# AC 2007-1962: TEACHING A LABORATORY-BASED IPV6 COURSE IN A DISTANCE EDUCATION ENVIRONMENT

**Philip Lunsford, East Carolina University**

Phil Lunsford received a B.S. in Electrical Engineering and a M.S. in Electrical Engineering from Georgia Institute of Technology and a Ph.D. in Electrical Engineering from North Carolina State University. He is a registered professional engineer and is currently an Assistant Professor at East Carolina University. His research interests include system simulation, telemedicine applications, and information assurance.

**John Pickard, East Carolina University**

John Pickard has more than 15 years in the Technical training profession and 9 years experience in the information technology field. John has held various positions and has experience involving management, designing, testing and teaching of data networks, enterprise networking systems, digital switching systems and transmission systems. Currently, John is a faculty member at East Carolina University and holds an instructor position in the Department of Technology Systems. John is also a senior trainer at Network Training and Consulting and teaches courses in networking, project management, and Cisco systems networking solutions. He holds a MBA from Wayland Baptist University. He also holds various industry certifications to include; A+, Network+, MCSE, MOUS, and CCNP.

**Chip Popoviciu, Cisco Systems, Inc.**

Dr. Ciprian Popoviciu, CCIE, is a Technical Leader at Cisco Systems with over nine years of experience in data and voice over IP communications technologies. As part of Cisco's Network Solution Integration Test Engineering (NSITE) organization, he currently focuses on the architecture, design and validation of large IPv6 network deployments in direct collaboration with Service Providers and Enterprises worldwide. Ciprian is a regular speaker or chair at conferences and industry events and contributes to various technology publications. He is an active contributor to the IETF standards, he is a Senior member of IEEE and member of several academic advisory boards. Ciprian is co-author of the "Deploying IPv6 Networks" book.

# TEACHING A LABORATORY-BASED IPV6 COURSE IN A DISTANCE EDUCATION ENVIRONMENT


## Abstract

Internet Protocol version 6 (IPv6) is being integrated into the Internet but often networking courses only present a brief overview of the new protocol. We present a case study of the laboratory development for a special topics course on IPv6 taught during the summer semester of 2006 in a distance education environment. The course emphasized a hands-on approach to network deployment and students were required to configure IPv6 networks using Cisco routers that were housed in an isolated lab. Extensive use of a remote access system developed at our university allowed remote students to access the console ports of the Cisco routers and perform configuration and troubleshooting tasks. Suggestions for future lab enhancement include integrating Linux-based networking devices, adding the use of a SmartBits system for traffic generation and network characterization, and Windows Vista. Course content was developed and delivered using Blackboard.


## Introduction

Internet Protocol version 6 (IPv6) is the new internet protocol that is being phased in, and will eventually replace the standard IPv4 that most networks currently use. IPv6 adoption in the United States has been slow so far, especially when compared to that of the European Union, China, Japan, and Korea, who have all made transitioning to IPv6 a national priority. But it appears that is all about to change rather quickly. In August of 2005, the Office of Management and Budget (OMB) mandated that by June of 2008 all federal agency infrastructures must be using IPv6 and agency networks must interface with this infrastructure[1]. This mandate follows in the footsteps of the similar one issued by the Department of Defense in 2003 which spurred the IPv6 interest in US.

In order to address the dearth of IPv6 information in standard IT curriculum, a special topics course at East Carolina University was offered during the summer of 2006. In order to provide access to the widest audience, it was offered in a distance education (DE) environment. Students were able to complete the entire course without being on campus. The motivation to offer the course DE was also driven by the university policies on faculty line generation for summer courses.

The university has "global" classroom equipped with audio-visual equipment. Lectures were streamed live on the internet for student viewing and also archived for student review or for students that had schedule conflicts. Students viewing the live stream also have the option to join a chat room to ask questions to the instructor. The course was delivered using Blackboard to distribute and collect assignments, post grades, and post announcements.

**DE Laboratory Access**

The main development effort in the course was to supply laboratory exercises for DE students. Our past experience offering advanced networking courses in a DE environment served as a basis for developing the lab exercises, the student access management, and the hardware configuration.

