IPv6 Certification and Course Development

Mr. John Pickard  
East Carolina University  
Greenville, NC  
011-252-328-9646  
pickardj@ecu.edu

John Spence  
Nephos6, Inc  
Raleigh, NC  
011-425-247-0520  
spence@nephos6.com

Dr. Phil Lunsford  
East Carolina University  
Greenville, NC  
011-252-328-9670  
lunsfordp@ecu.edu

ABSTRACT

The need to train IT professionals, especially network engineers, in the use of Internet Protocol version 6 (IPv6) continues to grow as adoption of IPv6 continues to rise. The adoption of IPv6 is driven by the IPv4 address space depletion, the proliferation of managed devices, the proliferation of mobile wireless devices, and government initiatives. An undergraduate standalone course in IPv6 is discussed including previous experiences starting in 2006. The current IPv6 course offering, based on a partnership with Nephos6 Inc. as the pilot of the first Nephos6 Academy, is reviewed including course topics, laboratory environment, and certification. The current course is delivered totally online and includes extensive remote-laboratory exercises, and has objectives that align with the IPv6 Forum Certified Engineer (Silver) objectives.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: Computer and Information Science Education – computer science education, curriculum, information systems education.

General Terms

Documentation, Performance, Design

Keywords

Certification, Course Development, Distance Education, Industry Collaboration, Internet, IPv6

1. INTRODUCTION

At the time of this writing, World IPv6 Launch Day, June 6, 2012 is only days away. First defined in January of 1995 by RFC1752, the “next generation” IP protocol, IPv6, has been around now for almost a generation. Yet seventeen years later, leaders in IP technology such as Cisco, Microsoft, Akamai, and Free Telecom are gathering forces to encourage organizations around the world to “launch” IPv6. For the past decade it has looked as if IPv6 would never become fully adopted and that IPv4, with features such as network address translation (NAT), carrier grade NAT (CGN), and classless inter-domain routing (CIDR), could continue to provide the world with the address space needed. However, this perspective is now changing as organizations and governments come realize that IPv4 cannot sustain the future demands of Internet connectivity. The transition to IPv6 is going to finally become a reality.

2. THE NEED FOR IPv6 IN EDUCATION

A 2010 IPv6 Curricula Studies survey funded by the European Commission found that IPv6 training and studies at universities were not rigorous enough and were not providing students with the IPv6 knowledge or skills necessary to have any critical impact [15]. One of the results of this finding was the launching of the IPv6 Education Certification Logo Program in 2010 by the IPv6 Forum [17]. The IPv6 Forum sees colleges and universities playing a key role as part of this program in accelerating the adoption and integration of IPv6 in the Education Curriculum Worldwide. The program has received laudatory comments of support from industry and government leaders from around the world, a few of which are listed here:

“We believe IPv6 Training will be quite necessary for the whole Internet industry and its users. There is huge demand in China, where IPv6 Internet is now considered as a national strategy,” states Liu Dong, Chair China IPv6 Council [17].

"Future Internet will be managed by current students and engineers in industry. It is highly required to provide IPv6 education to make them improve their knowledge and skill in IPv6 technology.” states Viho Cesar, IPv6 Ready Logo Regional Officer, IPv6 Forum Fellow, France [17].

"The IPv6 Curriculum study has abundantly demonstrated that hands-on IPv6 skills and field experience are dearly missing. Achieving parity between IPv4 and IPv6 deployment, quality expertise is the one pillar to focus on. This program is very welcome as it takes on this task globally." states Jacques Babot, IPv6 Team leader, European Commission [17].

