6net

IPv6

Deployment Guide

Javvin Technologies Inc. Distribution

An IPv6 Deployment Guide

Editor: Martin Dunmore

Javvin Technologies Inc. Distribution

http://www.javvin.com
http://www.networkdictionary.com

Table of Contents

TABLE OF CONTENTS ..... **I**

LIST OF FIGURES ..... **VII**

LIST OF TABLES ..... **IX**

PART I IPV6 FUNDAMENTALS **1**

CHAPTER 1 INTRODUCTION **3**

1.1 THE HISTORY OF IPV6 3
1.2 THE 6NET PROJECT 5

CHAPTER 2 IPV6 BASICS **7**

2.1 DATAGRAM HEADER 7
2.2 HEADER CHAINING 9
2.3 ROUTING HEADER 11
2.4 FRAGMENTATION 12
2.5 OPTIONS 13

CHAPTER 3 ADDRESSING **15**

3.1 ADDRESSING ESSENTIALS 15
3.2 UNICAST ADDRESSES 16
3.3 INTERFACE IDENTIFIER – MODIFIED EUI-64 17
3.4 ANYCAST ADDRESSES 18
3.5 MULTICAST ADDRESSES 19
3.6 REQUIRED ADDRESSES AND ADDRESS SELECTION 19
3.7 REAL-WORLD ADDRESSES 21

CHAPTER 4 ESSENTIAL FUNCTIONS AND SERVICES **24**

4.1 NEIGHBOUR DISCOVERY 24
4.1.1 Router Discovery *25*
4.1.2 Automatic Address Configuration *25*
4.1.3 Duplicate Address Detection *26*
4.1.4 Neighbour Unreachability Detection *27*
4.1.5 Router Configurations for Neighbour Discovery *27*
4.2 THE DOMAIN NAME SYSTEM 42
4.2.1 Overview of the DNS *42*
4.2.2 DNS Service for 6NET *43*
4.2.3 DNS Service Implementation *44*
4.3 DHCPV6 52
4.3.1 Using DHCP Together With Stateless Autoconfiguration *52*
4.3.2 Using DHCP Instead of Stateless Autoconfiguration *52*
4.3.3 Overview of the Standardisation of DHCPv6 ..... *52*
4.3.4 Overview of the DHCPv6 Specifications *54*
4.3.5 DHCPv6 Implementations Overview *55*

CHAPTER 5 INTEGRATION AND TRANSITION **59**

5.1 PROBLEM STATEMENT 59
5.1.1 Dual Stack *60*
5.1.2 Additional IPv6 Infrastructure (Tunnels) *61*
5.1.3 IPv6-only Networks (Translation) *61*
5.2 TUNNELLING METHODS 62
5.2.1 Configured Tunnels *62*
5.2.2 Tunnel Broker *62*
5.2.3 Automatic Tunnels *64*
5.2.4 6to4 ..... *64*

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

5.2.5 6over4 ... *65*
5.2.6 ISATAP ... *65*
5.2.7 Teredo ... *66*
5.2.8 Tunnel Setup Protocol ... *67*
5.2.9 Dual Stack Transition Mechanism (DSTM) ... *67*
5.2.10 The Open VPN based Tunnelling Solution ... *70*
5.3 TRANSLATION METHODS ... 74
5.3.1 SIIT, NAT-PT and NAPT-PT ... *74*
5.3.2 Bump in the Stack ... *74*
5.3.3 Bump in the API ... *76*
5.3.4 Transport Relay ... *77*
5.3.5 SOCKS ... *79*
5.3.6 Application Layer Gateway ... *79*
5.3.7 The 'Trick or Treat' DNS-ALG ... *80*
5.4 CONFIGURATION EXAMPLES: DUAL STACK ... 82
5.4.1 Dual-stack VLANs ... *82*
5.5 CONFIGURATION EXAMPLES: TUNNELLING METHODS ... 86
5.5.1 Manually Configured Tunnels ... *86*
5.5.2 6over4 ... *94*
5.5.3 6to4 ... *94*
5.5.4 ISATAP ... *100*
5.5.5 OpenVPN Tunnel Broker ... *106*
5.5.6 DSTM ... *116*
5.6 CONFIGURATION EXAMPLES: TRANSLATION METHODS ... 125
5.6.1 NAT-PT ... *125*
5.6.2 ALG ... *127*
5.6.3 TRT ... *134*

CHAPTER 6 ROUTING ... 140

6.1 OVERVIEW OF IP ROUTING ... 140
6.1.1 Hop-by-hop Forwarding ... *140*
6.1.2 Routing Tables ... *141*
6.1.3 Policy Routing ... *142*
6.1.4 Internet Routing Architecture ... *143*
6.1.5 Is IPv6 Routing Any Different? ... *145*
6.2 IMPLEMENTING STATIC ROUTING FOR IPV6 ... 146
6.2.1 Cisco IOS ... *146*
6.2.2 Juniper JunOS ... *148*
6.2.3 Quagga/Zebra ... *149*
6.3 RIP ... 151
6.3.1 RIPng Protocol ... *151*
6.4 IMPLEMENTING RIPNG FOR IPV6 ... 153
6.4.1 Cisco IOS ... *154*
6.4.2 Juniper JunOS ... *161*
6.4.3 Quagga ... *165*
6.5 IMPLEMENTING IS-IS FOR IPV6 ... 167
6.5.1 Cisco IOS ... *167*
6.5.2 Juniper JunOS ... *177*
6.6 IMPLEMENTING OSPF FOR IPV6 ... 181
6.6.1 LSA Types for IPv6 ... *181*
6.6.2 NBMA in OSPF for IPv6 ... *182*
6.6.3 Cisco IOS ... *183*
6.6.4 Juniper JunOS ... *186*
6.6.5 Quagga ... *189*
6.7 IMPLEMENTING MULTIPROTOCOL BGP FOR IPV6 ... 192
6.7.1 Cisco IOS ... *192*
6.7.2 Juniper JunOS ... *201*
6.7.3 Quagga/Zebra ... *201*

CHAPTER 7 NETWORK MANAGEMENT ... 204

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

7.1 MANAGEMENT PROTOCOLS AND MIBS IN THE STANDARDISATION PROCESS 204
7.1.1 SNMP for IPv6 204
7.1.2 MIBs 205
7.1.3 The Other Standards 206
7.1.4 Flow Monitoring (IPFIX, Netflow...) 206
7.1.5 Management of IPv6 Protocols and Transition Mechanisms 207
7.1.6 Remaining Work to be Done 207
7.2 NETWORK MANAGEMENT ARCHITECTURE 207
7.2.1 Conceptual Phase 207
7.2.2 Implementation Phase - Management Tools Set 209
7.3 MANAGEMENT TOOLS DEPLOYED IN 6NET 210
7.3.1 Management Tools for Core Networks (WAN) 211
7.3.2 Management Tools for End-sites (LAN) 214
7.3.3 Tools for all Networks 217
7.4 RECOMMENDATIONS FOR NETWORK ADMINISTRATORS 218
7.4.1 Network Management Architecture 218
7.4.2 End-site Networks 218
7.4.3 Core Networks 218

CHAPTER 8 MULTICAST 220

8.1 ADDRESSING AND SCOPING 220
8.1.1 Well Known / Static Addresses 222
8.1.2 Transient Addresses 222
8.1.3 Summary 224
8.2 MULTICAST ON THE LOCAL LINK 224
8.2.1 Multicast Listener Discovery (MLD) 224
8.2.2 MLD Snooping 225
8.3 BUILDING THE MULTICAST TREE: PIM-SMV2 225
8.4 INTER-DOMAIN MULTICAST 226
8.4.1 The ASM Case 226
8.4.2 The SSM Case 229
8.4.3 Future Work 230
8.5 MRIB - MULTICAST ROUTING INFORMATION BASE 230
8.5.1 Extensions to BGP (MBGP) 231

