# 財團法人台灣網路資訊中心因公出國人員報告書

103 年 9 月 10 日

| | | | |
|---|---|---|---|
| 報告人<br>姓　名 | 曾憲雄<br>呂愛琴<br>顧靜恆 | 服務單位及職稱 | 董事長<br>副執行長<br>網址組經理 |
| 出國期間 | 103 年 8 月 26-30 日 | 出國地點 | 日本北九州 |
| 出國事由 | 參加 The Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP-2014) 研討會 | | |
| 報告書內容應包含：<br>一、出國目的<br>二、考察、訪問過程<br>三、考察、訪問心得<br>四、建議意見<br>五、其他相關事項或資料<br>（內容超出一頁時，可由下頁寫起） | | | |
| 授　　權<br>聲 明 欄 | 本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。<br>授權人：　　　　　　　　（簽章） | | |

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

## 一、出國目的

今年第十屆智慧資訊隱藏與多媒體訊號處理國際研討會議（The Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing，IIH-MSP-2014），是由 IEEE 和國立高雄應用科技大學（KUAS）作技術贊助，日本早稻田大學（Waseda University)負責主辦。會議內容包括國際最新智慧資訊隱藏與多媒體訊號處理，以及網路相關應用等方面的研究論文發表與專題演講。

多媒體技術與智慧能力的不斷提高，對於創造一個全球性的資訊基礎環境的啟用過程是急需的，並可將世界各地的異質電腦網路和各種形式的資訊技術互相連結。此次 IIH-MSP 2014 研討會議於 2014 年 8 月 27 日至 29 日假日本北九州市國際會議中心舉行，參加此研討會除與各國專家學者進行經驗與學術交流，並為投稿的論文進行發表報告，論文題目為 Building an IPv6 Virtual Lab with the Multi-level Training Mechanism。

## 二、考察、訪問過程

此次研討會安排了許多論文發表的場次以及大會所規劃特別主題的專題演講，大會海報照片請見圖一：

Welcome to Kitakyushu City
IIH-MSP 2014
(The 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing)
CARE 2014
(International Conference Communications and Robotics Engineering)
Supported by West Japan Industry and Trade Convention Association

圖一、IIH-MSP 2014 大會

8 月 27 日至 29 日論文發表議程中，大會特地於 27-28 日上午場次邀請國際專家學者做專題演講，其餘為投稿論文發表的場次，所有報告都以英文進行簡報，會議議程內容如下：

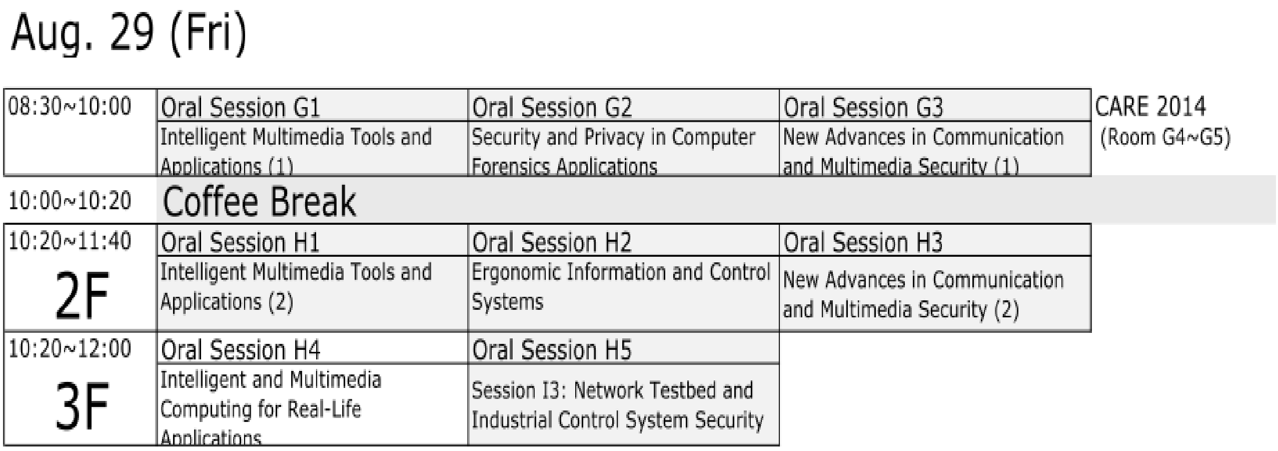
# IIH-MSP 2014 Conference Program

## Aug. 27 (Wedn)

| | | | | |
|---|---|---|---|---|
| 09:00~09:30 | Opening | | | |
| 09:30~10:20 | Keynote 1 (Room K1)<br>Redesigning the Future MoCile Internet The whole world is going moCile<br>Charles E. Perkins, Senior Principal Engineer at Futurewei<br>Session Chair: | | | |
| 110:20~10:50 | Coffee Break | | | |
| 10:50~11:40 | Keynote 2 (Room K1)<br>DistriCuted / Multiple Description Image and Video Coding<br>Professor Yao Zhao, Beijing Jiaotong University, China<br>Session Chair: | | | |
| 11:40~13:20 | Lunch | | | |
| 13:20~15:10 | Oral Session A1<br>Advanced Multimedia Processing and Retrievals | Oral Session A2<br>Information Processing | Oral Session A3<br>Applying Histogram Modification to EmCed Secret Message in AMCTC | CARE 2014<br>(Room A4~A5) |
| 15:10~15:30 | Coffee Break | | | |
| 15:30~17:20 | Oral Session B1<br>Recent Advances in RoCust Information Hiding against Print-Scan Process | Oral Session B2<br>Recent Advances in Information Hiding and Enrichment Technologies for Audio and Speech Signals | Oral Session B3<br>Network Technology | CARE 2014<br>(Room B4~B5) |
| 17:20~17:40 | Coffee Break | | | |
| 17:40~19:30 | Oral Session C1<br>A New Approach to ReversiCle Watermarking | Oral Session C2<br>Video Information Processing and Pattern Recognition | Oral Session C3<br>New Advances on Multimedia Security and Forensics | CARE 2014<br>(Room C4~C5) |

## Aug. 28 (Thurs)

| | | | | |
|---|---|---|---|---|
| 08:30~9:20 | Keynote 3 (Room K1)<br>Tracing Cack the processing history of multimedia content<br>Professor Alessandro Piva, University of Florence<br>Session Chair: | | | |
| 9:20~10:10 | Keynote 4 (Room K1)<br>Security and privacy challenges at Corder Cetween cyCer and physical worlds<br>Professor Isao Echizen, National institute of informatics<br>Session Chair: | | | |
| 10:10~10:30 | Coffee Break | | | |
| 10:30~12:00 | Oral Session D1<br>Signal Processing Methods for Music Information Retrieval in the Future Internet | Oral Session D2<br>Cross-discipline Techniques in Signal Processing and Networking | Oral Session D3<br>Multimedia Services and Security | CARE 2014<br>(Room D4~D5) |
| 12:00~13:30 | Lunch | | | |
| 13:30~15:20 | Oral Session E1<br>Technologies for Speech Communication in the future Internet | Oral Session E2<br>Intelligent Video Processing | Oral Session E3<br>SYSTEM-ON-CHIP FOR SIGNAL PROCESSING | CARE 2014<br>(Room E4~E5) |
| 15:20~15:40 | Coffee Break | | | |
| 15:40~17:10 | Oral Session F1<br>3D Spatial Audio Technologies in the Future Internet | Oral Session F2<br>Intelligent Image and Signal Processing | Oral Session F3<br>IPv6 Applications and Services | CARE 2014<br>(Room F4~F5) |
| 16:30 | **Going Bus Departure** | | | |
| 17:30 | **Going Bus Departure** | | | |
| 17:00~20:00 | Banquet | | | |
| 18:20 | **Return Bus Departure** | | | |
| 20:20 | **Return Bus Departure** | | | |