3. DRIVERS OF IPv6 ADOPTION

3.1 IPv4 Address Space Depletion

In February of 2011 the Internet Addressing and Numbers Authority (IANA) allocated the final five /8 IPv4 address blocks to the five Internet Regional Internet Registries (RIRs). Now that these final allocations have been made, each RIR will continue to make allocations according to their own established policies until no more IPv4 addresses remain. For one RIR this event has already taken place. The Asia Pacific network Information Centre (APNIC) [20] exhausted its remaining IPv4 address space in April of 2011 [20]. According to the IPv6 Forum web site, the other four registries are projected to exhaust their remaining space by 2014, with the European registry, RIPE NNC expected to run out next sometime in late 2012 [14].
3.2 Proliferation of Managed Devices
Service providers and enterprise networks have a vast number of devices that must be addressed for management purposes. Typically the RFC 1918 private IPv4 address space was used for management of these devices. However, the number of managed devices on these networks has grown to the point that the IPv4 private address space is not large enough to support all devices that need to be managed. Examples include the deployment of residential broadband access such as Verizon’s FiOS, and the significant numbers of devices deployed by large Multiple Systems Operators (MSOs), such as COMCAST and Time Warner Cable. The entire RFC1918 private address space only yields 16,846,847 unique addresses. COMCAST alone has more than 50 million set-top boxes deployed to customers. With each set top box requiring 2 IPv addresses, one for management and one for customer connections, 100 million addresses are needed [8]. A request to the North American Regional Registry (ARIN) to increase the size of the private address space was rejected forcing organizations use public IPv4 space to manage their devices [23].

3.3 Proliferation of Mobile Wireless Devices
Cisco Systems, the world’s largest network equipment maker, has predicted an 18-fold increase in global mobile data traffic by 2016 due in part to the projected rapid growth in mobile devices connected to the Internet. Cisco further believes that the number of mobile Internet connected devices will exceed 10 billion by 2016 [3].

According to analysts at International Data Corporation (IDC), the worldwide mobile worker population will reach 1.19 billion in 2013—34.9 percent of the global workforce. Employees around the world are increasingly mobile and want to use their favorite smart phones and other mobile devices, such as tablets and e-readers, for both work and personal purposes [19].

This proliferation of connected mobile devices, is forcing service providers and network owners to migrate to the new IPv6 Internet addressing scheme, resulting in an increase of IPv6 traffic across carrier and enterprise networks [2].

3.4 Proliferation of Smart Devices
The term, Internet of Things, was used by Mark Weiser in the 1990’s in a Scientific American article to refer to the interconnection between everyday devices or objects over a network [4]. Today the term is used to describe the point at which there are more “things” connected to the Internet than people. Examples of such “things” are radio frequency identification devices (RFID) tags, smart sensors and actuators, and machine-to-machine communication devices. In 2008, Atmel, Cisco, Intel, SAP, and Sun Microsystems, along with other companies, founded the IP for Smart Objects (IPSO) corporate alliance. This alliance promotes the implementation and use of IP for low-powered devices such as radio sensors, electricity meters, and other smart objects. Additionally, the Internet Engineering Task Force (IETF) has set up the IPv6 over Low Power Wireless Area Networks (6LoWPAN) working group to address issues related to supporting IPv6 over the 802.15.4 wireless communication standard [11].

3.5 Government Initiatives
In September of 2010, the United States Office of the Federal Chief Information Officer issued a memorandum to all chief information officers of executive departments and agencies that detailed the federal government’s commitment to the timely operational deployment and use of IPv6. The memorandum mandated that all United States executive agencies shall upgrade public/external facing servers and services to operationally use native IPv6 by the end of fiscal year 2012 [16].

Cisco Systems outlines in their 2010 white paper, “The Role of Government in IPv6 Adoption”, the national strategies and initiatives established by governments around the world to encourage the transition to IPv6 [7].

- The European Commission – i2010 initiative, an action plan to see IPv6 widely adopted in Europe by 2010 [7].
- Peoples Republic of China – Next Generation Internet Project (CNGI), a five year plan to corner a significant proportion of the Internet by implementing IPv6 early. CNGI showcased its IPv6 network infrastructure at the 2008 Beijing Olympics [7].
- Hong Kong – The government established an IPv6-Enabled Government E-Service system in 2010 so that all 231 government websites can be accessed through IPv6 [7].
- Australia – A government strategy for agencies to implement IPv6 capable hardware and software platforms by 2012 and to operate dual-stack IPv6/v4 environments by 2012 [7].