CHAPTER 9 SECURITY 232

9.1 WHAT HAS BEEN CHANGED IN IPV6 REGARDING SECURITY? 232
9.1.1 IPSec 232
9.1.2 IPv6 Network Information Gathering 233
9.1.3 Unauthorised Access in IPv6 networks 234
9.1.4 Spoofing in IPv6 Networks 235
9.1.5 Subverting Host Initialisation in IPv6 Networks 235
9.1.6 Broadcast Amplification in IPv6 Networks 236
9.1.7 Attacks Against the IPv6 routing Infrastructure 237
9.1.8 Capturing Data in Transit in IPv6 Environments 237
9.1.9 Application Layer Attacks in IPv6 Environments 237
9.1.10 Man-in-the-middle Attacks in IPv6 Environments 237
9.1.11 Denial of Service Attacks in IPv6 Environments 238
9.2 IPV6 FIREWALLS 239
9.2.1 Location of the Firewalls 239
9.2.2 ICMP Filtering 242
9.3 SECURING AUTOCONFIGURATION 245
9.3.1 Using Stateless Address Autoconfiguration 245
9.3.2 Using Privacy Extensions for Stateless Address Autoconfiguration 245
9.3.3 Using DHCPv6 245
9.3.4 Static Address Assignment 246
9.3.5 Prevention techniques 246
9.3.6 Fake router advertisements 246
9.4 IPV4-IPV6 CO-EXISTENCE SPECIFIC ISSUES 248
9.4.1 General Management Issues with Tunnels 248

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

9.4.2 IPv6-in-IPv4 tunnels ... *249*
9.4.3 6to4 ... *251*
9.4.4 ISATAP ... *253*
9.4.5 Teredo ... *253*
9.4.6 GRE Tunnels ... *255*
9.4.7 OpenVPN Tunnels ... *255*
9.4.8 Dual-stack ... *256*
9.4.9 DSTM ... *257*
9.4.10 NAT-PT/NAPT-PT ... *258*
9.4.11 Bump in the API (BIA) ... *259*

CHAPTER 10 MOBILITY ... 260

10.1 BINDINGS CACHE ... 260
10.2 HOME AGENT OPERATION ... 261
10.3 CORRESPONDENT NODE OPERATION ... 262
10.4 BINDING CACHE COHERENCE ... 263
10.4.1 Binding Update Messages ... *263*
10.4.2 Binding Acknowledgement Messages ... *264*
10.4.3 Binding Request Messages ... *264*
10.4.4 Binding Update List ... *264*
10.5 PROXY NEIGHBOUR DISCOVERY ... 264
10.6 HOME ADDRESS OPTION ... 265
10.7 HOME AGENT DISCOVERY ... 265
10.8 THE MOBILITY HEADER ... 266
10.9 THE RETURN ROUTABILITY METHOD ... 267
10.10 AVAILABLE IMPLEMENTATIONS ... 268
10.11 DEPLOYMENT CONSIDERATIONS ... 269
10.11.1 Hardware Requirements ... *269*
10.11.2 Software Requirements ... *270*
10.12 CISCO MOBILE IPV6 ... 271
10.12.1 Available Feature Set ... *271*
10.12.2 How to Get it ... *271*
10.12.3 Installation ... *271*
10.12.4 Configuration ... *272*
10.12.5 Configuration Commands ... *272*
10.12.6 Operation ... *275*
10.13 MOBILE IPV6 FOR LINUX ... 276
10.13.1 How to get it ... *276*
10.13.2 Installation ... *276*
10.13.3 Configuration ... *277*
10.13.4 Usage Notes/Problems ... *280*
10.14 KAME MOBILE IPV6 ... 281
10.14.1 How to get it ... *281*
10.14.2 Installation ... *281*
10.14.3 Configuration ... *282*
10.14.4 Remarks ... *284*

CHAPTER 11 APPLICATIONS ... 286

11.1 THE NEW BSD SOCKETS API ... 287
11.1.1 Principles of the New API Design ... *287*
11.1.2 Data Structures ... *288*
11.1.3 Functions ... *290*
11.1.4 IPv4 Interoperability ... *296*
11.2 OTHER PROGRAMMING LANGUAGES ... 296
11.2.1 Python ... *296*
11.2.2 Java ... *298*

PART II CASE STUDIES ... 301

CHAPTER 12 IPV6 IN THE BACKBONE ... 303

12.1 6NET BACKBONE CASE STUDY ... 303

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

12.1.1 Network Topology ... *304*
12.1.2 Addressing Scheme ... *304*
12.1.3 Naming Scheme ... *309*
12.1.4 DNS ... *311*
12.1.5 IGP Routing ... *311*
12.1.6 EGP Routing ... *314*
12.2 SURFNET CASE STUDY (NETHERLANDS) ... 316
12.2.1 The SURFnet5 Dual Stack network ... *316*
12.2.2 Customer Connections ... *317*
12.2.3 Addressing plan ... *317*
12.2.4 Routing ... *319*
12.2.5 Network Management and Monitoring ... *319*
12.2.6 Other Services ... *320*
12.3 FUNET CASE STUDY (FINLAND) ... 322
12.3.1 History ... *322*
12.3.2 Addressing Plan ... *324*
12.3.3 Routing ... *325*
12.3.4 Configuration Details ... *326*
12.3.5 Monitoring ... *329*
12.3.6 Other Services ... *329*
12.3.7 Lessons Learned ... *330*
12.4 RENATER CASE STUDY (FRANCE) ... 331
12.4.1 Native Support ... *331*
12.4.2 Addressing and Naming ... *331*
12.4.3 Connecting to Renater 3 ... *332*
12.4.4 The Regional Networks ... *333*
12.4.5 International Connections ... *333*
12.4.6 Tunnel Broker Service Deployment ... *334*
12.4.7 Network Management ... *335*
12.4.8 IPv6 Multicast ... *336*
12.5 SEEREN CASE STUDY (GRNET) ... 337
12.5.1 SEEREN Network ... *337*
12.5.2 Implementation Details of CsC/6PE Deployment ... *339*

CHAPTER 13 IPV6 IN THE CAMPUS/ENTERPRISE ... 341

13.1 CAMPUS IPV6 DEPLOYMENT (UNIVERSITY OF MÜNSTER, GERMANY) ... 341
13.1.1 IPv4 ... *342*
13.1.2 IPv6 ... *343*
13.1.3 IPv6 Pilot ... *344*
13.1.4 Summary ... *352*
13.2 SMALL ACADEMIC DEPARTMENT, IPV6-ONLY (TROMSØ, NORWAY) ... 354
13.2.1 Transitioning Unmanaged Networks ... *354*
13.2.2 Implementation of a Pilot Network ... *355*
13.2.3 Evaluation of the Pilot Network ... *360*
13.2.4 Conclusions ... *362*
13.3 LARGE ACADEMIC DEPARTMENT (UNIVERSITY OF SOUTHAMPTON) ... 364
13.3.1 Systems Components ... *364*
13.3.2 Transition Status ... *370*
13.3.3 Supporting Remote Users ... *372*
13.3.4 Next Steps for the Transition ... *372*
13.3.5 IPv6 Transition Missing Components ... *373*
13.4 UNIVERSITY DEPLOYMENT ANALYSIS (LANCASTER UNIVERSITY) ... 374
13.4.1 IPv6 Deployment Analysis ... *374*
13.4.2 IPv6 Deployment Status ... *378*
13.4.3 Next Steps ... *380*
13.5 OTHER SCENARIOS ... 384
13.5.1 Early IPv6 Testbed on a Campus ... *384*
13.5.2 School Deployment of IPv6 to Complement IPv4+NAT ... *385*
13.5.3 IPv6 Access for Home Users ... *385*
13.6 SUMMARY OF UNEXPECTED RESULTS AND UNFORESEEN DIFFICULTIES ... 385

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

13.7 SUMMARY OF TRADEOFFS MADE IN SOLUTIONS CHOSEN 386

CHAPTER 14 IPV6 ON THE MOVE 387

14.1 FRAUNHOFER FOKUS 387
14.1.1 MIPL-HA 388
14.1.2 Kame-HA 388
14.1.3 MCU-CN 389
14.1.4 IPSec 389
14.2 TESTBED COMPONENTS 389
14.3 LANCASTER UNIVERSITY 391
14.3.1 The Testbed 391
14.3.2 Components 392
14.3.3 Addressing and Subnetting 393
14.3.4 Testing 394
14.4 UNIVERSITY OF OULU 400
14.4.1 Testbed 400
14.4.2 Handover Performance 400