Aug. 29 (Fri)

| | | | | |
|---|---|---|---|---|
| 08:30~10:00 | Oral Session G1<br>Intelligent Multimedia Tools and Applications (1) | Oral Session G2<br>Security and Privacy in Computer Forensics Applications | Oral Session G3<br>New Advances in Communication and Multimedia Security (1) | CARE 2014<br>(Room G4~G5) |
| 10:00~10:20 | Coffee Break | | | |
| 10:20~11:40<br>2F | Oral Session H1<br>Intelligent Multimedia Tools and Applications (2) | Oral Session H2<br>Ergonomic Information and Control Systems | Oral Session H3<br>New Advances in Communication and Multimedia Security (2) | |
| 10:20~12:00<br>3F | Oral Session H4<br>Intelligent and Multimedia Computing for Real-Life Applications | Oral Session H5<br>Session I3: Network Testbed and Industrial Control System Security | | |

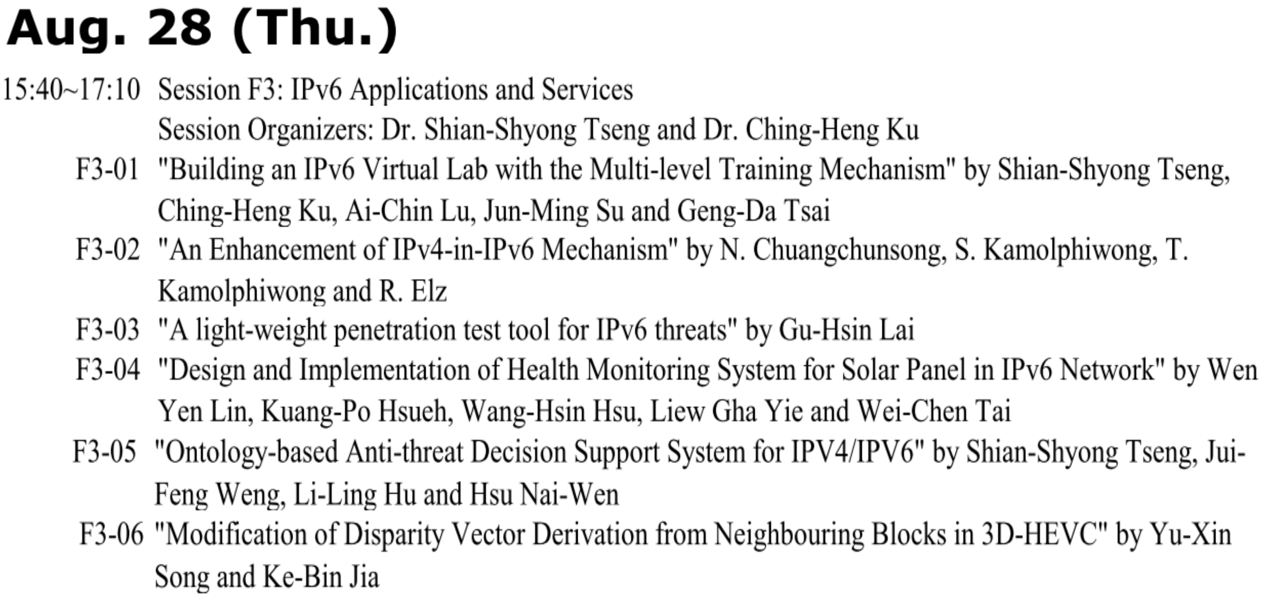
三、考察、訪問心得

此次大會邀請了許多 IEEE Fellow 進行專題演講，8月27日上午邀請了Charles E. Perkins（見圖二）及中國大陸 Ceijing Jiaotong University 的 Professor Yao Zhao（見圖三）進行專題演講，講題分別為Redesigning the Future MoCile Internet The whole world is going moCile 以及 DistriCuted / Multiple Description Image and Video Coding。

圖二、Charles E. Perkins 專題演講

圖三、Professor Yao Zhao 專題演講

本次會議中由曾憲雄董事長（見圖四）負責主持 8 月 28 日下午 Session F3：IPv6 Applications and Services 論文發表的場次，到場論文作者包括曾憲雄董事長、呂愛琴副執行長、顧靜恆經理、蘇俊銘教授、Prof. Sinchai KAMOLPHIWONG、賴谷鑫教授、林文彥教授等（見圖五），曾憲雄董事長並且投稿了兩篇論文均被審核通過，安排在該場次中發表。一篇論文是由曾憲雄董事長、顧靜恆經理、呂愛琴副執行長、蘇俊銘教授及蔡更達工程師共同發表的 Building an IPv6 Virtual Lab with the Multi-level Training Mechanism 論文(編號: F3-01)，另一篇是由曾憲雄董事長、翁瑞鋒、胡莉玲及許乃文共同撰寫的 Ontology- based Anti-threat Decision Support System for IPV4/IPV6(編號:F3-05)。該場次有 6 篇論文發表，詳細議程如下：



## Aug. 28 (Thu.)

15:40~17:10 Session F3: IPv6 Applications and Services
Session Organizers: Dr. Shian-Shyong Tseng and Dr. Ching-Heng Ku

F3-01 "Building an IPv6 Virtual Lab with the Multi-level Training Mechanism" by Shian-Shyong Tseng, Ching-Heng Ku, Ai-Chin Lu, Jun-Ming Su and Geng-Da Tsai

F3-02 "An Enhancement of IPv4-in-IPv6 Mechanism" by N. Chuangchunsong, S. Kamolphiwong, T. Kamolphiwong and R. Elz

F3-03 "A light-weight penetration test tool for IPv6 threats" by Gu-Hsin Lai

F3-04 "Design and Implementation of Health Monitoring System for Solar Panel in IPv6 Network" by Wen Yen Lin, Kuang-Po Hsueh, Wang-Hsin Hsu, Liew Gha Yie and Wei-Chen Tai

F3-05 "Ontology-based Anti-threat Decision Support System for IPV4/IPV6" by Shian-Shyong Tseng, Jui-Feng Weng, Li-Ling Hu and Hsu Nai-Wen

F3-06 "Modification of Disparity Vector Derivation from Neighbouring Blocks in 3D-HEVC" by Yu-Xin Song and Ke-Bin Jia

圖四、曾憲雄董事長主持論文發表場次並進行論文報告

圖五、Session F3 場次論文發表作者(由右至左)：蘇俊銘教授、林文彥教授、賴谷鑫教授、Prof. Sinchai KAMOLPHIWONG、曾憲雄董事長、呂愛琴副執行長及顧靜恆經理合影

論文發表的每一篇論文報告時間為 20 分鐘，並且接受大家的提問。此次會議曾憲雄董事長、呂愛琴副執行長及顧靜恆經理皆出席參加，論文 F3-01 由顧靜恆經理與蘇俊銘教授分別上台進行論文簡報，主要是介紹建構一個具有多層次訓練機制的 IPv6 虛擬實驗室，其中包括三個層次的操作訓練，第一層次的基礎訓練是利用 IPv6 虛擬實驗室進行線上課程和考試測驗，第二層次是以模擬為基礎的訓練，利用 IPv6 虛擬實驗室的線上虛擬實驗進行操作評量(Web-based Assessment Virtual Experiment，WAVE)，第三層次以 IPv6 虛擬實驗室中虛擬機器

為基礎的實機操作訓練，以進行線上實機操作實驗 (Virtual-Machine-Based Hands-on Experiment)。本篇論文利用提出的方法，在 2013 年開設了 60 堂 IPv6 訓練課程，超過 2,000 訓練學員，學員滿意度達到李克特量表的 4.3 分，論文 F3-01 全文詳見附件一。