4. CURRENT STATE AND TRENDS IN IPV6 ADOPTION
Statistics are showing that IPv6 adoption rates are rapidly increasing. According to the Global IPv6 Deployment Progress Report from Hurricane Electric, 85% of Top Level Domains (TLDs) now have IPv6 name servers and there are now more than 3,230,264 registered domains with IPv6 AAAA records, and 5682 registered IPv6 Autonomous Systems (AS). The number of tunnel broker accounts at Hurricane Electric has tripled in less than 2 years, growing from 100,000 in October of 2010 to 300,000 in May of 2012 [18].

In Akamai’s “The State of the Internet” 4th Quarter, 2011 report, growth of autonomous systems in the global IPv6 routing table during the fourth quarters of 2009, 2010, and 2011 grew at the rate of 11%, 13.7%, and 5.7% respectively [1].

Since 2008 Google has collected statistics measuring the availability of IPv6 connectivity among Google users. Their “IPv6 Statistics” site shows the percentage of Google users who are able to connect to Google.com in 2012 using IPv6, although still below 1%, has tripled from the previous year [12].

5. PREVIOUS EXPERIENCES DELIVERING IPV6 SPECIAL TOPICS CLASS
The Information Computer Technology (ICT) program at East Carolina University (ECU) offered its first IPv6 Special Topics as a pilot course during the summer semester of 2006. Due to student demand, the course has since been offered every other year as an elective summer course. Feedback obtained from the students through Student Opinion of Instruction Surveys (SOISs) and from industry partners has lead to the following areas of improvement for the course.
- The remote lab environment needs a more user-friendly graphical interface and an easier scheduling system. It should also have the capability for session sharing to allow for real-time collaboration between students and instructors.

- The curriculum should be certified by a recognized body and should map to an industry certification, preferably one that is also globally recognized.

- The class should include more synchronous “lecture” sessions in addition to more asynchronous recorded presentations for students to watch or download to mobile devices.

- More labs are needed to cover the course topics and the content of the labs should go into more depth.

- An industry partner is needed to guide the curriculum, provide advice on keeping course content current, provide internship and employment opportunities to students, and training for instructors.

The following sections of this paper describe how each of these improvements were implemented to create a new course based on IPv6 Forum certified curriculum, and designed to provide students with practical expertise and hands-on knowledge deploying IPv6.

6. IPv6 FOUNDATIONS COURSE

6.1 Working With An Industry Partner

Working with the Nephos6 Academy Program [12] in early 2012 we developed an IPv6 Foundations course that addressed each of the areas of improvement identified in our pilot course. The Nephos6 Academy provided ECU with curriculum certified by the IPv6 Forum that prepares students for the IPv6 Forum Certified Engineer (Silver) Exam [15]. Nephos6 additionally provided 10 labs modified to work on standard NETLAB+ pod topologies [22].

ECU is the pilot school in the Nephos6 Academy and was the first University to offer this course. The academy program is designed to introduce students to IPv6 and Cloud technologies and equip them with technical skills that compliment their chosen fields of study. The partnership with the Nephos6 Academy was instrumental in the successful development and offering of this course.

6.2 Class Delivery

The class was as a five week distance-education special topics class during the summer of 2012 to 28 students. Online synchronous lecture sessions were conducted by the instructor four nights each week using Saba Centra web conferencing software that allowed students to join the lecture session live or view a recording later. Asynchronous presentations were recorded by the instructor using Tegrity lecture capture software that is integrated with Blackboard. The software allowed the instructor to record presentations for students to view directly from the Blackboard web site or to be downloaded as a video file or podcast. A remote lab environment using NDG Lab Netlab+ provided students with 24/7 access to lab equipment [22].

6.3 Class Prerequisites

To maximize student success in the class, students must be familiar with Cisco IOS and basic networking concepts such as the OSI model, DNS, DHCP, IP addressing, and subnetting. For this course we required students to have completed the Cisco Networking Academy CCNA Routing course, or hold a current network certification such as Network + or CCNA as a prerequisite.

