

Netwerken

Deel 3 – Bedrijfsnetwerken, beveiliging en automatisering

Netwerken

Deel 3 – Bedrijfsnetwerken, beveiliging en automatisering

Versie 7

John Bakker

Boom beroepsonderwijs
info@boomberoepsonderwijs.nl
www.boomberoepsonderwijs.nl

Auteur: John Bakker
Redactie en opmaak: Henk Pel, Zeist
Titel: Netwerken – Deel 3 – Bedrijfsnetwerken, beveiliging en automatisering
ISBN 978 90 372 5910 0
Eerste druk / eerste oplage
© Boom beroepsonderwijs 2021

Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (www.reprorecht.nl). Voor het overnemen van gedeelte(n) uit deze uitgave in compilatiewerken op grond van artikel 16 Auteurswet kan men zich wenden tot de Stichting PRO (www.stichting-pro.nl).

De uitgever heeft ernaar gestreefd de auteursrechten te regelen volgens de wettelijke bepalingen. Degenen die desondanks menen zekere rechten te kunnen doen gelden, kunnen zich alsnog tot de uitgever wenden.

Door het gebruik van deze uitgave verklaart u kennis te hebben genomen van en akkoord te gaan met de specifieke productvoorwaarden en algemene voorwaarden van Boom beroepsonderwijs, te vinden op www.boomberoepsonderwijs.nl

Inhoud

- o **Bedrijfsnetwerken, beveiliging en automatisering 1**
- 1 Single area OSPFv2-concepten 3**
 - 1.0 Inleiding 3
 - 1.0.1 Waarom zou je dit hoofdstuk bestuderen? 3
 - 1.0.2 Wat leer je in dit hoofdstuk? 3
 - 1.1 OSPF-functies en -eigenschappen 3
 - 1.1.1 Inleiding in OSPF 3
 - 1.1.2 Onderdelen van OSPF 4
 - 1.1.3 Werking Link-State 5
 - 1.1.4 Single area en multi-area OSPF 8
 - 1.1.5 Multi-area OSPF 9
 - 1.1.6 OSPFv3 10
 - 1.1.7 Test je kennis – OSPF-functies en -eigenschappen 10
 - 1.2 OSPF-packets 12
 - 1.2.1 Video – OSPF-packets 12
 - 1.2.2 Soorten OSPF-packets 12
 - 1.2.3 Link-State-updates 12
 - 1.2.4 Hello-packet 13
 - 1.2.5 Test je kennis – OSPF-packets 14
 - 1.3 OSPF-werking 15
 - 1.3.1 Video – OSPF-werking 15
 - 1.3.2 OSPF operationele statussen 16
 - 1.3.3 Opbouwen van neighbor adjacencies 16
 - 1.3.4 Synchroniseren van de OSPF-databases 18
 - 1.3.5 De noodzaak voor een DR 20
 - 1.3.6 LSA-flooding met een DR 20
 - 1.3.7 Test je kennis – OSPF-werking 22
 - 1.4 Opdrachten en quiz 24
 - 1.4.1 Wat leerde je in dit hoofdstuk? 24
 - 1.4.2 Quiz – Single area OSPFv2-concepten 25
- 2 Single area OSPFv2 configureren 29**
 - 2.0 Inleiding 29
 - 2.0.1 Waarom zou je dit hoofdstuk bestuderen? 29
 - 2.0.2 Wat leer je in dit hoofdstuk? 29
 - 2.1 OSPF-router-ID 29
 - 2.1.1 OSPF-referentietopologie 29
 - 2.1.2 Routerconfiguratiemode voor OSPF 30
 - 2.1.3 Router-ID's 31
 - 2.1.4 Volgorde van prioriteit voor het router-ID 31
 - 2.1.5 Configureer een loopback-interface als het router-ID 32
 - 2.1.6 Een router-ID handmatig configureren 32
 - 2.1.7 Modificeer een router-ID 33
 - 2.1.8 Syntax Checker – Configureer R2 en R3 met router-ID's 34
 - 2.1.9 Test je kennis – OSPF-router-ID 34

