

# Securing IPv6

(3 days)

How to securely test and implement IPv6 on your networks.

## About this Course

IPv6 is now widely available. In some organisations and parts of the world IPv6 is in common use.

Whilst you may not have implemented IPv6 in your network yet, you still need to secure your network against abuse using IPv6 protocols.

Modern network operating systems, including Windows Vista and Windows Longhorn, use IPv6 in preference to IPv4 and have IPv6 turned on by default.

You need to ensure that your network is IPv6 secure and that you are ready for any future implementation of IPv6.

IPv6 brings many new security challenges and opportunities. New security techniques need to be understood and implemented. The transition to IPv6 from IPv4 presents particular security issues.

This course covers IPv6 security in detail. Each area is explained and practical guidance on mitigating each security threat is provided.

## Who Should Attend

This course is intended for IT security experts and network administrators.

A good knowledge of general networking concepts is assumed. Experience of IPv4 is necessary

## You will learn

- The current status of IPv6
- The security features of IPv6
- IPv6 security risks
- The differences in IPv4 and IPv6 security
- The risks associated with IPv6 transition mechanisms.
- How to mitigate the security risks associated with IPv6.
- How to build IPv6 firewalls.
- IPv6 security best practice.

## Relevant Platforms:

This briefing applies to all platforms, including:

- Linux & Unix
- FreeBSD
- AIX
- HP-UX
- Solaris
- Cisco IOS
- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Longhorn

## Course Contents

### IPv6 Basics

- Comparison of IPv6 and IPv4
- What is IPv6?
- Why is IPv6 required?
- Address Space
- Is there an address shortage?
- IPv6 improvements over IPv4
- New features in IPv6
- The benefits of IPv6
- Motivations to implement IPv6
- IPv6 status summary
- Timescale predictions

### Key IPv6 Protocols

- IPv6 addresses
- ICMPv6
- Neighbor discovery
- Router discovery
- Router Renumbering
- RIPng
- OSPFv3
- BGP and IPv6
- Multicast and IPv6
- IPv6 IPSec
- IPv6 Mobility
- IPv6 and QoS
- Dual stack

### IPv6 Transition Mechanisms

#### Threats

- Dual stack
- 6to4
- 6over4
- ISATAP
- Teredo
- BIS and BIA
- SIIT and NAT-PT
- DSTM
- TRT

### IPv6 Security (IPSec)

- Cryptographic techniques
- IPv6 and IPSec
- IPv6 AH & ESP Headers
- Transport and tunnel modes
- Security associations
- ISAKMP & IKE

### IPv6 Security Features

- Security features in IPv6
- Mobile IPv6 security
- Dynamic routing security
- Examples of IPv6 security

### IPv6 Security Threats

- Summary of IPv6 threats
- Comparison of IPv6 with IPv4 threats
- Threats common to IPv4 and IPv6
- IPv6 specific security threats
- End-to-end transparency
- Scanning in IPv6
- IPv6 extension header threats
- IPv6 router header abuse
- IPv6 fragmentation threats
- ICMPv6 threats
- Neighbor discovery threats
- ND threat examples

### Securing Neighbor Discovery

- Neighbor discovery threats
- Privacy addresses
- Temporary addresses
- Cryptographically Generated Addresses (CGA)

- SEcure Neighbor Discovery (SEND)
- Security at the datalink
- IEEE 802.1X

### IPv6 Transition Security Threats

- IPv6 transition mechanisms threats
- Transition mechanisms
- Transition security problems
- Dual stack threats
- Mitigating dual stack threats
- Tunnelling threats
- 6to4 threats
- Mitigating 6to4 threats
- ISATAP threats
- Mitigating ISATAP threats
- Teredo threats
- Mitigating Teredo threats
- Other mechanisms
- IPv6 DNS threats
- Transition security best practice

### Building IPv6 Firewalls

- Configuring IPv6 firewalls
- IPv6 firewall filtering rules
- Filtering ICMPv6
- IPv6 extension headers
- Implementing IPv6 Ingress filtering
- Assigned IPv6 addresses
- Status of IPv6 firewalls
- Deploying IPv6 firewalls

### IPv6 Deployment Risks

- IPv6 pilots
- IPv6 DNS server
- Addressing schemes
- Deploying ICMPv6
- End-to-end transparency
- IPSec transport mode
- Reduced functionality
- Operational issues
- ND proxies
- Training

### IPv6 Security Best Practice

- Creating an IPv6 security policy
- Summary of IPv6 security best practice

## Practicals

Each topic has an associated exercise or demonstration. Delegates choose to do exercises on Linux, Windows or Cisco IOS.

Hands-on practicals include:

- Basic IPv6 configurations
- Configuring IPv6 IPSec
- Using privacy and temporary addresses
- Implementing SEND and CGA
- Securing transition mechanisms
- Configuring IPv6 firewalls

## The Trainers

Erion's trainers are practising IPv6 consultants with extensive experience of IPv6.

Further information can be found at:  
[www.ipv6training.com](http://www.ipv6training.com)  
[www.ipv6consultancy.com](http://www.ipv6consultancy.com)  
[www.erion.co.uk](http://www.erion.co.uk)