Labs were conducted on equipment located on campus. Equipment was accessible to students anywhere with an Internet connection via secure shell (port 22) using IPv4 through an access server running custom scheduling software as shown is figure 1. This access topology and scheduling software was already developed and used in our DE advanced IPv4 networking courses.

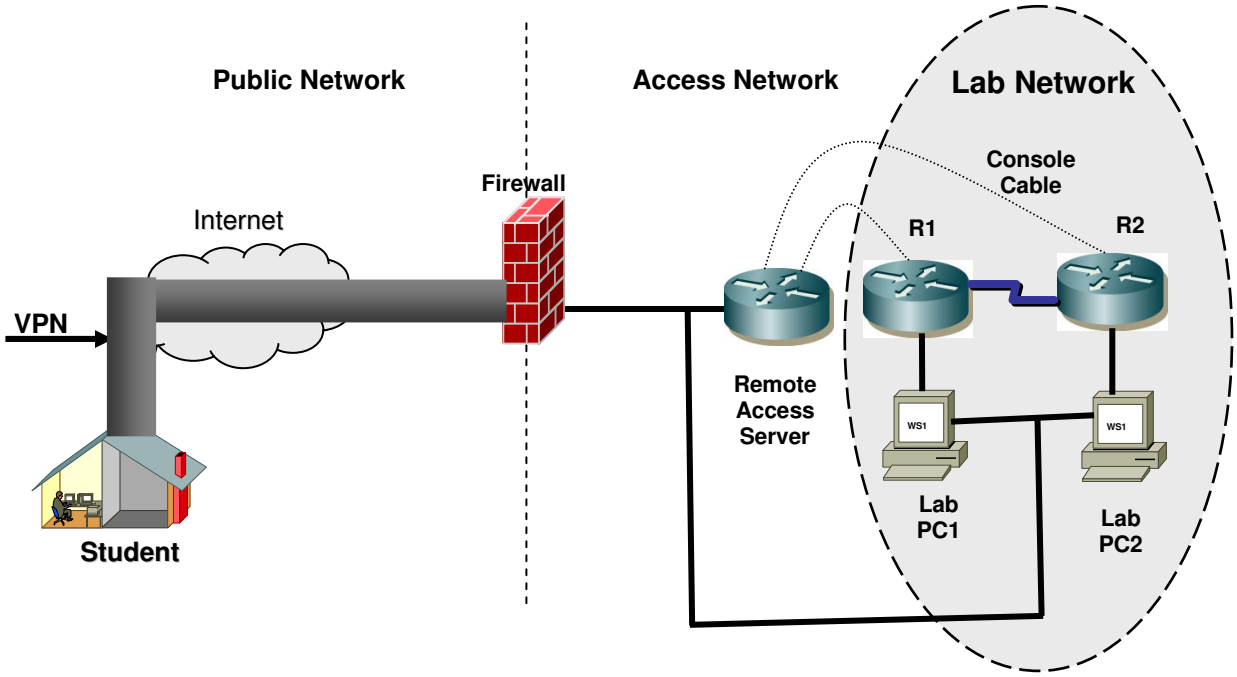


Figure 1. Remote Access Methodology

As shown in figure 1, the student uses Internet access to create a VPN tunnel based on SSL to the lab firewall. This firewall is a Linux-based machine with locally developed software that controls concurrent access to the lab network. Students must authenticate to the firewall and schedule a reservation to perform the lab exercise. During the reservation time, only the student with the valid reservation is allowed to pass through the firewall and use the access network to control the devices in the lab network. The remote access server is a router with serial interfaces that allow the student direct access to the console port of the lab routers (in this case R1 and R2). Each lab PC has two network interface cards (NICs), one NIC for accessing the lab network, and one NIC for remote control by the student through the access network. The lab network in figure

1 is a simple network shown just as an example. A group of network devices, in this case two PCs and two routers, are referred to as a pod. Figure 1 only shows one pod, but the lab firewall can provide student access to multiple pods, each with a different configuration. For the case of multiple pods, different students can concurrently access different pods, but for a given pod, only one student has access at a given time. Students can reserve a pod up to 1 week in advance and for as long as 6 hours. At the end of each reservation, each pod is 'scrubbed' automatically by the firewall to return all lab devices to an initial state. This scrubbing ensures that configuration changes performed by an earlier student will not interfere or affect the performance of the pod during a later reservation for a different student.

