Implementing and Securing IPv6 on Linux

How to plan implement and secure IPv6 on Linux **(5 days)**

Relevant Platforms:

RHEL, Ubuntu, Suse, Debian, CentOS, etc...

You will learn how to

- Migrate your network to IPv6
- Manage the differences between IPv4 and IPv6
- Implement new networking software and devices to support IPv6
- Implement IPv6 auto-configuration and manage IPv6 addresses
- Configure IPv6 migration techniques on different platforms.
- Configure transition techniques including; dual-stacks, 6to4, ISATAP and Teredo.
- Configure IPv6 on different platforms
- Configure IPv6 enabled network services (e.g DNS, DHCPv6, OSPFv3 and BGP)
- IPv6 enable networking applications (e.g. Apache, ping, FTP and e-mail)
- Write code using the basic IPv6 socket API
- Migrate legacy code to IPv6
- Use code migration tools
- The security features of IPv6
- IPv6 security risks
- The differences in IPv4 and IPv6 security
- Security threats of IPv6 transition mechanisms
- How to securely deploy IPv6
- How to secure your IPv4 network from IPv6 threats
- IPv6 threat mitigation
- How to build IPv6 firewalls

Course Benefits

IPv6 is the result of many years of research and activity by the international Internet community. IPv6 provides increased addressing space, improved routing, new features and support for transition from IPv4.

The implementation of IPv6 is inevitable and will impact on all companies that maintain, implement or use IP networks.

In this course, you will learn how to obtain, implement and secure IPv6 and related protocols within your organisation on Linux. This course provides extensive hands-on sessions and in-depth technical analysis.

Who Should Attend

This course is ideal for network administrators, network support personnel, network designers, networking consultants, security managers, IT managers and directors.

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

Course Contents

The Need for IPv6 *(Summary)*

- History of IP
- The problems with IPv4
- The IPv4 header format
- Address space & functionality
- IPv4 Security and QoS
- Reality Check: IPv6 vs IPv4

The Features of IPv6 I

- IPv6 datagram format and header
- IPv6 extension headers
- Hop-by-hop and destination options
- Routing header, fragmentation header
- Mobility header and No next header
- IPv6 addresses
- IPv6 address representation
- Unicast Multicast & Anycast in IPv6
- Link local, site local and unique local addresses

The Features of IPv6 II

- Summary of the new features of IPv6
- ICMPv6
- Path MTU discovery (PMTU)
- IPv6 multicast group management
- MLD and MLDv2

Auto-configuration of IPv6 I

- Autoconfiguration methods
- Choosing the interface identifier
- Modified EUI-64
- CGA, HBA, Privacy and Temporary Addresses
- Neighbour discovery in IPv6 (NDP)
- IPv6 router discovery (RS and RA)
- IPv6 Router renumbering

Auto-configuration of IPv6 II

- DHCPv6
- DHCPv6 Relay Agents
- DUIDs and IAIDs
- Stateless DHCPv6
- DHCPv6 prefix delegation (PD)

Internetworking IPv6 *(Summary)*

- IPv6 routing and IPv6 routing tables
- IPv6 default routes

IPv6 Dynamic Routing

- ICMPv6 redirects
- RIPng
- OSPFv3
- IS-IS and IPv6
- EIGRPv6
- BGP4 & IPv6
- IPv6 multicast dynamic routing
- IPv6 PIM

Interfacing IPv6 to the Lower Layers

- The Data-link and the physical layer
- Point to point and IPv6
- IPv6 over PPP
- NBMA networks and IPv6
- IPv6 over ATM
- IEEE802 and IPv6
- IPv6 in 3G, 4G, LTE and IMS
- MPLS and IPv6
- 6PE and 6VPE
- RADIUS and IPv6

The Transport Layer and IPv6 *(Summary)*

- Operation of TCP and UDP
- Changes to TCP for IPv6
- Changes to UDP for IPv6

IPv6 Transition Mechanisms I

- Overview of IPv6 transition mechanisms
- IPv6 dual stacks
- IPv4 compatibility addresses
- Automatic and configured tunnelling
- 6over4 and 6to4
- 6rd - IPv6 rapid deployment
- ISATAP
- Teredo
- Dual stack lite (DSLite)
- Dual stack transition mechanism
- IPv6 Tunnel brokers
- Tunnel setup protocol

