-grow-va-00 September. 2008.

### Biographies

#### He Baohong



He Baohong is the chairman of the Internet research area of the China Academy of Telecommunication Research (CATR), Ministry of Industry and Information Technology of China. He is also the vice chairman of the IP & Multimedia Communication Technical Committee of the China Communications

Standards Association (CCSA), and the rapporteur of ITU-T Q24/16. His research interests include the Internet technologies, standards, industry, and policies. He has presided over the making of more than 10 international standards, and published over 60 papers.

#### Zhu Gang



Zhu Gang received his doctoral degree from the Department of Electronic Engineering, Tsinghua University, and holds a postdoctoral position in CATR. His research interests include next generation Internet architecture, and routing scalability.

# MAC Protocols for Distributed Cooperative Communication Networks

## Abstract:

Distributed cooperative networks use the cooperation among nodes to fulfill network resource sharing. However, designing an efficient Media Access Control (MAC) protocol is a key issue for the distributed cooperative network. Based on the principle of MAC-layer cooperation, this paper discusses problems and challenges for MAC protocol design in the distributed cooperative network. Through the analysis of typical cooperative MAC protocols and their performance, this paper concludes that only a reasonable MAC protocol design with the features and demands of distributed networks taken into account can make cooperative communication technology a better application in the distributed network.

*Sheng Min*  
*Zhang Yan*  
*Li Jiandong*

(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, P. R. China)

Recently, distributed networks have been attracting greater attention because of their flexible networking and easy deployment. However, multiple access protocol design still poses a significant challenge. As an emerging communication form, cooperative communication technology has also attracted close attention. Making full use of the omnidirectional propagation feature of radio transmission, this technology fulfills network resource sharing through cooperation among multiple nodes. Eventually, it greatly improves the performance of the entire network<sup>[1]</sup>. Early research into cooperative communication technology has focused on the physical layer<sup>[1-3]</sup>, but lacks detailed study on how the cooperation concept influences

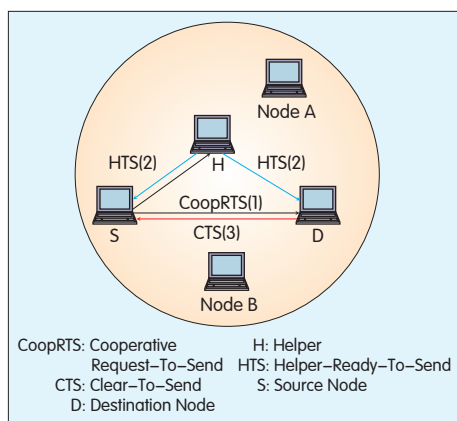
upper-layer protocols, especially Media Access Control (MAC) protocol. The MAC protocol determines resource usage, and optimizing resource allocation is an important part of cooperative communication technology, therefore, good MAC protocol design in the distributed cooperative communication system is most important for maximizing the advantages of the cooperative technologies.

## 1 Motive of MAC Cooperation

Currently, IEEE 802.11<sup>[4]</sup> multiple access protocols are the most popular Wireless Local Area Network (WLAN) access standards, and are widely applied to testing and simulation platforms of distributed networks. The 802.11 protocols can support multiple rates on the physical layer, and make adjustments according to different channel conditions. For example, IEEE 802.11b can support the rates of 1, 2, 5.5 and 11 Mbit/s separately. If the

distance between two nodes is great or the channel condition is bad, message transmission only occurs at low rates (eg. 1 or 2 Mbit/s). This decreases the performance of the whole distributed network because not only is the transmission performance of the involved nodes influenced, but also the neighboring nodes have to wait a long time for transmission opportunities. Therefore, it is necessary to use the cooperation among nodes to improve network performance. One simple and effective method is to introduce a helper node for improving the transmission from the source node to the destination node<sup>[5-11]</sup>. If the conditions of both channels from the helper node to the source and destination nodes are good, high-speed cooperative transmission can be fulfilled. Accordingly, the saturated throughput of the entire network is improved. With the introduction of cooperative communication technology, the MAC protocol design of the distributed network becomes complex, posing new

This work was supported by the National Basic Research Program of China ("973" Program) under Grant No. 2009CB320404, National High Technology Research and Development Program of China ("863" Program) under Grant No. 2007AA01Z217, and National Natural Science Foundation of China under Grant No. 60972048.



▲ Figure 1. Interaction of CoopMAC control frames.

problems and challenges.

## 2 Problems and Challenges of Distributed Cooperative Multiple Access Protocol Design

### 2.1 “Cooperation” or “Uncooperativeness”

From the standpoint of Information Theory, cooperation always brings system gain, for example, diversity gain. However, in a real life system, the MAC protocol has to introduce overhead information to enable cooperation between nodes. This may lead to poor cooperation performance, or even totally counteract the gain brought about by the cooperation, badly impacting the system as a whole. Therefore, in the design of a distributed network, various system parameters (such as packet length and transmission rate) should be taken into account to decide if cooperation technology is to be introduced.

### 2.2 Selection of Cooperative Node

The following factors should be considered when selecting the cooperative node in a distributed network:

- Rate improvement. The introduction of cooperative nodes should obviously improve the information transmission rate.
- Interference Decrease. Because the introduction of cooperation increases interference with other nodes

in the network, the cooperative nodes should minimize their interference with other data flows, in order to improve space reuse of the network.

- Fairness. The cooperative node consumes its own energy to help the source node finish its communication, so full consideration of network fairness should be given before the cooperative node is selected. Excessive use of certain nodes should also be avoided.

### 2.3 Problems of Hidden Terminals and Exposed Terminals

Hidden terminals and exposed terminals are important problems in the distributed network. The problems become more serious with the introduction of cooperation because cooperation necessarily increases handshake messages between nodes. They may greatly lower the probability of successful cooperation. Therefore, weakening or avoiding the influence of hidden terminal and exposed terminal problems is an important issue for the distributed cooperative protocol. Solutions include protocol optimization, and application of a smart antenna.

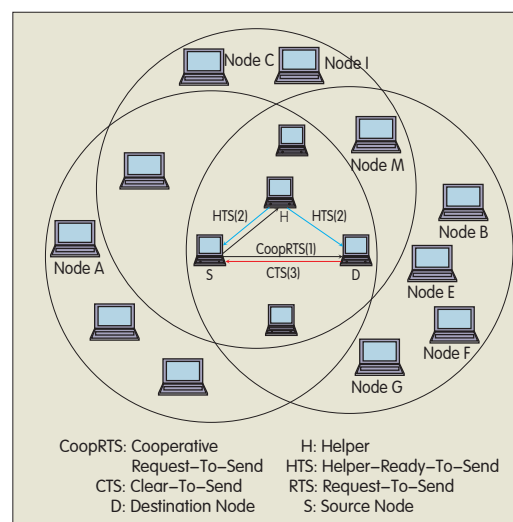
## 3 Typical Distributed Cooperative Multiple Access Protocols

### (1) CoopMAC Protocol

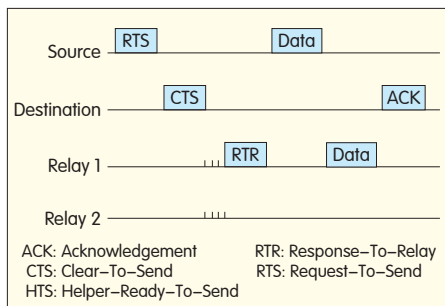
Based on IEEE802.11 protocols, P. Liu et al proposed a CoopMAC protocol<sup>[5-6]</sup>. This protocol uses high-speed nodes to help low-speed nodes finish transmission, which greatly improves network throughput, shortens the access delay of nodes, and decreases the total energy consumption of all the nodes. In CoopMAC protocol, every node maintains a cooperation table which includes the rate from the source node to a relay node, the rate from the relay node to the destination node, and the table update time. When transporting data, a node first checks the table to determine whether there is a cooperative node to use and then decides whether to use cooperative

transmission. When cooperative transmission is permitted, the source node sends Cooperative Request-To-Send (CoopRTS) first; the Helper node assesses whether it can support the expected rate after correctly receiving CoopRTS and, if possible, sends a Helper-Ready-To-Send (HTS); the destination node finally responds with Clear-To-Send (CTS), and the cooperative handshake process finishes. After that, the source node sends data at a high speed to the Helper, and the Helper transfers them at high speed to the destination node. Legacy 802.11b protocol is used when no cooperative transmission is required or there is no cooperative node. The handshake process of CoopMAC protocol is shown in Figure 1.

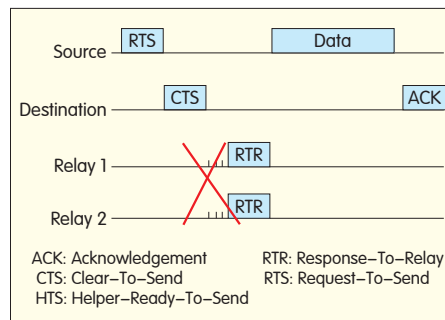
In a fully connected network, the 3-way handshake mechanism required by cooperative transmission is not so different to the legacy RTS/CTS handshake mechanism, which just makes handshakes longer and more complex. However, in the distributed multi-hop network, the three-time handshake mechanism is influenced more by the hidden terminal problem. As shown in Figure 2, when the source node sends CoopRTS, Nodes {B, C, E, F, G, M, I} are all hidden terminals, and any may influence the correct reception of CoopRTS when it sends messages. When the Helper sends HTS, Nodes {B, E, F, G} are still hidden terminals. In this



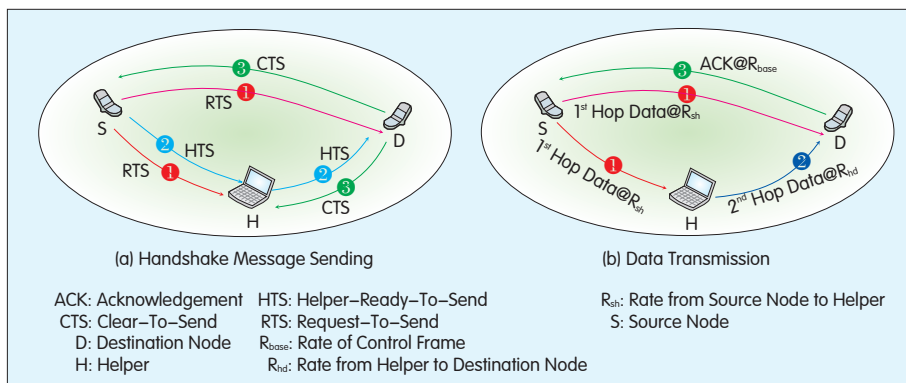
▲ Figure 2. Hidden terminal problem of CoopMAC.



▲ Figure 3. Successful neighboring node reservation.



▲ Figure 4. Collision in reservation process.



▲ Figure 5. Enhanced cooperative MAC protocol.

situation, Node B, for example, may interfere with the transmission of current handshake messages in a relative long time. Therefore, the hidden terminal problem may seriously influence the performance of CoopMAC protocol in a distributed multi-hop network.

#### (2) "On-Demand" Cooperative MAC Protocol

Some researchers believe each node in the CoopMAC protocol has to maintain the cooperative tables of its neighboring nodes, which increases storage overhead, and that node mobility and channel time-variance hinder the cooperative table from timely updating with the network status changes. Therefore, they have proposed an "on-demand" cooperative MAC protocol<sup>[8]</sup>. In this protocol, a node does not maintain any information of the cooperative node. When there is data to be sent, the source node first sends the RTS message, and the destination node responds to the CTS message after it has received the RTS. Then the potential cooperative node can obtain the channel information from the source

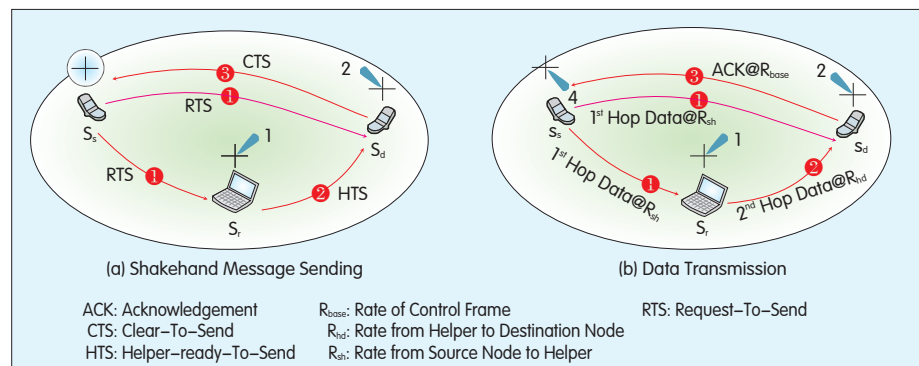
node to itself,  $H_{SR}$  and that from the destination node to itself,  $H_{RD}$  through the above two handshake messages. Cooperative nodes compete to participate in the cooperation by setting the backoff time  $T$ , as shown in Figure 3.  $T$  is the inversely proportional function of  $H_{SR}$  and  $H_{RD}$ . However, in this protocol, the possibility of collision taking place during the cooperative node reservation may lead to the failure of the whole handshake process, as Figure 4 shows.

#### (3) Cooperative MAC Protocol with Joint Signal Decomposition

Early CoopMAC protocol uses the multi-rate transmission feature of 802.11, but only when the destination node is able to jointly decompose the signals from the source and destination nodes, can a real virtual Multiple-Input Multiple-Output (MIMO) system be built. Since signals come at different times and from different nodes, the system can obtain space and time diversity. Feilu Liu et. al. proposed a corresponding enhanced CoopMAC protocol<sup>[9]</sup>, which has handshake and information transmission processes coherent with CoopMAC protocol, as shown in Figure 5. The destination receives two copies of the original packet, one from the source and one from the helper, and combines them for decoding. In a distributed multi-hop network, simulated performance of this enhanced protocol indicates about 10% throughput gain, when compared to that of the original CoopMAC protocol. However, this protocol has higher requirements of hardware devices.

#### (4) Cooperative MAC Protocol Supporting Directional Antenna

In terms of the network, the introduction of cooperative nodes decreases the spatial reuse level of the entire network during cooperative communications. How to make up for the loss is an important issue in cooperative MAC protocol design, and is currently of great interest to researchers<sup>[10]</sup>. Zhifeng Tao et. al. proposed a D-CoopMAC protocol<sup>[11]</sup> with the condition that nodes have directional antennas. As shown in Figure 6, when transporting data, the source node must first omnidirectionally



▲ Figure 6. D-CoopMAC.



broadcast the RTS message. The cooperative node, after receiving the message, then moves the transmitting antenna toward the destination and sends the HTS message. After successfully receiving RTS and HTS, the destination node responds with CTS to the source node; and the resultant data transmission is directional. This method resolves the decrease in network space reuse to some extent, but also increases the complexity and cost of equipment.

It is notable that, with the increased number of beams from directional antennas, D-CoopMAC performance is instead inferior to that of transmission directly through directional antenna. This is because the cooperative network needs space reuse to implement cooperation. Controlling overhead is also detrimental to network performance. Accordingly, the use of cooperation in any real network should be selective, or it may bring about the opposite result.

The above analysis of these typical cooperative MAC protocols shows that different design criteria and methods should be chosen for different network environments and configurations. This is the only way to realize the gain in cooperative communication theory and further improve the whole network performance.

## 4 Conclusions

In this paper, we have detailed the motives of MAC-layer cooperation in distributed networks, highlighted the problems and challenges facing the design of MAC protocols in the distributed cooperative network, and discussed typical cooperative MAC protocols and their performance. The study of cooperative MAC protocol in the distributed network is ongoing, and designing a simple and effective

cooperative MAC protocol with theoretical performance analysis will be one of the important research subjects in the future. Moreover, the existing cooperative MAC protocols involve no discussion about fairness between nodes, an issue which may throw the network into an uncooperative state.

## References

- [1] LANEMAN J N, TSE D, WORNELL G W. Cooperative diversity in wireless networks: efficient protocols and outage behavior [J]. IEEE Transactions on Information Theory, 2004, 50(12): 3062–3080.
- [2] SENDONARIS A, ERKIP E, AAZHANG B. User cooperation diversity, part I: system description [J]. IEEE Transactions on Communications, 2003, 51(11): 1927–1938.
- [3] SENDONARIS A, ERKIP E, AAZHANG B. User cooperation diversity, part II: implementation aspects and performance analysis [J]. IEEE Transactions on Communications, 2003, 51(11): 1939–1948.
- [4] ANSI/IEEE Std 802.11. IEEE LAN MAN Standard, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [S]. 1999.
- [5] LIU P, TAO Z, PANWAR S. A cooperative MAC protocol for wireless local area networks [C]// Proceedings of IEEE International Conference on Communications (ICC'05): Vol 5, May 16–20, 2005, Seoul, Korea. Piscataway, NJ, USA: IEEE, 2005: 2962–2968.
- [6] LIU P, TAO Z, NARAYANAN S, et al. CoopMAC: a cooperative MAC for wireless LANs [J]. IEEE Journal on Selected Areas in Communications, 2007, 25(2): 340–354.
- [7] ZHU H, CAO G.. rDCF: a relay-enabled medium access control protocol for wireless ad hoc networks [C]//Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05): Vol 1, Mar 13–17, 2005, Miami, FL, USA. Piscataway, NJ, USA: IEEE, 2005: 12–22.
- [8] MOH S, YU C, PARK S M, et al. CD-MAC: cooperative diversity MAC for robust communication in wireless ad hoc networks [C]// Proceedings of IEEE International Conference on Communications (ICC'07), Jun 24–28, 2007, Glasgow, UK. Piscataway, NJ, USA: IEEE, 2007: 3636–3641.
- [9] TAO Guo, CARRASCO R, WAI Lok Woo. Performance of a cooperative relay-based auto-rate MAC protocol for wireless ad hoc networks [C]//Proceedings of the 67th Vehicular Technology Conference (VTC-Spring'08), May 11–14, 2008, Singapore. Piscataway, NJ, USA: IEEE, 2008: 11–15.
- [10] LIU Feilu, KORAKIS T, TAO Zhifeng, et al. A MAC-PHY cross-layer protocol for wireless ad-hoc networks [C]//Proceedings of Wireless

- Communications and Networking Conference (WCNC'08), Mar 31–Apr 3, 2008, Las Vegas, NV, USA. New York, NY, USA: IEEE, 2008: 1792–1797.
- [11] TAO Zhifeng, KORAKIS T, LIU Feilu, et al. Cooperation and directionality: Friends or foes? [C]//Proceedings of IEEE International Conference on Communications (ICC'08), May 19–23, 2008, Beijing, China. Piscataway, NJ, USA: IEEE, 2008: 4424–4430.