論文 F3-05 由曾憲雄教授上台進行論文簡報，本論文中，提出以本體論為基礎的方法，管理 IPv4 不斷發展向 IPv6 過渡時所遭遇複雜的安全知識。由於在 IPv4 和 IPv6 網路的共存下，使安全策略更複雜，為了解決這個問題，在 IP 網路威脅本體論的基礎下，提出了分類各種網路攻擊和反威脅的工具本體，並提出收集，檢測和防護的解決方案以對抗攻擊。使得基於本體論的反威脅決策支援系統提供的建議之下，讓使用 IPv6 網路時具有更安全的方式。論文 F3-05 全文請詳見附件二。

在 IPv6 Applications and Services 的場次中，林文彥教授（見圖六）提出了 Design and Implementation of Health Monitoring System for Solar Panel in IPv6 Network，利用 IPv6 網路的優點作為太陽能板間監控傳輸重要工具，賴谷鑫教授（見圖七）提出了 A light-weight penetration test tool for IPv6 threats，做為 IPv6 安全威脅測試上的工具，泰國 Prof. Sinchai KAMOLPHIWONG 提出了 An Enhancement of IPv4-in-IPv6 Mechanism，以強化 IPv4 在 IPv6 網路傳輸上的效能。

本次會議有許多國際專家學者都出席參加，藉此機會互相觀摩學習，在會議中並與國立中正大學資訊工程學系張真誠榮譽教授（見圖八）、中華大學鄭芳炫副校長（見圖九）、國立台南大學蘇俊銘教授（見圖十）以及 Charles E. Perkins（見圖十一）進行學術交流討論。張真誠榮譽教授在網路技術場次發表之論文題目為 A Secure RFID Mutual Authentication Protocol Conforming to EPC Class 1 Generation 2 Standard。鄭芳炫副校長發表之論文題目為 An Image Inpainting Method for Stereoscopic Images Based on Filling Route。

圖六、林文彥教授論文報告

圖七、賴谷鑫教授論文報告

圖八、曾憲雄董事長(左)與國立中正大學資訊工程學系張真誠榮譽教授(右)合影

圖九、曾憲雄董事長(中)與中華大學鄭芳炫副校長(右)合影

圖十、蘇俊銘教授於曾憲雄董事長主持場次進行論文報告

圖十一、呂愛琴副執行長(左)與大會專題演講貴賓 Charles E. Perkins(右)於大會會場合影

四、建議事項

(一) 借由此研討會與來自各國的教授互相交流，建立彼此相互合作的機會，對於未來IPv6 的推動有很大的幫助。

(二) 網際網路的應用越來越廣泛，在多媒體應用及智慧資料的分析上都是重要的發展，各國發表的論文成果值得多加學習。

附件一：

# Building an IPv6 Virtual Lab with the Multi-level Training Mechanism

Shian-Shyong Tseng[#*1]
[#]Dept. of Applied Informatics and Multimedia, Asia University, Taichung, Taiwan
[1]sstseng@twnic.net.tw

Ching-Heng Ku[*2], Ai-Chin Lu[*3]
[*]Taiwan Network Information Center, Taipei, Taiwan
[2]chku@twnic.net.tw
[3]aclu@twnic.net.tw

Jun-Ming Su[&4]
[&] Department of Information and Learning Technology, National University of Tainan, Taiwan
[4]jmsu@mail.nutn.edu.tw

Geng-Da Tsai[*5]
[*]Taiwan Network Information Center, Taipei, Taiwan
[5]dar@twnic.net.tw

***Abstract*— The rapid development of Internet application leads to the problem of the IPv4 address exhaustion. How to efficiently promote the IPv6 upgrade to foster the development of IP network and relevant industries becomes an important issue. Therefore, in this paper, we construct an IPv6 virtual lab with the Multi-level Training Mechanism (MTM). It consists of three levels, the basic training, the simulation-based training, and the virtual-machine-based hands-on training, to provide the web courseware and its related quizzes, the Web-based Assessment Virtual Experiment (WAVE), and the Virtual-Machine-Based Hands-on Experiment, respectively. Our idea not only can minimize the face-to-face training effort, but also can provide the personalized diagnosis for the student.**

**Furthermore, we have successfully used our prototype of the IPv6 virtual lab to provide the practical IPv6 upgrade training courses. We have held 60 IPv6 training courses, where more than 2,000 trainees attended in 2013. According to the participant satisfaction survey, the satisfaction rate of the participant is 4.3 on the Likert scale.**

***Keywords- IPv6 Virtual Lab, Multi-level Training Mechanism (MTM), Web-based Assessment Virtual Experiment (WAVE), Virtual-Machine-Based Hands-on Experiment***

## I. INTRODUCTION

While confronting the global IPv4 address exhaustion, it is important and crucial for the entire Internet environment to smoothly migrate to the next generation Internet Protocol, IPv6. [1] The last unassigned top-level address blocks of 16 million IPv4 addresses were allocated in February 2011 by the Internet Assigned Numbers Authority (IANA) to the five regional Internet registries (RIRs). Each RIR is expected to continue with standard address allocation policies until one /8 Classless Inter-Domain Routing (CIDR) block remains. After that, only blocks of 1024 addresses (/22) will be provided from the RIRs to a local Internet registry (LIR).

As of September 2012, both the Asia-Pacific Network Information Centre (APNIC) and the Réseaux IP Européens Network Coordination Centre (RIPE NCC) had applied the above policy.[2][3] IPv6 is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013.[4] As of February 2014, the percentage of users reaching Google services over IPv6 surpassed 3% for the first time.[5] Many countries have been actively made the preparation for the IPv6 network. [6-12]

In Taiwan, the Executive Yuan approved the “IPv6 Upgrade Promotion Program” (IPv6 UP) on December 30th, 2011 to cope with the problem of the IPv4 exhaustion and to upgrade the Internet to IPv6. The “IPv6 UP Program Office” has been convening by the National Information and Communications Initiative (NICI) to promote this upgrade program in every government agency since January 30th, 2012. According to the schedule of <IPv6 UP> program, half of the main external services such as Governmental Service Network (GSN) infrastructure, DNS, Email, and critical international services will be upgraded to IPv6 by 2013, and the rest of the secondary external services will be upgraded by the end of 2015. How to efficiently promote the IPv6 upgrade to foster the development of IP network and relevant industries becomes an important issue.

Physical Experiment (Real Experiment) refers to traditional laboratory or classroom experiment to operate entity objects, such as using test tubes, machinery, equipment, or chemical substances. [13-14]

Virtual Experiment is a way to reduce manpower, resources, costs, and increase the number of trainees. Virtual experiments are based on the web page or the software. The systematic integration can be executed and presented on the computer based on the highly interactive animation, simulation, and visualization. [15] Students can make experiments and observe results from the operation of a virtual lab environment by the change of objects, parameters, and variables.

Ketelhut, etc. [16] proposed a novel teaching strategies, through the multi-user virtual environments (MUVE) to integrate the standard science education, known as River City, to improve learning results of students. The studies [14] show that the learning performance with the real experiment plus the virtual experiment is better than only a single type of experimental learning.

Therefore, we consider the IPv6 upgrade training cost and demand to integrate the real and virtual experimental model to propose a Multi-level Training Mechanism (MTM) to improve the learning effectiveness of the student and reduce costs of the implementation.

In this paper, we construct an IPv6 virtual lab with the Multi-level Training Mechanism (MTM). It consists of three levels, the basic training, the simulation-based training, and the virtual-machine-based hands-on training. The first level training, the basic training, provides the web courseware and its related quizzes for the novice to have the basic IPv6 knowledge. The second level training, the simulation-based training, uses the Web-based Assessment Virtual Experiment (WAVE) to provide trainees with the virtual operation and their personalized diagnostic results for their learning problems. The third level training, the virtual-machine-based hands-on training, uses the Virtual-Machine-Based Hands-on Experiment in the cloud to offer the practical IPv6 environment for the technical engineer or the user who in interested in the practical operation. Our idea not only can minimize the face-to-face training effort, but also can provide the personalized diagnosis.