6.4 Course Topics

The topics for the course were mapped to the IPv6 Forum Certified Engineer (Silver) objectives. The curriculum used is IPv6 Forum Certified Curriculum (Silver) and provided as part of the Nephos6 Academy Program. The following topic areas were covered in the course:

- IPv6 Address Architecture and Scheme – IPv6 addresses, extension headers, Stateless Automatic Address Configuration (SLAAC), ICMPv6, and Default Address Selection (DAS).
- IPv6 Services – DHCPv6 and DNS.
- OS IPv6 Configuration – Windows 7 and Linux.
- IPv6 Device Configuration – Cisco IOS.
- Introduction to Tunneling - Manual Tunnels, ISATAP and 6to4 Tunnels.

6.5 Remote Lab Environment

Hands-on lab experience for the students was an essential element of this course. In the literature there are numerous examples showing that lab experience plays a critical role in student learning [5, 6, 10, 24, 25, 29].

Because this course was taught completely distance education, the labs had to be either remote or simulation. Literature shows that simulation software can limit student curiosity and experimentation [13]. Therefore, to allow students the fullest possible learning experience and maximum opportunities for experimentation the remote lab option was chosen.

The remote lab solution used for the course was the NETLAB+ server appliance by Network Development Group (NDG) [22]. NETLAB+ enables academic institutions to host physical lab equipment on the Internet for distance learning. NDG currently supports twelve courses offered by the Cisco Networking Academy, virtualization programs offered by the VMware IT Academy Program [26], and storage courses offered by the EMC Academic Alliance [9].

The lab equipment was physically located on the ECU campus and is shown in Fig. 1. Through the NETLAB+ system the lab resources could be scheduled, automated, and accessed remotely 24/7 by the students over the Internet through a web browser. The TCP Ports required to access the equipment are port 80 for the NETLAB+ web interface and TCP port 2201 for the remote equipment access.

Students can log into the remote lab environment through a web interface from any PC and browser connected to the Internet using the username and password provided by the instructor. Once logged in the student uses the Scheduler to schedule lab time on an available “pod”. Students can schedule reservations in advance for any day or time that is not already reserved by another student. The maximum duration of a reservation can be set by the instructor. At the end of a student lab reservation the Netlab+ server performs the following actions: (1) archive the final device...
configurations and command logs under the student’s account; (2) reset all equipment back to a pre-defined state; and (3) return any unused time back to the Scheduler for another student to use.

![Image](image-url)

**Fig. 1:** The Netlab+ server, six Cisco 1941 routers, and the ESXi servers.

### 6.6 Remote Lab Topology

Six Cisco 1941 routers were grouped into two “pods” with identical topologies, as shown in Fig. 2. Each of the two “pods” consisted of three Cisco 1941 routers running IOS release 15.2, two Windows 7 virtual machines, and two Linux CentOS virtual machines. The virtual machines were implemented in VMware using ESXi version 4.1 and managed through a VMware vCenter server [27]. The routers and virtual machines connect to the Netlab+ server appliance through an isolated control network. Because traffic on the two “pods” is isolated by the control network, both “pods” can be in use simultaneously by students without conflict.

The specific topology used was designed by ECU and the Nephos6 Academy to match existing “cookie-cutter” Cisco Networking Academy topologies that are supported by default in the NETLAB+ server appliance. This design makes it seamless for any academic institution that is currently using NETLAB+ to support Cisco Network Academy courses to implement the labs on any of the following NETLAB+ Topologies: Multi-purpose Academy POD; Cuatro Router POD; and Basic Router POD version 2 [22].

Using this topology the students completed the ten labs detailed in the next section as part of the IPv6 Foundations course. Each lab was designed to take a student about an hour to complete and integrates extensive use of the Wireshark protocol analyzer so students could see, visually, the operation of the IPv6 protocol.

![Image](image-url)

**Fig. 2:** The lab topology used for the course lab exercises.

### 6.7 Lab Exercise Details

Each student completed ten labs during the course on the Netlab+ remote lab environment. Final configurations and session logs were automatically saved by the Netlab+ server and were used by the instructor to verify lab completion. Students were encouraged to go beyond the scope of the labs and experiment with various IPv6 configurations and investigate IPv6 packets with Wireshark captures. By the end of the course the 28 students in the class logged 334 hours in the lab environment.