## Biographies

### Sheng Min



Sheng Min is a professor and doctoral advisor at the State Key Laboratory of Integrated Services Networks, Xidian University. Her main research fields include mobile communications, wireless ad hoc networks and cognitive radio networks. She has participated or led 10 state-level science research projects, published 2 technical books, and more than 60 papers among which 40 can be retrieved in SCI and EI.

### Zhang Yan



Zhang Yan is a doctoral candidate at the State Key Laboratory of Integrated Services Networks, Xidian University. His research interests include mobile communications and wireless ad hoc networks.

### Li Jiandong



Li Jiandong is a professor and doctoral advisor at the State Key Laboratory of Integrated Services Networks, Xidian University. His research interests include wireless ad hoc networks, broadband wireless mobile communications, software radio, and cognitive radio. He has participated or led 30 state-level science research projects, published 7 technical books, and more than 200 papers among which 160 can be retrieved in SCI and EI.

AD Index

A1–A3, Back Cover:  
ZTE Corporation

# Optimization of One-Plane Packet Loss in IP Bearer Networks

## Abstract:

The problem of one-plane packet loss of the IP bearer network in an Mc-interface mobile Softswitch system impacts Softswitch services in the active/standby access mode, and in the load balancing access mode. This paper focuses on optimization of the load balancing access mode. It also puts forward detailed suggestions for network optimization, providing a reference for mobile Softswitch network optimization and network security.

**Lu Weifeng**

(Mobile Product Support Center of ZTE Corporation, Nanjing 210012, P. R. China)

In a mobile Softswitch system, the Mc interface refers to the interface between the gateway Mobile Switching Center Server (MSCS) and Media Gateway (MGW). The transmission protocol of the interface can be based on IP or Asynchronous Transfer Mode (ATM). In practice, the IP-based bearing mode is most commonly used in networks.

Since the MGW sometimes functions as the signaling gateway, the transported controlling messages between MSCS and MGW in the IP bearer network include H248 signaling of the Mc interface, as well as interface-A signaling for the Base Station System Application Part (BSSAP)/Signaling Connection Control Part (SCCP) and inter-office signaling for the ISDN User Part (ISUP)/Telephone User Part (TUP). Mobile Application Part (MAP)/SCCP signaling for the Mobile Switching Center Mobile Application Part (MSCMAP), Visitor Location Register Mobile Application Part (VLRMAP), and Home Location Register Mobile Application Part (HLRMAP) is required.

Therefore, the IP bearer network is necessary and important for the normal running of the Softswitch system.

The IP bearer network is generally designed in a dual-plane mode.

Therefore, the interruption of any plane should not affect the Softswitch service. However, in practice, when one-plane packet loss occurs in the IP bearer network, the Softswitch service is severely affected with symptoms of coupling congestion, coupling interruption, and low connection ratio.

This paper takes the ZXWN CS system as an example to analyze one-plane packet loss of the IP bearer network from the viewpoint of Softswitch. It also proposes a solution for network planning and optimization.

## 1 Active/Standby Access Mode and Load Balancing Access Mode

In the early stages of replacing traditional switching devices with mobile Softswitch devices, (when the universal IP bearer network was not accessible), a dedicated IP bearer network mode was used, providing point-to-point IP bearing. With the improvement of the IP bearer network, Softswitch devices were implemented in the universal IP bearer network<sup>[1]</sup>.

When Softswitch devices access the IP bearer network, two typical networking modes are used: active/standby access mode, and load balancing access mode.

The active/standby access mode has the following features:

(1) At the Softswitch side, one pair of Signaling IP Interface (SIPI) boards are installed. Each board provides one Fast Ethernet (FE) interface connected to two L2 switches, and then connected to two Customer Edges (CEs).

The function of the L2 switch is to ensure the independent implementation of the SIPI active/standby switchover, and Virtual Router Redundancy Protocol (VRRP). When a certain CE supports L2 interface, the L2 switch will not be configured independently.

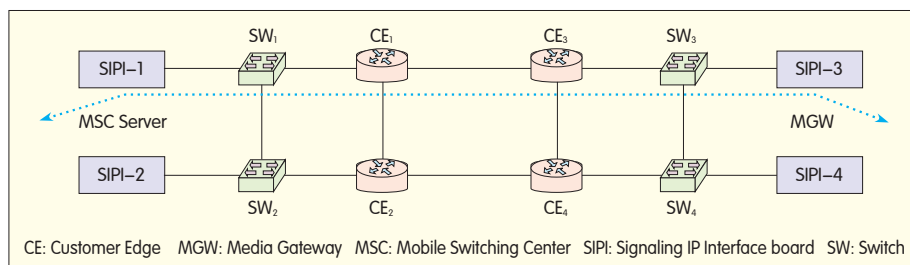
(2) The interface board at the Softswitch side uses the active/standby working mode. CE enables VRRP for the softswitch side.

(3) Fault detection between the SIPI and CE is implemented independently. The basis of SIPI active/standby switchover detection is the port status between the SIPI and L2 switch. The basis of switchover detection in the CE is the heartbeat message between CEs.

(4) Normally, in the active/standby mode, as shown in Figure 1, one transmission channel (active channel) is used between MSCS and MGW.

Features of the load balancing access mode include:

(1) One pair of SIPI boards are configured at the Softswitch side. Each



▲ Figure 1. Networking example of active/standby mode.

board provides an FE interface accessing the CE, or accessing the CE after switch convergence.

(2) The interface board at the Softswitch side uses the load balancing mode. CE also uses the load balancing mode.

(3) Bidirectional Forward Detection (BFD) is performed between SIPI and CE.

(4) Normally, as shown in Figure 2, between the MSCS and MGW using load balancing mode, two transmission channels can be used.

## 2 IP Bearer Network One-Plane Packet Loss in Two Networking Modes

(1) In the active/standby mode, the service is carried by the active transmission channel only. The symptoms of one-plane packet loss in the bearer network are as follows.

The Softswitch service is not carried by the standby channel, so when packets are lost in the standby transmission channel, the service is not affected. The Softswitch device cannot detect whether packets have been lost in the standby channel.

Softswitch services are carried by the active transmission channel, so when packets are lost in the active transmission channel, the service is affected and the impact is related to the packet loss rate. The Softswitch device can detect packet loss in the active channel but cannot control the switchover to the standby channel of the IP bearer network.

When the active channel is interrupted, the IP bearer network can detect the interruption and switch to the standby channel. When the packets are lost in the active channel, the IP bearer

network cannot detect it and thus the service will not be switched to the standby channel.

Therefore, when the active/standby access mode is used, and packet loss occurs in one plane in the IP bearer network, optimization cannot proceed at the Softswitch side.

(2) In the load balancing mode, the service is carried by two transmission channels. The symptoms of one-plane packet loss in the bearer network are as follows.

When packets are lost in one transmission channel, only that channel's service will be affected. At the same time, the Softswitch side can detect the transmission channel with packet loss and choose the better channel for data transmission.

Therefore, when the load balancing access mode is used, and packet loss occurs in one plane in the IP bearer network, optimization can proceed at the Softswitch side.

## 3 Optimization Solution to One-Plane Packet Loss of IP Bearer Network in Load Balancing Mode

According to the preceding analysis, when the active/standby access mode is used and packets are lost in the active transmission channel, the router

does not provide the link quality detection function, and the route cannot be switched. As a result, the upper level service carried will be seriously affected. When the load balancing access mode is used, the upper level service will not be affected.

In practice, although the load balancing networking mode is used in some cases, when a transmission channel fails, the service carried is affected. The following are the key reasons:

(1) Route Configuration Mode of the Stream Control Transmission Protocol (SCTP)<sup>[2]</sup> Destination Address

At the Softswitch side, the route to the SCTP destination IP address should be configured. For the load balancing access mode, the common setting modes are as follows:

Route configuration mode 1: configure a route; select the interface address of one router for the next hop.

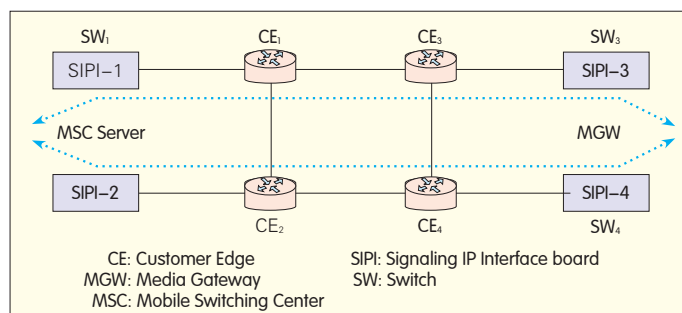
Route configuration mode 2: configure two equivalent routes; select the interface addresses of the two routers for the next hop; the two routes are equivalent and they are valid at the same time.

Route configuration mode 3: configure two non-equivalent routes; select the interface addresses of the two routers for the next hop; the two routes are not equivalent. Normally, only the routes with higher priority are valid. When the route with higher priority is not available, the route with lower priority is valid.

Route configuration modes 1 and 3 are single next-hop modes. Compared to mode 1, a standby route is added in mode 3. Route configuration mode 2 is a multiple-next-hop mode.

(2) To Use SCTP Multiple Homing or Not

Figure 2. Networking example of the load balancing mode.



In the SCTP protocol, the definition of multiple homing states that "if multiple destination transmission addresses can be used as the destination address of one end, the SCTP end can be considered to be multiple homing. Moreover, the Upper Level Protocol (ULP) of the end can select one address as the primary channel of the multiple-homing SCTP point." This feature is the major difference between SCTP and TCP.

When SCTP multiple homing is not used, there is only one transmission address to the destination address. For route configuration modes 1 and 3, there is only one valid route to the destination IP address. When the packets are lost in the route, the SCTP transmission service is affected. For route configuration mode 2, if packets are lost in one route, the SCTP transmission service will be affected.

When SCTP multiple homing is used, there are two or more transmission addresses to the destination address. And between the two ends, there are two or more channels. For route configuration modes 1 and 3, different destination IP addresses can be transmitted over different routes. When packets are lost in one route, only the relevant channel is affected. If the channel is the primary channel of the SCTP, the transmission service of the SCTP will not be affected. For route configuration mode 2, all channels are transmitted over the two routes. As a result, when packets are lost in one route, the SCTP transmission service will be affected.

#### (3) Impacts of SCTP Congestion on Addressing

The above mentioned reasons (1) and (2) are for a single SCTP. In practice, the upper level service usually uses a pair of SCTPs to transmit data. Taking Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA) as an example, this paper analyzes the impact on the upper level service of SCTP failures.

In the M3UA protocol, the definition of fault resilience is "the capability that the signaling service re-routes to the alternative server process or application server process group when

the current Application Server Process (ASP) is faulty or is unavailable. Fault resilience is also used to return to the previously unavailable application server process."

ASP contains the SCTP ends. When some SCTPs in the ASP group are faulty or unavailable, according to the protocol, the upper level service will not select the faulty SCTP. But when some SCTP is congested but not interrupted, the upper level service can select the congested SCTP. As a result, the service is affected.

## 4 Networking Optimization Suggestions

Considering the previous analysis, optimization suggestions for the mobile Softswitch and IP bearer network are as follows:

(1) Use the load balancing access mode: in the active/standby access mode, the forwarding plane or path cannot be switched and the NE has no initiative for switching. Therefore, the load balancing access mode should be selected.

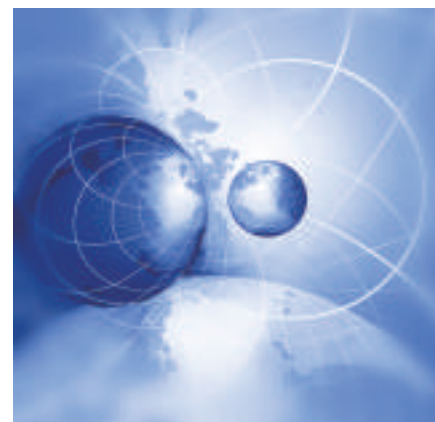
(2) SCTP supports transmission quality monitoring: when the SCTP channel has multiple transmission paths, the transmission quality of each channel in the SCTP layer should be monitored and a path with better transmission quality automatically selected.

This function requires that a crossover node cannot exist in multiple transmission paths. Otherwise, when the packets are lost in the crossover node, the link quality of all transmission paths will decrease.

(3) Use the SCTP multiple homing configuration: each SCTP active channel and standby channel takes different routes and there is no crossover node.

By default, when the number of failures or re-transmission attempts of the active channel exceed 5 (this parameter is configurable), switchover of the SCTP primary channel is performed automatically.

When transmission quality monitoring is supported, the SCTP can detect the transmission quality of each channel.



When the transmission quality of the active channel is degraded but the channel is not interrupted, the SCTP can switch over the channel and automatically select the channel with better transmission quality.

(4) Optimize the SCTP congestion control: when the upper level service is dynamically selecting a route, the uncongested SCTP is automatically selected according to the SCTP congestion status. At the same time, the threshold of congestion reporting is set. Only when the threshold is exceeded, is the congestion reported to the upper level user, and the upper level user controls the congestion of the service traffic.

#### References

- [1] YD/T 1194—2002. 流控制传送协议(SCTP) [S]. 2002.  
YD/T 1194—2002. Stream Control Transport Protocol (SCTP) [S]. 2002.
- [2] YD/T 1192—2002. No.7 信令与IP互通适配层技术规范——消息传递部分(MTP)第三级用户适配层(M3UA) [S]. 2002.  
YD/T 1192—2002. Technical Specification of Adaption Layer for No.7 Signalling Interworking with IP—Message Transfer Part (MTP) Level 3 User Adaption Layer (M3UA) [S]. 2002.

#### Biography

Lu Weifeng



Lu Weifeng graduated from South East University. He is a technical support engineer at the Mobile Customer Service Department (Nanjing) of the Mobile Product Support Center, ZTE Corporation.



# Routing in Cognitive Networks

## Abstract:

Cognitive networks are capable of learning and reasoning. They can dynamically adapt to varying network conditions in order to optimize end-to-end performance and utilize network resources efficiently. This paper proposes a cognitive network routing scheme that includes a context information collection entity, a route manager entity, a route reconfiguration entity, and reasoning and learning entity.

*Li Hongyan*  
*Li Jiandong*  
*Hou Ronghui*

(State Key Lab of Integrated Service  
Networks, Xidian University, Xi'an 710071,  
P. R. China)

## 1 Origin of Cognitive Networks

It was Mitola<sup>[1]</sup> who first proposed the concept of Cognitive Radio (CR) and the architecture of the cognitive loop. A CR system senses the spectrum environment and automatically reconfigures its radio transceiver to use spectrum holes for communication. The CR system has the capability of learning and reasoning, and adjusts itself intelligently to achieve efficient spectrum resource use.

The Cognitive Packet Network (CPN) was proposed by Gelenbe<sup>[2]</sup>. In a CPN, intelligent packets which carry executable codes are responsible for collecting network information. When an intelligent packet arrives at a node in the network, it exchanges context information with the node, and updates the route table of the node. In this way, the route is optimized.

With the Cognitive Network (CN) concept, Ramming<sup>[3]</sup> applies the concept of cognitive loop to the network level. The definition of a CN according to Thomas<sup>[4]</sup> is a network composed of elements that, through learning and reasoning, dynamically adapt to varying network conditions in order to optimize end-to-end performance. Thomas analyzed the learning and reasoning mechanism of cognitive

networks, and provided a functional description of the architecture and component units. During their discussion of integration architecture of heterogeneous wireless access networks, the IEEE adopted the concept of cognitive networking<sup>[5]</sup>.

## 2 Routing Algorithm Frame of Cognitive Networks

The future network will be a large-scale heterogeneous network. In such an environment, there are many alternative routes for each pair of ends. Conditions for efficient use of network resources are thereby achieved. However, designing the routing algorithm in heterogeneous networks is a big challenge. First, in a heterogeneous network, the performance of links belonging to different networks is quite different. Second, the heterogeneous network environment often varies. Link transmission data rate and reliability change with the environment. In addition, in an overlapped network scenario it is difficult to predict and control spectrum interference of wireless links. Routing strategy is affected by factors such as the ability to access multiple networks, link throughput, user preference, QoS requirements, and location.

In this complicated network environment, routing algorithm needs to solve the issues of context adaptation,

efficient use of link, network, user resources, and end-to-end optimization. Figure 1 shows a cognitive routing scheme of policy-based for heterogeneous networks. The framework includes the following functional entities:

(1) Situation Awareness Entity

This is responsible for sensing context and mapping a service request to an end-to-end QoS request.

(2) Route Manager Entity

This is responsible for construction, update, and restoration. It selects routing policies according to context information and optimization object.

(3) Route Reconfiguration Entity

This is responsible for route configuration. If the cross-layer routing protocol has been adopted, the entity instructs the configuration of the network layer, data link layer, and physical layer.

(4) Reasoning and Learning Entity

This is responsible for evaluation, amendment, and generation of the policies in order to adapt to context.

## 3 Key Problems

### 3.1 Situation Awareness Entity

A cognitive network implements decision-making, reasoning, and learning functions according to context aware information. The coverage, timeliness, consistency, accuracy, and reliability of context information directly

affects the performance of the cognitive network. Retrieval and distribution of the context information directly affects the network load.