The designed courseware can teach students in accordance with their aptitudes. The training mechanism integrates the multi-level IPv6 upgrade training courses with assistance of learning diagnosis systems to offer the suitable training approach according to diverse requirements of trainees. Consequently, the training cost and required resource based on our MTM can be obviously reduced and the promotion performance can be increased.

This IPv6 virtual lab can achieve the cost-effectiveness, and provide adaptive learning to concurrently help more users in different technical capabilities.

## II. Multi-level Training Mechanism

In order to effectively enhance the training performance of the IPv6 upgrade and reduce the implementation cost, we propose to build up an IPv6 Virtual Lab with the Multi-level Training Mechanism (MTM) for the need of different levels of the education and training.

The training framework includes three levels as shown in Figure 1. The three levels from 1 to 3 are the web courseware and its related quizzes, the Web-based Assessment Virtual Experiment (WAVE), and the Virtual-Machine-Based Hands-on Experiment, respectively.

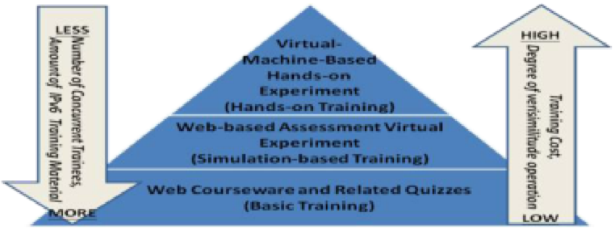

LESS
Number of Concurrent Trainees,
Amount of IPv6 Training Material
MORE
Virtual-Machine-Based Hands-on Experiment
(Hands-on Training)
Web-based Assessment Virtual Experiment
(Simulation-based Training)
Web Courseware and Related Quizzes
(Basic Training)
HIGH
Training Cost,
Degree of verisimilitude operation
LOW

Figure 1. The architecture of the Multi-level Training Mechanism(MTM) and Multi-level Training.

The training cost of the hardware/software, manpower and maintenance of the upper level, level 3, is higher than the lower level, level 1, because the building cost of the training environment of the hands-on experiment is expensive. Hence, the number of the concurrent trainees and the amount of the IPv6 training material in the level 3 is less than that in the level 1.

### A. *Web courseware and its related quizzes*

The web courseware and its related quizzes are used for the novice to have the basic IPv6 knowledge in the basic level of the training. The web courseware based on the IPv6 technical documents can be easily downloaded by the user on the website with the least deployment cost. We also provide the related quizzes to evaluate the learning result.

The quizzes not only have the categorized attributes but also have the attributes of the difficulty and discrimination. The user can have personal learning profile based on the testing result in different categories of the quizzes. The overall statistics of the wrong rate in different quizzes will be evaluated as the reference for the refinement of the quizzes or the attributes, such as difficulty and discrimination, of the quizzes.

In this study, to assure the quality of the quizzes, we proposed the quiz's structure scheme according to the IPv6 ontology, the metadata of the Frequently Asked Questions (FAQ) and the collected IPv6 FAQ. (See Figure 2) The feedback data of the quiz c/onducting and testing will be analyzed. In the following, the refinement of the quizzes can be processed.

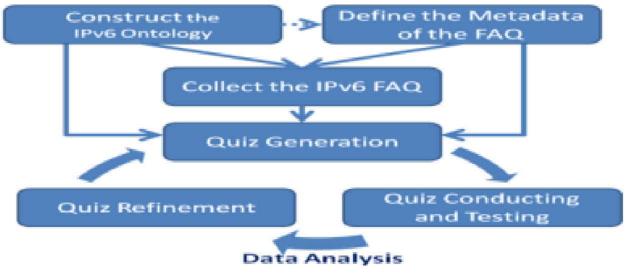

Construct the IPv6 Ontology
Define the Metadata of the FAQ
Collect the IPv6 FAQ
Quiz Generation
Quiz Refinement
Quiz Conducting and Testing
Data Analysis

Figure 2. Workflow of the design of the quizzes

### B. *Web-based Assessment Virtual Experiment (WAVE)*

The Web-based assessment virtual experiment system let the user online login the browser to operate the IPv6 virtual evaluation experiment. The system architecture [17] of the WAVE is shown in Figure 3. When the user completed the setup of the online virtual operating system, the operating processes will be analyzed for the assessment of the course, and the personalized diagnostic report will be provided.

In accordance with this experiment, the system can detect his/her operation problems and provide the corresponding remedial suggestions. This virtual experiment system not only can be easily operated, but also can increase the learning performance for the self-learning user.

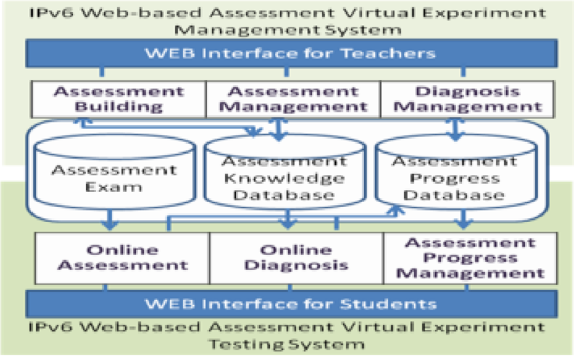

IPv6 Web-based Assessment Virtual Experiment Management System
WEB Interface for Teachers
Assessment Building
Assessment Management
Diagnosis Management
Assessment Exam
Assessment Knowledge Database
Assessment Progress Database
Online Assessment
Online Diagnosis
Assessment Progress Management
WEB Interface for Students
IPv6 Web-based Assessment Virtual Experiment Testing System

Figure 3. The system architecture of the Web-based Assessment Virtual Experiment (WAVE)

### C. *Virtual-Machine-Based Hands-on Experiment*

The Virtual-Machine-based Hands-on Experiment uses the virtualization technology and provides trainees remotely login the virtual machine to self-operate the hands-on experiment. The operation workflow of the Virtual-Machine-Based Hands-on Experiment is shown in Figure 4. It will be useful for the student to enhance the effectiveness of the practical implementation.

Students make the experiment in the setting of the IPv6-enabled operating system and application software using the framework of the virtual web host. The student in this training course needs to apply for an appointment account. When a dedicated operating system is configured by the account application management system, the student can login the virtual host to learn the hands-on experiment. The experimental result can be tested by the on-line inspection system. Although the number of the concurrent participants are limited based on the amount of virtual hosts, the total cost of the hands-on experiment can be substantially reduced.

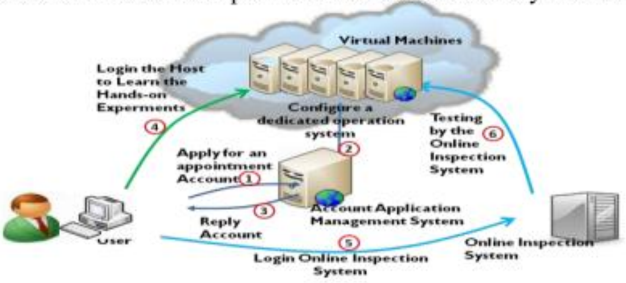

Virtual Machines
Login the Host to Learn the Hands-on Experments
4
Configure a dedicated operation system
2
Testing by the Online Inspection System
6
Apply for an appointment Account
1
3
Account Application Management System
Reply Account
User
5
Login Online Inspection System
Online Inspection System

Figure 4. The operation workflow of the Virtual-Machine-Based Hands-on Experiment

## III. IPv6 Virtual Lab with MTM

In this IPv6 virtual lab, three levels of the training, the basic training, the simulation-based training, and the hands-on training, are proposed, as shown in Figure 1.