BIBLIOGRAPHY 403

GLOSSARY OF TERMS AND ACRONYMS 412

APPENDICES 419

APPENDIX A1: LIST OF PER-POP LOCATION SUPPORT DOMAINS 419

APPENDIX A2: SYSTEMS PROVIDING DNS SERVICE FOR 6NET 420

APPENDIX B: ENABLING IPV6 423

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

List of Figures

Figure 2-1 Basic IPv6 Datagram Header 7
Figure 2-2 IPv4 and IPv6 Header Comparison 9
Figure 2-3 Header Chaining Examples 11
Figure 2-4 Changes in the Routing Header During Datagram Transport 12
Figure 3-1 Structure of the Global Unicast Address 16
Figure 3-2 Real-world Structure of the Global Unicast Address 17
Figure 3-3 Conversion of MAC Address to Interface Identifier 18
Figure 3-4 Structure of the IPv6 Multicast Address 19
Figure 3-5 Structure of the Real-world Global Unicast Address Prefix 22
Figure 5-1 Tunnel broker components and setup procedure 63
Figure 5-2 6to4 Service Overview 64
Figure 5-3 Teredo Infrastructure and Components 66
Figure 5-4 DSTM Architecture 68
Figure 5-5 Tunnel Broker Scenario 70
Figure 5-6 Interaction of tunnel broker components 71
Figure 5-7 Types of Tunnel Broker Clients 72
Figure 5-8 The BIS Protocol Stack 75
Figure 5-9 The BIA Protocol Stack 76
Figure 5-10 Transport Relay Translator in Action 78
Figure 5-11 ALG Scenario 80
Figure 5-12 Sample Address Assignment and Routing Configuration 111
Figure 5-13 Sample Subnet Routing 111
Figure 5-14 Test Network Infrastructure 116
Figure 5-15 Example Setup of Faithd TRT 137
Figure 6-1 Classical IP Forwarding 141
Figure 6-2 Internet Routing Architecture 144
Figure 6-3 RIPng Message 152
Figure 7-1 The Unified MIB II 206
Figure 8-1 The MSDP Model 227
Figure 8-2 Embedded-RP Model 228
Figure 8-3 MRIB and RIB 231
Figure 9-1 Internet-router-firewall-protected Network Setup 240
Figure 9-2 Internet-firewall-router-protected Network Setup 241
Figure 9-3 Internet-edge-protected Network Setup 241
Figure 10-1 MIPv6 Routing to Mobile Nodes (Pre Route Optimisation) 262
Figure 10-2 Mobile IPv6 Routing to Mobile Nodes (Post Route Optimisation) 262
Figure 10-3 The Mobility Header Format 266
Figure 10-4 Return Routability Messaging 267
Figure 10-5 Simple Mobile IPv6 Testbed 269
Figure 11-1 Partial Screenshot of the Applications Database 286
Figure 12-1 The 6NET Core and NREN PoPs 304
Figure 12-2 6NET IS-IS Topology 312
Figure 12-3 BGP peering with 6NET participants 314
Figure 12-4 Logical topology for SURFnet5 317
Figure 12-5 Anonymous-FTP over IPv6 volume 320
Figure 12-6 Funet Network by Geography 323
Figure 12-7 Funet Network by Topology 324
Figure 12-8 The Renater3 PoP Addressing Scheme 331
Figure 12-9 Density of IPv6 Connected Sites on Renater3 332
Figure 12-10 The Renater3 Network 334
Figure 12-11 The RENATER Tunnel Broker 335
Figure 12-12 IPv6 Traffic Weathermap 336
Figure 12-13 SEEREN Physical Network Topology 337
Figure 12-14 SEEREN Logical Topology 338
Figure 12-15 Label Exchange in the CsC Model 338
Figure 12-16 Routing Exchange in SEEREN 339
Figure 13-1 Ideal Overview of University's IPv4 Network 342
Figure 13-2 IPv6 Test Network 344

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Figure 13-3 Overview of Tromsø and Transmission Points 356
Figure 13-4 Topology Overview 357
Figure 13-5 Traffic Statistics of Røstbakken Tower and faithd 360
Figure 13-6 Use of IPv6 VLANs at Southampton 370
Figure 13-7 MRTG Monitoring Surge Radio Node (top) and RIPE TTM view (bottom) 372
Figure 13-8 Basic Configuration of the Upgrade Path 378
Figure 13-9 Alternative Configuration Providing Native IPv6 to the Computing Dept 380
Figure 14-1 Schematic Representation of the Testbed Setup 388
Figure 14-2 Lancaster University MIPv6 Testbed 391
Figure 14-3 Simple MIPv6 Handover Testbed 396
Figure 14-4 Processing Router Solicitations 397
Figure 14-5 University of Oulu Heterogeneous Wireless MIPv6 Testbed 400
Figure 14-6 TCP Packet Trace During Handover from AP-5 to AP-4 401
Figure 14-7 TCP Packet Trace During Handover from AP-4 to AP-5 402

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

List of Tables

Table 2-1 Extension Headers 10
Table 2-2 Hop-by-hop Options 13
Table 2-3 Destination Options 14
Table 3-1 IPv6 Address Allocation 21
Table 3-2 Global Unicast Address Prefixes in Use 21
Table 5-1 The Teredo Address Structure 66
Table 8-1 IPv6 Multicast Address Format 220
Table 8-2 The Flags Field 220
Table 8-3 Multicast Address Scope 221
Table 8-4 Permanent IPv6 Multicast Address Structure 222
Table 8-5 Unicast Prefix-based IPv6 Multicast Address Structure 223
Table 8-6 Embedded RP IPv6 Multicast Address Structure 223
Table 8-7 SSM IPv6 Multicast Address Structure 223
Table 8-8 Summary of IPv6 Multicast Ranges Already Defined (RFCs or I-D) 224
Table 9-1 Bogon Filtering Firewall Rules in IPv6 234
Table 9-2 Structure of the Smurf Attack Packets 236
Table 9-3 ICMPv6 Recommendations 244
Table 10-1 Mobile IPv6 Bindings Cache 261
Table 10-2 IPv6 in IPv6 Encapsulation 261
Table 10-3 IPv6 Routing Header Encapsulation 263
Table 10-4 Mobile IPv6 Home Address Option 265
Table 10-5 Available MIPv6 Implementations 268
Table 10-6 MIPL Configuration Parameters 278
Table 11-1 Values for the Hints Argument 293
Table 12-1 6NET Prefix 305
Table 12-2 PoP Addressing 306
Table 12-3 SLA Usage 306
Table 12-4 Switzerland Prefixes 307
Table 12-5 Loopback Addresses 307
Table 12-6 6NET PoP to NREN PoP Point-toPoint-Links 308
Table 12-7 Point-to-point links between 6NET PoPs 309
Table 12-8 Link Speed IS-IS Metric 313
Table 12-9 CLNS Addresses 314
Table 12-10 SURFnet Prefix 318
Table 12-11 SURFnet prefixes per POP 318
Table 14-1 Fokus MIPv6 Testbed Components 389
Table 14-2 Lancaster MIPv6 Testbed Components 392
Table 14-3 Results of RA Interval Tests 397
Table 14-4 Using Unicast RAs 398
Table 14-5 Handover Duration and TCP Disruption Time 401

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

PART I

IPv6 Fundamentals

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 1

Introduction

Internet Protocol version 6 (IPv6) is the new generation of the basic protocol of the Internet. IP is the common language of the Internet, every device connected to the Internet must support it. The current version of IP (IP version 4) has several shortcomings which complicate, and in some cases present a barrier to, the further development of the Internet. The coming IPv6 revolution should remove these barriers and provide a feature-rich environment for the future of global networking.