IPv6 Transition Mechanisms II

- Protocol translators
- SIIT
- Application layer gateways
- NAT64 and DNS64
- NAT-PT & NAPT-PT
- TRT
- IPv6 SOCKS
- BIS and BIA
- Transition mechanisms and DNS

IPv6 Security (IPsec)

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

Mobile IPv6

- Mobile IPv4 vs Mobile IPv6
- Mobile IPv6 Home agents
- Binding updates & binding cache
- Mobile IPv6 in operation
- Mobile IPv6 Security
- NEMO

IPv6 and Quality of Service

- Traffic class in IPv6
- The IPv6 Flow label
- Differential services (DiffServ)
- Integrated services (IntServ)
- Traffic flows in IPv6
- RSVP and IPv6 QoS

DNS and IPv6

- Changes to DNS for IPv6
- Historic DNS support for IPv6
- IPv6 AAAA resource records
- PTR records and IPv6
- Reverse lookups in IPv6
- ip6.arpa. & ip6.int.

IPv6 Application Changes *(Summary)*

- Basic Internet commands
- IPv6 ping, telnet and FTP
- Mail systems and IPv6
- IPv6 enabled web-servers

The IPv6 Programming Interface

- The basic IPv6 programming API
- IPv4 socket API vs IPv6 socket API
- Address structures
- Socket functions
- Name resolution
- Interface identification
- New constants, macros and header files
- Sockets and Winsock
- Support for IPv6 in Perl, Java and C#

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

Company Registration: 3521142

VAT Number: 698 3633 78

- IPv6 fragmentation threats
- ICMPv6 threats
- IPv6 neighbor discovery (ND) threats
- ND threat examples

IPv6 Security Features

- Security features in IPv6
- Mobile IPv6 security
- RA-Guard and DHCPv6-Shield
- Dynamic routing security
- Examples of IPv6 security

Securing Neighbor Discovery

- Neighbor discovery threats
- Privacy addresses
- Temporary addresses
- Monitoring Neighbor Discovery (ND)
- Mitigating Router Advertisement (RA) attacks
- Cryptographically Generated Addresses (CGA)
- SEcure Neighbor Discovery (SEND)
- Security at the datalink
- IEEE 802.1X
- Securing Router Advertisements (RAs)

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

Hands-on IPv6 Practical Labs

Each module includes detailed exercises. Lab work will be carried out on Linux servers & workstations.

Hands-on IPv6 practical exercises include:

- Installing and configuring IPv6
- Capturing and decoding IPv6 datagrams
- Basic IPv6 operation
- IPv6 router configuration
- Assigning IPv6 addresses
- Configuring IPv6 auto-configuration
- Configuring and using DHCPv6
- IPv6 dynamic routing (OSPFv3 & BGP)
- Security configuration using IPv6 IPsec
- Configuring IPv6 transition mechanisms
- Configuring 6to4, ISATAP, Teredo, NAT64 etc.
- Configuring and testing Mobile IPv6
- Examining QoS and IPv6
- Network monitoring of IPv6
- Upgrading and configuring IPv6 DNS servers
- Configuring IPv6 applications and services
- Writing code using the basic IPv6 socket API
- Examining IPv6 threats
- Using the IPv6 hackers toolkit
- Using Scapy and IPv6
- Configuring IPv6 IPsec
- Using privacy and temporary addresses
- Protecting against router advertisement attacks
- Detecting and mitigating ND attacks
- Implementing SEND and CGA
- Securing transition mechanisms including 6to4, ISATAP, Teredo and NAT64
- Configuring IPv6 firewalls
- IPv6 security policy and best practice

The IPv6 Trainers

Trainers are practising IPv6 consultants with extensive experience of IPv6. Further information can be found at www.erion.co.uk.

Erion is the world's leading IPv6 training company.

Erion
Certified IPv6 Training