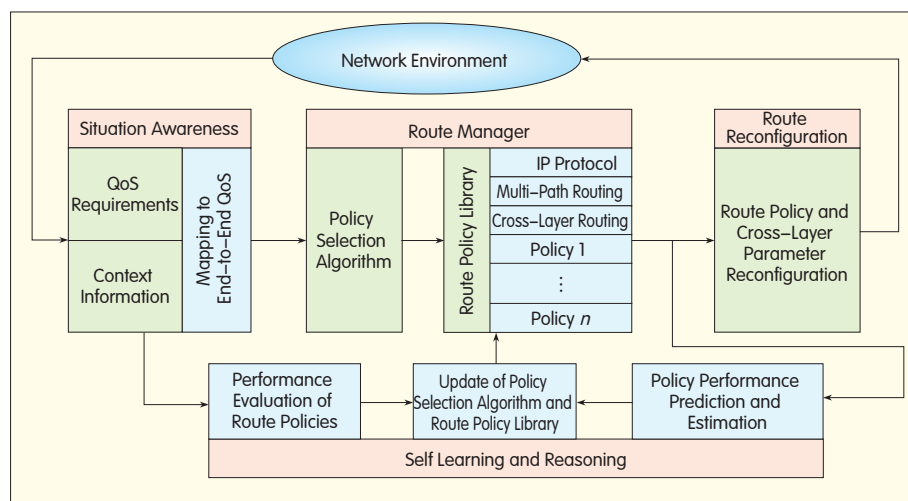
In a large-scale network, many factors affect route selection between two ends; for example, link parameters, services carried by the network, and available networks between ends. The nodes of a cognitive network exchange their obtained context information using various methods. In a large-scale heterogeneous network, it is difficult to synchronize context information. Various cognitive nodes may have different understandings of the network status, and as a result, routing algorithm oscillation may occur. Inconsistent node information may mislead the route manager entity to make a suboptimal decision, so as to cause route oscillation.

Generally speaking, network information is collected in three ways: active retrieval, passive retrieval, and a combination of both. The information collection mode, frequency, and range affect the performance of routing algorithm and network load. Therefore, the collection mode of context information and parameter settings should be adjusted to the network environment. The adjustments of situation awareness entity parameters also constitute a cognitive loop.

### 3.2 Route Manager Entity

The objective of the routing algorithm is to construct a transmission path satisfying certain QoS for end-to-end nodes in the network. Considering the issue of resource optimization, when the network load is heavy, the cognitive routing algorithm enables services to be distributed evenly in the network. When the network load is light, the cognitive routing algorithm can improve users' satisfaction by utilizing storage capabilities of the network and users to pre-consume network resources.

The cognitive routing algorithm is a complicated decision-making issue. First, in a heterogeneous network, the number of available link modes is large. The number of end-to-end paths constructed by multiple-mode links is also large. In order to adapt to varying



▲ Figure 1. Routing frame of policy-based cognitive networks.

contexts, and to use network resources efficiently, route evaluation criteria and a multiple path mode should be adopted. Second, nodes in a large-scale heterogeneous network generally determine routes in a distributed way. Decision-making processes are concurrent. Conflict between node policies may occur, leading to inconsistent routing tables within the nodes after the reconfiguration.

The relationship between NEs is competitive but also cooperative. The scale of the heterogeneous network is large, and the issue of complex decision-making is difficult to model and solve. How to design a cognitive routing algorithm in the complicated network is an academic problem to be solved. For complex decision-making, a solution based on policy library may be adopted. In Figure 1, existing and newly developed routing strategies are kept in a routing policy library. According to the context information and service requirements, the policy selection algorithm is responsible for selecting policy. This algorithm may be considered as mapping from the context to the policy.

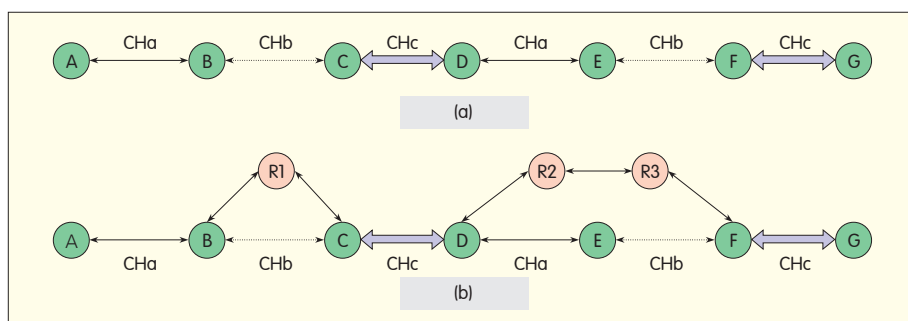
The routing policy library contains regular routing protocols such as IP protocol. However, new routing protocols applicable to the heterogeneous network can be facility added into the library (e.g. the routing algorithm applicable to MIMO link, and

the cross-layer routing algorithm supporting link cooperation and network cooperation<sup>[6]</sup>). Figure 2 illustrates the link cooperation scheme of Ad hoc networks. Between any two nodes of an Ad hoc network, multi-hop links compose the end-to-end multi-channel "cooperative path". In Figure 2(a), adjacent links on the same path are configured with different channels. When the node is working in a half-duplex mode, links A-B, C-D, and E-F, or links B-C, D-E, and F-G can transmit concurrently. As a result, the capacity of the path is increased and "cooperative path" gain is achieved. When channel configuration of the path conflicts with the neighboring path, a cooperative path shown in Figure 2 (b) can be constructed.

### 3.3 Self Learning and Reasoning Entity

The reasoning and learning mechanism distinguishes the cognitive process from the adaptive process. In the cognitive routing algorithm, the reasoning and learning entity evaluates the execution results of routing policy and then amends the policy selection algorithm and routing policy itself.

In the large-scale heterogeneous network environment, the scope of service QoS varies greatly. Network links can be quite different from each other. Different networks have different management modes, QoS capabilities, and power consumption. In addition,



▲ Figure 2. Multi-channel cooperative path mode.

user preferences are different. In such a network environment, it is impossible for one routing policy to meet the requirements of various networks and users. The routing policy library should be constructed to adapt to service and network context.

In a complicated network environment, routing policy selection from the policy library, and configuration and reconfiguration of routing policy parameters, are two problems affecting the implementation of policy-based routing algorithms. A routing policy library contains multiple routing policies, including single path routing, multi-path routing and cross-layer routing. Selection rules are therefore necessary for selecting a routing policy. Because the large-scale heterogeneous network environment is so complex, a learning mechanism should be adopted to construct and update the selection rules. Reasoning and learning belong to machine learning, and the reasoning and learning entity uses context information and policy selection results as inputs.

Benedetto<sup>[7]</sup> has proposed a cognitive solution to routing policy update in Ultra Wideband (UWB) networks, providing a route update mechanism based on reinforcement learning. Thomas has designed a cross-layer routing update solution based on game theory. But whether the decision-making tree and Bayesian reasoning (and their associated learning algorithms) are applicable to cognitive networks needs further study. For the design of the reasoning and learning mechanism, the following theoretical and technical problems<sup>[8]</sup> need to be solved:

- The convergence rate of the reasoning and learning algorithm should be faster than the change in context.
- Coordination in the distributed reasoning and learning algorithm.
- Design of routing performance evaluation functions.

## 4 Conclusions

With expansion of the network scale, network configuration cannot be optimized manually. The coexistence of heterogeneous networks also brings about a more complicated networks environment. Cognitive technology provides a way of configuring networks dynamically, and of optimizing the usage of link, network, and user resources. In this paper, a cognitive routing scheme for heterogeneous networks has been proposed. This scheme involves a routing algorithm frame composed of a situation awareness entity, route manager entity, route reconfiguration entity, and reasoning and learning entity.

## References

- [1] MITOLA J, MAGUIRE G Q. Cognitive Radio: Making Software Radios More Personal [J]. IEEE Personal Communications, 1999, 6(4): 13–18.
- [2] GELENBE E, XU Z, SEREF E. Cognitive Packet Networks [C]// Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'99), Nov 8–10, 1999, Chicago, IL, USA. Los Alamitos, CA, USA: IEEE Computer Society, 1999: 47–54.
- [3] CLARK D D, PARTRIGE C, RAMMING J C, et al. A Knowledge Plane for the Internet [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM'03), Aug 25–29, 2003, Karlsruhe, Germany. New York, NY, USA: ACM, 2003: 25–29.
- [4] THOMAS R W. Cognitive Networks [D]. Blacksburg, VA, USA: Virginia Polytechnic and State University, 2007.
- [5] IEEE Std 1900.1–2008. IEEE Standard for

Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks [S]. 2009.

- [6] SHI Y, HOU Y T. A Distributed Optimization Algorithm for Multi-hop Cognitive Radio Networks [C]// Proceedings of 27th IEEE Conference on Computer Communications (INFOCOM'08), Apr 13–18, 2008, Phoenix, AZ, USA. Piscataway, NJ, USA: IEEE, 2008: 1292–1300.
- [7] DI BENEDETTO M G, De NARDIS L. Cognitive Routing Models in UWB Networks [C]// Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom'08), May 15–17, 2008, Singapore. Piscataway, NJ, USA: IEEE, 2008: 1–6.
- [8] JEE Minsoo, YE Xiaohui, MARCONETT D, et al.. Autonomous Network Management Using Cooperative Learning for Network-wide Load Balancing in Heterogeneous Networks [C]// Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'07), Nov 30–Dec 4, 2008, New Orleans, LA, USA. Piscataway, NJ, USA: IEEE, 2008: 2547–2551.

## Biographies

### Li Hongyan



Dr. Li Hongyan is a professor at Xidian University. Her research interests include cognitive networks, Ad-hoc networks, and heterogeneous network integration. She has published over 20 papers.

### Li Jiandong



Li Jiandong is a professor and doctoral advisor at Xidian University. He is also a fellow of the China Institute of Communications, IEEE senior member, senior member of the Chinese Institute of Electronics, and a Cheung Kong Scholar professor. His research interests include mobile communications,

personal communications, cognitive networks, software defined radio, Ad-hoc networks, and broadband wireless IP technology.

### Hou Ronghui



Hou Ronghui is associate professor at Xidian University. She has worked as a post-doctoral fellow at the Department of Electrical and Electronic Engineering of the University of Hong Kong between 2007 and 2009. Her research interests include network quality of service issues, routing algorithm design, and wireless cognitive networks.

# Impacts of GPS Synchronization Loss on TD-SCDMA Network Performance

*Ji Shuping, Liu Zhijian, Dong Hui*

(ZTE Corporation, Shenzhen, 518004, P. R. China)

## Abstract:

In Time Division Synchronous Code Division Multiple Access (TD-SCDMA) systems, the Global Positioning System (GPS) signal is often blocked or experiences interference. As a result, the GPS satellite cannot be found and synchronization cannot occur. Long out-of-sync periods can lead to timing differences between base stations, and if these differences are too large, they can affect the ability of Mobile Stations (MS) to search neighboring cells. This can also affect cell switchover, and cause Downlink Pilot Time Slot (DwPTS) to interfere with Uplink Pilot Time Slot (UpPTS). All these manifest as handover failures, call dropouts during handover, and a declining rate of call completion. As a consequence, user experience within the network is diminished. Researchers have found that when GPS synchronization is lost for more than 4 chips, network quality deteriorates noticeably. When the loss is more than 10 chips, the MS may fail to locate a neighboring cell. When the loss is below 16 chips, the interference of DwPTS with UpPTS is not obvious in the first and second circles of the GPS out-of-sync cells. Studies show that, to protect network performance, the TD-SCDMA system allows for up to 4 chips of timing difference in the case of GPS synchronization loss.

Of the three 3G standards, CDMA2000 and Time Division Synchronous Code Division Multiple Access (TD-SCDMA) are both systems with synchronized base stations. The TD-SCDMA system is synchronized on a network-wide basis, and requires that all base stations be strictly synchronous. Handover and roaming functions between cells also require precise timing control. Synchronization is therefore a significant issue in TD-SCDMA communication systems. However, due to the lack of advanced

network synchronization technology, TD-SCDMA base stations employ Global Positioning System (GPS) for synchronization purposes<sup>[1-14]</sup>. In current TD-SCDMA networks, base stations sometimes fail to catch GPS satellite signals and lose synchronization for the following reasons:

(1) GPS signals experience interference from external signals

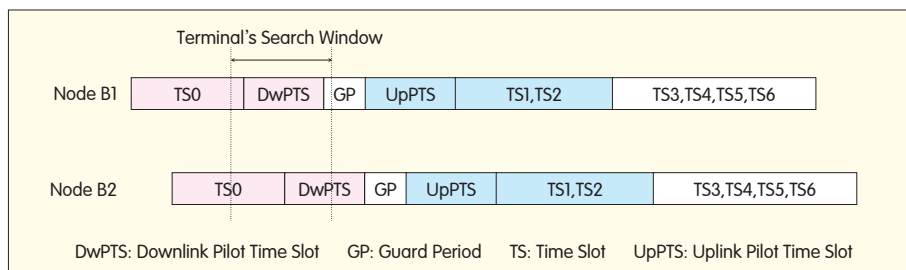
The working frequency of GPS is 1,575 MHz. The GPS signal, once transmitted from satellite to the ground, becomes very weak and is susceptible to outside interference. There are many

factors that cause interference with a GPS signal; for example, interference from solar flares, interference from the ionized stratum and aerosphere environment, and interference from irregular weather conditions (such as lightning and thunderstorms). When interference occurs, the quality of the signals being received from the satellite is degraded—the Signal-to-Noise Rate (SNR) falls and the Bit Error Rate (BER) increases. There can even be cases where satellite signals cannot be received at all.

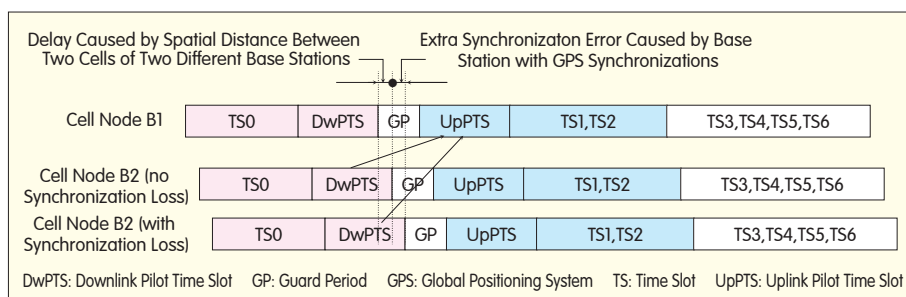
(2) Engineering construction

When a large number of sites are being set up, if the GPS antennas are installed where there are nearby obstacles, or if the quality of construction is less than perfect, problems such as high feeder impedance, feeder connector problems and water in the feeder cable can cause the received GPS signals to be quite weak. If synchronization is lost for an extended period of time, timing difference will occur between base stations. If this difference is too large, the Mobile Stations (MS) have problems searching neighboring cells, cell switchover is affected, Downlink Pilot Time Slot (DwPTS) interferes with Uplink Pilot Time Slot (UpPTS), and service timeslots overlap each other. All these problems affect network quality, giving rise to handover failures, call dropouts during handover, and a decline in call completion rates. As a consequence, user experience in the network is diminished. By testing how the timing difference between base stations (caused by synchronization loss) affects network performance, this paper concludes upon the degree of the





▲ Figure 1. Impact of GPS synchronization loss on neighboring cell measurement (or neighboring cell search).



▲ Figure 2. Schematic diagram of DwPTS interference with UpPTS due to lost GPS synchronization.

timing difference that a TD-SCDMA system can tolerate. Thus, it serves as a reference when considering alternative GPS synchronization schemes.

## 1 Theoretical Analysis

GPS synchronization loss causes significant differences in GPS timing between base stations. From the perspective of TD-SCDMA frame structure, and the work mode of User End (UE) and system, it can be seen that synchronization loss impacts the system in three ways:

(1) Neighboring cell measurement (or neighboring cell search) during handover and cell reselection

The UE normally searches for neighboring cell DwPTS using the timing of the current cell DwPTS as a benchmark. If the timing difference with neighboring cells is too large, the UE will not search for the neighboring cell DwPTS in the DwPTS search window. Even if it can search for the neighboring cell, the Primary Common Control Physical Channel (PCCPCH) of the neighboring cell will have low-quality signals and low Signal-to-Interference Ratio (SIR). This will negatively effect the network's Key Performance Index (KPI), resulting in the UE reselection

and handover problems. Figure 1 shows the impact of GPS synchronization loss on neighboring cell measurement.

Because the relay handover in the TD-SCDMA system cuts short the UE UpPTS access process, it speeds up the handover process and brings about a higher handover success rate. However, this requires strict synchronization between the base stations. Once GPS synchronization is lost between base stations, and the UE fails to synchronize on the dedicated channel, the handover will fail. The UE sends special burst data on the dedicated channel, and the base station receives the data and gives confirmation. This process represents a successful uplink synchronization. When the base station sends special burst data and the UE receives it, successful downlink synchronization has occurred.

(2) Interference of DwPTS with UpPTS  
As shown in Figure 2, to avoid DwPTS interfering with UpPTS between cells, the TD-SCDMA system has a 96-chip Guard Period (GP) timeslot between the two timeslots. In the event GPS synchronization is lost, the valid GP time between DwPTS and UpPTS becomes shorter.

An increase in UpPTS interference leads to a shrinking of UpPTS coverage, and this affects user uplink access at a cell's border. (In a TD-SCDMA system, the circuit-switched domain 64k visible telephone service (CS64k) has the smallest coverage, and therefore the coverage of UpPTS traffic channel should be at least the same as that of CS64k.) In a real network, however, because a very small proportion of the area has PCCPCH Received Signal Code Power (RSCP) of less than -95 dBm, the influence on call completion rate is relatively low.

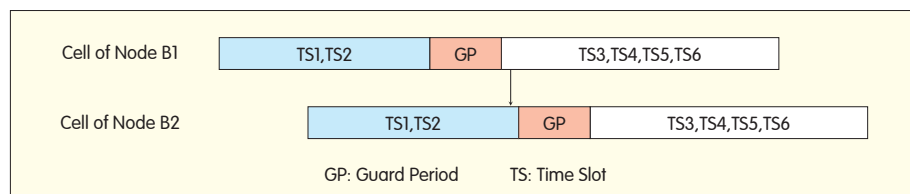
(3) Cross interference of service time slot

A 16-chip GP exists at the end of every time slot in the TD-CDMA system for uplink and downlink conversion, as shown in Figure 3. However, if the timing difference between cells is too great, cross interference of service time slots between cells will occur.