1.1 The History of IPv6

The IPv6 story began in the early nineties when it was discovered that the address space available in IPv4 was vanishing quite rapidly. Contemporary studies indicated that it may be depleted within the next ten years – around 2005! These findings challenged the Internet community to start looking for a solution. Two possible approaches were at hand:

1. Minimal: Keep the protocol intact, just increase the address length. This was the easier way promising less pain in the deployment phase.
2. Maximal: Develop an entirely new version of the protocol. Taking this approach would enable incorporating new features and enhancements in IP.

Because there was no urgent need for a quick solution, the development of a new protocol was chosen. Its original name IP Next Generation (IPng) was soon replaced by IP version 6 which is now the definitive name. The main architects of this new protocol were Steven Deering and Robert Hinden.

The first set of RFCs specifying the IPv6 were released at the end of 1995, namely, RFC 1883: Internet Protocol, Version 6 (IPv6) Specification [RFC1883] and its relatives. Once the definition was available, implementations were eagerly awaited. But they did not come.

The second half of the nineties was a period of significant Internet boom. Companies on the market had to solve a tricky business problem: while an investment in IPv6 can bring some benefits in the future, an investment in the blossoming IPv4 Internet earns money now. For a vast majority of them it was essentially a no-brainer: they decided to prefer the rapid and easy return of investments and developed IPv4-based products.

Another factor complicating IPv6 deployment was the change of rules in the IPv4 domain. Methods to conserve the address space were developed and put into operation. The most important of these was Classless Inter-Domain Routing (CIDR). The old address classes were removed and address assignment rules hardened. As a consequence, newly connected sites obtained significantly less addresses than in previous years.

The use of CIDR may well have delayed the need for IPv6 in the eyes of many people, but not in all. Somewhat perversely, the use of CIDR accelerated the perception of a lack of address space in the

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 2

IPv6 Basics

Inside this chapter we cover the protocol basics: the datagram format, the headers and related mechanisms. You will see that these aspects have been simplified significantly in comparison to IPv4 to achieve higher performance of datagram forwarding.

2.1 Datagram Header

The core of the protocol is naturally the datagram format defined in RFC 2460 [RFC2460]. The datagram design focused mainly on simplicity - to keep the datagram as simple as possible and to keep the size of the headers fixed. The main reason for this decision was to maximise processing performance - simple constant size headers can be processed quickly, at or very close to wire-speed.

The IPv4 header format contains a lot of fields including some unpredictable optional ones leading to fluctuating header sizes. IPv6 shows a different approach: the basic header is minimised and a constant size. Only essential fields (like addresses or datagram length) are contained. Everything else has been shifted aside into so called extension headers, which are attached on demand - for example a mobile node adds mobility related extension headers to its outgoing traffic.

Figure 2-1 Basic IPv6 Datagram Header

The basic datagram header format is showed in Figure 2-1. The contents of individual fields are following:

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 3

Addressing

Rapid depletion of the available IPv4 address space was the main initiator of IPv6. In consequence, the demand to never again have to develop a new protocol due to the lack of addresses was one of the principal requirements to the new address space design. Let's look how it was fulfilled.

The basic rules of IPv6 addressing are laid down by RFC 3513 [RFC3513]. Some accompanying RFCs define the specialties and rules for specific address types.

3.1 Addressing Essentials

The address length has been increased significantly to expand the available address space. The IPv6 address is 128 bits (or 16 bytes) long, which is four times as long as its predecessor. Because every single bit of added address length doubles the number of addresses available, the size of the IPv6 address space is really huge. It contains 2^{128} which is about 340 billion billion billion billion different addresses which definitely should suffice for a very long time.

Addresses are written using 32 hexadecimal digits. The digits are arranged into 8 groups of four to improve the readability. Groups are separated by colons. So the written form of IPv6 address looks like this:

2001:0718:1c01:0016:020d:56ff:fe77:52a3

As you can imagine DNS plays an important role in the IPv6 world, because the manual typing of IPv6 addresses is not an easy thing. Some abbreviations are allowed to lighten this task at least a little. Namely: leading zeroes in every group can be omitted. So the example address can be shortened to

2001:718:1c01:16:20d:56ff:fe77:52a3

Secondly, a sequence of all-zero groups can be replaced by pair of colons. Only one such abbreviation may occur in any address, otherwise the address would be ambiguous. This is especially handy for special-purpose addresses or address prefixes containing long sequences of zeroes. For example the loopback address

0:0:0:0:0:0:0:1

may be written as

::1

which is not only much shorter but also more evident. Address prefixes are usually written in the form:

prefix::/length

Where prefix defines the value of bits in the address beginning and length contains the number of important bits from the start. Because the rest of the prefix is not important, zeroes are used in this part

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 4

Essential Functions and Services

This chapter looks at what we consider to be 'essential' functions and services of IPv6. In other words, without these functions and services we would not be able to achieve satisfactory IPv6 operation (or even no connectivity at all). First, we briefly describe Neighbour Discovery and look at several router configurations. Next we detail how DNS works in IPv6 and describe how this worked in the 6NET network. Finally, we describe DHCPv6 along with several available implementations.

4.1 Neighbour Discovery

Neighbour discovery is a protocol that allows different nodes on the same link to advertise their existence to their neighbours, and to learn about the existence of their neighbors. It is a basic functionality all implementations of IPv6 on any platform must include.

Neighbor discovery for IPv6 replaces the following IPv4 protocols: router discovery (RDISC), Address Resolution Protocol (ARP) and ICMPv4 redirect.

Neighbor discovery is defined in the following documents:

- RFC 2461, Neighbor Discovery for IP Version 6 [RFC2461]
- RFC 2462, IPv6 Stateless Address Autoconfiguration [RFC2462]
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification. [RFC2463]

RFC 2461 and 2462 are currently in the process of being revised by the IPv6 working group of the IETF. These drafts [RFC2461bis], [RFC2462bis] will eventually replace the older RFCs.

The combination of these protocols allow IPv6 hosts to automatically detect the presence of other hosts on the link including, of course, the presence of on-link routers. From the messages sent by routers, IPv6 hosts can automatically configure themselves with appropriate addresses and other state necessary for operation. Neighbour Discovery mandates duplicate address detection so that a host cannot try to use an IPv6 address already in use by another host on the link and also allows a host to detect when another host on the link becomes unreachable.

Neighbor discovery uses the following Internet Control Message Protocol Version 6 (ICMPv6) messages:

- router solicitation (RS)
- router advertisement (RA)
- neighbor solicitation (NS)

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 5

Integration and Transition

In this chapter we look at the problem of IPv6 integration and transition with existing IPv6 networks. Expanding IPv6 functionality from a small infrastructure to a large site network can be a complex and difficult venture. But if it is planned effectively, the deployment can be done in a phased and controlled manner that maximises the chances of a smooth service introduction. For a large site there are a lot of different requirements, and different conditions which make it necessary to employ various transition mechanisms according to the peculiarities of, for example, a given subnet, wireless or mobile environment or dial-in technology. In this chapter we explain which potential options and techniques exist to integrate IPv6 into a site network, which solution is appropriate for any special kind of network infrastructure and of course how exactly one has to set up and configure these techniques. Where possible, we also point to existing (current) problems and interoperability issues, for example in running IPv4 and IPv6 in parallel or having IPv6-only hosts which still need to be able to communicate with IPv4-only hosts on occasion. Numerous transitioning mechanisms and procedures are described including tunnelling methods such as IPv6-in-IPv4 tunnelling, Tunnel Brokers, ISATAP, 6to4, Teredo and translation methods such as NAT-PT, SIIT, SOCKS, ALGs and Bump-in-the-Stack/API.

An overview of security issues in transition is available as an Internet Draft that was originally produced as a result of 6NET experience [DKS05]. The security issues of individual transition mechanisms are discussed in Chapter 9.

5.1 Problem Statement

With an IPv6 host or local network configured, getting connectivity to the global IPv6 Internet is vital if you wish to communicate with other IPv6 systems. Today, this is usually accomplished either natively or, more commonly, with an IPv6-in-IPv4 tunnelling technique using either manual or automatic tunnel configuration methods.

The academic participants of the 6NET project are mostly fortunate enough to have native connectivity to their National Research and Education Networks (NRENs) and from there to a globally connected native IPv6 network (spanning GÉANT, and links to Abilene in the US and WIDE in Japan). Other sites may not be so lucky; for them a tunnelling mechanism is the only realistic option for IPv6 connectivity.