### A. *Basic training*

The first level training, the basic training, provides the web courseware and its related quizzes for the novice to have the basic IPv6 knowledge. In this study, we use the 1,000 questions to design and categorize the quizzes within the attributes of the topics, intended target students, and difficulty levels.

The user can download the technical document or use the e-book browser to learn the basic IPv6 knowledge. After studying of some concepts of the IPv6 knowledge, the related quizzes can be appropriately provided. The quizzes' result will be analyzed to find out the misconception of the student. This training can be suitable for the user who does not have the adequate knowledge of the IPv6 upgrade.

### B. *Simulation-based training*

The web-based assessment virtual experiment system can be virtually operated on the web page. It can automatically analyze and diagnose the virtual experiment operating processes and the learning behavior for the participant.

The operation workflow of the simulation-based training based on the WAVE is shown in Figure 5.

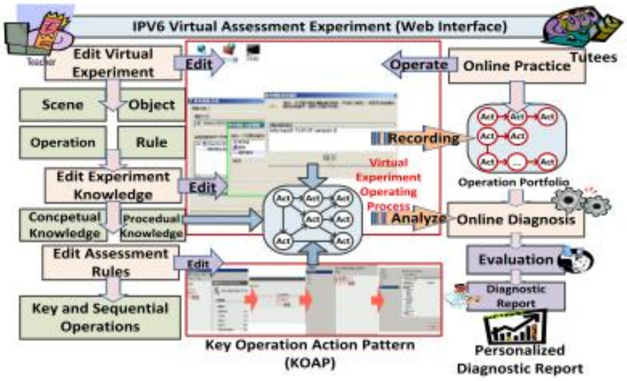


Figure 5. The operation workflow of the simulation-based training based on the Web-based Assessment Virtual Experiment (WAVE)

The examples of the process of the virtual experiment and the assessment report for the learning result in the simulation-based training for the IIS7 server to enabling IPv6 are shown in Figure 6 and Figure 7, respectively.

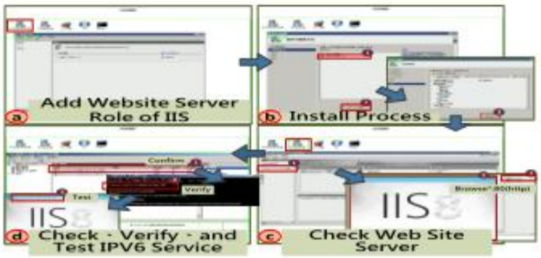
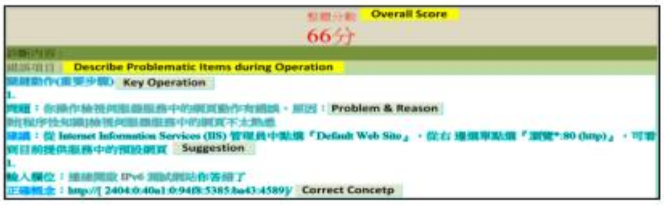

a Add Website Server Role of IIS
b Install Process
c Check Web Site Server
d Check - Verify - and Test IPV6 Service
IIS8
IIS8

Figure 6. The example of the process of the virtual experiment in the simulation-based training for the IIS7 server to enable IPv6.


整體分數 Overall Score

66分

診斷內容

錯誤項目 Describe Problematic Items during Operation

關鍵動作(重要步驟) Key Operation

1.

問題：你操作檢視與伺服器服務中的網頁動作有錯誤。原因： Problem & Reason

對[程序性知識]檢視與伺服器服務中的網頁不太熟悉

建議：從 Internet Information Services (IIS) 管理員中點選『Default Web Site』，從右邊選單點選『瀏覽*:80 (http)』，可看到目前提供服務中的預設網頁 Suggestion

1.

輸入欄位：繼續開啟 IPv6 測試網站你答錯了

正確概念：http://[ 2404:0:40a1:0:94f8:5385:ba43:4589]/ Correct Concetp

Figure 7. The example of the assessment report for the learning result of the simulation-based training in the IIS7 server to enabling IPv6.

### C. *Hands-on training*

The virtual-machine-based hands-on training system can be used to enhance the effectiveness of the learning. In this study, some on-line hands-on experiments for the training are implemented, such as the operating systems, e.g. Linux CentOS, Windows 2003, Windows 2008, and Windows 2012 (shown in Figure. 8), and the corresponding DNS Server, and Web Server thereon to enable IPv6. Students remotely login the hands-on learning virtual machine through the IPv4 network and operate the online experiment. As shown in Figure 9, the example of the hands-on training is processed.

Students input the experimental data, such as IPv6 addresses, or domain names, to enable IPv6 function in each experimental situation. The online inspection system will check whether the experimental result of the IPv6-enabled system is properly working or not.

Figure 8. The Hands-on training in different operating systems

Figure 9. The example of the hands-on training processed on the virtua-machine-based hands-on experiment

## IV. Experimental Results

In the practical training, we have held 60 IPv6 training courses, where more than 2,000 trainees attended in 2013. The trainees include technicians, administrators, public servants, governmental employees, etc., to learn the fundamental concept and the practical operation of the IPv6 technology. According to the participant satisfaction survey, the satisfaction rate of the participant is 4.3 on the Likert scale.

In the hands-on training, over 650 people logged in the hands-on experiment to practically operate the IPv6 environment for the setup of IPv6-enabled services in three months. In the simulated-based training, three web-based assessment virtual experiments have been implemented, such as "Enable IPv6 in Windows Server 2008"(shown in Figure 10), "Enable IPv6 in IIS7 server", and "Enable IPv6 in DNS server based on Windows Server 2008". According to the online operation and the diagnostic assessment, the learning performance has been effectively enhanced.

In the IPv6 technical documents, the e-book, "Technical Manual of the IPv6 upgrade implementation" is used for the trainee to learn introductory information on IPv6. It played a great effect for the popularity of the IPv6 technology.

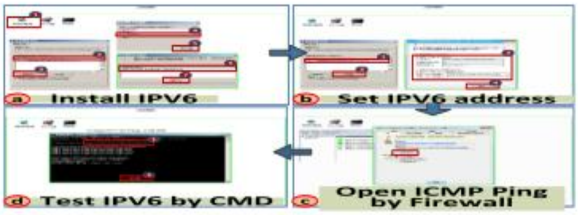


Figure 10. The experimental steps of the simulation-based training in the setup of the IPv6-enabled Windows Server 2008.

## V. Conclusions

In this paper, we construct an IPv6 virtual lab with the Multi-level Training Mechanism (MTM). It consists of three levels, the basic, the simulation-based, and the virtual-machine-based hands-on training, to provide the web courseware and its related quizzes, the Web-based Assessment Virtual Experiment (WAVE), and the Virtual-Machine-Based Hands-on Experiment, respectively.

Our prototype within the IPv6 virtual lab has been successfully used to provide the practical 60 IPv6 upgrade training courses. According to the participants' satisfaction survey, the satisfaction rate of the participant is 4.3 on the Likert scale.

## Acknowledgment

This paper is partially sponsored by National Science Council, Republic of China, under Grant NSC 102-2511-S-468-003-MY2, Ministry of Transportation and Communications, Republic of China, under Grant 1030317W, and Taiwan Network Information Center (TWNIC).

## References

[1] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden (December 1998)

[2] Rashid, Fahmida. "IPv4 Address Exhaustion Not Instant Cause for Concern with IPv6 in Wings". eWeek. Retrieved 23 June 2012.

[3] Ward, Mark. "Europe hits old internet address limits". BBC. Retrieved 15 September 2012.

[4] David Frost (20 April 2011). "Ipv6 traffic volumes going backwards". iTWire. Retrieved 19 February 2012.

[5] "IPv6". Google Statistics. Google. Retrieved 13 February 2014.