- 2.2 Point-to-point OSPF-netwerken 35
 - 2.2.1 De network-commandosyntax 35
 - 2.2.2 Het wildcard-masker 35
 - 2.2.3 Test je kennis – Wildcard-maskers 36
 - 2.2.4 Configureer OSPF met het network-commando 36
 - 2.2.5 Syntax Checker – Configureer R2 en R3 met het network-commando 37
 - 2.2.6 Configureer OSPF met het commando ip ospf 37
 - 2.2.7 Syntax Checker – Configureer R2 en R3 met het commando ip ospf 38
 - 2.2.8 Passive-interface 38
 - 2.2.9 Commando passive-interfaces 39
 - 2.2.10 Syntax Checker – Configureer passive-interfaces op R2 en R3 40
 - 2.2.11 OSPF-point-to-point-netwerken 40
 - 2.2.12 Loopbacks en point-to-point-netwerken 41
 - 2.2.13 Packet Tracer – Point-to-point single area OSPFv2-configuratie 42
- 2.3 Multi-access-OSPF-netwerken 42
 - 2.3.1 OSPF-netwerktypen 42
 - 2.3.2 OSPF-designated router 43
 - 2.3.3 OSPF-multi-access-topologie 44
 - 2.3.4 Verifiëren van OSPF-routerrollen 44
 - 2.3.5 Verifieer de DR/BDR-adjacencies 46
 - 2.3.6 Default DR/BDR-verkiezingsproces 47
 - 2.3.7 DR-uitval en herstel 48
 - 2.3.8 Het commando ip ospf priority 50
 - 2.3.9 OSPF-prioriteit configureren 51
 - 2.3.10 Syntax Checker – Configureer OSPF-prioriteit 52
 - 2.3.11 Packet Tracer – Bepaal de DR en BDR 52
- 2.4 Wijzig single area OSPF 53
 - 2.4.1 Cisco OSPF cost metric 53
 - 2.4.2 De referentiebandbreedte aanpassen 53
 - 2.4.3 Gecumuleerde OSPF-costs 55
 - 2.4.4 Handmatig OSPF-cost-waarde instellen 55
 - 2.4.5 Test failover via de back-uproute 57
 - 2.4.6 Syntax Checker – Pas de cost-waarden voor R2 en R3 aan 57
 - 2.4.7 Hello-packet-intervallen 57
 - 2.4.8 Verifieer de Hello- en Dead-intervallen 58
 - 2.4.9 Aanpassen van de OSPFv2-intervallen 59
 - 2.4.10 Syntax Checker – Hello- en Dead-intervallen op R3 aanpassen 60
 - 2.4.11 Packet Tracer – Single area OSPFv2 aanpassen 60
- 2.5 Default routepropagatie 60
 - 2.5.1 Doorgeven van een statische default route in OSPFv2 60
 - 2.5.2 De gepropageerde default route verifiëren 61
 - 2.5.3 Packet Tracer – Propagatie van een default route in OSPFv2 62
- 2.6 Verifieer single area OSPFv2 63
 - 2.6.1 Verifieer OSPF-neighbors 63
 - 2.6.2 Verifieer OSPF-protocolinstellingen 64
 - 2.6.3 Verifieer OSPF-procesinformatie 65
 - 2.6.4 Verifieer OSPF-interface-instellingen 65
 - 2.6.5 Syntax Checker – Verifieer single area OSPFv2 66
 - 2.6.6 Packet Tracer – Verifieer single area OSPFv2 67
- 2.7 Oefeningen en quiz 67
 - 2.7.1 Packet Tracer – Single area OSPFv2-configuratie 67
 - 2.7.2 Lab – Single area OSPFv2-configuratie 67
 - 2.7.3 Wat leerde je in dit hoofdstuk? 67
 - 2.7.4 Quiz – Single area OSPFv2-configuratie 71

3	Netwerkbeveiligingsconcepten	75
3.0	Inleiding	75
3.0.1	Waarom zou je dit hoofdstuk bestuderen?	75
3.0.2	Wat leer je in dit hoofdstuk?	75
3.0.3	Ethical hacker-verklaring	75
3.1	Huidige staat van de cybersecurity	76
3.1.1	Huidige stand van zaken	76
3.1.2	Vectoren van netwerk-attacks	76
3.1.3	Dataverlies	77
3.1.4	Test je kennis – Huidige staat van cybersecurity	78
3.2	Threat-actors	79
3.2.1	De hacker	79
3.2.2	Evolutie van hackers	80
3.2.3	Cybercriminelen	80
3.2.4	Hacktivists	80
3.2.5	State-sponsored hackers	80
3.2.6	Test je kennis – Threat-actors	81
3.3	Threat-actor-tools	81
3.3.1	Video – Threat-actor-tools	81
3.3.2	Inleiding attacking-tools	82
3.3.3	Evolutie van beveiligingstools	82
3.3.4	Attacktypen	84
3.3.5	Test je kennis – Threat-actor-tools	84
3.4	Malware	85
3.4.1	Overzicht van malware	85
3.4.2	Virussen en Trojan horses	86
3.4.3	Andere soorten malware	87
3.4.4	Test je kennis – Malware	88
3.5	Veelvoorkomende netwerk-attacks	89
3.5.1	Overzicht van netwerk-attacks	89
3.5.2	Video – Reconnaissance-attacks	90
3.5.3	Reconnaissance-attacks	90
3.5.4	Video – Access- en social engineering-attacks	92
3.5.5	Access-attacks	92
3.5.6	Social-engineering-attacks	94
3.5.7	Lab – Social engineering	95
3.5.8	Video – Denial of Service-attacks	96
3.5.9	DoS- en DDos-attacks	96
3.5.10	Test je kennis – Veelvoorkomende netwerk-attacks	97
3.6	IP-vulnerabilities en -threats	98
3.6.1	Video – Veelvoorkomende IP- en ICMP-attacks	98
3.6.2	IPv4 en IPv6	98
3.6.3	ICMP-attacks	98
3.6.4	Video – Amplificatie-, reflectie- en spoofing-attacks	99
3.6.5	Amplificatie- en reflectie-attacks	99
3.6.6	Adres-spoofing-attacks	100
3.6.7	Test je kennis – IP-vulnerabilities en -threats	101
3.7	TCP- en UDP-vulnerabilities	102
3.7.1	TCP-segmentheader	102
3.7.2	TCP-services	103
3.7.3	TCP-attacks	103
3.7.4	UDP-segmentheader en werking	105
3.7.5	UDP-attacks	106
3.7.6	Test je kennis – TCP- en UDP-vulnerabilities	106