IPv6-only deployments are rare, especially in Europe, but are an interesting exercise with a view to the end game of IPv6 deployment. However, the practical reality is that sites deploying IPv6 will not transition to IPv6-only, but transition to a state where they support both IPv4 and IPv6 (dual-stack). The dual-stack environment then allows IPv6-only devices to be introduced, as a site slowly phases out IPv4. For this reason, translation mechanisms between IPv4 and IPv6 systems are less frequently

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 6

Routing

In this chapter we briefly explain IP routing, paying particular attention to IPv6-specific features. The first section contains a general overview of the Internet routing architecture and explains several important concepts. In the subsequent sections we describe the various routing protocols available to the IPv6 implementor and how these may be configured and deployed in various router platforms such as Cisco and Juniper.

6.1 Overview of IP Routing

Conceptually, IP routing is remarkably simple. It provides a mechanism for connectionless communication between any two hosts that are connected to the global Internet. In the simplest but very common setting, every router along the path between the two hosts is really required to perform just one action for every received datagram, namely next-hop forwarding based on the destination address. Also, all datagrams arriving asynchronously on all router interfaces are essentially handled on the best-effort, first come – first served basis.

Of course, even this is far from easy, if for nothing else then for the sheer number of networks involved. Yet compared both to various extensions of IP (QoS provisioning, traffic engineering, even multicast) and to competitive technologies like ATM, plain IP routing is rather straightforward. Having this relatively "dumb", stateless and policy-free network near the bottom of the protocol stack have had two important consequences:

1. IP routing technology scaled so far extremely well without any strict control mechanisms.
2. The protocol layers above IP (applications in particular) have enough degrees of freedom to implement many different policies and approaches.

In the following subsections we give an overview of the key elements and concepts of IP routing. Most of them are common to IPv4 and IPv6, but we will specifically point out those (relatively few) cases where both protocols differ.

6.1.1 Hop-by-hop Forwarding

IP communication between two hosts A and B that are not on the same LAN segment must pass through one or more routers as indicated in Figure 6-1.

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 7

Network Management

Network management and monitoring is a critical part of operating any production quality network, whatever the nature of the network. It is one of the essential building blocks of the 6NET network, and must be so for any IPv6 public network, especially in the Internet service provider area. If IPv6 backbone networks are not subject to the same (or even an improved) standard of management and monitoring as existing IPv4 networks, the existing IPv4 user base will be unwilling to migrate to IPv6.

Network Management covers many areas (also called network segments) of the network. Usual classification distinguishes Local area Networks (LAN) from Metropolitan (MAN) and Wide Area Networks (WAN). In this regard sets of very different functions have to be provided to the manager, from straightforward monitoring of link status, to traffic statistics gathering and analysis. These sets could roughly be classified in two categories: those needed for day to day network control operations and those dedicated to network behaviour analysis. The latter allows the manager to optimise the network or parts of it and to schedule the necessary evolutions.

This chapter brings together all the important network monitoring and management work conducted by the network management workpackage of 6NET. This chapter is designed as a “cookbook”, summarising the issues required for managing and monitoring an IPv6 network, and suggests appropriate tools that can be used to support the network management and monitoring function. The end result should be that this will be both a useful guide to designers of new IPv6 networks, and as a reference for more experienced network managers.

7.1 Management protocols and MIBs in the standardisation process

As the main management standard used for IPv4 networks is SNMP (Simple Network Management Protocol), [RFC3416], it was an obvious goal to pursue to also make SNMP management available for and via IPv6. This section focuses on SNMP for IPv6, the corresponding MIBs (Management Information Base) and standardisation process and also gives a brief history on the evolution of the SNMP protocol in general.

7.1.1 SNMP for IPv6

Today many network vendors (6WIND, CISCO, HITACHI, JUNIPER etc.) support SNMP over IPv6 and can be monitored in an IPv6-only environment. One could note that equipment not supporting SNMP over IPv6 can be managed over IPv4 as most IPv6 networks are running dual stack.

The number of SNMP applications able to poll remote SNMP agents over IPv6 remains low. Most of the tools today use the netSNMP open source SNMP library. Recently however, some integrated

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 8

Multicast

We will explain differences between IPv4 and IPv6 multicast. We will first look at the basics and go through the different types of addressing and allocations available. Then we will look at how to deploy IPv6 multicast intra-domain, followed by inter-domain.

8.1 Addressing and Scoping

The complete multicast architecture defined today in different RFCs and Internet Drafts is described in this section. It is very important to know all the different address types defined because the allocation mechanisms will depend of the architecture used.

RFC 3513 (IP Version 6 Addressing Architecture) defines the IPv6 multicast address. As shown in Table 8-1, IPv6 multicast addresses are derived from the FF00::/8 prefix. The octet following the initial obligatory "FF" value contains four flags and 4-bit value defining the scope of the multicast group.

Table 8-1 IPv6 Multicast Address Format

8 bits	4 bits	4 bits	---------- 112 bits ----------
FF	Flags	Scope	Group ID

The flags field is a set of 4 flag bits.

Table 8-2 The Flags Field

x	R	P	T

Only bit T is described in RFC 3513 and indicates if the address is permanent (value 0) or temporary (value 1). Bits P and R are described in RFC 3306 [RFC3306] and RFC 3956 [RFC3956]. The high order flag bit is not yet used. The use of the flags makes it possible to distinguish different address type that will be detailed in the following sections.

The meaning of the 4-bit scope value is summarized in Table 8-3.

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 9

Security

This chapter provides an overview of the current security issues in an IPv6 based networking environment and suggests a number of helpful security "guidelines".

First we will analyse how the IPv6 changed the security of IP networking environment. We will concentrate on the threat analysis compared with IPv4. Then we will discuss the major building block of a security architecture: IPv6 firewalls. Finally we will discuss the security implications of deploying various IPv4-IPv6 co-existnce and transitioning mechanisms.

9.1 What has been Changed in IPv6 Regarding Security?

In this section will enumerate the different threats that you can face when you operate a IP networking environment and we trying to provide some sort of solution in IPv6 in mind.

9.1.1 IPSec

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provide security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (peers), such as Cisco routers. IPSec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of these services:

- ? Data confidentiality—The IPSec sender can encrypt packets before sending them across a network.
- ? Data integrity—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- ? Data origin authentication—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- ? Anti-replay—The IPSec receiver can detect and reject replayed packets.

With IPSec, data can be sent across a public network without observation, modification or spoofing.

IPSec functionality is essentially identical in both IPv6 and IPv4; however, IPSec in IPv6 can be deployed from end-to-end - data may be encrypted along the entire path between a source node and destination node. (Typically, IPSec in IPv4 is deployed between border routers of separate networks.) In IPv6, IPSec is implemented using the authentication extension header and the ESP extension header. The authentication header provides integrity and authentication of the source. It also provides

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 10

Mobility

The Mobile IPv6 (MIPv6) protocol [RFC3775] is a proposed standard by the IETF to provide transparent host mobility within IPv6. The protocol enables a Mobile Node to move from one network to another without the need to change its IPv6 address. A Mobile Node is always addressable by its home address, which is the IPv6 address that is assigned to the node within its home network. When a Mobile Node is away from its home network, packets can still be routed to it using the node's home address. In this way, the movement of a node between networks is completely invisible to transport and other higher layer protocols.

Mobile Nodes participating in the MIPv6 protocol each have a persistent home address, which can be used to address the Mobile Node irrespective of its current point of attachment to the IPv6 network. The IPv6 network which matches the home address' prefix is known as the home network. Mobile Nodes also adopt a Home Agent - an IPv6 capable router directly connected to the home network. This process may either be static, or dynamic, via the MIPv6 Home Agent discovery mechanism. The Home Agent is responsible for the interception and forwarding of IPv6 packets to the Mobile Node which are incorrectly routed to the home network while the Mobile Node is away from home.