**DE Laboratory Configuration**

The course used two pods shown in figures 2 and 3. These figures do not show the access network for simplification. The pod topologies are complex, but still can support simple topologies. Interfaces that are not needed can simply be turned off by the student. For example, figure 4 shows a fairly simple example of a lab topology that would be given to the student. The student could configure this topology using pod 2 by:

- All routers: Turn off all frame relay interfaces
- Router R1: Turn off interfaces Fa0/0, S0/0/0, Fa0/1, S0/2/0, S0/2/1, BRI0/0
- Router R2: Turn off interfaces S0/2/0, Fa0/1, S0/2/1,S0/3/1, BRI0/0, Fa0/0
- Router R3: Turn off interface S0/2/0
- Router R4: Turn off interface E0, S0/3/1

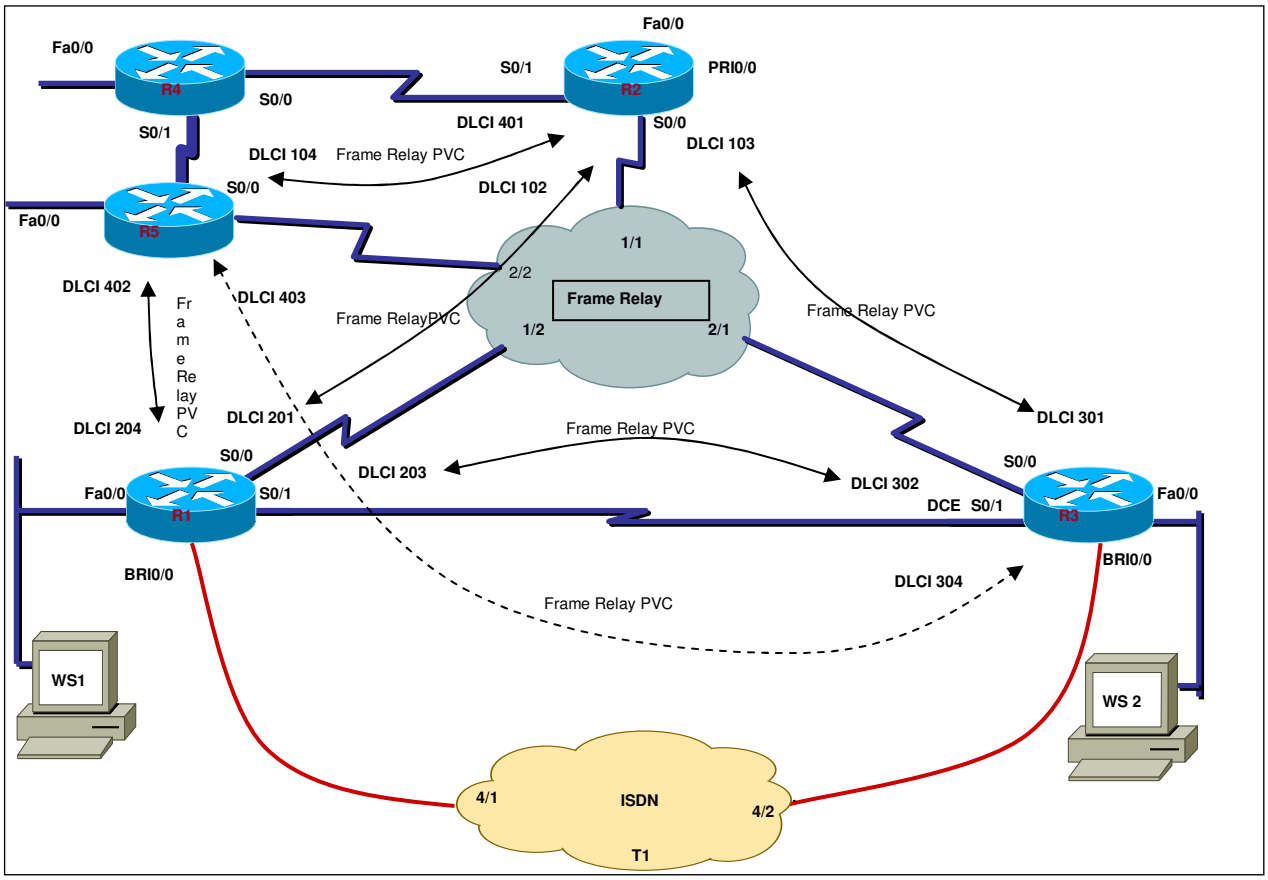

Figure 2. Pod 1 topology

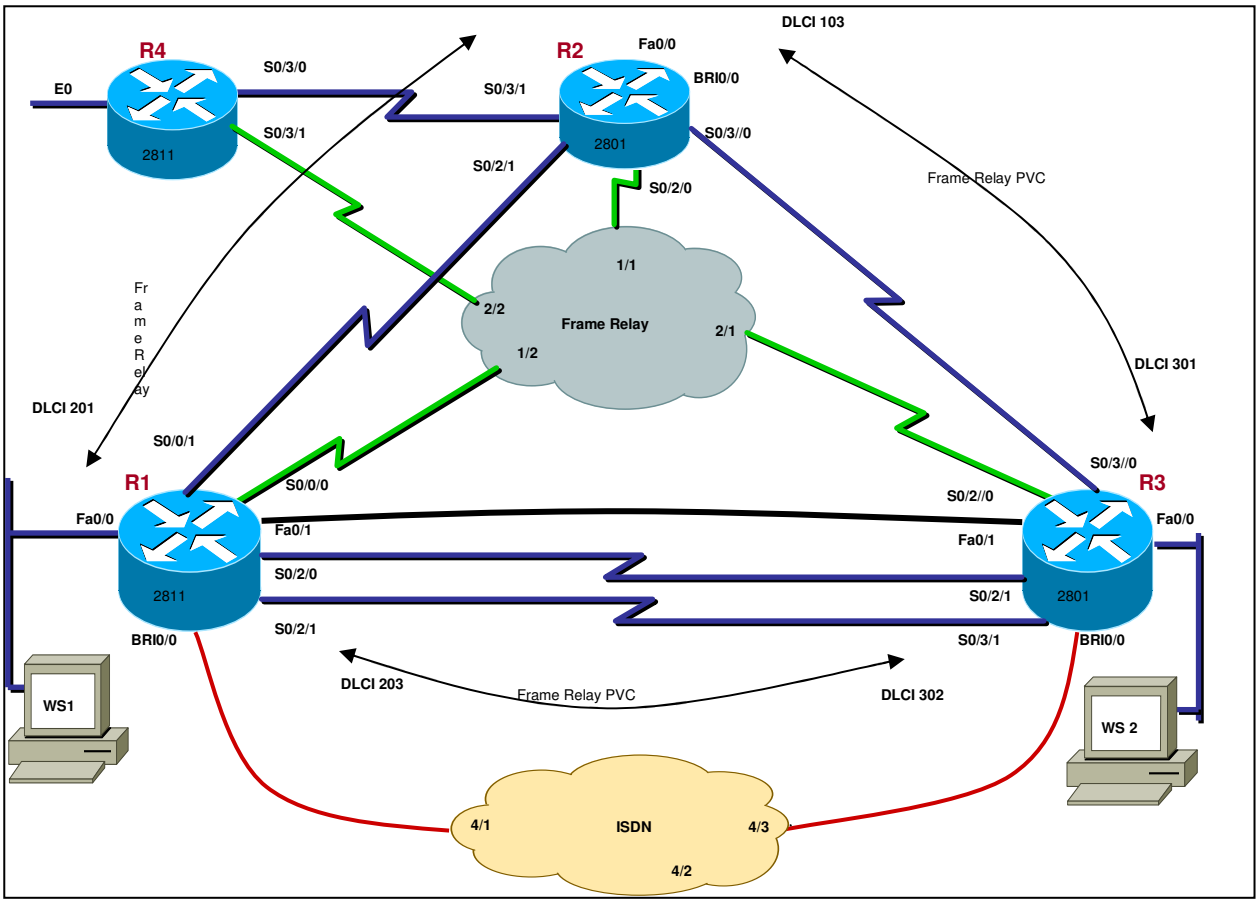