- 3.8 IP-services 107
 - 3.8.1 ARP-vulnerabilities 107
 - 3.8.2 ARP-cache-poisoning 108
 - 3.8.3 Video – ARP-spoofing 109
 - 3.8.4 DNS-attack 110
 - 3.8.5 DNS-tunneling 111
 - 3.8.6 DHCP 112
 - 3.8.7 DHCP-attacks 112
 - 3.8.8 Lab – Onderzoek DNS-verkeer 114
- 3.9 Netwerksecurity ‘best practices’ 115
 - 3.9.1 Confidentiality, integrity en availability 115
 - 3.9.2 Defense-in-Depth-aanpak 115
 - 3.9.3 Firewalls 117
 - 3.9.4 IPS 118
 - 3.9.5 Content-beveiligingsapparaten 118
 - 3.9.6 Test je kennis – Netwerksecurity ‘best practices’ 120
- 3.10 Cryptografie 121
 - 3.10.1 Video – Cryptografie 121
 - 3.10.2 Communicatie beveiligen 121
 - 3.10.3 Data-integriteit 121
 - 3.10.4 Hash-functies 122
 - 3.10.5 Oorsprongauthenticatie 123
 - 3.10.6 Datavertrouwelijkheid 125
 - 3.10.7 Symmetrische encryptie 126
 - 3.10.8 Asymmetrische encryptie 127
 - 3.10.9 Diffie-Hellman 129
 - 3.10.10 Test je kennis – Cryptografie 130
- 3.11 Opdrachten en quiz 131
 - 3.11.1 Wat leerde je in dit hoofdstuk? 131
 - 3.11.2 Quiz – Netwerkbeveiligingsconcepten 132
- 4 ACL-concepten 135**
 - 4.0 Inleiding 135
 - 4.0.1 Waarom zou je dit hoofdstuk bestuderen? 135
 - 4.0.2 Wat leer je in dit hoofdstuk? 135
 - 4.1 Doel van ACL's 135
 - 4.1.1 Wat is een ACL? 135
 - 4.1.2 Packetfiltering 136
 - 4.1.3 ACL-werking 137
 - 4.1.4 Packet Tracer – ACL-demonstratie 138
 - 4.1.5 Test je kennis – Doel van ACL's 138
 - 4.2 Wildcardmaskers in ACL's 139
 - 4.2.1 Overzicht wildcardmaskers 139
 - 4.2.2 Wildcardmaskertypen 139
 - 4.2.3 Wildcardmaskerberekening 140
 - 4.2.4 Wildcardmasker-keywords 141
 - 4.2.5 Test je kennis – Wildcardmaskers in ACL's 142
 - 4.3 Richtlijnen voor het aanmaken van ACL's 142
 - 4.3.1 Beperkt aantal ACL's per interface 142
 - 4.3.2 ACL best practices 143
 - 4.3.3 Test je kennis – Richtlijnen voor het aanmaken van ACL's 144
 - 4.4 Soorten IPv4-ACL's 144
 - 4.4.1 Standard en extended ACL's 144
 - 4.4.2 Numbered en named ACL's 145