When a Mobile Node is attached to its home network it operates as any other network node, so no special routing is required. When a Mobile Node moves to a foreign network, it uses IPv6 autoconfiguration to discover the new network and to allocate a care-of address within the address space of that network. However, to ensure that IPv6 packets destined for the Mobile Node's home address reach the proper location as efficiently as possible, the routing information pertaining to the Mobile Node's home address must be updated in both the Home Agent and any relevant Correspondent Nodes. MIPv6 provides this functionality by the introduction of a bindings cache on the Mobile and Correspondent Nodes and binding update messages which are transmitted in a new IPv6 extension header called the mobility header.

Although MIPv6 implementations have been around since 1998 most have fallen out of date as the MIPv6 protocol has progressed over the years. However, there are a handful of available implementations that are fairly up to date with either MIPv6 draft version 24 or RFC 3775 (which is based on draft version 24). Yet these implementations can still differ slightly in their supported features and are not likely to be completely 100% interoperable in most cases.

10.1 Bindings Cache

The relationship between a Mobile Node's home address and its current care-of address is known as a binding. All Nodes participating in MIPv6 are required to maintain a table of these bindings in a binding cache. One entry is held in the binding cache for each Mobile Node with which communication is currently taking place. The binding cache holds four pieces of information per binding which are central to the operation of MIPv6, as illustrated by Table 10-1 (other fields are

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 11

Applications

A number of middleware and user applications were developed or ported by the 6NET project. These included the SIP-based telephony system (including a PSTN gateway), the AccessGrid conferencing tool (including an IPv4-IPv6 gateway), IPv6 versions of the IBM WebSphere e-business applications, an IPv6 version of the FLUTE multicast file transfer tool, and MIPv6-based video streaming for PDAs. The 6NET project also created IPv6 versions of the Globus Toolkit (GT3.x) which is used to develop Grid-aware applications (e.g., IPv6 WeatherStation and eProtein), and the Open H.323 Toolkit, used to develop an IPv6 version of GnomeMeeting. Other network management tools such as NetSNMP, MRTG, OpenEye, Smokeping and Weathermap have been developed or ported for traffic measurement and visualisation purposes.

6net **Applications summary**

These are the application being ported, tested or developed by 6NET.
Our aim is to perform trials on the suitability and robustness of IPv6 applications with a view to wide-scale deployment.
Click on the column headers to change sorting order.

name	category	class	summary	status	responsible	modified	passed test
TUR	Streaming Radio	A	Trondheim Underground Radio	Running. Publicly available. Multicast support planned by mid 2003.	UNINETT	2004-03-11	✔
VideoLAN	Streaming	A	Streaming video server and player	Works. A multicast demonstrator. A first implementation of RTSP is available for better stream control.	SURFnet	2004-02-27	✔
Quake	Gaming	B	Multiplayer FPS action game	Works.	GARR	2004-02-27	✔
Kphone	Conferencing	A	SIP based Voice-over-IPv6 telephony application.	Demo version released	FhG Fokus	2004-03-11	✔
WMA through ftunnel	Streaming	A	Streaming of Windows Media using ftunnel	working	SURFnet bv	2004-03-11	✔
SER	Conferencing Support	A	SIP server	Operational	FhG Fokus	2004-03-11	✔
VIC	Conferencing	A	Video Conferencing Tool	VIC is currently fairly stable, and provides good performance. Further work is required on use of direct video display and integration of more codecs.	UCL	2004-03-17	✔
MCast6	Streaming	A	Tool for multimedia streaming in a computer network	testing phase	PSNC	2004-05-13	✔

Figure 11-1 Partial Screenshot of the Applications Database

Deliverable D5.1 [D5.1] of the 6NET project listed the applications initially identified as candidates to run on the 6NET IPv6 network. Since the development and porting of applications to support IPv6 is not a static activity, it is very difficult, if not impossible, to capture the ever-evolving status of the different applications mentioned in a single document.

Therefore, the Applications workpackage of 6NET decided that the applications list and current status would be in the form of a web page. This approach enables application owners to keep the status of

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

PART II

Case Studies

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 12

IPv6 in the Backbone

In this chapter we present case studies of IPv6 in the backbone. First we look at the core 6NET backbone and the NRENs that were connected to it before the core network was decommissioned in January 2005.

Next, we detail case studies of IPv6 deployment by the NRENs themselves inside their own country backbone networks. The most common method to introduce IPv6 services into IPv4 networks will be through dual-stack networking. This complements the backbone transition and pushes the issue of deployment to the edge, e.g. to the universities.

In the timeframe of 6NET, many NRENs migrated to dual stack; the specific experiences of SURFnet, Funet and Renater are reported here.

12.1 6NET Backbone Case Study

A backbone IPv6 network connecting sixteen countries and running at 155 Mbps was established in 2002. This ran IPv6 over dedicated links, although for cost reasons, four links (to Greece, Hungary, Poland and Portugal) were provided by POS (Packet-over-SONET/SDH) over a Layer 2 VPN infrastructure.

Local access was provided through national IPv6 testbeds operated by partner NRENs (National Research and Education Networks) such as JANET (UK), RENATER (France) and SWITCH (Switzerland). Connectivity to the non-European 6NET partners in Japan and South Korea was provided via connections to London and RENATER respectively, and there are were connections to Abilene in the US (via SURFnet), Euro6IX (via the JANET- UK6X, GARR-TILab and SWITCH-Swisscom exchange points) and to the 6Bone.

The 6NET backbone, and interconnected national testbeds, collectively formed the largest native IPv6 network in the world. This provided plenty of scope for trialling the new technology, testing interoperability with existing networks, and demonstrating services and applications. In fact, it demonstrated that the IS-IS and BGP4+ routing protocols, IPv6 over IPv4 tunnelling, and DNS support were stable and usable. In addition, a multicast overlay network (M6Bone) was established and has been utilised for conferencing and radio broadcasting (e.g., Trondheim Underground Radio).

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 13

IPv6 in the Campus/Enterprise

In this chapter we present case studies of IPv6 in the Campus/Enterprise. Since the vast majority of the 6NET partners were academic related, this case studies in this chapter are indeed related to Universities and academic departments. Nevertheless, there are many similarities between University/Campus based deployments and Enterprise deployments.

First, we we look at the Campus IPv6 deployment at the University of Münster. Next we describe two deployments at small and large academic departments (Tromsø and Southampton University respectively). A second University Campus deployment case study is given for Lancaster University and finally, we briefly describe some other deployment scenarios relating to the Campus/Enterprise class of network.

13.1 Campus IPv6 Deployment (University of Münster, Germany)

As the University of Münster is quite large, with a widespread network and is using at large set of different hardware and network techniques, several considerations had to be taken into account.

If one wants to integrate IPv6 in the network, the most desirable form of integration is always to run in dual-stack mode on each and every interface and node. However, while nowadays support for IPv6 is present in nearly every new product, there are still older hardware and technologies that do not easily support IPv6 capabilities or don't support them at all.

Especially in large sites, that have been in place for a long time, the network infrastructure has evolved over a number of years. Such networks often have a modern core, but still use old technology in some areas and on internal "stubby" edges. In such environments it is practically impossible to run full dual-stack mode. Several of the transition methods described in this cookbook can be used to reach such areas.

In addition, network administrators often hesitate to introduce IPv6, because they fear that they will destabilise their IPv4 infrastructure or because they are unfamiliar with IPv6 and IPv6 management. To overcome these fears it is helpful to start with IPv6 just in a few parts of the network and to leave the IPv4 infrastructure untouched.

A good method for this is using VLAN technology (802.1q). VLANs are very common and often used in modern networks, and it is especially easy to integrate IPv6 in these networks. If a dedicated IPv6 router is used, it can get access to only those VLANs where IPv6 is desired. So the IPv4 network remains unchanged, and all IPv6 traffic is routed and managed over a different set of hardware.. If no additional hardware is available, it might be sufficient to use only a small set of the existing routers to do IPv6 routing.

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Chapter 14

IPv6 on the Move

This chapter describes three case studies of 6NET partners who deployed and trialled Mobile IPv6 testbeds. We first look at the testbed at Fraunhofer Fokus and after that we describe the testbeds at Lancaster University and the University of Oulu.