**Lab 1: IPv6 Hosts configuration**

In this lab the students first verify the network is fully converged with IPv4 before configuring IPv6 on the network devices. Next they examine the data structures using the Wireshark protocol analyzer. The learning objectives for this lab are: (1) validate the lab environment and device configurations as a baseline; (2) configure and verify IPv6 operation on Linux; (3) configure and verify IPv6 operation on Windows 7; (4) observe IPv6 header and packet format of actual packets on the wire.

**Lab 2: IPv6 on Cisco IOS configuration**

This lab begins with all devices configured for IPv4 and fully converged. Linux and Windows hosts are set to IPv4 and IPv6 default configurations. IPv6 static address and default gateways are then configured on the hosts. Next, IPv6 routing, interface addresses, and static routes are configured on the routers. Students use appropriate “show” commands to verify IPv6 operation and configuration on the routers. The learning objectives for this lab are: (1) validate route configuration; (2) understand IPv6 configuration on Cisco routers; (3) understand static IPv6 routes and importance of link-local addresses.

**Lab 3: Neighbor Discovery and SLAAC**

The network in this lab begins as a dual-stacked environment. Static IPv4 and IPv6 routes are configured and IPv6 Router Advertisements (RAs) are disabled at this point. Students use Wireshark to capture and analyze IPv6 Neighbor Discovery (ND) packets from the hosts and routers. Next, Stateless Address Auto Configuration (SLAAC) is enabled on the router LAN interfaces so RAs will be sent. Students again use Wireshark to capture and analyze the RA packets send by the routes. The students also observe the protocol configurations, IPv6 neighbor cache, and routing tables of the Linux and Windows hosts. The learning objectives for this lab are: (1) understand ND and SLAAC concepts and configuration; (2) use and understand Cisco, Linux,
and Windows Neighbor Discovery Protocol (NDP) commands and appropriate “show” commands; (3) understand the various IPv6 address types.

**Lab 4: DHCPv6**

In this lab the routers are dual-stacked and hosts are set to auto-configure IPv4 and IPv6 addresses. The Linux Core server is acting as a DHCPv6 server. A second DHCPv6 server is configured on the Athens LAN Linux server. Students observe default IPv6 SLAAC operation with Wireshark. Next, students change the NDP configuration on the Athens router so that LAN hosts will use DHCPv6. Students capture and analyze RA and Router Solicitation (RS) packets with Wireshark. The students also use Windows and Linux commands to observe the protocol configurations, IPv6 neighbor cache, and routing tables. The learning objectives for this lab are: (1) observe and understand the interplay between RA and RS packets in the operation of DHCPv6; (2) configure hosts and routers to support a fully converged DHCPv6 environment; (3) identify various NDP packets and their functions in the DHCPv6 process.

**Lab 5: OSPFv3**

This lab begins with a dual-stacked network using static routes for both IPv4 and IPv6 convergence. Students implement multi-area OSPFv3 and use Cisco IOS show and debug commands to observe the OSPFv3 neighboring process. The learning objectives for this lab are: (1) understand the basic steps to configuring OSPFv3 on a Cisco router; (2) understand the operation OSPFv3 uses to form neighbor relationships; (3) understand the purpose and configuration of OSPFv3 summarization; (4) understand the purpose and configuration of OSPFv3 interface cost metrics.

**Lab 6: EIGRP for IPv6**

The lab begins with the network in a dual-stacked state with static routes. Students implement EIGRP for IPv6 and use Cisco IOS show and debug commands to observe the EIGRP for IPv6 neighboring process. The learning objectives for this lab are: (1) understand the basic steps to configuring OSPFv3 on a Cisco router; (2) understand the operation EIGRP for IPv6 uses to form neighbor relationships; (3) understand the purpose and configuration of EIGRP for IPv6 redistribution between Autonomous Systems (ASs); (4) understand the purpose and configuration of EIGRP for IPv6 routing preferences using the administrative distance.

**Lab 7: DNS**

In this lab students perform AAAA queries and add new AAAA records over both IPv4 and IPv6 connections. Students use Wireshark to capture and analyze DNS traffic on the network. The learning objectives for this lab are: (1) understand the hierarchical nature of DNS and the impact that has on the IPv6 deployment; (2) verify the sending of DNS queries occurs as expected, and under what conditions this process varies; (3) observe Destination Address Selection (DAS) at work.