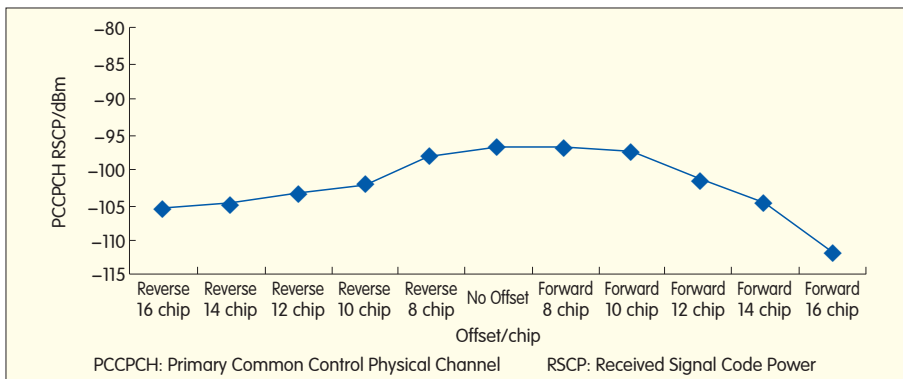
In the TD-SCDMA system, every service timeslot is 864 chips long. Therefore, cross interference caused by GPS synchronization loss affects some chips of the service timeslot. Obvious interference only occurs when GPS synchronization is lost to a large extent.

## 2 Test and Verification

To study the impact of GPS synchronization loss on network performance in a quantitative way, a



▲ Figure 3. Schematic diagram of cross interference of service time slot due to GPS synchronization loss.



▲ Figure 4. Changes of neighbor cell PCCPCH\_RSCP after GPS synchronization has been lost.

verification test in a real network environment is performed.

#### (1) Selection of Test Environment

A high site in a real network should be selected. Base station software for simulating GPS synchronization loss is then uploaded. This software can control and modify the timing difference caused by synchronization loss. The test conditions should also provide for one or two circles of base stations working with normal GPS synchronization, and with coverage extending to between 30 and 40 adjacent cells.

#### (2) Selection of Test Terminal

The Drive Test (DT) software is Pilot Navigator. The DT terminals are: two ZTE U85s, and one Datang 8120, which supports video phone.

#### (3) Simulation Uploading

Simulation uploading to the cell: 75% simulation uploading; that is, uploading 75% code channel to a single timeslot with power of 27 dBm.

#### (4) Design of Test Examples

In total, eight test examples are designed.

#### (a) GPS timing forward difference of base stations

- Testing the ability of base station cells to search for neighboring cells when GPS synchronization has been lost.
- Testing UpPTS interference changes for base station cells when GPS synchronization has been lost.
- Testing service timeslot interference of cells that neighbor base station cells when GPS synchronization has been lost.
- Testing network performance KPI.

#### (b) GPS timing backward difference of base stations

- Testing the ability of base station cells to search for neighboring cells when GPS synchronization has been lost.
- Testing UpPTS interference changes for cells that neighbor base station cells when GPS synchronization has been lost.
- Testing service timeslot interference for base station cells when GPS synchronization has been lost.
- Testing network performance KPI.

## 3 Analysis of Test Results

### 3.1 Test Data of Base Station Ability

This analysis is concerned with neighboring cell search tests, and UpPTS interference changes for base station cells when GPS synchronization has been lost. A test point with PCCPCH\_RSCP ranging from  $-65$  to  $-75$  dBm should be selected from the base station cells where GPS synchronization has been lost. A neighboring cell also needs to be selected for observation. Start the on/off function of the DT terminal five times and wait 2 mins every time it is on. Observe value changes of the neighboring cell's PCCPCH\_RSCP measured by the DT terminal, and then obtain the average value. The test results are shown in Figure 4.

(1) The neighboring cell's PCCPCH\_RSCP tends to shrink as the offset value grows, indicating an error made by the terminal in measuring the signal strength of the neighboring cell.

This error will grow in proportion to the offset value.

(2) When the GPS forward offset is 12 chips or less, and the reverse offset is 10 chips or less, the neighboring cell's PCCPCH\_RSCP value changes by around 3dB compared with the value when there is no offset. Considering fluctuation of radio signals, such change is normal.

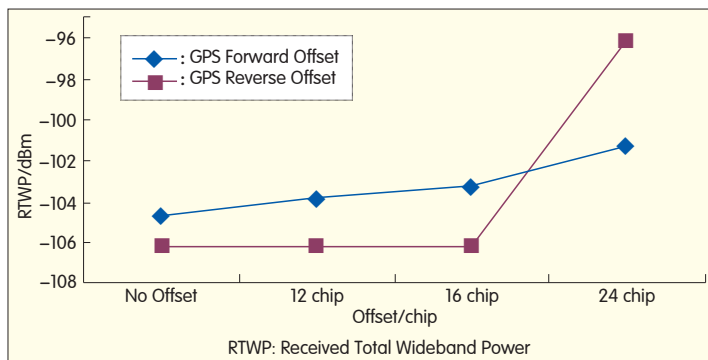
(3) Tests show that for the terminal not to be affected when searching for neighboring cells, the GPS forward offset must be 12 chips or less and the reverse offset 10 chips or less. That is, 10 chips is the upper limit for synchronization loss of GPS base stations before the terminal's ability to search for neighboring cells is affected.

### 3.2 Test Data of UpPTS Interference Changes

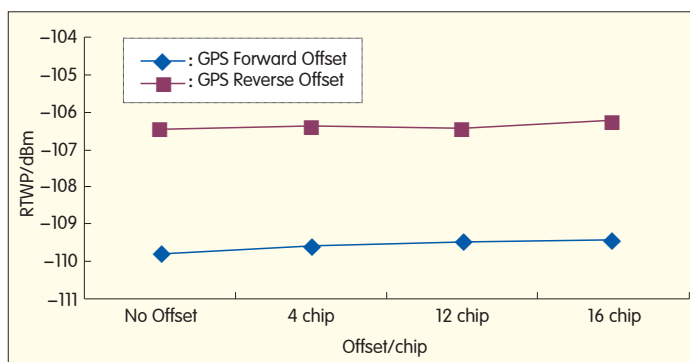
This analysis is concerned with UpPTS interference change for both base station cells and neighboring cells when GPS synchronization has been lost. When the forward offset of a base station with GPS synchronization loss is out of step, the DwPTS of base station cells other than those with the GPS synchronization loss interfere with the UpPTS of the base station with the GPS synchronization loss. When the reverse offset of a base station with GPS synchronization loss is out of step, the DwPTS of base station cells with synchronization loss interfere with the UpPTS of base stations other than those with GPS synchronization loss. This interference relationship is shown in Figure 5.

To ensure the UpPTS timeslot has the same coverage as that of a CS64k service, the interference surplus of UpPTS is 3 dB according to the link estimation. That is, when the UpPTS timeslot rise exceeds  $-103.3$  dBm ( $-103.3$  dBm =  $-106.3$  dBm + 3 dBm), the coverage of a UpPTS timeslot will become smaller than that of CS64k service. This is contrary to the TD-SCDMA network plan rules. From these tests, it can be concluded from that when the GPS offset is smaller than 16 chips, the UpPTS interference is below  $-103.3$  dBm, the offset exceeds 16 chips, and the interference grows

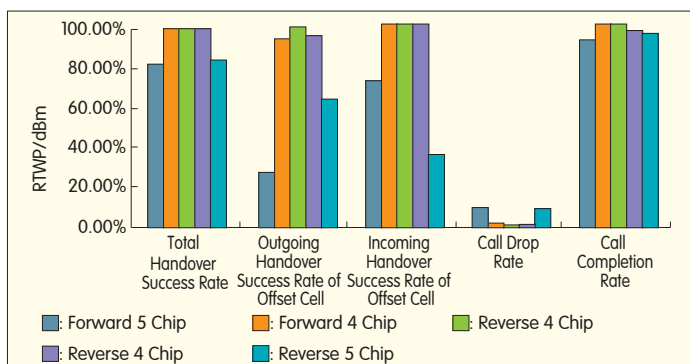
Ji Shuping, Liu Zhijian, Dong Hui



◀ Figure 5.  
RTWP changes of  
UpPTS time slot with  
interference after  
GPS synchronization  
is lost.



◀ Figure 6.  
RTWP changes of  
uplink time slot 2 with  
interference after GPS  
synchronization is lost.



◀ Figure 7.  
Network KPI after  
GPS synchronization  
is lost.

further. This is also contrary to the network plan rules. The tests show that 16 chips of GPS offset is the upper limit of interference that UpPTS can experience before the network plan rules are breached.

### 3.3 Test Data of Service Timeslot Interference

This analysis is concerned with service timeslot interference for both base station cells and neighboring cells when GPS synchronization has been lost. In this test, the service timeslot of the cells is configured as 2:4 (2 uplink timeslots are Timeslot 1 and Timeslot 2; 4 downlink timeslots are Timeslot 3, Timeslot 4, Timeslot 5, and Timeslot 6).

When the forward offset of a base station with GPS synchronization loss is out of step, downlink Timeslot 3 of base station cells with synchronization loss interferes with uplink Timeslot 2 of base station cells without GPS synchronization loss. When the reverse offset of a base station with GPS synchronization loss is out of step, downlink Timeslot 3 of base station cells without GPS synchronization loss interfere with uplink Timeslot 2 of the base station cells with GPS synchronization loss. In the test, 75% code channel is created for interference Timeslot 3, and 27 dBm power is uploaded to simulate the service traffic in a real network

environment. In these conditions, a dial test of service CS12.2k (circuit switched domain) is performed on the uplink Timeslot 2 with interference, and the RTWP value of uplink Timeslot 2 with interference is recorded. Figure 6 shows the value changes.

The test shows that the call completion rate of CS12.2k is 100%, and the RTWP of uplink Timeslot 2 with interference does not increase significantly.

### 3.4 Test Data of Network Performance KPI

This analysis is concerned with the network performance KPI. The network KPI test is carried out for the CS12.2k service in a real network. Test details are: two terminals (handsets); the CS12.2k call is held for 2 mins; the hang-up interval is 15 seconds; attempts to initiate calls is 50 times or more, and the attempts of handover is 100 times or more. Figure 7 shows the test result.

(1) As the GPS offset value increases, the handover success rate and call completion rate fall, and the call dropout rate rises. These all have negative effects on network KPI.

(2) The handover success rate is more than 98% when the GPS offset remains no more than 4 chips. This is necessary to keep the network KPI normal.

(3) When the GPS offset is more than 5 chips, the handover success rate and call completion rate fall, and the call dropout rate rises significantly.

(4) GPS offset drives down the terminal's reselection efficiency, and results in a decrease in call completion rate.

## 4 Conclusions

From the above tests, it can be concluded that:

(1) Compared with the terminal's neighboring cell measurement (search), UpPTS time slot interference, and service time slot cross interference, network KPI is most affected by GPS synchronization loss. The maximum allowable offset value for synchronization loss in a terminal's

neighboring cell measurement (search) is 10 chips (12 chips and 10 chips, the lower value is taken). The maximum allowable offset value for synchronization loss in UpPTS time slot interference is 16 chips. No rise in interference is found for service timeslot interference in the above conditions of synchronization loss. The maximum allowable offset value for synchronization loss in network KPI is 4 chips.

(2) 3GPP Specifications 25.123<sup>[15]</sup> state that a base station requires synchronization within 3  $\mu$ s. Tests show that 4 chips (3.125  $\mu$ s) is the maximum allowable value for inter base station synchronization loss. The test results are therefore consistent with these specifications.

(3) At present, synchronization of TD-SCDMA systems is totally dependent on the GPS of the United States. This can translate into security concerns. China's CDMA network has already broken down once due to a GPS authorization problem. For this reason, it is very important for TD-SCDMA to find an alternative synchronization system. This paper presents the precision requirements for any new synchronization scheme.

#### References

- [1] HOLMA H, TOSKALA A. HSDPA/HSUPA 技术与系统设计: 第三代移动通信系统宽带无线接入 [M]. 叶银法, 陆健贤, 周胜, 等译. 北京: 机械工业出版社, 2007.
- [2] HOLMA H, TOSKALA A. HSDPA/HSUPA for UMTS: High Speed Radio Access for Mobile Communications [M]. Translated by Ye Yinfa, Lu Jianxian, Zhou Sheng, et al. Beijing: China Machine Press, 2007.
- [3] 常永宇. TD-HSPA 移动通信技术 [M]. 北京: 人民邮电出版社, 2008.
- [4] CHANG Yongyu. TD-HSPA Technology for Mobile Communications [M]. Beijing: Posts and Telecommunications Press, 2008.
- [5] 彭木根, 王文博. TD-SCDMA 移动通信系统—增强和演进 [M]. 北京: 机械工业出版社, 2008.
- [6] PENG Mugen, WANG Wenbo. TD-SCDMA Mobile Communication System—Enhancement and Evolution [M]. Beijing: China Machine Press, 2008.
- [7] 彭木根, 王文博. TD-SCDMA 移动通信系统 [M]. 2 版. 北京: 机械工业出版社, 2007.
- [8] PENG Mugen, WANG Wenbo. TD-SCDMA Mobile Communication System—Enhancement and Evolution [M]. Edition 2. Beijing: China Machine Press, 2007.
- [9] 谢显中. TD-SCDMA 第三代移动通信系统技术与实现 [M]. 北京: 电子工业出版社, 2004.
- [10] XIE Xianzhong. Technology and Implementation of TD-SCDMA Mobile Communication System [M]. Beijing: Publishing House of Electronics Industry, 2004.
- [11] 李世鹤. TD-SCDMA 第三代移动通信系统标准 [M]. 北京: 人民邮电出版社, 2004.
- [12] LI Shihe. Standards for TD-SCDMA Mobile Communication System [M]. Beijing: Posts and Telecommunications Press, 2004.
- [13] 段玉宏, 夏国忠, 胡剑, 等. TD-SCDMA 无线网络设计与规划 [M]. 北京: 人民邮电出版社, 2007.
- [14] DUAN Yuhong, XIA Guozhong, HU Jian, et al. TD-SCDMA Wireless Network Design and Planning [M]. Beijing: Posts and Telecommunications Press, 2007.
- [15] 朱东照, 罗建迪, 汪丁鼎, 等. TD-SCDMA 无线网络规划设计与优化 [M]. 2 版. 北京: 人民邮电出版社, 2008.
- [16] ZHU Dongzhao, LUO Jiandi, WANG Dingding, et al. TD-SCDMA Wireless Network Planning and Optimization [M]. Edition 2. Beijing: Posts and Telecommunications Press, 2008.
- [17] 张传福, 彭灿, 李巧玲, 等. TD-SCDMA 通信网络规划与设计 [M]. 北京: 人民邮电出版社, 2009.
- [18] ZHANG Chuanfu, PENG Can, LI Qiaoling, et al. TD-SCDMA Communication Network Planning and Design [M]. Beijing: Posts and Telecommunications Press, 2009.
- [19] ZHU Jinkang. Wireless Mesh Technology and Network [J]. ZTE Communications, 2008, 6(2): 1–4.
- [20] WU Meng, JI Lina, WANG Kun. Key Technologies of Wireless Heterogeneous Network Security [J]. ZTE Communications, 2008, 6(3): 34–39.
- [21] 吕应权, 周冲. WCDMA 系统有效提高切换成功率的方法 [J]. 中兴通讯技术, 2008, 14(4): 56–60.
- [22] LÜ Yingquan, ZHOU Chong. A Valid Way to Improve the Success Ratio of Switching in WCDMA Systems [J]. ZTE Communications, 2008, 14(4): 56–60.
- [23] 糜正琨. 移动 IP 技术 [J]. 中兴通讯技术, 2008, 14(4): 59–62.
- [24] MI Zhengkun. Mobile IP technology [J]. ZTE Communications, 2008, 14(4): 59–62.
- [25] 阎凯力. 无线城市的运行模式 [J]. 中兴通讯技术, 2008, 14(6): 50–52.
- [26] KAN Kaili. Business Model of the Wireless City [J]. ZTE Communications, 2008, 14(6): 50–52.
- [27] 3GPP TS 25.123 V6.11.0. 3rd Generation Partnership Project: Technical Specification Group Radio Access Network: Requirements for Support of Radio Resource Management (TDD) (Release 4) [S]. 2007.

#### Biographies

##### Ji Shuping



Ji Shuping received his doctoral degree from Harbin Institute of Technology. He is a senior engineer at ZTE Corporation. His research interests include wireless technologies for TD-SCDMA system. He has published more than 30 papers, and has 3 patents.

##### Liu Zhijian



Liu Zhijian graduated from Dalian Institute of Light Industry. Working at ZTE Corporation, he is engaged in TD-SCDMA wireless system testing.

##### Dong Hui



Dong Hui graduated from Shanghai Polytechnic University. Working at ZTE Corporation, he is responsible for TD-SCDMA wireless system testing. He has published 5 papers, and has 5 patents.

#### Roundup

### ZTE Sells World's Fastest HSPA+ 28.8M Data Card with Greece's COSMOTE

ZTE Corporation announced on April 19, 2010 that it has started selling world's fastest HSPA+ 28.8M data card with COSMOTE in Greece, moving the industry forward with record speeds for mobile broadband services by using advanced HSPA+ MIMO technology.

COSMOTE became the first company in Greece to offer 28.8Mbit/s with its "COSMOTE Internet on the Go" data transfer package—the country's most popular mobile broadband offering. The new speeds are available through the updated ZTE MF662 data card.

By deploying advanced HSPA+ MIMO technology with the MF662, COSMOTE's customers can enjoy up to 28.8 Mbit/s download speed and 5.8 Mbit/s upload speed for easy access to the Internet, wherever and whenever they want.