14.1 Fraunhofer Fokus

The Fokus Mobile IPv6 testbed has undergone several changes throughout the 6NET project. The current environment does not longer distinguish between an internal and an external part as before when there was a local, experimental testbed not constantly connected to the 6NET network and another part with continous provision of native IPv6 connectivity to the outer 6NET world. Furthermore the test environment was completed by several components providing for VoIP and video conferencing capabilities.

The Mobile IPv6 testbed consists of the components illustrated in Figure 14-1.

Connected to the central router “adrahil” there are basically two different networks with prefixes 2001:638:806:2002::/64 and 2001:638:806:2001::/64. Attached to those networks are the corresponding Home Agents for the MIPL- and the KAME-Mobile IP implementation, respectively. A MCU connected to the “2001”-network was used as Corresponding Node for Mobile IPv6 functionality- and interoperability testing: Using a MN with video conferencing equipment, i.e. the GnomeMeeting application with camera and headset, this scenario allowed for establishing a connection to the CN-MCU and subsequently changing the IPv6 network point of attachment while maintaining the connection to the MCU.

Currently the Fokus testbed is made up of the different components:

- End systems with different operating systems

  At the leaves of the network, standard PCs with different operating systems (Windows Server 2003, Windows XP, Linux, FreeBSD) are installed. They are used for testing IPv6 network applications like video conferencing, web surfing, downloading audio and video streams, IP telephony applications etc.

- Home Agents

  Mobile IPv6 Home Agents as offered by the MIPL- and KAME project.

- IP softphone

Bibliography

[8021x] LAN MAN Standards Committee of the IEEE Computer Society, "*Port Based Network Access Control*", IEEE Standard 802.1x, June 2001.

[AD05] C. Aoun, E. Davies, "*Reasons to Move NAT-PT to Experimental*", IETF Internet Draft draft-ietf-v6ops-natpt-to-exprmntl-01.txt (work in progress), January 2005.

[BCKR05] T. Bates, R. Chandra, D. Katz, Y, Rekhter, "*Multiprotocol Extensions for BGP-4*", IETF Internet Draft draft-ietf-idr-rfc2858bis-07.txt, August 2005.

[Bel57] R. Bellman, "*Dynamic Programming*", Princeton University Press, 1957.

[BG92] D. Bertsekas, R. Gallagher, "*Data Networks*", Second edition, Prentice Hall, 1992, ISBN 0-13-200916-1.

[BP02] M. Blanchet, O. Medina, F. Parent, "*DSTM Tunnel Setup using TSP*", IETF Internet Draft draft-blanchet-ngtrans-tsp-dstm-profile-01.txt, July 2002.

[BP05] M. Blanchet , F. Parent, "*IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)*", IETF Internet Draft draft-blanchet-v6ops-tunnelbroker-tsp-03.txt (work in progress), August 2005.

[Bou05] J. Bound, "*Dual Stack IPv6 Dominant Transition Mechanism (DSTM)*", IETF Internet Draft draft-bound-dstm-exp-03.txt (work in progress), June 2005.

[Cho04a] T. Chown, "*IPv6 Campus Transition Scenario Description and Analysis*", IETF Internet Draft draft-chown-v6ops-campus-transition-01.txt, October 2004.

[Cho04b] T. Chown, "*Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks*", IETF Internet Draft, draft-chown-v6ops-vlan-usage-02.txt, October 2004.

[Cla05] B. Claise, "*IPFIX Protocol Specification*", IETF Internet Draft draft-ietf-ipfix-protocol-19.txt, September 2005.

[D1.1] 6NET Deliverable 1.1, "*Design and Implementation of the Testbed Infrastructure*", April 2002.

[D1.2] 6NET Deliverable 1.2, "*Operational Procedures to be Followed by 6NET NOC*", April 2002.

[D2.2.4] 6NET Deliverable 2.2.4, "*Final IPv4 to IPv6 Transition Cookbook for Organisational/ ISP (NREN) and Backbone Networks.*", February 2005.

[D2.3.4] 6NET Deliverable 2.3.4, "*Final IPv4 to IPv6 transition cookbook for end site networks/ universities*", June 2005.

[D2.4.2] 6NET Deliverable 2.4.2, "*Final report on IPv6-specific implications for Wireless LAN/MAN transition to IPv6*", September 2003.

[D2.5.3] 6NET Deliverable 2.5.3, "*Issues for IPv6 deployment (missing pieces for IPv6 deployment and IPv6-only operation)*", June 2005.

[D3.1.1] 6NET Deliverable 3.1.1, "*IPv6 Routing Plan for the 6NET Network*", March 2002.

[D3.1.2] 6NET Deliverable 3.1.2, "*IPv6 cookbook for routing, DNS, intra-domain multicast, inter-domain multicast, security*", November 2004.

[D3.2.1] 6NET Deliverable 3.2.1, "*IPv6 DNS service for the 6NET network*", March 2002.

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Glossary of Terms and Acronyms

6PE	IPv6 Provider Edge Router (over MPLS)
ABR	Area Border Router
ACL	Access Control List
AH	Authentication Header
ALG	Application Layer Gateway
AP	Access Point
API	Application Programming Interface
AR	Access Router
ARP	Address Resolution Protocol
AS	Autonomous System
ASM	Any Source Multicast
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BA	Binding Acknowledgement
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BGMP	Border Gateway Multicast Protocol
BIA	Bump in the Stack
BIND	Berkeley Internet Name Daemon
BIS	Bump in the Stack
BOOTP	Bootstrap Protocol
BR	Binding Request
BU	Binding Update
BSD	Berkeley Software Distribution
CIDR	Classless Inter-Domain Routing
CA	Certificate Authority
CCC	Circuit Cross Connect
CEF	Cisco Express Forwarding
CGA	Cryptographically Generated Address
CN	Correspondent Node
CoA	Care-of Address
CoT	Care-of Test
CoTI	Care-of Test Init

To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Appendices

Appendix A1: List of per-PoP Location Support Domains

Every PoP has its own subdomain within 6net.org. The subdomain name corresponds to the two letter country code of the country where the PoP is located, i.e., <cc>.6net.org. The country codes are the following:

at - Austria

be - Belgium

ch - Switzerland

cz - Czech Republic

de - Germany

es - Spain

fr - France

gr - Greece

hu - Hungary

ie - Ireland

it - Italy

lu - Luxemburg

nl - Netherlands

pl - Poland

pt - Portugal

se - Sweden

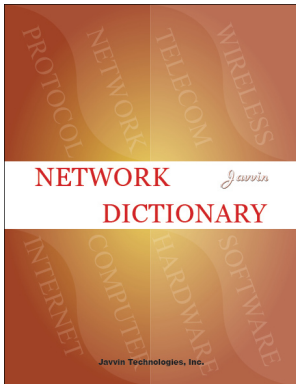
si - Slovenia

sk - Slovakia

uk - United Kingdom

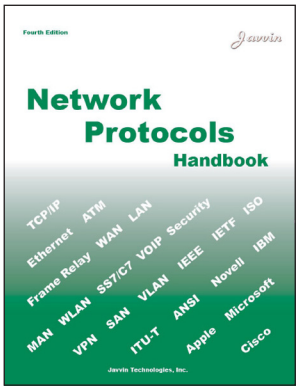
To order this book and other Network Protocols titles, please visit: http://www.javvin.com

Javvin Networking Technology Series



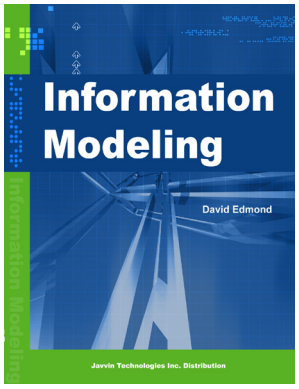
Network Dictionary

Networking, Internet, telecom, wireless, computer, hardware and software - multiple dictionaries in one. A “Must have” reference for IT/Networking professionals and students!