- 4.4.3 Waar ACL's te plaatsen 145
- 4.4.4 Voorbeeld van plaatsing van een standard ACL 146
- 4.4.5 Voorbeeld van plaatsing van extended ACL's 147
- 4.4.6 Test je kennis – Soorten IPv4-ACL's 148
- 4.5 Oefeningen en quiz 149
 - 4.5.1 Wat heb je in dit hoofdstuk geleerd? 149
 - 4.5.2 Quiz – ACL-concepten 151
- 5 ACL's voor IPv4-configuraties 155**
- 5.0 Inleiding 155
 - 5.0.1 Waarom zou je dit hoofdstuk bestuderen? 155
 - 5.0.2 Wat leer je in dit hoofdstuk? 155
- 5.1 Configureer standard IPv4-ACL's 155
 - 5.1.1 Maak een ACL aan 155
 - 5.1.2 Syntax genummerde standard IPv4-ACL's 156
 - 5.1.3 Syntax named standard IPv4-ACL's 156
 - 5.1.4 Koppel een standard IPv4-ACL 157
 - 5.1.5 Voorbeeld genummerde standard IPv4-ACL 157
 - 5.1.6 Voorbeeld named standard IPv4-ACL 159
 - 5.1.7 Syntax Checker – Configureer standard IPv4-ACL's 160
 - 5.1.8 Packet Tracer – Configureer genummerde standard IPv4-ACL's 161
 - 5.1.9 Packet Tracer – Configureer named standard IPv4-ACL's 161
- 5.2 IPv4-ACL's aanpassen 161
 - 5.2.1 Twee methoden om een ACL aan te passen 161
 - 5.2.2 Teksteditormethode 162
 - 5.2.3 VolgnummERMethode 162
 - 5.2.4 Voorbeeld van het wijzigen van een named ACL 163
 - 5.2.5 ACL-statistieken 164
 - 5.2.6 Syntax Checker – Wijzig IPv4-ACL's 164
 - 5.2.7 Packet Tracer – Configureer en wijzig standard IPv4-ACL's 165
- 5.3 Beveilig VTY-poorten met een standard IPv4-ACL 165
 - 5.3.1 Het commando access-class 165
 - 5.3.2 Voorbeeld van beveiligde VTY-toegang 166
 - 5.3.3 Verifieer of de VTY-poort beveiligd is 167
 - 5.3.4 Syntax Checker – Beveilig de VTY-poorten 168
- 5.4 Configureer extended IPv4-ACL's 169
 - 5.4.1 Extended ACL's 169
 - 5.4.2 Syntax genummerde extended IPv4-ACL 169
 - 5.4.3 Protocollen en poorten 170
 - 5.4.4 Voorbeelden van protocollen- en poortnummerconfiguratie 172
 - 5.4.5 Een genummerde extended IPv4-ACL koppelen 173
 - 5.4.6 TCP established extended ACL 173
 - 5.4.7 Syntax named extended IPv4-ACL 175
 - 5.4.8 Voorbeeld named extended IPv4-ACL 175
 - 5.4.9 Extended ACL's bewerken 176
 - 5.4.10 Nog een named extended IPv4-ACL-voorbeeld 177
 - 5.4.11 Verifieer extended ACL's 178
 - 5.4.12 Packet Tracer – Configureer extended IPv4-ACL's – scenario 1 180
 - 5.4.13 Packet Tracer – Configureer extended IPv4-ACL's – scenario 2 180
- 5.5 Opdrachten en quiz 181
 - 5.5.1 Packet Tracer – Challenge IPv4-ACL-implementatie 181
 - 5.5.2 Lab – Configureer en verifieer extended IPv4-ACL's 181
 - 5.5.3 Wat heb je in dit hoofdstuk geleerd? 181
 - 5.5.4 Quiz – ACL's voor IPv4-configuraties 183

- 6 NAT voor IPv4 187**
- 6.0 Inleiding 187
 - 6.0.1 Waarom zou je dit hoofdstuk bestuderen? 187
 - 6.0.2 Wat leer je in dit hoofdstuk? 187
- 6.1 NAT-eigenschappen 187
 - 6.1.1 Private IPv4-adresruimte 187
 - 6.1.2 Wat is NAT? 188
 - 6.1.3 Hoe NAT werkt 189
 - 6.1.4 NAT-terminologie 190
 - 6.1.5 Test je kennis – NAT-eigenschappen 191
- 6.2 Soorten NAT 192
 - 6.2.1 Statische NAT 192
 - 6.2.2 Dynamische NAT 193
 - 6.2.3 Port Address Translation 193
 - 6.2.4 Volgende beschikbare poort 194
 - 6.2.5 Vergelijking NAT – PAT 195
 - 6.2.6 Packets zonder laag-4-segment 196
 - 6.2.7 Packet Tracer – Onderzoek NAT-operaties 196
- 6.3 NAT voor- en nadelen 197
 - 6.3.1 Voordelen van NAT 197
 - 6.3.2 Nadelen van NAT 197
 - 6.3.3 Test je kennis – NAT-voor- en nadelen 198
- 6.4 Statische NAT 198
 - 6.4.1 Scenario statische NAT 198
 - 6.4.2 Statische NAT configureren 199
 - 6.4.3 Statische NAT analyseren 199
 - 6.4.4 Statische NAT verifiëren 200
 - 6.4.5 Packet Tracer – Statische NAT configureren 201
- 6.5 Dynamische NAT 201
 - 6.5.1 Scenario dynamische NAT 201
 - 6.5.2 Dynamische NAT configureren 202
 - 6.5.3 Dynamische NAT analyseren – inside naar outside 203
 - 6.5.4 Dynamische NAT analyseren – outside naar inside 204
 - 6.5.5 Dynamische NAT verifiëren 205
 - 6.5.6 Packet Tracer – Dynamische NAT configureren 207
- 6.6 PAT 207
 - 6.6.1 PAT-scenario 207
 - 6.6.2 Configureer PAT om een enkel IPv4-adres te gebruiken 208
 - 6.6.3 Configureer PAT om een adrespool te gebruiken 208
 - 6.6.4 Analyseer PAT – PC naar server 209
 - 6.6.5 Analyseer PAT – server naar PC 210
 - 6.6.6 PAT verifiëren 211
 - 6.6.7 Packet Tracer – Configureer PAT 211
- 6.7 NAT64 212
 - 6.7.1 NAT voor IPv6? 212
 - 6.7.2 NAT64 212
- 6.8 Opdrachten en quiz 213
 - 6.8.1 Packet Tracer – Configureer NAT voor IPv4 213
 - 6.8.2 Lab – Configureer NAT voor IPv4 213
 - 6.8.3 Wat leerde je in dit hoofdstuk? 213
 - 6.8.4 Quiz – NAT voor IPv4 216