Figure 3. Pod 2 topology

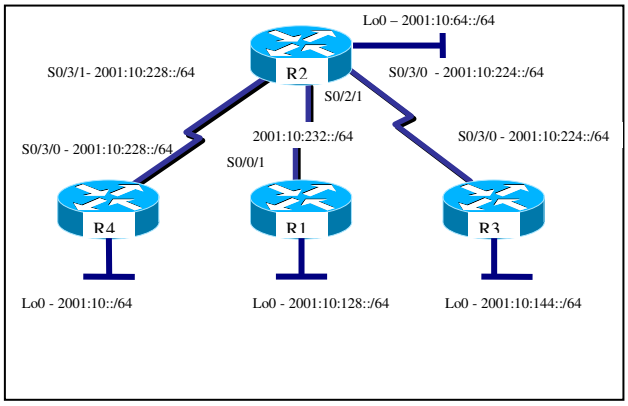

Figure 4. Simple network topology

The course used two pods shown in figures 2 and 3. These figures do not show the access network for simplification. The pod topologies are complex, but still can support simple

topologies. Interfaces that are not needed can simply be turned off by the student. For example, figure 4 shows a fairly simple example of a common lab topology that would be given to the student. The student could configure this topology using pod 2 by:

- All routers: Turn off all frame relay interfaces
- Router R1: Turn off interfaces Fa0/0, S0/0/0, Fa0/1, S0/2/0, S0/2/1, BRI0/0
- Router R2: Turn off interfaces S0/2/0, Fa0/1, S0/2/1,S0/3/1, BRI0/0, Fa0/0
- Router R3: Turn off interface S0/2/0
- Router R4: Turn off interface E0, S0/3/1