Network Protocols Handbook

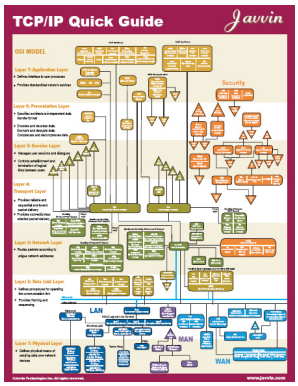
Fully explains and reviews all active protocols. Illustrates latest networking technologies.



Information Modeling

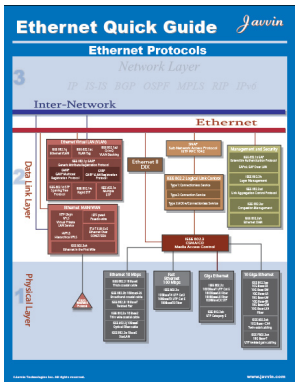
Information modeling is a critical process in content management. This book provides basic concepts of information models and explains how to design database based on data analysis and SQL models. It also provides case studies of database design based on information modeling techniques.

Visit www.javvin.com for details about the networking technology series and a complete list of titles.



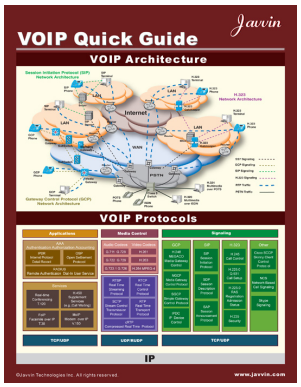
TCP/IP Quick Guide

Practical TCP/IP information extracted from hundreds of pages of TCP/IP books. A comprehensive and clear map of all TCP/IP protocols in OSI 7 layers model. A portable tool for you to carry, insert into a folder or put on your desk.



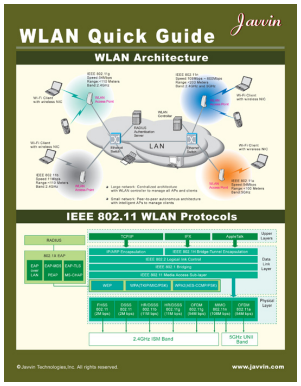
Ethernet Quick Guide

Practical Ethernet information extracted from hundreds of pages of Ethernet books. A comprehensive and clear map of all Ethernet protocols. A portable tool for you to carry, insert into a folder or put on your desk.



VOIP Quick Guide

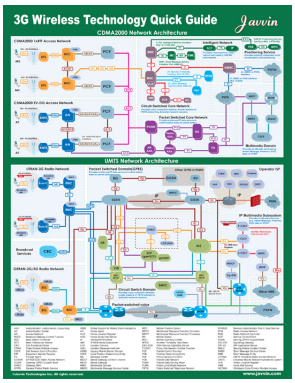
All must known VOIP technologies included in this comprehensive yet portable quick reference.



WLAN (WiFi) Quick Guide

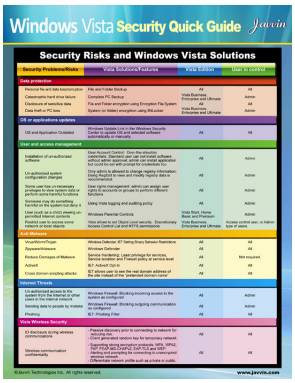
A comprehensive quick reference to assist you in WiFi WLAN implementation, learning and operation.

Visit www.javvin.com for details about the networking technology series and a complete list of titles.



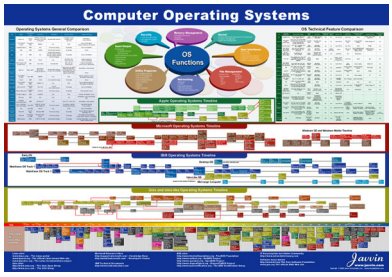
3G Wireless Tech Quick Guide

Highlights the third generation wireless technologies in one portable quick guide.



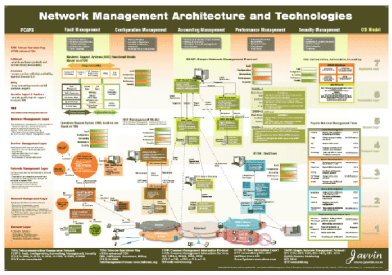
Windows Vista Security Quick Guide

All you must to know about Windows Vista Security on this handy quick guide...useful for all Windows Vista users!



Computer Operating Systems (OS) Poster

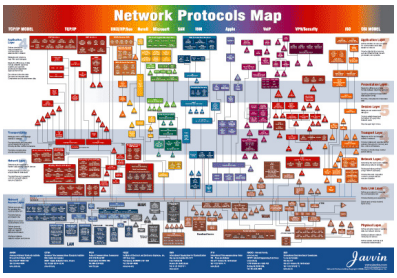
Illustrates the computer operating systems now and their evolution path over the past 60 years.



Network Management Architecture and Technology Map

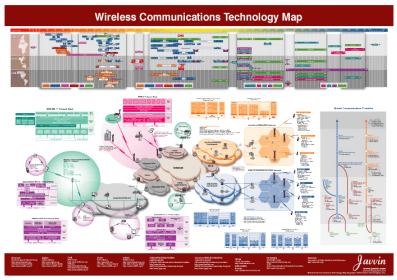
All network management architecture and technologies for both telecom and data communications displayed on one chart.

Visit www.javvin.com for details about the networking technology series and a complete list of titles.



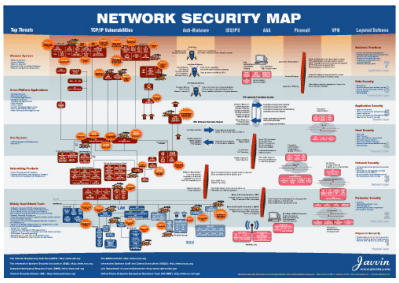
The Network Protocols Map Poster

All network protocols illustrated on one Chart. A “must have” for all networking, IT and Telecom professionals and students.



Wireless Communications Technology Map Poster

All major wireless technologies displayed in one chart: WLAN, WiMAX (WMAN), WPAN and mobile wireless technologies (WWAN)...



Network Security Map

All you must know about network security on one chart! A unique gift for yourself, your colleagues, partners and customers.

Network dictionary

www.NetworkDictionary.com

Free networking technology library, comprehensive network protocol and network security knowledge, telecom encyclopedia, computer hardware and software terms and white-papers.

A site for you to learn and share knowledge, ask experts, write blogs and get connected with peers.

IPv6 Deployment Guide

6NET was a three-year European IST project to demonstrate that continued growth of the Internet can be met using new IPv6 technology. The project built and operated a pan-European native IPv6 network connecting sixteen countries in order to gain experience of IPv6 deployment and the migration from existing IPv4-based networks.

6NET involved thirty-five partners from the commercial, research and academic sectors and represented a total investment of €18 million; €7 million of which came from the project partners themselves, and €11 million from the Information Society Technologies Programme of the European Commission. The project commenced on 1st January 2002 and officially finished on 30th June 2005. The network itself was decommissioned in January 2005, handing over the reigns of pan-European native IPv6 connectivity to GÉANT.

When we began 6NET, IPv6 code was in the form of early beta releases from most commercial companies. The 6BONE had been built but was only using tunnels; there were very few native IPv6 networks and none of these ran production traffic. One thing we strived for in the early days of 6NET was developing a pan-European testbed that had as much native IPv6 connectivity as was affordable. This gave everyone involved the chance to really exercise the IPv6 protocol developments we planned without the added complexity of tunnels that might detract from the real work. Soon we were able to peer with other IPv6 networks in the US (Abilene, 6TAP), Japan (NTT) and S.Korea (KOREN) to provide global IPv6 connectivity. The final stages of the project moved into exploiting the protocol and providing demonstrations that IPv6 was ready for full production service.

The information contained in this book is taken from the project's deployment cookbooks and other deliverables. Since each cookbook/deliverable generally concentrates only on specific IPv6 features or deployment scenarios (e.g. site transition, multicast, mobility, DHCP, routing etc.), we believe that providing all the important information in a single reference book is much more preferable to the reader than negotiating our multitude of project deliverables.

ISBN: 978-1-60267-005-1

9 781602 670051 >