(ZTE Corporation)



# Full-Service Operation and IMS Network Management

**Chen Jian, Wang Dezheng, Liu Wei**

(Network Management Product Department of ZTE Corporation, Nanjing 210012, P.R China)

## Abstract:

IP Multimedia Subsystems (IMS) is considered as a comprehensive approach for full-service operation. However, traditional network management concepts are not applicable to IMS network management. This is because IMS is characterized by a flat, all-IP architecture, simplified functionality of Network Elements (NE), and a variety of NEs. This paper introduces an IMS network management system design that covers full-service operation. It then discusses the significant role IMS network management plays in the unification of NE management layers, the increasing importance of end-to-end applications, and the convergence of Enhanced Telecom Operation Map (eTOM) and IT Infrastructure Library (ITIL).

multiple angles to provide insight into management of large scale network construction<sup>[1-4]</sup>.

## 2 IMS Networks Require Unified NE Management

Telecom equipment management suppliers provide Operation and Maintenance Centers (OMC) according to the network type and NE type. Although it is simple for equipment vendors to configure network management according to NE types, operators have to set multiple OMC Network Management Systems (NMS) for only one network. This not only increases operators' hardware investment in network management servers and client-end PCs, but also requires more device space and heavier workload on operation and maintenance personnel. In addition, the management interfaces of OMCs differ from each other, which increases training costs for users and leads to complaints from O&M personnel. Therefore, operators seek to reduce the number of network management servers. Devices from the same supplier should be managed by one central OMC to lower investment and maintenance costs. For terminals and access devices, the management modes, device features, and required quantity are different from that of the core control layer. Therefore, operators with large-scale commercial networks usually set an independent OMC for the management of terminals and access devices.

The architecture of OMC/Element Management Systems (EMS) in IMS is shown in Figure 1. The Element Management Layers (EML) of NEs in different areas are managed by different OMCs/EMSs. In the IMS

## 1 Background of IMS in Full-Service Operation

All three Chinese telecom operators have obtained qualifications for full-service operation. Therefore, they need to carefully consider the technologies used to implement full-service operations, and the appropriate solutions for improving their weaknesses.

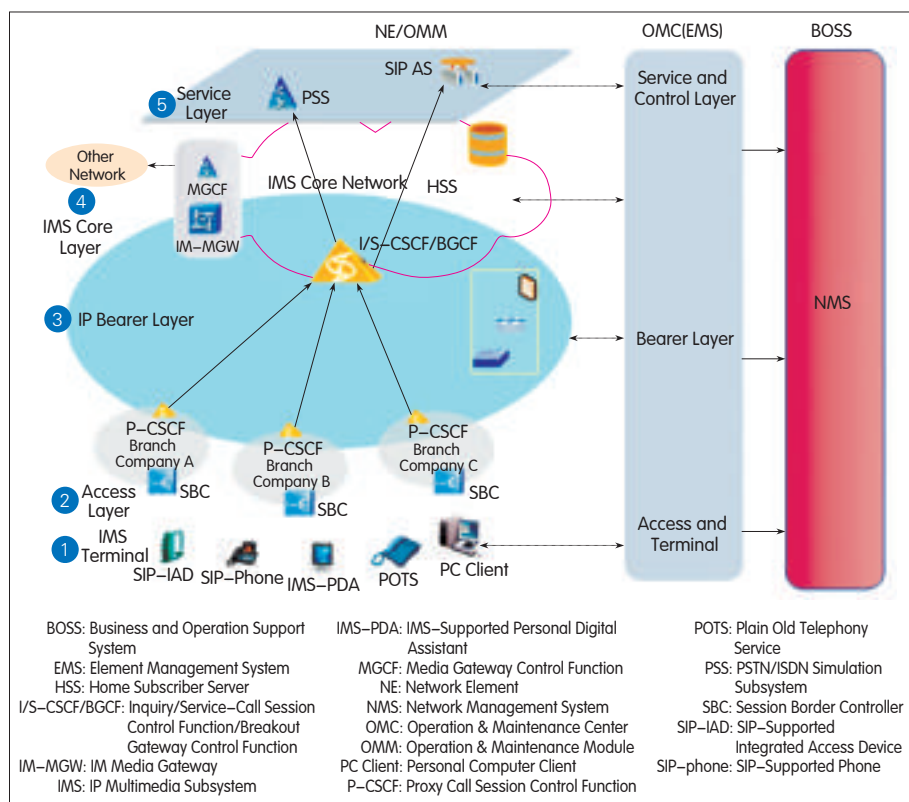
Prior to 2009, Chinese operators such as China Telecom and China Mobile invited many IP Multimedia Subsystem (IMS) vendors to test and validate the basic functions of IMS. An all-IP-based IMS network makes full use of multiple access modes of mobile and fixed line networks. It can also provide new services, which are attractive to operators. Since 2009, in the era of full-service operation, original mobile and fixed network

operators have incorporated the construction of IMS networks into their development plans.

With the trend towards mobile and fixed convergence, equipment vendors in the field of network management have begun to consider the implementation of unified network management to meet market demands for easier operation, maintenance and management.

It has become necessary to devise a management concept for the IMS network in the full-service operation mode, and to construct a management network that meets the requirements of telecommunication operation. Only after the sticking points of IMS network management are removed, can successful large-scale network construction be achieved.

In this paper, IMS serves as one of the approaches to full-service operation. Management of full-service IMS networks is also discussed from



▲ Figure 1. Architecture of OMC/EMS in IMS.

network, the unified OMC/EMS is maintained by the same maintenance personnel. This overcomes the isolation of NEs in different areas. For a unified OMC/EMS, the following features are required:

(1) The interface style must be uniform, and different NEs should use the same management style in the IMS NMS. The uniformity of the interface style lowers the cost of training personnel in IMS operation and maintenance, and can improve operational efficiency.

(2) The IMS network is an organic whole. Tracing and managing network quality and alarms is necessary, and unified reporting is a must for IMS network management.

(3) The IMS network accesses the upper-level Business Operations Support System (BOSS) system as a whole network. The unified northbound interface reduces the work load of the interconnection and thus decreases the possibility of failure.

In short, the IMS NMS should enhance report management,

northbound interface and unification of interface styles, as well as providing traditional functions such as performance management, alarm management, configuration management and security management.

### 3 End-to-End Application is a Precondition for Large-Scale Commercial IMS

The all-IP architecture of IMS brings about a flat network, intensive function division, and an increase in NE types. Delivery of one subscriber service requires passing through many NEs. Moreover, it may be necessary to pass through one NE many times for one service, creating a Session Initiation Protocol (SIP) link. In addition, there are many types of IMS services, and service logic is complicated and highly associated. Management and interconnection also require intensive effort.

The features of an IMS network make

it difficult to locate service faults. The quality of end-to-end service is a precondition of telecommunication services. The area-based quality assurance method for traditional networks is not applicable to all-IP IMS with simple but varying NEs.

Therefore, when NE management is unified, a prerequisite for large-scale commercial IMS in full-service operation is to ensure end-to-end service quality by developing end-to-end applications and tools.

For example, when the quality of user call is poor, corresponding media analysis and quality tools must be provided for analyzing Real-Time Transport Protocol (RTP) communications for voice or video. This involves the automatic analysis of the process and details of the expected call. When the subscriber service fails, automatic cross-NE signaling analysis is required to trace the service processing, locate the fault, and determine the reason.

Therefore, the introduction of an IMS network significantly impacts the traditional telecommunications management system, and thus the development of end-to-end application analysis tools is necessary.

### 4 Security of IMS NMS

NMS security should be enhanced in an all-IP based network. In the IMS domain, the implementation of NMS security involves networking, operating system, database, OMC and anti-virus.

The following measures should be adopted to accomplish the desired security:

(1) A single network management domain should be implemented in the IMS domain.

(2) An independent Virtual Local Area Network (VLAN) should be established for network management.

(3) The outband networking mode should be used.

(4) The network management domain and devices should be physically isolated in the outband networking mode by setting a hardware firewall between networks.

(5) The Unix operating system should

be used and regularly updated.

(6) The minimum system configuration should be customized to restrict the breaches of system security.

(7) Security patches for the OMC database should be obtained and user rights should be controlled to lower the possibility of security risks.

The multiple-OMC system should use encrypted protocol such as Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) to transmit data. Sensitive data, such as username and password, should be encrypted before storage. Forcible password authentication is used. Both the working time and the hierarchical user rights are set, and the management scope is also defined according to the rights division and domain division.

## 5 IMS Accelerates Integration of eTOM and ITIL

The Information Technology Infrastructure Library (ITIL) was developed by the British Department of Commerce. It defines a framework for delivering best practice, high quality IT services. It is service orientated, and helps decision makers invest in specific parts of the IT infrastructure to maximize their yield on investment.

With service management as its core, and service strategy as its guide, ITIL creates a process framework that incorporates service design, conversion and operation. The introduction of "lifecycle" and continuous improvement of services results in best practice.

The Telecommunications Forum has put forward proposals that would construct a bridge between the enhanced Telecom Operations Map (eTOM) and ITIL, proposing a trend towards integration. IMS development is accelerating the integration of eTOM in the telecom field and ITIL in the IT field. Existing functions in the eTOM will become elements in the construction of the integration process. These functions offer service for the final business flow, and provide unified and standard services for end users.

With the introduction of IMS,

telecommunication hardware, including control-plane and service NEs but not gateways interconnected with traditional telecommunication systems, can use Advanced Telecommunications Computing Architecture (ATCA)-based blade servers or universal servers to implement their functions. The situation is changed whereby traditional telecommunications systems use a closed hardware platform for each supplier. The hardware devices approach current open platform IT devices. This accelerates the integration of the two concepts.

Operators have changed from being device-oriented to service-oriented and customer-oriented services. Currently, one operator provides hundred of types of services for end users. However, it is difficult for operators to manage, select and promote services. ITIL is constructed with the core concept of service. Operators and IT service providers are becoming more alike in their service concepts. This may eventually lead to the integration of eTOM and ITIL.

In the evolution process, integration and mutual complementation are progressive. eTOM establishes the commercial process framework for the entire telecommunication industry and also the global requirements. ITIL, on the other hand, provides a detailed service-oriented framework.

ITIL provides the methodology and process framework for IT service management. However, the actual telecommunication service processes should be analyzed and designed in detail. These designs will require the adjustment of operators' BOSS business flow to adapt to the service-oriented concept.

## 6 Conclusions

IMS applied in full-service operation is a new business. It poses a challenge to traditional network operation and management. More efforts are required to adapt the development of new network concepts for traditional operators and equipment vendors. It is clear that an all-IP based IMS network

would be used for full-service operation.

### References:

- [1] 邱雪松. 全业务运营环境下中国联通OSS规划建议[J]. 通信世界, 2009(22): 13-14.  
QIU Xuesong. Proposal of China Unicom OSS under full-service operation [J]. Communications World, 2009(22):13-14.
- [2] 孙明忠, 张建, 杨兆江. 网“稳”心“安”综合网管挑起运维托管重担[J]. 中兴通讯技术(简讯), 2009(7):14-15.  
SUN Mingzhong, ZHANG Jian, YANG Zhaojiang. Integrated network management plays a significant role in Operation and Trusteeship. ZTE Technologies [J], 2009(7): 14-15.
- [3] 李明春. 中国电信EV-DO 蓄势全业务运营[J]. 通信世界, 2008(44): 11-14.  
LI Mingchun. China Telecom's EV-DO concentrates on full-service operation [J]. Communications World, 2008(44): 11-14.
- [4] 张智江, 朱士钧, 肖征荣, 等. 基于IMS融合、开放的下一代网络[M]. 北京: 人民邮电出版社, 2007.  
ZHANG Zhijiang, ZHU Shijun, XIAO Zhengrong, et al. IMS-based integrated open next generation networks [M]. Beijing: Posts and Telecom Press, 2007.

### Biographies

#### Chen Jian



Chen Jian graduated from the South East University with a Master's degree. He is working as a director of the Network Management Product Department of ZTE Corporation. He worked as the General Manager of the CDMA Core Network Products. He has more than ten years of working experience in the telecommunication industry, and his current research interests include telecommunication network management, and CDMA mobile communications

#### Wang Dezheng



Wang Dezheng graduated from Zhejiang University with a Master's degree. He is working as a chief engineer at the Network Management Product Department of ZTE Corporation. His main research interests include cloud computing network management, and web technology applications in network management. He has published 3 papers.

#### Liu Wei



Liu Wei graduated from Wuhan University with a Master's degree. He is working as a chief engineer at IMS Network Management Planning of ZTE Corporation. His research interests include IMS Unified Network Management Planning and Solution, end-to-end signaling trace, and QoS management.

# Integrated Network Management System for CSL

**Yi Sa, Ma Zhiyong**

(Network Management Product Department of ZTE Corporation, Chengdu 610041, P. R. China)

## Abstract:

CSL is a subsidiary of Australia's Telstra Corporation and is the biggest mobile operator in Hong Kong. In March 2008, CSL contracted ZTE to evolve its existing mobile network into a new all-IP mobile network. To reduce the high Operating Expense (OPEX) of network operation and maintenance, CSL sought an Integrated Network Management System (INMS) to consolidate alarms from various network segments, and to improve network operation and maintenance efficiency. ZTE provided CSL with an integrated network solution based on Software Defined Radio (SDR) soft base stations. The SDR solution supports upgrade to High Speed Downlink Packet Access (HSDPA+) and enables a smooth transition to a Long Term Evolution (LTE) network.

**W**ith the rapid development of technology, telecom markets have grown in scale. Existing network equipment has become increasingly complex, and newly-introduced services have significantly increased the workload on such equipment. This raises the cost of network management and maintenance. It has therefore become imperative that operators monitor the state of network operation—to improve efficiency of network maintenance, to reduce costs, and to improve Quality of Service (QoS). They can do this by using an Integrated Network Management System (INMS).

INMS is a manager-of-managers on the Operations Support Systems (OSS) platform for fault management. It fulfills the following requirements:

(1) Functional Requirements

- Fault management
- Event acknowledgement/de-acknowledgement
- Severity change/non-change
- Troubleshooting tools
- Alarm notification to workflow system
- User roles
- Journal logging
- Alarm notification
- Other alarm management functions, such as alarm synchronization with Element Management Systems (EMS)
- (2) Integrational Requirements
  - Integration with Remedy Action Request System (ARS)
  - Alarm integration

## 1 CSL's Demands of INMS

CSL has 25 years' best network

operation experience. Its newly-built advanced network is an important asset that relies on scalable operation support systems for management. Efficient operational management is critically important to CSL. Both internal operation service level agreements and external customer-centred service level agreements depend on whether the OSS can effectively consolidate alarms from various network segments and provide meaningful, actionable messages.

Therefore, CSL required the ZTE-designed network to have a single domain Network Management System (NMS) which could manage alarms from the Core Network (CN), Radio Access Network (RAN), Value Added Services (VAS), Microwave, and Repeater.

## 2 ZTE's INMS Solution

ZTE's INMS solution delivers a platform that can aggregate, enrich, correlate, and consolidate information across various networks. Its architecture contains the following three layers:

(1) Alarm Collection Layer

Two probe types are used on this layer:

- A Simple Network Management Protocol (SNMP) Element Management System (EMS) probe that receives SNMP traps and performs SNMP operations (SNMP GET and SET) from EMSs in various network segments.
- An SNMP probe that receives SNMP traps from IP networking devices such as switches and routers.

Both probe types support Peer-to-Peer (P2P) failover functionality. They run simultaneously; one acts as the master probe, sending events to the upper layer ObjectServer (a Netcool module), while the other acts as a slave probe on standby. If the master fails, the slave will be activated. Although the slave receives heartbeats from the master, it does not forward events to the ObjectServer. If the master shuts down, the slave probe stops receiving heartbeats, and any events it receives thereafter are forwarded to the ObjectServer on behalf of the master. When the master



is running again, the slave continues to receive events, but no longer sends them to the ObjectServer.

### (2) Consolidation Layer

The collected alarms are forwarded to the ObjectServer for consolidation, and there they perform various event processing functions (including de-duplication and kick starting other event processing workflows). Two event workflow types can be identified on this layer:

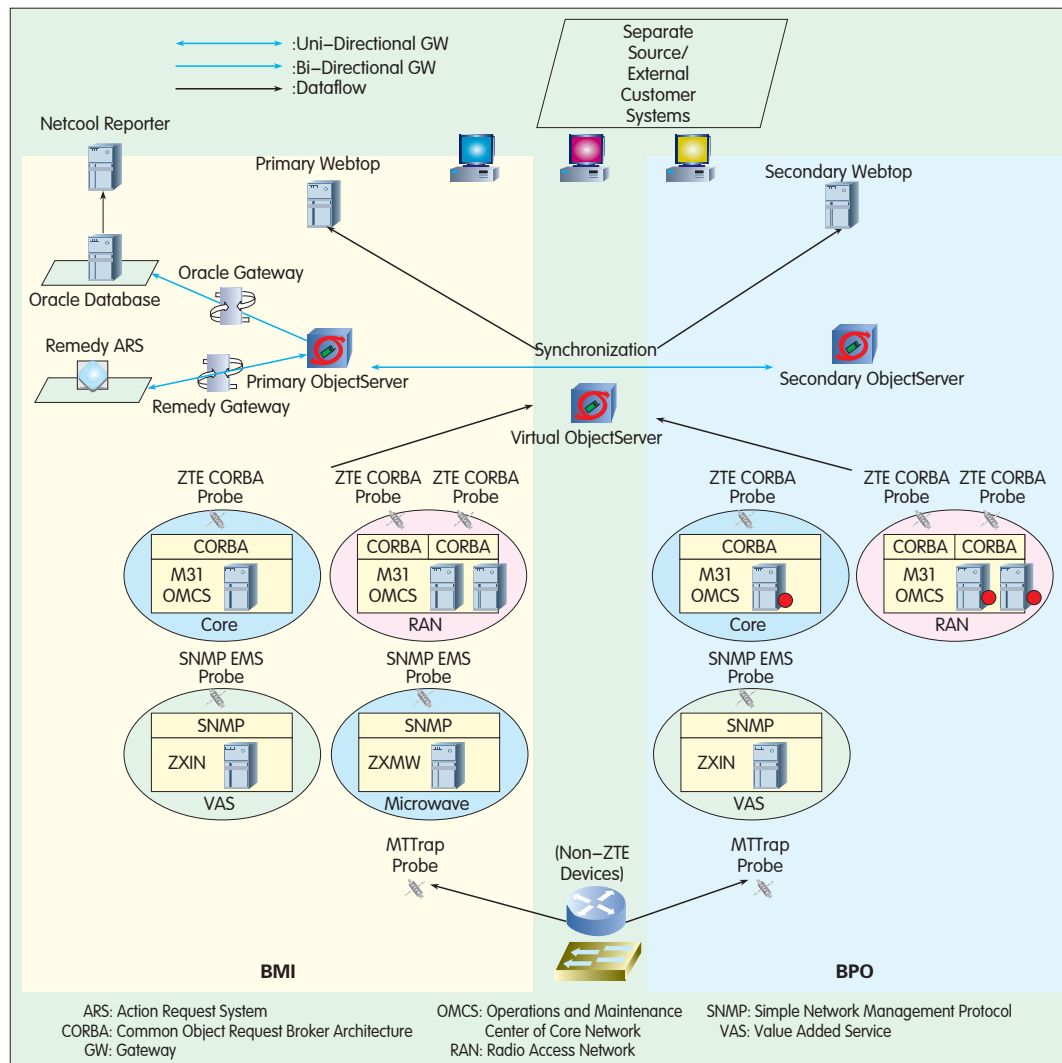
- Reporting workflow: received event data is forwarded via the Netcool Oracle gateway to an external commercial database, such as Oracle, for storage and reporting. Netcool Reporter is proposed as an event reporting tool for treating Oracle database as an event data source.