7	WAN-concepten	219
7.0	Inleiding	219
7.0.1	Waarom zou je dit hoofdstuk bestuderen?	219
7.0.2	Wat leer je in dit hoofdstuk?	219
7.1	Doel van WAN's	219
7.1.1	LAN's en WAN's	219
7.1.2	Private en publieke WAN's	220
7.1.3	WAN-topologieën	221
7.1.4	Carrier-verbindingen	223
7.1.5	Evoluerende netwerken	224
7.1.6	Test je kennis – Doel van WAN's	227
7.2	Werking van WAN's	228
7.2.1	WAN-standaarden	228
7.2.2	WAN's in het OSI-model	228
7.2.3	Veelgebruikte WAN-terminologie	229
7.2.4	WAN-apparaten	230
7.2.5	Seriële communicatie	232
7.2.6	Circuit-switched communicatie	232
7.2.7	Packet-switched communicatie	233
7.2.8	SDH, SONET en DWDM	234
7.2.9	Test je kennis – Werking van WAN's	235
7.3	Traditionele WAN-verbindingen	236
7.3.1	Traditionele WAN-verbindingsopties	236
7.3.2	Veelgebruikte WAN-terminologieën	237
7.3.3	Circuit-switched opties	238
7.3.4	Packet-switched opties	238
7.3.5	Test je kennis – Traditionele WAN-verbindingen	239
7.4	Moderne WAN-verbindingen	239
7.4.1	Moderne WAN's	239
7.4.2	Moderne WAN-verbindingsopties	240
7.4.3	Ethernet WAN	241
7.4.4	MPLS	242
7.4.5	Test je kennis – Moderne WAN-verbindingen	243
7.5	Internet-based verbindingen	243
7.5.1	Internet-based verbindingsopties	243
7.5.2	DSL-technologie	244
7.5.3	DSL-verbindingen	245
7.5.4	DSL en PPP	246
7.5.5	Kabeltechnologie	246
7.5.6	Glasvezel	247
7.5.7	Draadloos internet-based breedband	247
7.5.8	VPN-technologie	249
7.5.9	ISP-verbindingsopties	250
7.5.10	Vergelijking van breedbandoplossingen	251
7.5.11	Lab – Onderzoek de breedbandinternetopties	251
7.6	Opdrachten en quiz	251
7.6.1	Packet Tracer WAN-concepten	251
7.6.2	Wat leerde je in dit hoofdstuk?	252
7.6.3	Quiz – WAN-concepten	254
8	VPN- en IPsec-concepten	257
8.0	Inleiding	257
8.0.1	Waarom zou je dit hoofdstuk bestuderen?	257
8.0.2	Wat leer je in dit hoofdstuk?	257

- 8.1 VPN-technologie 257
 - 8.1.1 Virtuele Private Netwerken 257
 - 8.1.2 Voordelen van VPN 258
 - 8.1.3 Site-to-site- en remote-access-VPN's 259
 - 8.1.4 Bedrijfs- en serviceprovider-VPN's 259
 - 8.1.5 Test je kennis – VPN-technologie 260
 - 8.2 Soorten VPN's 261
 - 8.2.1 Remote-access-VPN's 261
 - 8.2.2 SSL-VPN's 262
 - 8.2.3 Site-to-site-IPsec-VPN's 262
 - 8.2.4 GRE over IPsec 263
 - 8.2.5 Dynamische Multipoint-VPN's 264
 - 8.2.6 IPsec Virtual Tunnel Interface 265
 - 8.2.7 Serviceprovider-MPLS-VPN's 266
 - 8.2.8 Test je kennis – Soorten VPN's 267
 - 8.3 IPsec 267
 - 8.3.1 Video – IPsec-concepten 267
 - 8.3.2 IPsec-technologieën 267
 - 8.3.3 Inpakprotocol voor IPsec 269
 - 8.3.4 Vertrouwelijkheid 270
 - 8.3.5 Integriteit 271
 - 8.3.6 Authenticatie 273
 - 8.3.7 Beveiligde sleuteluitwisseling met Diffie-Hellman 275
 - 8.3.8 Video – IPsec-transport en -tunnelmode 275
 - 8.3.9 Test je kennis – IPsec 276
 - 8.4 Oefeningen en quiz 277
 - 8.4.1 Wat leerde je in dit hoofdstuk? 277
 - 8.4.2 Quiz – VPN- en IPsec-concepten 278
- 9 QoS-concepten 281**
- 9.0 Inleiding 281
 - 9.0.1 Waarom zou je dit hoofdstuk bestuderen? 281
 - 9.0.2 Wat leer je in dit hoofdstuk? 281
 - 9.1 Netwerktransmissiekwaliteit 281
 - 9.1.1 Video – Het doel van QoS 281
 - 9.1.2 Prioritering van dataverkeer 281
 - 9.1.3 Bandbreedte, congestie, vertraging en jitter 282
 - 9.1.4 Packet loss 283
 - 9.1.5 Test je kennis – Netwerktransmissiekwaliteit 285
 - 9.2 Verkeerskenmerken 285
 - 9.2.1 Video – Verkeerskenmerken 285
 - 9.2.2 Trends in netwerkverkeer 285
 - 9.2.3 Spraak 286
 - 9.2.4 Video 286
 - 9.2.5 Data 287
 - 9.2.6 Test je kennis – Verkeerskenmerken 288
 - 9.3 Queuing-algoritmen 289
 - 9.3.1 Video – QoS-algoritmen 289
 - 9.3.2 Overzicht queuing 289
 - 9.3.3 First In First Out 289
 - 9.3.4 Weighted Fair Queuing (WFQ) 290
 - 9.3.5 Class Based Weighted Fair Queuing (CBWFQ) 291
 - 9.3.6 Low Latency Queuing (LLQ) 291
 - 9.3.7 Test je kennis – Queuing-algoritmen 292