**Lab 8: ISATAP**

The ISATAP lab allows an IPv6 host located within an IPv4-only enterprise network environment to obtain IPv6 services by tunneling the IPv6 packets inside IPv4 packets to the target IPv6-enabled device. Students configure ISATAP on a workstation to obtain limited IPv6 connectivity, then, configure an ISATAP router on the Core to provide more robust IPv6 services to the ISATAP enabled workstations. Wireshark is used to capture and observe ISATAP packets on the network. The learning objectives for this lab are: (1) describe the most common use for ISATAP technology; (2) observe and understand Windows 7 default ISATAP behavior; (3) understand the limitations of using link-local-only ISATAP implementations; (4) configure an ISATAP router and understand its role in ISATAP operations.

**Lab 9: Manual IPv6-in-IPv4 Tunnels**

This lab begins with the network running IPv4 and network convergence provided by OSPF. IPv6 is then enabled to dual-stack the network and two IPv6-in-IPv4 manual tunnels are configured. Finally, students configure OSPFv3 to route IPv6 packets between the isolated IPv6 networks across the IPv4 core. The learning objectives for this lab are: (1) understand manual IPv6-in-IPv4 tunnel encapsulation and addressing semantics; (2) recognize the scaling limitations of manual tunnels; (3) understand the concepts of virtual interfaces and virtual point-to-point links.

**Lab 10: 6to4 Automatic Tunnels**

The network will begin as an IPv4 only network. Then the Rome pc will be configured for IPv6 only while the Athens-pc will be dual-stacked. The two site routers will be dual-stacked and 6to4 tunnels configured. Students will send ICMP packets from the dual-stacked Athens-pc across the IPv4 only core to the Rome-pc using the 6to4 tunnel. The learning objectives for this lab are: (1) understand automatic 6to4 tunnels, specifically the 6to4 encapsulation and addressing semantics; (2) recognize the scaling benefits of 6to4 automatic tunnels versus manual tunneling; (3) observe and understand the traffic flow from a 6to4 site to another 6to4 site and a native IPv6 site.

**6.8 Nephos6 Academy Program**

The Nephos6 IT Academy Program is an important component of Nephos6 education programs. The academic institutions that agree to participate in the Nephos6 IT Academy Program are business alliances of Nephos6 with an objective of delivering educational services to their students at high quality standards. Eligibility to become a Nephos6 Academy is open to accredited, degree-granting higher education institutions worldwide offering 2- or 4- year college programs and technical schools offering accredited degrees through distance education programs [21].

**6.9 Future Plans**

We are currently working with the Nephos6 Academy to create an advanced IPv6 topics class that will cover topics such as ISIS, MP-BGP, MPLS, IPv6 Multicast, and Mobile IPv6 and an IPv6 Security class. These classes will follow a similar format to the IPv6 Foundations course using the Netlab+ remote lab environment and with curriculum that will map to IPv6 Forum certifications.

We are also working with the Nephos6 Academy to grow the network of colleges and universities participating in the academy. We freely offer our experiences and knowledge to other institutions interested in incorporating IPv6 into their curriculum.

**7. GLOBAL RECOGNIZED IPV6 CERTIFICATION**

We place a high value in our courses mapping to industry recognized certification. The curriculum in our IPv6 Foundations class maps to the IPv6 Forum Certified Engineer (Silver).

The IPv6 Forum launched the IPv6 Education Certification Logo Program in 2010 with the intent of acceleration, adoption, and
integration of IPv6 in the education curriculum worldwide. The program defines and certifies courses, engineers and trainers with Silver and Gold Logo levels and requires IPv6 implementation on the web site of the education program.

8. CONCLUSION
It is vital that our ICT program provides the knowledge and hands-on skills our students will need in tomorrow’s information society. We view close relationships with our industry partners as a key component to this objective. The IPv6 Fundamentals class is a case study in the successful collaboration between industry and education.

9. REFERENCES