- Trouble ticketing workflow: event data is forwarded to a Trouble Ticket System, such as Remedy Help Desk, for creating trouble tickets. Remedy Gateway is proposed for the bidirectional exchange of information.

In order to fulfill the requirement on redundancy, a secondary ObjectServer is proposed to synchronize events from the primary ObjectServer. The alarm collection probes can be configured to send alarms to an ObjectServer regardless of which ObjectServer is active. A bidirectional ObjectServer gateway performs the described synchronization.

### (3) Presentation Layer

The collected and processed events are grouped, filtered, and presented in operationally meaningful ways. This is done using Webtop presentation tools such as filters, event lists, and maps. The Webtop server is configured to access both primary and secondary ObjectServers.



▲ Figure 1. Architecture of ZTE's INMS.

ZTE's INMS is built on IBM Netcool platform for offering network availability management. Figure 1 illustrates the overall architecture of ZTE INMS, which is fully redundant above the ObjectServer (or data aggregation collection) level. The core of its design lies in two Netcool ObjectServers, one of which is the primary server residing on the site BMI, the other is the secondary server on the site BPO. Similarly, there are two sets of Netcool probes and two Netcool/Webtop servers which reside on the BMI and BPO respectively. Events flow from the probe boxes into the virtual ObjectServer (or logical ObjectServer), and probes enrich the contents based on rule files. A bidirectional object

server gateway keeps the synchronization of events in the two object servers, supporting warm backup. All events are archived in an Oracle database using a high-speed Oracle gateway. The data in the Oracle database can be queried by Netcool/Reporter with historical reporting capabilities.

This solution integrates five types of EMS: core EMS, RAN EMS, VAS EMS, Microwave EMS, and Repeater EMS. Core and RAN EMS alarms are integrated by a ZTE Netcool Common Object Request Broker Architecture (CORBA) probe, and power and environment alarms are transmitted to Netcool/Omnibus through ZTE RAN EMS. ZTE VAS EMS, Microwave EMS,

and Repeater EMS alarms are integrated by a ZTE SNMP EMS probe. Other IT equipment is managed by Mtrtrap probe. These various EMS and IT equipment alarms are handled by relevant probes and transported to Netcool/Omnibus. The automations in Netcool/Omnibus correlate the alarms.

To streamline problem management and notification processes, a Remedy gateway creates trouble tickets, and an object server automatically pages administrative personnel.

Based on CSL's requirements, ZTE's solution provides the following major functions:

- ZTE EMS alarm integration: ZTE EMS alarms are managed through CORBA and SNMP interfaces.
- IT device alarm integration: SNMP trap enabled IT equipment is managed through MTTTrap interfaces.
- Reports: reports for CSL are created using NetNumen™ Netcool/Reporter.
- Webtop logical view: webtop monitoring views are delivered to CSL using Netcool/Webtop.
- HelpDesk integration: the Remedy gateway is used to transport Netcool/Omnibus alarms to CSL Remedy ARS helpdesk.
- Netcool/Omnibus Failover function: Netcool/Omnibus Failover is built through the Netcool/Bi-Gateway.
- Migration of five existing subsystems to the new INMS platform.

### 3 NetNumen™ Netcool Portfolio

The NetNumen™ Netcool portfolio performs real-time management and allows complex enterprise environments to be visible. The main components are:

#### (1) Netcool/Webtop

Netcool/Webtop combines Netcool's real-time fault management and service assurance capabilities with the convenience of the Internet. Authorized users can access the IT systems and services in real time, and through any browser.

Netcool/Webtop delivers graphical maps, tables, and event lists in HTML and Java to the remote operator.

Netcool users can manage alerts through flexible interfaces and advanced management capabilities.

The Netcool/Webtop application extends Netcool/Omnibus capabilities by adding a new set of graphical views and flexible management functions.

#### (2) Netcool/Omnibus

Netcool/Omnibus was specifically designed for IT service providers such as telecom operators, banks, entertainment service providers, Internet service providers, cable TV operators, and corporate enterprises.

Netcool/ObjectServer is the core component of the Netcool/Omnibus application. It is a high-speed memory-resident database that collects fault information from the network infrastructure and allows operators to see relationships between faults and the availability of network-based business services.

Netcool/Omnibus acquires fault data and status data from a variety of network devices and management environments including servers, mainframes, NT systems, UNIX applications, circuit switches, voice switches, IP routers, SNMP devices, and network management applications and frameworks. The fundamental collectors of data are lightweight code supersets called NetNumen™ Netcool Probes & Monitor. These collect fault messages from throughout the network and forward them to Netcool/ ObjectServer for filtering.

Besides capturing host names and IP addresses, Netcool/Omnibus can easily accommodate other meaningful attributes in order to enrich network events and faults. This allows events to be managed not only from a network perspective but also from a business and operational perspective.

Netcool/Omnibus can be deployed quickly to achieve rapid return on investment. Its distributed architecture allows network operators to customize real-time views of whole



enterprise-wide services. Based on an open client-server architecture, the Netcool suite runs with UNIX, Windows NT, and Web browsers.

In the Netcool/Omnibus application, both SNMP and non-SNMP management systems become strategic management elements. Netcool/Omnibus is commonly used as the core management desktop since it consolidates data from network management consoles, transmission infrastructure, telephony devices, data networks, Local Area Networks (LANs), Wide Area Networks (WANs), and applications.

Netcool/Omnibus consists of the following elements:

- ObjectServer: an in-memory database optimized for collecting events and designing filters and views. It provides the core processing functions for the Netcool suite.
- Probes: passive supersets of code that collect event data from more than 300 management data sources. Collected data is filtered, stored, viewed, and manipulated in the ObjectServer.
- Desktops: a suite of graphical operator tools running under X Windows, Windows NT, or Java, which provide the front end for customizing filters and service views.
- Console: the object-based screen interface that shows the status of enterprise-wide services. It uses color-coded histograms or "lava lamps" which represent a summary of event severity within each service.
- EventLists: spreadsheet-like interfaces into NetNumen™ Netcool/ObjectServer event data that

Yi Sa, Ma Zhiyong

show events color-coded according to severity. This allows access to useful information for troubleshooting each event.

- FilterBuilder: a desktop interface based on Boolean correlation tools that allows operators to associate collected event data with the availability of business services.
- ViewBuilder: point-and-click desktop equipment that allows operators to design personalized views of events and services, supporting customization of service views and EventLists.
- Gateways: bidirectional interfaces that allow ZTE Netcool/ObjectServer data to be shared with other ObjectServers, Relational Database Management System (RDBMS) archives (such as Oracle, Sybase, Informix), or trouble-ticketing applications (such as Remedy AR System™, Peregrine Service Center™, Clarify ClearSupport™, and ODBC).

## 4 Conclusions

ZTE's NetNumen™ INMS provides a

solid, modular, distributed architecture, and an open development environment. It fulfills the required off-the-shelf integrated network management. It can be easily integrated with multiple third-party systems. ZTE's INMS is designed according to the principle of 'bottom to top'. It is characterized by its high user-orientation, telecom-level and multi-platforms. It can manage multiple network elements quickly, flexibly, conveniently, and economically according to actual needs. This provides operators with various social and economic benefits. Moreover, it has flexible scalability, which enables smooth upgrade and minimal impact on the existing system when expanding system capacity or adding new network devices.

In the CSL project, ZTE's INMS aggregates alarms from different domains and provides unified visualization and presentation for operators. With centralized management of topology, faults and reports, INMS can monitor the running status of overall networks in real-time and on a single console. In this way,

CAPEX and OPEX can be reduced.

## Biographies

Yi Sa



Yi Sa received her Master's degree from Sichuan University, China. She is a solutions manager in the Network Management Product Department of ZTE Corporation. She is engaged in researching Operation Support System (OSS) technology, especially the Integrated Network Management System (INMS). She was responsible for the INMS solution in the CSL project.

Ma Zhiyong



Ma Zhiyong received his Master's degree from University of Electronic Sciences and Technology of China. He is the marketing director of Network Management Product Department of ZTE Corporation. He is engaged in researching Operational Support System (OSS) technology, especially the Integrated Network Management System (INMS).

## Roundup

### ZTE and Innofidei Achieve Industry's First Field IOT on Multiple TD-LTE USB Dongles in a Mobile Network Cell

ZTE Corporation, a leading global provider of telecommunications equipment and networking solutions, announced on May 11, 2010 that ZTE Corporation and Innofidei have jointly delivered a significant breakthrough for the Time Division Long Term Evolution (TD-LTE) industry with the industry's first successful Inter-Operability Test (IOT) of multiple TD-LTE USB dongles in a single mobile network cell. The successful test was first performed in Hong Kong, and subsequently in Shanghai during the opening days of Shanghai World Expo. Using the ZTE TD-LTE Shanghai field network, a number of TD-LTE USB dongles provided by Innofidei accessed the field TD-LTE cell simultaneously to provide a

number of diversified services including streaming and FTP services, among others.

Innofidei Inc., China's largest mobile TV chip maker, has been actively promoting the development of the TD-LTE industry and in 2007 began its TD-LTE baseband project in partnership with the Hong Kong Applied Science and Technology Research Institute Company Limited (ASTRI). In recognition of its industry leadership, Innofidei won the bid to provide 4G TD-LTE data cards as part of the Shanghai World Expo TD-LTE terminal project in early 2010. In April this year, Innofidei and ASTRI released the first TD-LTE baseband chip for the 20MHz TD-LTE bandwidth, which is also in use at

Shanghai World Expo.

ZTE Corporation has been leading the Time Division Duplex (TDD) industry through strong innovation and product development capability, and continues to invest in the industry to maintain this lead. ZTE Corporation is the first Chinese telecoms equipment provider to pass TD-LTE indoor phase I test, field test and indoor phase II test organized by the Ministry of Industry and Information Technology of the People's Republic of China (MIIT) and China Mobile. ZTE Corporation has deployed five commercial LTE networks to date, and more than 40 trial LTE networks with operators throughout Europe, North America, Asia and the Middle East.

(ZTE Corporation)

# Using OBSAI to Build the Baseband–RF Interface of Multi–Mode Base Stations

**Mao Ming**

(ZTE Corporation, Shenzhen 518004, P. R. China)

## Abstract:

The unique frame structure of Open Base Station Architecture Initiative (OBSAI) is well–suited to transmitting data of different wireless standards. In a multi–mode base station built with OBSAI, the baseband–RF interface can effectively screen out the influence of different wireless standards over the data transport link. It can also support multiple wireless standards on a single hardware platform. With such an interface, the Baseband Unit (BBU) and Remote RF Unit (RF) need only be changed to support a new wireless standard, and as long as the rate of the optical interface remains the same, no software, hardware, or logic of other units needs modification.

Originally, 3G standards included Wideband Code Division Multiple Access (WCDMA), CDMA2000, and Time Division Synchronous Code Division Multiple Access (TD–SCDMA). A fourth, Worldwide Interoperability for Microwave Access (WiMAX), appeared in 2007. Together with 2G standards and the Long Term Evolution (LTE) standard, a total of seven wireless standards currently exist in the telecommunications industry. This places a burden on equipment vendors. If standards can be integrated on one hardware platform (the multi–mode base station), R&D and device expenditure of equipment vendors will be substantially reduced.

As its name implies, a multi–mode base station is able to support several different wireless standards. Because multi–mode base stations cut down hardware costs and make it easy for operators to launch new services, vendors are now developing them in the hope of winning an upper hand in future competition.

One of the problems in developing multi–mode base stations, however, is the baseband–RF interface. The interface is a data transport link between the BBU and RF, and contains auxiliary information—such as signaling and timing—that cannot be easily integrated for transmission. This is because the data format and rate varies from standard to standard.

The two most commonly used baseband–RF interface standards are the Common Public Radio Interface (CPRI) and the Open Base Station Architecture Interface (OBSAI). The frame structure and layered design of OBSAI is particularly suitable for simultaneous transmission of baseband data of different wireless standards.<sup>[1]</sup> Although CPRI also allows for such transmission, the individual data frames are too large and must be split into smaller blocks. Moreover, since the rate of baseband data and size of data blocks varies according to different wireless standards, CPRI cannot be easily applied. It is therefore necessary to use OBSAI as the standard for the baseband–RF interface in a multi–mode base station.

## 1 Brief Introduction of OBSAI Protocol

The OBSAI is a standardization organization established by Nokia, ZTE, LG, Hyundai, and Samsung. It aims to create a public interface between the BBU and RF so that devices of different vendors can be interconnected.

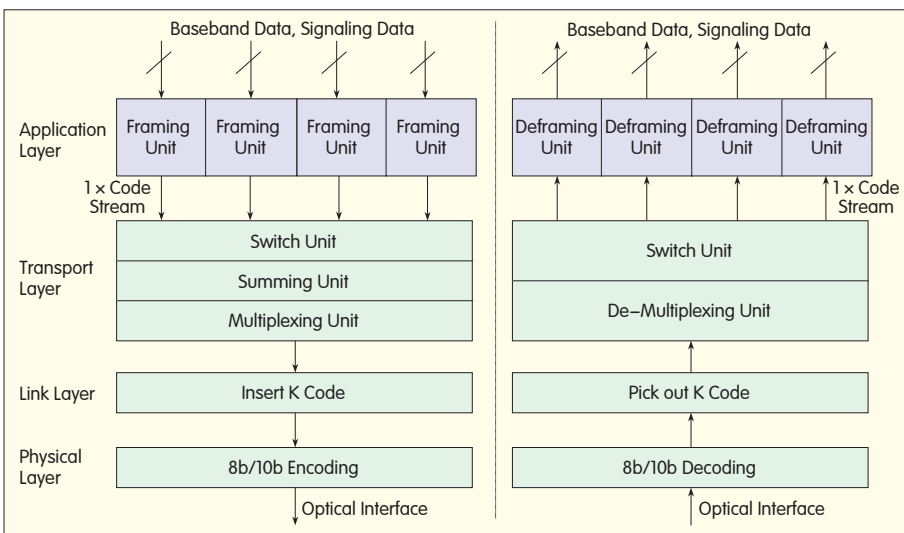
The minimum unit of the OBSAI standard is a message of 19 bytes, which includes the destination address, data type, time stamp, and payload. Table 1 details the length and meaning of each part of the message.

The OBSAI standard divides the baseband–RF interface into 4 layers from the top down: the application layer, transport layer, link layer, and physical layer. During transmission, the application layer inserts baseband data and signaling data into the message; the transport layer cross–connects, sums up, multiplexes, and combines the message data streams into one channel; the link layer inserts regular special code into the data stream for marking the good/bad status of the link; and the physical layer performs 8b/10b encoding and decoding, serial–to–parallel conversion, and serial transmission. During reception, this process is reversed. Every layer transmits data that it extracts to the upper layer, and finally the baseband data and signaling data are extracted.



▼ Table 1. Length and meaning of every part of an OBSAI standard message

Name	Length/bit	Meaning
Destination Address	13	Indicates which node the message will be sent to
Data Type	5	Indicates the payload type, wireless standard, signaling frame and control frame of the message
Time Stamp	6	Indicates the time when the message is sent out
Payload	128	The payload carried by the message (16 bytes in total) which is able to carry the data of 4 sampling points for CDMA/WCDMA



▲ Figure 1. Structure of OBSAI protocol.

The summing step occurs during transmission but not at reception. It is also necessary for CDMA/WCDMA, but not WiMAX. Figure 1 shows the structure of the whole standard.

Both the BBU and RF have 4 layers because they need to extract the baseband data. However, only the bottom 3 layers need data extraction.

The OBSAI standard sets down 3 optical fiber rates: 768 Mbit/s, 1,536 Mbit/s and 3,072 Mbit/s (usually referred to as 1x, 2x, and 4x). Two 1x data streams can be converged into one 2x data stream through message cross-connection multiplexing, and likewise two 2x data streams can be converged into one 4x data stream. Because the 1x data stream has a low rate and is convenient for processing, the 2x and 4x data streams are usually de-multiplexed into several 1x data streams, processed, and then finally multiplexed back into 2x and 4x data

streams.

An optimal module comes with several fixed rates including 1.25 Gbit/s, 2.5 Gbit/s, and 3.125 Gbit/s. This is why the three rates of OBSAI should be fixed at these values. However, since they are not, there is some bandwidth waste, and the transmission efficiency of OBSAI is comparatively low. CPRI has high transmission efficiency because its rates are well matched to those of the optical module. In R&D, the parameters may be adjusted so that OBSAI can work at the same rates as CPRI while the interior structure remains

unchanged.