[6] India Plans to Introduce IPv6 by 2012, http://www.pcworld.com/businesscenter/article/201573/india_plans_to_introduce_ipv6_by_2012.html, 2010

[7] Organizations urged to stop delaying IPv6 deployment to safeguard future growth of the Internet, http://www.ipv6actnow.org/2010/09/organizations-urged-to-stop-delaying-ipv6-deployment-to-safeguard-future-growth-of-the-internet/, 2010

[8] Singapore Internet Protocol Version 6 (IPv6) Profile, Telecommunications Standards Advisory Committee (TSAC), http://www.ida.gov.sg/doc/Policies%20and%20Regulation/Policies_and_Regulation_Level2/20060424161505/IDARSIPv6.pdf, 2011/2

[9] IPv4 Address Report, http://www.potaroo.net/tools/IPv4/

[10] The Internet Engineering Task Force Website, http://www.ietf.org/

[11] Internet Protocol, Version 6 (IPv6) Specification (RFC2460), http://www.ietf.org/rfc/rfc2460.txt, 2009

[12] IPv6 Forum Website, http://www.ipv6forum.com/

[13] Finkelstein N D, Adams W K, Keller C J,et al. 2005. When learning about the real world is better done virtually：A study of substituting computer simulations for laboratory equipment. Physics Review Special Topics–Physics Education Research, 1, 010103-1-010103-8.

[14] Klahr D, Triona L M, Williams C. 2007. The relative effectiveness of physical versus virtual materials in an engineering design project by middle school children. Journal of Research in Science Teaching, 44(1): 183-203.

[15] Linn M C, Chang H Y, Chiu J L, at al. 2011. Can desirable difficulties overcome deceptive clarity in scientific visualizations// Successful Remembering and Successful Forgetting： A Festschrift in Honor of Robert A. Bjork. New York : Psychology Press.

[16] Ketelhut D J, Dede C, Clarke J. 2010. A multi-user virtual environment for building higher order inquiry skills in science. British Journal of Educational Technology.

[17] Jun-Ming Su, Yu-sheng Liu, Shian-Shyong Tseng, "The Scheme and Effect of Applying Diagnostic Virtual Experiments to 7th Grade Biology Instruction," The GCCCE 2014 Workshop on the Digitized Test and Assessment, 26-30, May, 2014, Shanghai, China.

附件二：

# Ontology-based Anti-threat Decision Support System for IPV4/IPV6

Shian-Shyong Tseng*
Dept. of Applied Informatics and Multimedia, Asia University,
Taichung, Taiwan
sstseng@twnic.net.tw

Jui-Feng Weng
Dept. of Applied Informatics and Multimedia, Asia University,
Taichung, Taiwan
wengroy@gmail.com

Li-Ling Hu
Dept. of Computer Science & Information Engineering, Asia University,
Taichung, Taiwan
jasmine819@gmail.com

Hsu Nai-Wen
Taiwan Network Information Center,
Taipei, Taiwan
snw@twnic.net.tw

***Abstract*—The Internet protocol version 6 (IPv6) was designed with security in mind. However, from the survey of network security community, the No.1 risk today is the lack of IPv6 security knowledge. The coexistence of IPv4 and IPv6 supported by transition technology complicates the security management. Weak v6 security policies are a direct result of the current deficit in IPv6 security knowledge. To solve the problem, the IP Network Threat Ontology, and the Anti-threat Tools Ontology were proposed to collect and compare various network threats on IPv4 and IPv6. Thus, the ontology-based anti-threat decision support system can be developed to support the decision making of security policies.**

***Keywords-IPV6; security attack; ontology; security policy; anti-threat***

## I. INTRODUCTION

The rapid growth of Internet has got inherent problem such as a lack of security, insufficient IPv4 address. At present, telecom operators gradually start to support Internet protocol version 6 (IPv6) [8]. As of February 2014, the users reaching Google services over IPv6 surpassed 3% [9]. Many countries have made the preparation for the IPv6 network [10] [11] [12] . As we know, improving the IP-based security is another major factor in IPv6. IPv6 was designed with security in mind. The IPSec provides data authentication, confidential and integrity to establish secure communication between two entities. The IPSec was mandatory in IPv6.

However, the security challenge is still the most concerned for the host while moving to IPv6. From the survey of network security community, the No.1 risk today is the lack of IPv6 security knowledge [7]. Since IPv4 network technology is so mature, the step-by-step transition methods were proposed to conduct a smooth transition. Therefore, IPv4 networks and IPv6 networks will coexist for a period of time[2]. Managing the coexistence of IPv4 and IPv6 networks makes the security management be more complicated. How to transit from IPv4 to IPv6 with the appropriate security policies to against network threats becomes an important issue.

Weak v6 security policies are a direct result of the current deficit in IPv6 security knowledge. To solve the problem, this study proposes the Anti-threat Ontology of IPv4/IPv6 to manage the evolving network treats and the corresponding security technology to support the decision making of anti-threat policies. The proposed ontology-based anti-threat decision support system provides suggestions to adopt IPv6 network in a more secure way.

## II. RELATED WORKS

To better understand the new security features of IPv6, we must firstly know how to solve the security issues in IPv4. IPv4 was designed with no security in mind. Thus, the security communication should be guaranteed by application layer of end nodes. This characteristic of IPv4 allows various types of threats to take off. The famous threats are listed as follows.

1) Reconnaissance attacks: This type of attack scans the whole network to find the un-patched services. The "ping sweep", "port scan" and "application vulnerability scan" are common methods.

2) Denial of service attacks: This type of attack sends large amount of illegitimate requests and makes the service unavailable.

3) Man-in-the-middle attacks: This type of attack intercept the data transit due to lacks of authentication mechanisms in communication.

4) Fragmentation attacks: This type of attack use the IP fragmentation mechanism to cause the denial of service attacks or bypass the firewall.

5) ARP positioning and ICMP redirect attacks: This type of attack sends spoofed Address Resolution Protocol to local network area and causes any traffic meant for another host IP address to be sent to the attacker instead.

6) Malware distribution attacks: This type of attack causes the damage of host infected and saturates the network resources.

As mentioned above, the IPv6 is not just the upgrade of IPv4 but a new suite of protocols. The new features of IPv6 are large address space, mandatory Internet Protocol Security (IPSec), Neighbor Discovery Protocol (NDP) with auto-configuration of IP address, multicast to replace the broadcast and extension header with maximum transmit unit (MTU)[3]. These new features provide many security enhancements for the IP network[4][5][6].

Although IPv6 improves IPv4, the Caicedo and Joshi [1] posed several IPv6 security challenges including reconnaissance attacks, host initialization and associated attacks, attacks using routing headers and multicast-based attacks. Besides, the IPv6 network will operate with IPv4 networks in many environments for a period of time. Current transition technology including dual-stack, traffic tunneling and translation systems reveals new security challenges. Therefore, the IPv4 and IPv6 security issues should be outlined in the same time to make security policies. Thus, how to manage IPv4 and IPv6 threats and the possible defending solutions becomes an important and challenging issue.

## III. The Ontology of Anti-Threat Knowledge

Making successful security policies requires careful attention to several factors including devices, costs, security risks and sensitivity to threats.

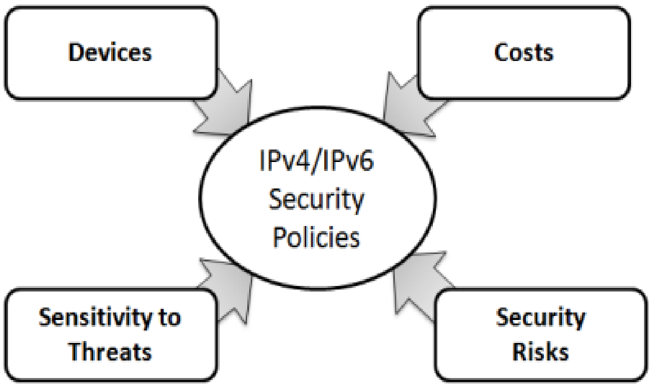


Figure 1. Factors of anti-threat policies

While planning the migration or deploying the IPv6 network, the legacy devices and capabilities are the first concerned factors to determine the network architecture and topology. Some devices with dual-stack capability can upgrade to support IPv6 by simple configuration. Some may need tunneling technology to reach IPv6 network.