9.4	QoS-modellen	293
9.4.1	Video – QoS-modellen	293
9.4.2	Een geschikt QoS-policy-model selecteren	293
9.4.3	Best effort	294
9.4.4	Integrated Services	294
9.4.5	Differentiated services	295
9.4.6	Test je kennis – QoS-modellen	297
9.5	QoS-implementatietechnieken	297
9.5.1	Video – QoS-implementatietechnieken	297
9.5.2	Voorkoming van packet loss	298
9.5.3	QoS-tools	298
9.5.4	Classificatie en markering	299
9.5.5	Markering op laag 2	300
9.5.6	Markering op laag 3	300
9.5.7	Type of Service- en Traffic Class-veld	301
9.5.8	DSCP-waarden	302
9.5.9	Class selector bits	302
9.5.10	Trust boundaries	303
9.5.11	Congestion avoidance	304
9.5.12	Shaping en policing	305
9.5.13	Richtlijnen voor QoS-policy	305
9.5.14	Test je kennis – QoS-implementatietechnieken	306
9.6	Oefeningen en quiz	306
9.6.1	Wat leerde je in dit hoofdstuk?	306
9.6.2	Quiz – QoS-concepten	309
10	Netwerkbeheer	313
10.0	Inleiding	313
10.0.1	Waarom zou je dit hoofdstuk bestuderen?	313
10.0.2	Wat leer je in dit hoofdstuk?	313
10.1	Apparaten verkennen met CDP	313
10.1.1	Overzicht CDP	313
10.1.2	CDP configureren en verifiëren	314
10.1.3	Verken apparaten door CDP te gebruiken	315
10.1.4	Syntax Checker – Configureer en verifieer CDP	318
10.1.5	Packet Tracer – Gebruik CDP om een netwerk in kaart te brengen	318
10.2	Apparaten verkennen met LLDP	318
10.2.1	Overzicht LLDP	318
10.2.2	LLDP configureren en verifiëren	319
10.2.3	Verken apparaten door LLDP te gebruiken	319
10.2.4	Syntax Checker – Configureer en verifieer LLDP	321
10.2.5	Test je kennis – Vergelijk CDP en LLDP	321
10.2.6	Packet Tracer – Gebruik LLDP om een netwerk in kaart te brengen	321
10.3	NTP	321
10.3.1	Tijd- en kalenderservices	321
10.3.2	Werking van NTP	322
10.3.3	NTP configureren en verifiëren	323
10.3.4	Packet Tracer – Configureer en verifieer NTP	325
10.4	SNMP	325
10.4.1	Inleiding in SNMP	325
10.4.2	Werking van SNMP	326
10.4.3	SNMP-agent-traps	327
10.4.4	SNMP-versies	328
10.4.5	Test je kennis – SNMP-versies	330
10.4.6	Communitystrings	331