## 2 Principles of the OBSAI–Based Baseband–RF Interface

Connection between the separated BBU and RU can occur in 2 ways: the BBU may connect with the RF by itself through the optical interfacer, or several BBUs may send their own data to the cross-connection unit for summing and then connect with the RF through the optical interface. If data of different standards is to be sent through one optical fiber, then only the second way can be adopted. Only using the second way can the various baseband data be mixed together. Figure 2 depicts the two types of connection, where optical fiber may also be replaced by high-rate cable.

A multi-mode base station will most likely adopt the second way of connecting for the sake of resource sharing and easy cabling. The rationale of OBSAI baseband–RF interface will now be examined using the second way of connecting.

One BBU supports several sectors. Each sector has the same data rate and format but the rate and format of baseband data varies with different wireless standards. To use the same transport link for varying baseband data, the baseband data cannot be transmitted in its original format; instead, it must be encapsulated in one container. An OBSAI message may serve as such a container for storing baseband data of different standards. Every message works individually and allows for any switch and forwarding, independent of the wireless standard.

As far as CDMA and WCDMA are concerned, baseband data also requires the summing process; that is, summing up the data sent by several BBUs to the same sector and then

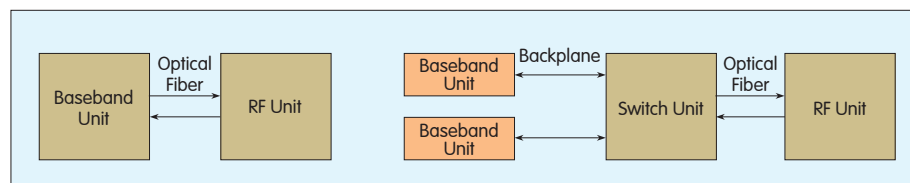
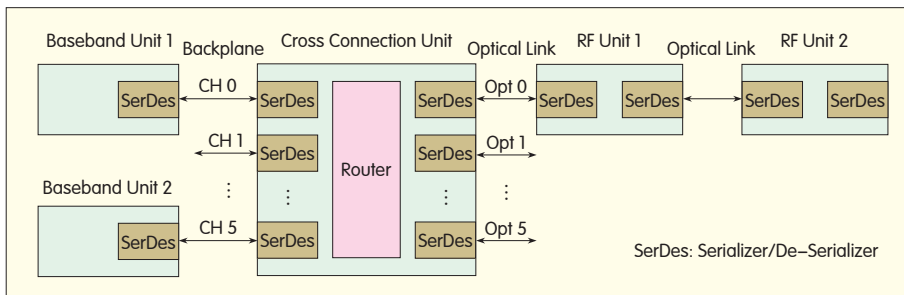


Figure 2. Two ways of connecting the BBU and RF in a base station with separate BBU and RF.



▲ Figure 3. Structure of a OBSAI-based multi-mode base station.

sending the result to the RF. Thus, more baseband processing resource of the sector is available, and resource sharing and dynamic allocation of resources is possible. Summing was once performed directly on original baseband data, which is suitable if only one wireless standard is involved. When several standards are involved, however, it is very difficult to pick data of the same standard and accommodate data of different rates. The problem can be solved if all baseband data is carried in an OBSAI message. The OBSAI standard comes with a message summing function; summing is performed on messages with exactly the same destination address and data type, and only the payload is summed up while the address and type remain the same. Since one message can carry data of 4 sampling points, and the format of the messages is uniform, the result of the messages summing is identical to that done directly on original data. In other words, it is not necessary to extract the payload before summing, and this makes the design of switch unit much simpler.

As for the RF, when an optical fiber carries data of different standards, the payload is traditionally extracted first before being forwarded as required by the configuration. As long as the payload is extracted, its relevance with wireless standard cannot be ignored. And once the standard changes, the corresponding functional module should also be changed. This is uncondusive to stable product versions. With the OBSAI standard, the payload need not be extracted; instead, whether the message is forwarded or not is determined by the

destination address, not the payload. Only those messages sent to a local address should have their payload (baseband data) extracted and sent to mid-frequency and RF processing modules. The local unit will not be affected even if the RF of other wireless standards are involved later. This gives rise to much better version stability.

### 3 Block Diagram of OBSAI-Based Multi-Mode Base Stations

Figure 3 shows the structure of a multi-mode base station built with the OBSAI standard.

In Figure 3, BBUs 1 and 2 support different wireless standards. Suppose CDMA is used for BBU 1 and WCDMA for BBU 2, and RFs 1 and 2 correspond to BBU 1 and 2 respectively. Two BBUs separately adapt their own baseband data into the OBSAI data stream and forward it to the switch unit. The rate of the path matches that of the baseband data, but the rates of paths need not be the same. Figure 4 shows the logic diagram of the BBU (those below the link layer are omitted).

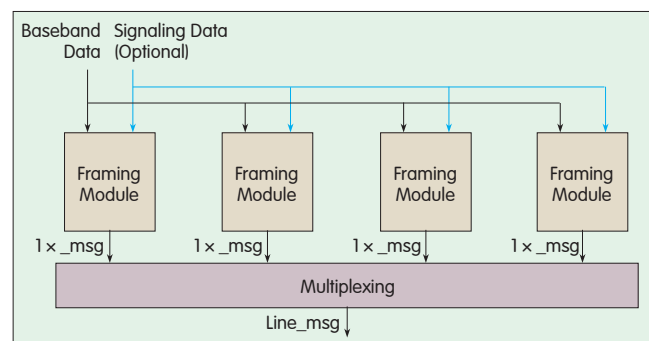
In Figure 4, the framing module adapts the baseband data and signaling data into the 1x OBSAI data stream. At most, there are four channels of 1x data streams sent to the multiplexing module. The multiplexing module combines (in the sequence of message switch) the four data streams into a single 4x data stream. If the baseband data

does not use the 4x data stream, the first two framing modules are enough. The multiplexing module converges the two 1x data streams into a 2x data stream in order to make flexible use of the rates.

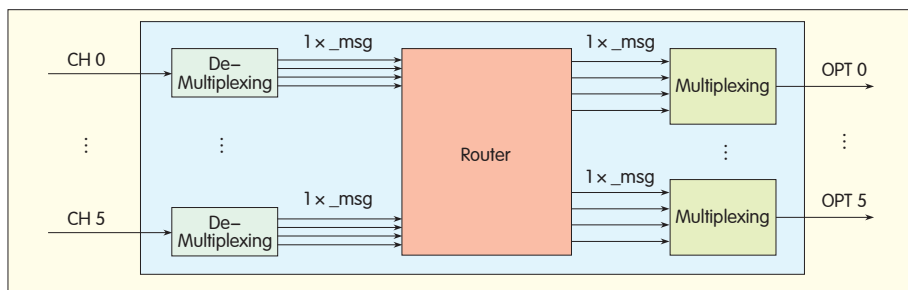
The OBSAI logic diagrams of all BBUs are the same. The framing modules, however, are different because they are closely related to the wireless standard of the baseband data. The CDMA and WCDMA standards are quite similar in that the data of the sectors is sent in at the same time and in the same data format. The rates of data are different, and therefore they have the same method of framing (reading the data of four sampling points of every sector by turn, and inserting them into one message). The format of WiMAX baseband data is noticeably different, as the data of each sector is sent in turn—each being one sign wide. Therefore, the OBSAI reads data of the first sector first, and data of the second sector next. Such a reading sequence requires only a First-In First-Out (FIFO) queue to be added to the design. WiMAX equipment manufactured by ZTE has an OBSAI module designed in this way.

It is notable that in the framing module, the destination address of baseband data is added to the header of every message. The destination address can be worked out according to the sector number and it is useful for switch and forwarding by downstream units.

A standard OBSAI data stream reaches the switch unit. The switch unit is a public module where the baseband data of all wireless standards are cross-connected and summed up



▲ Figure 4. Logic diagram of the baseband unit.



▲ Figure 5. Logic diagram of the switch unit.

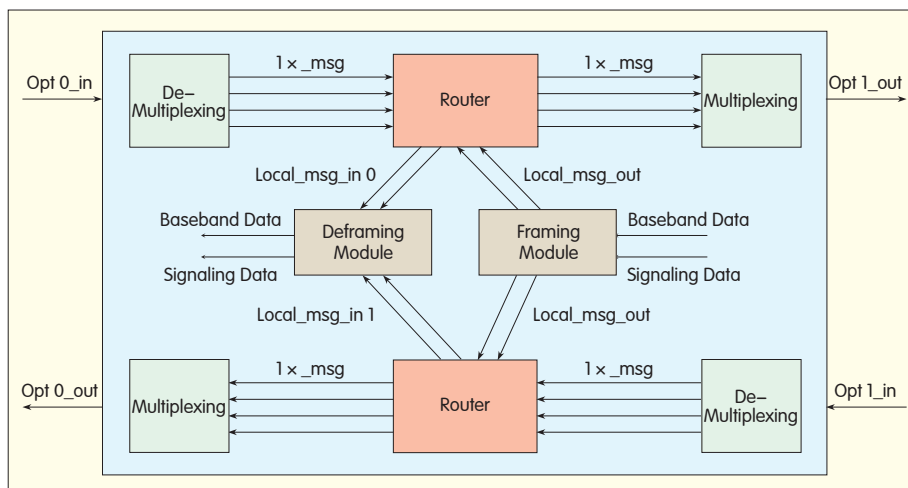
before they are forwarded to a related optical interface. This unit should be unrelated to the wireless standard so that it can support different standards. Figure 5 shows the logic diagram of the switch unit.

As shown in Figure 5, CH0-CH5 are the data streams (4x rate employed) coming from six BBUs. These data streams run through the De-Multiplexing module first where they are broken into four 1x data streams. Next, the router module routes the data streams to different optical interfaces according to information given in the Message Header, and every optical interface accepts four 1x data streams (at most). Finally, the multiplexing module combines the data streams into one data stream and sends it out through the optical fiber.

The switch unit only employs the bottom three layers of the OBSAI, not the application layer. Therefore, it is insensitive to the format of the payload data. Baseband data of different standards can all be routed through the

same switch unit and then forwarded to related optical interfaces. They can be mixed in one optical link for transmission, and the downstream units will know from the destination address whether to send the message to local destinations or forward it on.

The RF receives the OBSAI data streams from the optical interface, breaks them into several 1x data streams using the De-Multiplexing module, and determines where they will go using the routing module. The streams may go to the local application layer for extracting the baseband data (if the destination address is a local one), or to downstream units (if the destination address is not a local one). The data stream sent from the local unit also comprises several 1x data streams. These are sent to two optical interfaces at the same time and then multiplexed together with the forwarded data streams onto one link before being sent out. Figure 5. shows the block diagram of the module with 4x optical interface.



▲ Figure 6. Logic diagram of the RF unit.

To make the logic design simpler, a 1x data stream can be divided into a maximum of two 0.5x data streams. One RF can take up at least one 0.5x data stream, and one optical link can support a concatenation of eight RFs (at most).

In Figure 6, only the framing and deframing modules are closely related to the wireless standard while other modules are public ones and are exactly the same. Therefore, devices can be developed much faster to support new standards.

## 4 Conclusions

When building the interface between the BBU and RF of a multi-mode base-station using OBSAI, the BBU and radio unit must be changed to support the new wireless standard. If the optical interface rate remains the same, changing other software, hardware, or logic within the units is unnecessary. The bottom transport modules of the BBU and RF module are the same; existing modules can be used so that R&D can focus on the wireless standard.

The biggest drawback of using OBSAI is the low transmission efficiency due to high overhead. This is why the OBSAI standard is used less than CPRI. However, the layered structure of OBSAI can effectively screen out the impact of wireless standards so that different standards are supported on one hardware platform with a single optical fiber. This makes OBSAI a valuable standard for multi-mode base stations.

### Reference

- [1] OBSAI reference point 3 specification [R]. OBSAI SIG, 2005.

### Biography

Mao Ming



Mao Ming holds an MA from Sichuan University, and is an engineer at ZTE Corporation. He is currently engaged in researching CDMA/WiMAX base stations, especially the baseband-RF interface.

# Cloud Computing (2)

**Wang Bai**  
**Xu Liutong**

(School of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, P. R. China)

## Editor's Desk:

Cloud computing is a topic of intense interest in the Internet field. Major IT giants have launched their own cloud computing products. This four-part lecture series discusses cloud computing technology in the following aspects: The first part provided a brief description of the origin and characteristics of cloud computing from the users view of point; the other parts introduce typical applications of cloud computing, technically analyze the specific content within the cloud, its components, architecture and computational paradigm, compare cloud computing to other distributed computing technologies, and discuss its successful cases, commercial models, related technical and economic issues, and development trends.

As well as cloud computing infrastructure, Google provides conventional Web-based office software such as Gmail, Google Calendar, Google Talk, Google Docs, and Google Earth. Google Docs stores data at a certain place in the Internet, which users can easily access through any Internet-connected system. Google has granted permission for third parties to run large-scale parallel applications by Google App Engine within its clouds. The company deserves praise because it is not conservative; Google has already made its three cloud computing trumps public in academic publications. The technologies have been enthusiastically taken up by universities and research institutes alike, and have become important tools for constructing cloud computing platforms and programmes.

## 5 Typical Applications of Cloud Computing

The development of grid computing has been a topic of great interest in academia but not in business. Cloud computing, on the other hand, has tended to attract more interest from industrial enterprises. Since Google CEO Eric Schmidt coined the term “cloud computing” in 2006, the whole industry has become involved in it. Soon thereafter, major IT players released successive plans on cloud computing, and propounded their cloud computing services. Such concerted action by IT enterprises has rarely been seen in the industry.

### 5.1 Google

Google has been the initiator and

biggest player in cloud computing. In the process of building its empire, and with the support of over one million servers, Google has distributed its search engines in more than 200 locations. Moreover, the number of these facilities is rapidly rising. In order to facilitate communication and cooperation between these servers, Google developed Google File System (GFS), MapReduce, and BigTable. These technologies enable hundreds of thousands, even millions of computers to compose the “Cloud”, a powerful data center. GFS, MapReduce, and BigTable are therefore known as the three trumps of cloud computing. Kaifu Lee, ex-CEO of Google China, stated that the “Clouds” are the true competence of Google, which have provided the company with unique capabilities in storage and global data computation.

### 5.2 IBM

IBM’s “Blue Cloud” offers paid subscribers an available cloud computing platform. The IBM cloud includes a suite of automated, self-managing, and self-healing virtual cloud computing software. It enables applications worldwide to access distributed large-scale server pools, creating a data center which can perform computing tasks in an Internet-like environment. IBM leads a joint research initiative of 17 European partners on cloud computing. The 170 million Euro EU-funded initiative is called RESERVOIR—Resources and Services Virtualization Without Barriers. In August 2008, IBM announced plans to invest about \$400 million for the transformation of its cloud computing data centers in North Carolina and Tokyo and later in 2009, announced an investment plan worth \$300 million for the creation of 13 cloud computing



centers in 10 countries.

### 5.3 Amazon

Amazon's entry into the emerging field of cloud computing serves as a good precedent for other enterprises considering the same move. With Amazon Web Services (AWS), users can rent Elastic Compute Cloud (EC2) computers to run their own programs through simple Web service interfaces, and can utilize the limitless storage space of Simple Storage Service (S3). Amazon provides hourly billing for virtual machines, and also billing depending on the amount of data being transported. Within only 2 years, Amazon transformed cloud computing into big business. It currently has 440,000 registered developers and numerous enterprise-level clients. Based on data from third-party statistical agencies, Amazon's cloud-derived income has reached \$100 million. Cloud computing has become one of Amazon's fastest growing services.

### 5.4 Microsoft

Microsoft launched its Windows Azure cloud operating system in October 2008. The Azure service platform is a cloud application platform, providing Live, Azure Data, .NET, SharePoint, and Dynamics CRM services. The platform implements application development, management, and trusteeship in cloud. Azure has its foundations in Microsoft's global basic service system, composed of its transworld data centers. Microsoft owns hundreds of millions of Windows user desktops and browsers around the world, and now connects them into the "blue sky". Its online cloud computing products also include MSN, Hotmail, Bing, and Product Service & Support.

### 5.5 Salesforce

Salesforce is a pioneer Software as a Service (SaaS) vendor. It provides web-access-enabled automatic application software, and following in its footsteps, a number of SaaS vendors have mushroomed. Platform as a Service (PaaS) is Salesforce's next goal. It is in the process of creating a web application software platform,

Force.com, which will serve as the basis for its enterprise clients to create their own software services. Force.com includes a relational database, user interface options, enterprise logic, and an integrated developing environment called Apex.

### 5.6 Oracle

Oracle continues to be one of the pioneer promoters of enterprise grid applications. Its products include Real Application Clusters (RAC), Automated Storage Management (ASM), and storage grid. Oracle CEO Larry Ellison gave the following remarks on September 26, 2008: "We've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements." Oracle and Amazon has joined in cooperation to provide AWS-based products and services including Oracle software deployed in the cloud, and Oracle database backup in the cloud.

### 5.7 Development of Cloud Computing in China

In China, cloud computing has also developed rapidly and vigorously. The Chinese Institute of Electronics established the Cloud Computing Experts Association on November 25, 2008, and held the first China Cloud Computing Conference at the China World Hotel, Beijing, on May 22, 2009. On May 10, 2008, IBM established its first Cloud Computing Centre at Tai Hu New Town Science and Industrial Park in WuXi, followed by a second at its Business Innovation Centre on June 24, 2008. After signing a strategic cooperation framework agreement with the Nanjing Municipal Government in December 2008, Alisoft.com, a subsidiary of Alibaba.com, set up the first Chinese e-commerce Cloud Computing Centre in Nanjing City at the beginning of 2009.

China Mobile's Research Institute also played a part in early cloud computing research, and has completed cloud computing tests. Mr. Wang Jianzhou, President and CEO of China Mobile, believes that cloud computing and mobile Internet are

inevitable future trends. "Cloud Security" created by Chinese enterprises is a highly original concept in the international cloud computing field. This security technology uses numerous client ends on the Internet to monitor abnormal software behavior. It sends up-to-date information about Trojans and malware to the cloud security end for automatic analysis and handling, and then distributes solutions to each client end. The development of cloud security is like a gust of wind, and web security companies such as Rising, Trend Micro, Kaspersky, McAfee, and Symantec have released cloud security solutions. Rising's 2009 product based on cloud security can intercept millions of Trojan attacks everyday. With the help of the cloud, Trend Micro prevents up to 10 million virus infections a day.