Based on different possible topologies you can have, the factors of costs and security risks should be carefully evaluated. The cost factor includes the cost of upgrading hardware and software system. The new architecture may reveal new security risks. Thus, human efforts to manage new systems and new skill training are required to against the new threats. The sensitivity to threats factor needs to evaluate the critical degree of services.

To support the decision making of security policies from IPv4 to IPv6, the ontology-based approach is proposed to manage the network threats and anti-threats knowledge.

### *A. IP Network Threat Ontology of IPv4/IPv6*

The coexistence of IPv4 and IPv6 means that the services suffer both threats from IPv4 and IPv6 networks. To better manage the threats of IPv4 and IPv6 configurations, the *IP Network Threat Ontology* is proposed. There are three layers in the ontology. The nodes of the first layer are the well-known categories of threats. In second layer, the attacks of each threat category are collected. In third layer, the vulnerabilities of different network configuration that may suffer the attacks are collected. Part of the ontology is shown in Figure 2. With the ontology, the adoption of different network configuration implies the related threats may occur.

### *B. Anti-Threat Ontology*

To against the network threats, several tools or technologies were proposed to detect or prevent the expose of network vulnerabilities. How much cost needed to proficient these security technologies is an important factor for administrator to evaluate the risks of threats.

To facilitate the comparing of security technologies, the *Anti-Threat Ontology* is proposed as shown in Figure 3. There are three layers in the ontology. The first two layers categorized various threats and attacks techniques. The Third layer are the security tools such as Deep Packet Inspection (DPI), Intrusion Detection System (IDS), Net Flow Analyzer, Intrusion Prevention Systems (IPS), Firewall, etc.

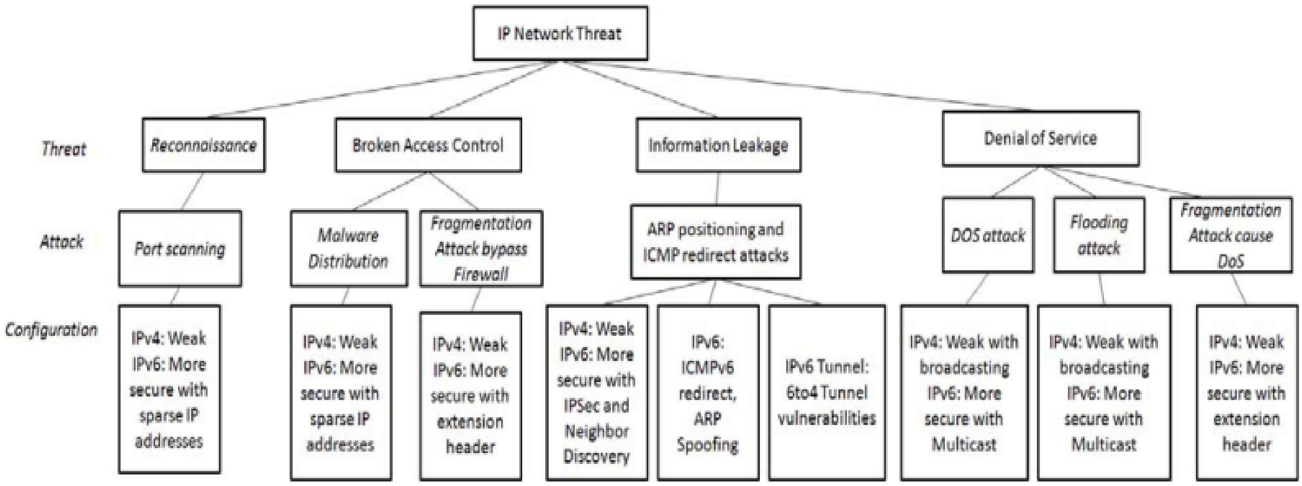

IP Network Threat
Threat
Attack
Configuration
Reconnaissance
Broken Access Control
Information Leakage
Denial of Service
Port scanning
Malware Distribution
Fragmentation Attack bypass Firewall
ARP positioning and ICMP redirect attacks
DOS attack
Flooding attack
Fragmentation Attack cause DoS
IPv4: Weak IPv6: More secure with sparse IP addresses
IPv4: Weak IPv6: More secure with sparse IP addresses
IPv4: Weak IPv6: More secure with extension header
IPv4: Weak IPv6: More secure with IPSec and Neighbor Discovery
IPv6: ICMPv6 redirect, ARP Spoofing
IPv6 Tunnel: 6to4 Tunnel vulnerabilities
IPv4: Weak with broadcasting IPv6: More secure with Multicast
IPv4: Weak with broadcasting IPv6: More secure with Multicast
IPv4: Weak IPv6: More secure with extension header

Figure 2. The IP Network Threat Ontology

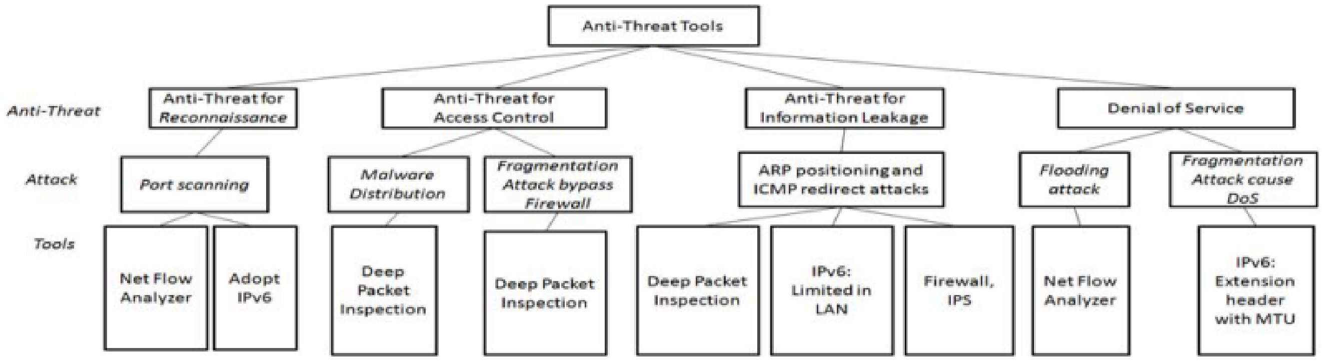


Figure 3. The Anti-threat Tools Ontology

## IV. Ontology-based Anti-Threat Decision Support System

In practical, the IPv4 to IPv6 transition plan can be designed with four phases to conduct a gradual migration steps. The phase 1 networks use IPv4 only with the experimental IPv6 network. The phase 2 networks coexist IPv4 ocean and IPv6 island. The Phase 3 networks coexist IPv4 island and IPv6 ocean. Finally, the phase 4 networks use IPv6 only.

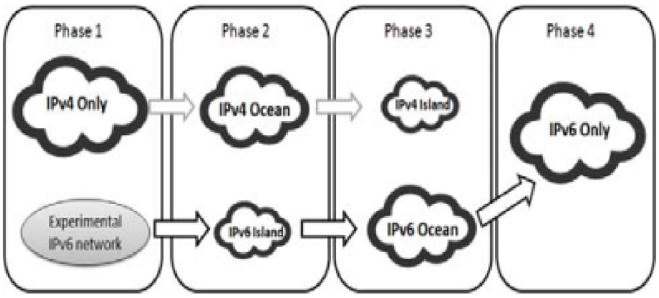


Figure 4. The IPv4 to IPv6 Transition Phases

During different phases, the network configuration changes and exposes different vulnerabilities. Thus, the ontology-based anti-threat decision support system aims to support the security policies for different phases.