- 10.4.7 MIB-object-ID 332
- 10.4.8 SNMP-polling-scenario 333
- 10.4.9 SNMP-objectnavigator 334
- 10.4.10 Lab – Onderzoek netwerkmonitorsoftware 335
- 10.5 Syslog 335
 - 10.5.1 Introductie Syslog 335
 - 10.5.2 Werking van syslog 336
 - 10.5.3 Syslog-berichtformaat 336
 - 10.5.4 Syslog-faciliteiten 337
 - 10.5.5 Configureer de syslog timestamp 338
 - 10.5.6 Test je kennis – Werking van syslog 338
- 10.6 Router- en switch-bestandsbeheer 339
 - 10.6.1 Routerbestandssysteem 339
 - 10.6.2 Switch-bestandssysteem 341
 - 10.6.3 Gebruik een tekstbestand voor een back-up van een configuratie 342
 - 10.6.4 Gebruik een tekstbestand om een configuratie terug te zetten 342
 - 10.6.5 Gebruik TFTP om een configuratie te back-uppen en terug te zetten 343
 - 10.6.6 USB-poorten op een Cisco-router 344
 - 10.6.7 Gebruik USB om een configuratie te back-uppen en terug te zetten 344
 - 10.6.8 Wachtwoordrecoveryprocedures 346
 - 10.6.9 Voorbeeld van wachtwoordrecovery 347
 - 10.6.10 Packet Tracer – Configuratiebestanden back-uppen 348
 - 10.6.11 Lab – Gebruik Tera Term om routerconfiguratiebestanden te beheren 348
 - 10.6.12 Lab – Gebruik TFTP, flash en USB om configuratiebestanden te beheren 349
 - 10.6.13 Lab – Onderzoek wachtwoordrecoveryprocedures 349
- 10.7 IOS-image-beheer 349
 - 10.7.1 Video – Cisco IOS-images beheren 349
 - 10.7.2 TFTP-servers als back-uplocatie 349
 - 10.7.3 Voorbeeld van een back-up naar een TFTP-server 350
 - 10.7.4 Voorbeeld van het kopiëren van IOS-image naar een apparaat 351
 - 10.7.5 Het commando boot system 352
 - 10.7.6 Packet Tracer – Gebruik een TFTP-server om een Cisco IOS-image te upgraden 353
- 10.8 Oefeningen en quiz 353
 - 10.8.1 Packet Tracer – Configureer CDP, LLDP en NTP 353
 - 10.8.2 Lab – Configureer CDP, LLDP en NTP 354
 - 10.8.3 Wat leerde je in dit hoofdstuk? 354
 - 10.8.4 Quiz – Netwerkbeheer 357
- 11 Netwerkontwerp 361**
 - 11.0 Inleiding 361
 - 11.0.1 Waarom zou je dit hoofdstuk bestuderen? 361
 - 11.0.2 Wat leer je in dit hoofdstuk? 361
 - 11.1 Hiërarchische netwerken 361
 - 11.1.1 Video – Drie-lagen-netwerkontwerp 361
 - 11.1.2 De noodzaak om een netwerk op te schalen 361
 - 11.1.3 Borderless switched netwerken 363
 - 11.1.4 Hiërarchie in het borderless switched netwerk 363
 - 11.1.5 Access, distribution en core layer-functies 365
 - 11.1.6 Voorbeelden three tier en two tier 366
 - 11.1.7 Rol van switched netwerken 367
 - 11.1.8 Test je kennis – Hiërarchische netwerken 368
 - 11.2 Schaalbare netwerken 368
 - 11.2.1 Ontwerpen voor schaalbaarheid 368
 - 11.2.2 Plan voor redundantie 371
 - 11.2.3 Verminder de grootte van het failure-domein 371

11.2.4	Bandbreedte verhogen	374
11.2.5	De access layer uitbreiden	374
11.2.6	Routingprotocollen tunen	375
11.2.7	Test je kennis – Schaalbare netwerken	376
11.3	Switch-hardware	376
11.3.1	Switch-platforms	376
11.3.2	Switch-vormfactoren	378
11.3.3	Poort-density	380
11.3.4	Forwarding-snelheden	381
11.3.5	Power over Ethernet	381
11.3.6	Multilayer-switching	382
11.3.7	Zakelijke overwegingen bij het selecteren van een switch	383
11.3.8	Test je kennis – Switch-hardware	383
11.4	Router-hardware	384
11.4.1	Routereisen	384
11.4.2	Cisco-routers	385
11.4.3	Router-vormfactoren	386
11.4.4	Test je kennis – Router-hardware	389
11.5	Opdrachten en quiz	389
11.5.1	Packet Tracer – Vergelijk laag-2- en laag-3-apparaten	389
11.5.2	Wat heb je in dit hoofdstuk geleerd?	389
11.5.3	Quiz – Netwerkontwerp	391
12	Netwerk troubleshooten	395
12.0	Inleiding	395
12.0.1	Waarom zou je dit hoofdstuk bestuderen?	395
12.0.2	Wat leer je in dit hoofdstuk?	395
12.1	Netwerkdokumentatie	395
12.1.1	Overzicht documentatie	395
12.1.2	Netwerktopologietekeningen	396
12.1.3	Documentatie van de netwerkapparaten	398
12.1.4	Stel een netwerk-baseline vast	399
12.1.5	Stap 1 – Bepaal welke soorten data je gaat verzamelen	400
12.1.6	Stap 2 – Bepaal de interessante apparaten en poorten	400
12.1.7	Stap 3 – Bepaal de duur van de baseline	400
12.1.8	Datameting	402
12.1.9	Test je kennis – Netwerkdokumentatie	403
12.2	Het troubleshootproces	403
12.2.1	Algemene troubleshootprocedures	403
12.2.2	Troubleshootproces in zeven stappen	404
12.2.3	Bevraag eindgebruikers	406
12.2.4	Verzamel informatie	407
12.2.5	Troubleshooten met gelaagde modellen	407
12.2.6	Gestructureerde troubleshootmethoden	408
12.2.7	Richtlijnen voor het selecteren van een troubleshootmethode	411
12.2.8	Test je kennis – Troubleshootproces	412
12.3	Troubleshooting-tools	413
12.3.1	Softwaretroubleshooting-tools	413
12.3.2	Protocol-analyzers	414
12.3.3	Hardware-troubleshooting-tools	414
12.3.4	Syslog-server als troubleshoot-tool	416
12.3.5	Test je kennis – Troubleshoot-tools	417
12.4	Symptomen en oorzaken van netwerkproblemen	418
12.4.1	De fysieke laag troubleshooten	418
12.4.2	De data-linklaag troubleshooten	421