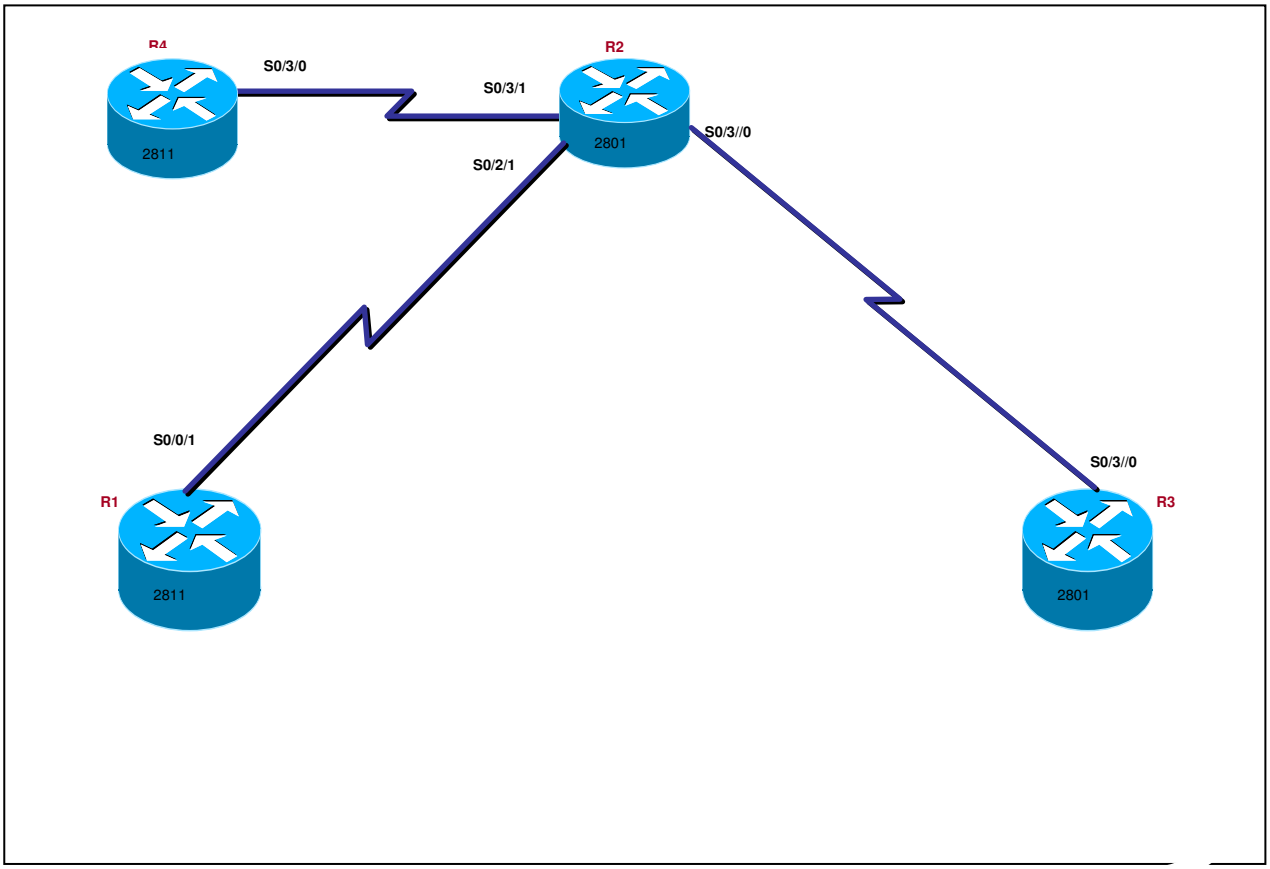


Figure 5. Pod 2 topology configure for the equivalent topology shown in figure 4.

**Laboratory Topics and Observations**

The following topics were covered in the laboratory exercises:

- Simple IPv6 commands
- RIPng
- OSPF for IPv6
- ISIS for IPv6
- Dual stack topologies (IPv4 and IPv6)
- Stateless Autoconfiguration
- 6 to 4 tunnels

Lab development was based on the new aspects of IPv6 and also the laboratory exercises of the existing IPv4 networking courses.

One problem that was encountered was the capabilities of the existing routers. All routers required at least an operating system upgrade, and most also required a RAM upgrade. Pod 1 consists of five Cisco 2600 series routers that were purchased as part of a Cisco CCNP Academy bundle. The router IOS was upgraded to c2600-advipservicesk9-mz.12.3-21.bin and memory upgrades were installed to allow for at least 96 MB RAM and 32 MB of Flash memory. Pod 2 uses Cisco 2800 series routers. The IOS was upgraded to c2800nm-advipservicesk9-mz.124-7.bin for the 2811s and c2801-adventerprisek9-mz.123-14.T5.bin for the 2801 routers. The routers in pod 2 did not require a memory upgrade.

Future offerings of the course could be improved in many ways.

- Linux based routing systems such as Quagga could be integrated into the lab exercises.
- Microsoft Vista operating system could be used on the host machines. This is especially pertinent since the default protocol for Vista is IPv6. Vista will first try to connect to a network using IPv6, and if that fails, then use IPv4.
- Linux based PC's could be used as endpoints. The current pod configurations exclusively use Windows XP.
