

# IPv6 for Security Professionals

## Fact Sheet

**Course Title:** IPv6 for Security Professionals

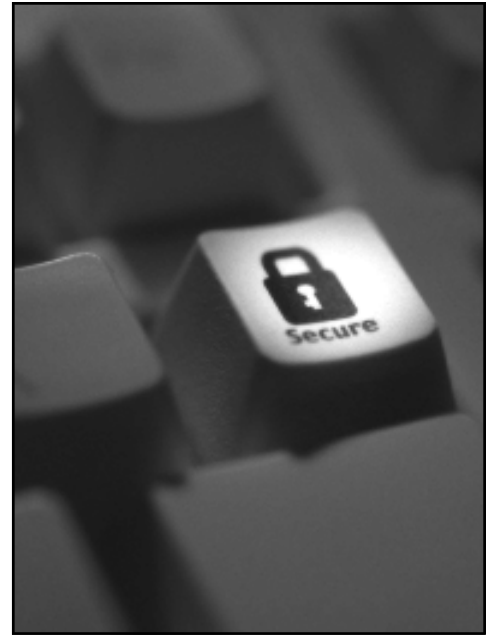
**Course Duration:** 4 days

**Course Type:** Instructor led training with over 10 hours of lab exercises

**Intended Audience:** Network and system security engineers and administrators that will be responsible for the rollout of secure IPv6-based networks

**Prerequisites:** Attendees should have a solid knowledge of IPv6, a basic knowledge of network security, and familiarity with operational security challenges.

**CISSP CPE Credit:** *This course qualifies as a Type A CPE credit under the CISSP Certification Program*



---

### Course Overview

Now, more than ever, organizations are beginning to consider the sweeping impact of IPv6 technology. With the enhanced next generation protocol, organizations will face new security issues and concerns. This

course is designed to provide Network Security personnel with an introduction to the fundamentals of IPv6, and help them develop a broad understanding of the transition process, focusing on some of the more salient security ramifications of IPv6 integration and the change in the overall IT security model when IPv6 is introduced. By working with our IPv6 security SMEs, participants will gain the practical knowledge required to contend with the new security paradigm that IPv6 creates.

***“IPv6 training is a critical next step for anyone in the security field. This course is one of the best IPv6 security courses I’ve seen.”*** Andrew Afifi,  
Managing Director and Founder, CISSP.com

### Course Basics

Subject materials covered in this course include an overview of IPv6 fundamentals, followed by a detailed examination of IPv6 security issues. Included topics are: IPv6 address structure; Neighbor Discovery; Path MTU and fragmentation; DNS/DHCP Security; IPsec implementation and routing; and IPv6 transition issues. Advanced security topics such as multicasting and multihoming are also covered.

***For more information and course schedules, please contact us at 866.456.IPv6 or [ipv6training@commandinformation.com](mailto:ipv6training@commandinformation.com)***



Native6 courseware provided by Command Information, Inc.

### COURSE OUTLINE

- |                                   |   |
|-----------------------------------|---|
| 1. Introduction to IPv6           | 11. IPsec For IPv6                          |
| 2. IPv6 Header Formats            | 12. Security in an IPv6 Environment         |
| 3. IPv6 Address Structure         | 13. Protecting Network Infrastructure       |
| 4. Neighbor Discovery (ND)        | 14. IPv6 & Routing                          |
| 5. Path MTU & Fragmentation       | 15. Transition Overview                     |
| 6. IPv6 DNS                       | 16. Transition-related security issues      |
| 7. DHCPv6                         | 17. Advanced Topics – Multicasting and IPv6 |
| 8. DNS/DHCPv6 Security            | 18. Multihoming                             |
| 9. Renumbering                    | 19. Consequences of NAT-free environment    |
| 10. IPv6 Security Concepts Review | 20. Securing an IPv6 environment            |

### INFRASTRUCTURE LABS

*Enabling IPv6 on a node*

*TCP wrappers on IPv6, ipchains*

*Enabling IPv6 on a router*

*Enabling OSPFv3*

*Neighbor discovery & autoconfiguration*

*Implementing authenticated OSPF*

*DNS implementation with IPv6 records*

*Establishing IPv6 tunnels*

*Renumbering*

*Enabling ISATAP*

*Using IPsec in an IPv6 environment*

*IPSec-based VPN with ISATAP*

*Securing IPv6 host-to-host communications*

*Implementing 6to4*

**For a more detailed outline, additional information or course schedules, please contact us at 866.456.IPv6 or [ipv6training@commandinformation.com](mailto:ipv6training@commandinformation.com)**