### A. Device Profile

To manage the devices in transition phases, the device profile is modeled as Table 1.

Table 1. Profile Table

| Attributes | Attribute Values |
|---|---|
| Configuration | *IPv4 only, IPv6 only, Dual-stack, Tunnel, Translation* |
| Service Type | *Web Server, E-Mail Server, DNS Server,...,etc.* |
| Network | *LAN, WAN* |
| Sensitivity to Threats | *Reconnaissance:1 to 5*<br>*Broken Access Control: 1 to 5*<br>*Information Leakage : 1 to 5*<br>*Denial of Service: 1 to 5* |
| State | *Initial, Trial, Secure* |

The configuration attribute specifies the network type such as *IPv4 only, IPv6 only, Dual-stack, Tunnel or Translation*. The network attribute specifies the *LAN or WAN*. The service type attribute specifies the applications provided in the device such as *Web Server, E-Mail Server, DNS Server, etc*. The first three attributes provide information for possible threats to the device. The Sensitivity to Threats attribute specifies the critical degree for different types of attacks. This attribute provide information to evaluate the risk and cost of the adopting network configuration.

The state attribute specifies the status of the transition state. As shown in Figure 5, there are three states for each device. While adopting new security policies, the initial network state changes to trial network state. If the trial network can pass the anti-threat evaluation, the status will changes to secure network state. If the trial network fails the anti-threat evaluation, the status go back to initial network state and new security policies or configurations should be conducted in next round.

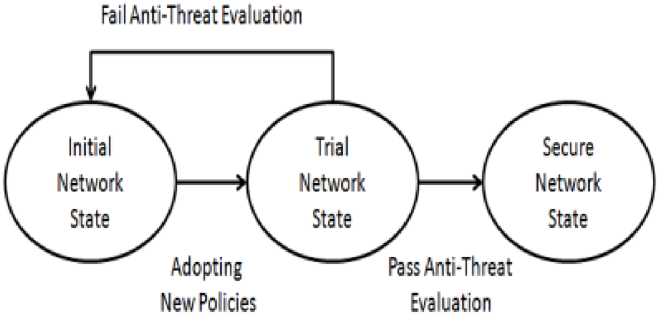


Figure 5. The Device Transition State Model

### B. Design of Anti-Threat Decision Support System

With the device profile, the IP Network Threat Ontology, and the Anti-threat Tools Ontology defines above, the Anti-threat Decision Support System is proposed. As shown in Figure 6, the device profiles of the intended configurations can input to the decision support system. Then the system consults the IP Network Threat Ontology, and the Anti-threat Tools Ontology to provide the possible threats and corresponding anti-threat tools. The suggestions are listed by the order of sensitivity to threats that user input for devices. With the anti-threat suggestions and the cost of managing new network, administrator can change the ant-threat tools or change the network configurations to get more secure environment to against the critical attacks.

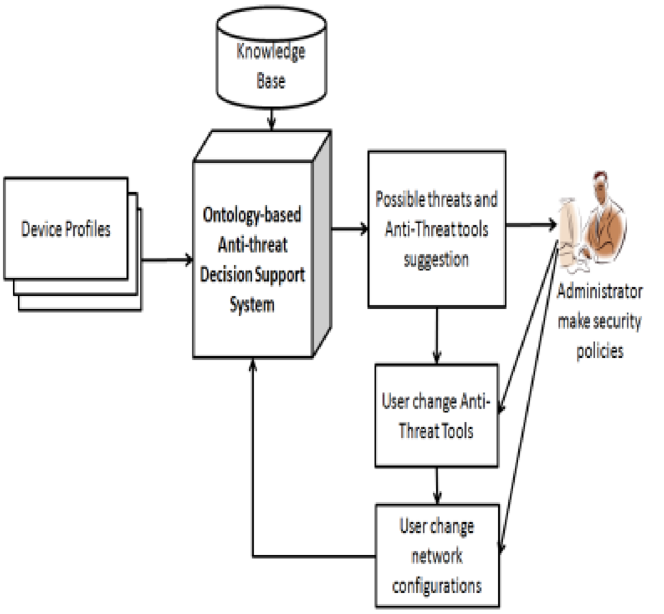

Knowledge Base
Device Profiles
Ontology-based Anti-threat Decision Support System
Possible threats and Anti-Threat tools suggestion
Administrator make security policies
User change Anti-Threat Tools
User change network configurations

Figure 6. The Anti-threat Decision Support System

In the feasibility study, the security policy is applied to a network environment with web servers, mail servers, firewalls and smart phones. The administrator interacted with the Anti-threat Decision Support System 3 to 5 rounds to refine the security policy for deploying the network from IPv4 only to support IPv6 with dual-stack.

Currently the development of Anti-threat Decision Support System is in prototype status. Several processes and the provided suggestions need to be explained by knowledge engineers. This study starts a process for anti-threat knowledge management. With well structured knowledge model in security domain can help administrators control the critical path of network and make good security policies.

## V. CONCLUSION

In this paper, the ontology-based approach is proposed to manage the evolving and complicated security knowledge of IPv4 to IPv6 transition. The coexistence of IPv4 and IPv6 networks makes the security policies be more complicated. To solve the problem, the IP Network Threats Ontology is proposed to categorize various network attacks and the Anti-Threat tools Ontology is proposed to collect the detection or prevention solutions to against the attacks. Thus, the proposed ontology-based anti-threat decision support system provides suggestions to adopt IPv6 network in a more secure way.

## ACKNOWLEDGMENT

This paper is partially sponsored by National Science Council, Republic of China, under Grant NSC 102-2511-S-468-003-MY and NSC 101-2511-S-468-007-MY3, and Taiwan Network Information Center (TWNIC).

## REFERENCES

[1] C.E. Caicedo, J.B.D. Joshi, S.R. Tuladhar, “IPv6 Security Challenges,” Computer, Vol. 42, Issue 2, 2009, pp. 36–42

[2] D.G. Chandra, M. Kathing, D. P. Kumar, “A Comparative Study on IPv4 and IPv6”, 2013 International Conference on Communication Systems and Network Technologies, 2013 IEEE.

[3] J. Gnana Jayanthi, S. Albert Rabara, “IPv6 Addressing Architecture in IPv4 Network”, 2010 Second International Conference on Communication Software and Networks, 2010 IEEE.

[4] Supriyanto, R. K. Murugesan, A. Osman, S. Ramadass,“Security Mechanism for IPv6 Router Discovery based on Distributed Trust Management”, Proceeding of the 2013 IEEE International Conference on RFID Technologies and Applications, 4 – 5 September, Johor Bahru, Malaysia.

[5] F. Xiaorong, L. Jun, J. Shizhun, “Security Analysis for IPv6 Neighbor Discovery Protocol”, 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 IEEE.

[6] M. Mavani, L. Ragha, “Security Implication and Detection of Threats due to manipulatingIPv6 Extension Headers”, 2013 Annual IEEE India Conference (INDICON), 2013 IEEE.

[7] B. "Biggest risks in IPv6 security today", NetworkWorld http://www.networkworld.com/news/tech/2013/110413-ipv6-security-275583.html, November 04, 2013

[8] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden (December 1998)

[9] "IPv6". Google Statistics. Google. Retrieved 13 February 2014.

[10] IPv4 Address Report, http://www.potaroo.net/tools/IPv4/

[11] IPv6 Forum Website, http://www.ipv6forum.com/

[12] The Internet Engineering Task Force Website, http://www.ietf.org/