- A Smartbits system could be integrated into a pod to allow for performance testing of the network or a single network device. Typical implementations of IPv6 include dual stack (both IPv4 and IPv6) configurations. Running two protocols greatly increases the load on network devices and affects measurements such as CPU utilization, memory utilization, and network convergence. By designing lab exercises where these issues are shown and measured would greatly enhance the effectiveness of the course.

A more detailed look at the motivation for the course and the development of the course content can be found in the article "IPv6: A Course Development and Delivery Case Study" [2].

**Conclusion**

A special topics course covering IPv6 with extensive laboratory exercises was successfully taught in a DE environment. Access to the laboratory equipment allowed students to configure real, not simulated, IPv6 networks with complex topologies using access topologies that are

entirely IPv4 based. The network equipment can be set up once using complex topologies, and then a wide variety of effective topologies can be configured by turning off interfaces that are not needed. Careful consideration of network device capabilities is needed when developing an IPv6 course as many older devices may not support the new protocol. Lastly, this course should eventually be phased out because the existing basic and advanced networking courses that are currently based on IPv4 will eventually cover all aspects of IPv6 as it becomes more widely adopted.

**Bibliography**

1. David A. Powner and Keith A. Rhodes, "Internet Protocol Version 6. Federal Government in Early Stages of Transition and Key Challenges Remain", United States Government Accounting Office Report to the Chairman, Committee on Government Reform, House of Representatives, June 2006.
2. John Pickard, Philip Lunsford, and Chip Popoviciu, "IPv6 Course Development for Information Technology Curriculums", under review for publication in the proceedings to the ASEE 2007 Annual Conference & Exposition.