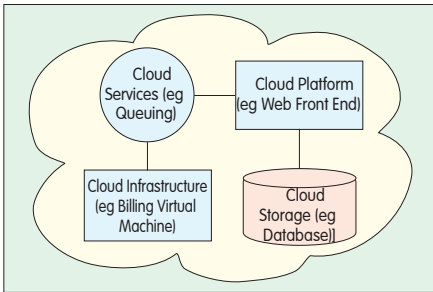
## 6 Architecture of the Cloud Computing System

To understand what cloud computing is about, it is necessary to look inside the cloud—at its components and architecture.

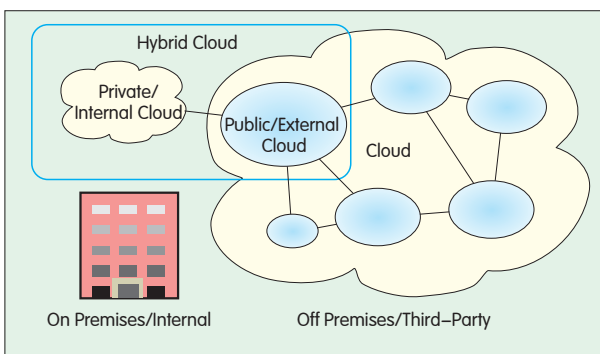
The architecture of a software-hardware application system usually includes views from different angles. The same depiction can be made of a cloud computing system. Its internal components and organizational structure affect its functionality and use. The following will describe the cloud composition, classification, and service levels from different viewpoints, as well as Cloud Computing Open Architecture and Market-Oriented Cloud Computing. Certainly, cloud computing technology has not reached maturity. Different viewpoints give the reader a better understanding of the technology.

### 6.1 Composition of the Cloud

As seen from the overview diagram in the preceding lecture, a cloud computing system consists of multiple cloud computing service providers. In terms of software and hardware, a cloud system is composed of many types of computers, storage devices, communications equipment, and software systems running on such



▲ Figure 2. Composition of the cloud.



▲ Figure 3. Classification of the cloud.

devices.

Figure 2 is a very simple diagram showing the composition of the cloud, but it cannot illustrate what the cloud can do. In the environment of cloud computing, most data remains in certain Internet servers, while application programs run on cloud servers and user browsers.

## 6.2 Classification of the Cloud

Some researchers divide the cloud into public, private, and hybrid spheres, as shown in Figure 3.

### (1) Public Cloud

Public cloud or external cloud describes cloud computing in the mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis.

### (2) Private Cloud

Private cloud and internal cloud are neologisms that some vendors have recently used to describe offerings that emulate cloud computing on private networks. These (typically virtualisation

automation) products claim to "deliver some benefits of cloud computing without the pitfalls", capitalising on data security, corporate governance, and reliability concerns. They have been criticized on the basis that users "still have to buy, build and manage them" and as such do not benefit from lower up-front capital costs and less hands-on management, essentially "lacking the economic model that makes cloud computing such an intriguing concept".

### (3) Hybrid Cloud

A hybrid cloud environment consisting of multiple internal and/or external providers "will be typical for most enterprises".

Generally speaking, cloud computing emphasizes a new model of Internet resource use, and is a means of treating

IT resources as services. Almost all IT resources can be offered as cloud services, including application programs, computing capability, storage capacity, network communication service, and cooperation tools. Therefore, we will discuss cloud computing from the viewpoint of services.

## 6.3 Service Levels of the Cloud

By the end of 2009, most cloud computing infrastructures were composed of trusted services delivered by data centers and different level virtualization technologies based on servers. People can use these services at any place where there is available network infrastructure. Cloud computing software and data is stored at data centers and offered for general commercial application through web services. Users can then use browsers to access online application services.

Cloud computing services generally include SaaS, PaaS, and Infrastructure as a Service (IaaS). Figure 4 shows the often seen service stacks of the cloud computing system.

(1) A cloud client consists of computer hardware (including mobile

devices) and/or computer software which relies on cloud computing for application delivery, or which is specifically designed for delivery of cloud services.

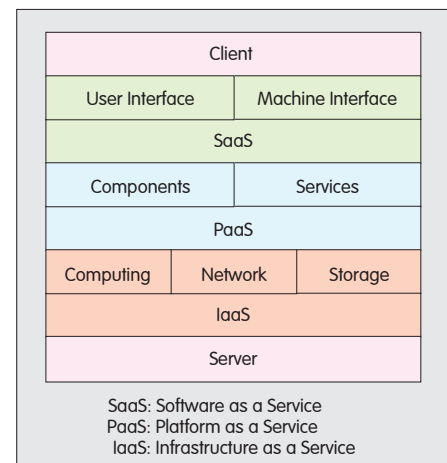
(2) A cloud service leverages cloud computing in software architecture, often eliminating the need to install and run the application on the customer's own computer, thus alleviating the burden of software maintenance, ongoing operation, and support. Typical applications on this level include Facebook and YouTube web applications, Google Apps (such as Gmail) and Salesforce SaaS, and BitTorrent content distribution.

(3) A cloud platform (PaaS) delivers a computing platform and/or solution stack as a service, generally consuming cloud infrastructure and supporting cloud services. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. Paypal, Google App Engine and Amazon S3 are typical PaaS applications.

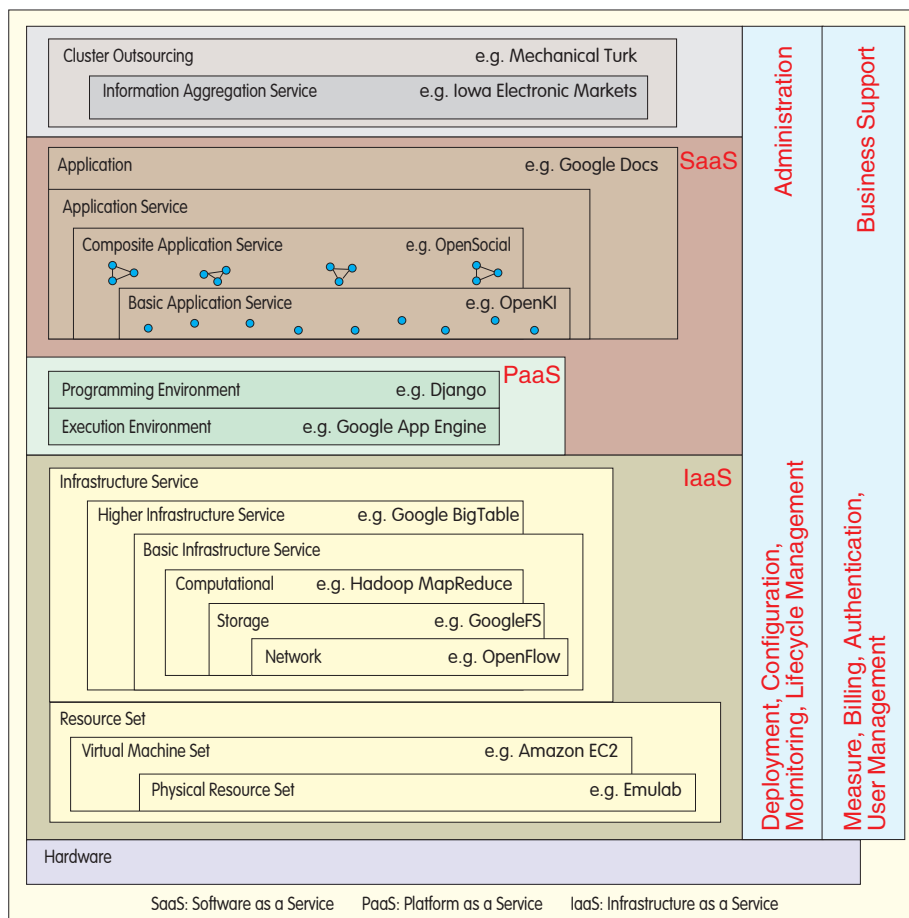
(4) Cloud infrastructure (IaaS) is the delivery of computer infrastructure, typically a platform virtualization environment, as a service. Amazon EC2 is an IaaS application.

(5) The servers layer consists of computer hardware and/or computer software products which are specifically and solely designed for the delivery of cloud services.

The Everything as a Service (XaaS)



▲ Figure 4. Service stacks of cloud computing system.



▲ Figure 5. Detailed service stacks in cloud computing system.

concept is closely related to cloud computing. Some researchers have even included human group intelligence into service stacks of cloud computing. This uses the power of the

public to contribute to some services, such as Wikipedia and “newsworthy” video streaming. Figure 5 shows the detailed service stacks.

Simple services can be further

combined into complex and various application services. This can be achieved on the SaaS layer, and on lower layers also. For example, AWS GrepTheWeb uses Simple Queue Service (SQS) to implement decoupling of the controller, Hadoop MapReduce is fulfilled in clusters of EC2 instances, and S3 and SimpleDB are used for data storage and retrieval.

(To be continued)

### Biographies

#### Wang Bai



Wang Bai is a professor and vice dean of the School of Computer Science and Technology, Beijing University of Posts and Telecommunications (BUP). Her research interests include next generation telecom operation supporting system, distributed computing technologies, and visualization analysis of complex networks. She has published more than 60 papers and 3 books.

#### Xu Liutong



Xu Liutong is a professor at the School of Computer Science and Technology, BUP. His research interests include data mining, grid computing, and distributed systems and their application in telecom field. He has published more than 20 papers.

### Roundup

## ZTE Hosts IEEE 10G-EPON Interoperability Showcase

Interoperability of symmetric 10G-EPON products was demonstrated successfully in Shanghai, China in April 2010.

Interoperability among products was successfully demonstrated by four vendors: Broadcom, PMC-Sierra, Opulan and ZTE. Each vendor supplied an OLT and a variety of ONUs (supporting both 1G-EPON and symmetric 10G-EPON), connected in a multi-vendor

configuration to demonstrate complete interoperability.

System performance was examined for realistic and challenging test configurations that reflected the specific requirements of major service providers. These tests included physical-layer connectivity, MAC connectivity, MPCP discovery, dynamic bandwidth allocation, service setup, security and authentication, and connection management.

Coexistence of 1G-EPON and 10G-EPON on the same network was also demonstrated successfully, thus validating a critical feature for operators with large volumes of 1G-EPON deployed in their networks. 10G-EPON's robust and cost-effective coexistence solution protects network operators' existing 1G-EPON deployments and allows a gradual migration to higher data rates. (ZTE Corporation)

# Abbreviation Index

## A

ANA: Autonomic Network Architecture  
 ARS: Action Request System  
 ASM: Automated Storage Management  
 ASP: Application Server Process  
 ATCA: Advanced Telecommunications  
 Computing Architecture  
 ATM: Asynchronous Transfer Mode  
 AWS: Amazon Web Services

## B

BER: Bit Error Rate  
 BFD: Bidirectional Forward Detection  
 BGCF: Breakout Gateway Control  
 Function  
 BGP: Border Gateway Protocol  
 BOSS: Business Operation Support  
 System  
 BSSAP: Base Station System  
 Application Part

## C

CE: Customer Edge  
 CN: Cognitive Network  
 CN: Core Network  
 CONMan: Complexity Oblivious  
 Network Management  
 CoopRTS: Cooperative  
 Request-To-Send  
 CORBA: Common Object Request  
 Broker Architecture  
 CPN: Cognitive Packet Network  
 CPRI: Common Public Radio Interface  
 CR: Cognitive Radio  
 CTS: Clear-To-Send

## D

DDOS: Distributed Denial-of-Service  
 DE: Decision Element  
 DNS: Domain Name System  
 DT: Drive Test  
 DwPTS: Downlink Pilot Time Slot

## E

EC: Enterprise Customer

EC2: Elastic Compute Cloud  
 EIA: Evolvable Internet Architecture  
 EML: Element Management Layer  
 EMS: Element Management System  
 eTOM: Enhanced Telecom Operation  
 Map

## F

FARA: Forwarding Directive,  
 Association and Rendezvous  
 Architecture  
 FE: Fast Ethernet  
 FIB: Forwarding Information Base  
 FIFO: First-In First-Out  
 FIND: Future Internet Design  
 FIRE: Future Internet Research and  
 Experimentation  
 FOCALE: Foundation, Observation,  
 Comparison, Action  
 and Learning Environment  
 FP7: Seventh Framework Programme  
 for Research and Technological  
 Development  
 FPNB: Future Packet Based Network  
 FR: Frame Relay

## G

GAN: General Autonomic Network  
 Architecture  
 GE: Gigabit Ethernet  
 GENI: Global Environment for Network  
 Innovations  
 GFS: Google File System  
 GP: Guard Period  
 GPRS: General Packet Radio Service  
 GPS: Global Positioning System  
 GW: Gateway

## H

HCL: Hierarchical Control Loop  
 HLRMAP: Home Location  
 Register Mobile  
 Application Part  
 HSS: Home Subscriber Server  
 HTS: Helper-Ready-To-Send

## I

I/S-CSCF: Inquiry/Service-Call  
 Session Control Function  
 IaaS: Infrastructure as a Service  
 ICT: Information and Communication  
 Technologies  
 IMS: IP Multimedia Subsystems  
 IMS-PDA: IMS-Supported Personal  
 Digital Assistant  
 INMS: Integrated Network Management  
 System  
 IOT: Internet of Things  
 IrDA: Infrared Data Association  
 IS: Information Service  
 ISP: Internet Service Provider  
 ISUP: ISDN User Part  
 ITIL: IT Infrastructure Library

## K

KPI: Key Performance Index

## L

LAN: Local Area Network  
 LSP: Label Switching Path  
 LTE: Long Term Evolution

## M

M2M: Machine to Machine  
 M3UA: MTP3 User Adaptation  
 MAC: Media Access Control  
 MAP: Mobile Application Part  
 ME: Managed Element  
 MGCF: Media Gateway Control Function  
 MGW: Media Gateway  
 MIMO: Multiple-Input Multiple-Output  
 MMS: Multimedia Messaging Service  
 MPLS: Multi-Protocol Label Switching  
 MSC: Mobile Switching Center  
 MSCMAP: Mobile Switching Center  
 Mobile Application Part  
 MSCS: Mobile Switching Center Server  
 MTP: Message Transfer Part

## N

NACF: Network Attachment Control



## Abbreviation Index

### Function

NAT: Network Address Translation  
NE: Network Element  
NFC: Near Field Communication  
NGN: Next Generation Network  
NMS: Network Management System  
NNI: Network Node Interface  
NS: Name Service

### O

OAM: Operation, Administration and Maintenance  
OBSAI: Open Base Station Architecture Interface  
OMC: Operation and Maintenance Center  
OMCS: Operation and Maintenance Center of Core Network  
OMM: Operation and Maintenance Module  
OS: Operating System  
OSI: Open System Interconnection  
OSPF: Open Shortest Path First  
OSS: Operations Support Systems

### P

P2P: Peer-to-Peer  
PaaS: Platform as a Service  
PBT: Provider Backbone Transport  
PCCPCH: Primary Common Control Physical Channel  
P-CSCF: Proxy Call Session Control Function  
PDN: Packet Data Network  
PE: Provider Edge  
PIC: Programmable Interrupt Controller  
POTS: Plain Old Telephony Service  
PSS: PSTN/ISDN Simulation Sub-System  
PTDN: Public Telecom Packet Data Network

### R

RAC: Real Application Cluster  
RACF: Resource and Admission

### Control Function

RAN: Radio Access Network  
RBA: Role-Based Architecture  
RDBMS: Relational Database Management System  
RDF: Resource Description Framework  
RFID: Radio Frequency Identity  
RNA: Recursive Network Architecture  
RSCP: Received Signal Code Power  
RTP: Real-Time Transport Protocol  
RTS: Request-To-Send  
RTWP: Received Total Wideband Power

### S

S3: Simple Storage Service  
SaaS: Software as a Service  
SBC: Session Border Controller  
SCCP: Signaling Connection Control Part  
SCTP: Stream Control Transmission Protocol  
SDH: Synchronous Digital Hierarchy  
SDR: Software-Defined Radio  
SerDes: Serializer/De-Serializer  
SFTP: Secure File Transfer Protocol  
SI: Service Integrator  
SILO: Services Integration, Control, and Optimization  
SIP: Session Initiation Protocol  
SIPI: Signaling IP Interface  
SIP-IAD: SIP-Supported Integrated Access Device  
SIR: Signal-to-Interference Ratio  
SL: Site Local  
SMS: Short Message Service  
SNI: Service Node Interface  
SNMP: Simple Network Management Protocol  
SNR: Signal-to-Noise Ratio  
SONET: Synchronous Optical Network  
SQS: Simple Queue Service  
SSH: Secure Shell  
SW: Switch

### T

TCP/IP: Transfer Control Protocol/Internet Protocol  
TCP: Transmission Control Protocol  
TD-SCDMA: Time Division Synchronous Code Division Multiple Access  
TE: Traffic Engineering  
T-MPLS: Transport MPLS  
TS: Time Slot  
TUP: Telephone User Part

### U

ULP: Upper Level Protocol  
UNI: User Network Interface  
UpPTS: Uplink Pilot Time Slot  
URI: Uniform Resource Identifier  
USSD: Unstructured Supplementary Service Data  
UWB: Ultra-Wide Band

### V

VAS: Value Added Service  
VLAN: Virtual Local Area Network  
VLRMAP: Visitor Location Register Mobile Application Part  
VPLS: Virtual Private LAN Service  
VPN: Virtual Private Network  
VRRP: Virtual Router Redundancy Protocol

### W

WAN: Wide Area Networks  
WAP: Wireless Application Protocol  
WCDMA: Wideband Code Division Multiple Access  
WDM: Wavelength Division Multiplexing  
Wi-Fi: Wireless Fidelity  
WiMAX: Worldwide Interoperability for Microwave Access  
WLAN: Wireless Local Area Network

### X

XaaS: Everything as a Service  
XML: Extensible Markup Languages