- 12.4.3 De netwerklaag troubleshooten 423
- 12.4.4 De transportlaag troubleshooten – ACL's 424
- 12.4.5 De transportlaag troubleshooten – NAT voor IPv4 426
- 12.4.6 De applicatielaag troubleshooten 427
- 12.4.7 Test je kennis – Symptomen en oorzaken van netwerkproblemen 428
- 12.5 Troubleshooten van IP-connectiviteit 429
 - 12.5.1 Onderdelen voor het troubleshooten van end-to-end-connectiviteit 429
 - 12.5.2 End-to-end-connectiviteitsprobleem veroorzaakt troubleshooten 430
 - 12.5.3 Stap 1: Verifieer de fysieke laag 432
 - 12.5.4 Stap 2: Controleer op duplex-mismatches 434
 - 12.5.5 Stap 3: Verifieer de adressering van het lokale netwerk 435
 - 12.5.6 Voorbeeld van het troubleshooten van VLAN-toewijzing 437
 - 12.5.7 Stap 4: Verifieer de default gateway 439
 - 12.5.8 Voorbeeld troubleshooten van IPv6 default gateway 440
 - 12.5.9 Stap 5: Verifieer het juiste pad 442
 - 12.5.10 Stap 6: Verifieer de transportlaag 444
 - 12.5.11 Stap 7: Verifieer de ACL's 446
 - 12.5.12 Stap 8: Verifieer DNS 447
 - 12.5.13 Packet Tracer – Bedrijfsnetwerken troubleshooten 448
- 12.6 Oefeningen en quiz 448
 - 12.6.1 Packet Tracer – Troubleshooting challenge – Documenteer het netwerk 448
 - 12.6.2 Packet Tracer – Troubleshooting challenge – Gebruik de documentatie om problemen op te lossen 448
 - 12.6.3 Wat heb je in dit hoofdstuk geleerd? 448
 - 12.6.4 Quiz – Netwerk troubleshooten 451
- 13 Netwerkvirtualisatie 455**
- 13.0 Inleiding 455
 - 13.0.1 Waarom zou je dit hoofdstuk bestuderen? 455
 - 13.0.2 Wat leer je in dit hoofdstuk? 455
- 13.1 Cloud computing 455
 - 13.1.1 Video – Cloud en virtualisatie 455
 - 13.1.2 Overzicht clouds 455
 - 13.1.3 Cloudservices 456
 - 13.1.4 Cloudmodellen 456
 - 13.1.5 Cloud computing versus datacenter 457
 - 13.1.6 Test je kennis – Cloud computing 458
- 13.2 Virtualisatie 458
 - 13.2.1 Cloud computing en virtualisatie 458
 - 13.2.2 Dedicated servers 459
 - 13.2.3 Servervirtualisatie 460
 - 13.2.4 Voordelen van virtualisatie 461
 - 13.2.5 Abstractielagen 461
 - 13.2.6 Type 2 hypervisors 462
 - 13.2.7 Test je kennis – Virtualisatie 463
- 13.3 Virtuele netwerkinfrastructuur 464
 - 13.3.1 Type 1 hypervisors 464
 - 13.3.2 Een VM op een hypervisor installeren 464
 - 13.3.3 De complexiteit van netwerkvirtualisatie 465
 - 13.3.4 Test je kennis – Virtuele netwerkinfrastructuur 466
- 13.4 Software-defined netwerken 467
 - 13.4.1 Video – Software-Defined Networking 467
 - 13.4.2 Control-plane en data-plane 467
 - 13.4.3 Netwerkvirtualisatietechnologieën 469
 - 13.4.4 Traditionele en SDN-architecturen 469
 - 13.4.5 Test je kennis – Software-Defined Networking 471

- 13.5 **Controllers 471**
 - 13.5.1 SDN-controller en werking 471
 - 13.5.2 Video – Cisco ACI 472
 - 13.5.3 Core-componenten va ACI 473
 - 13.5.4 Spine-Leaf-topologie 473
 - 13.5.5 SDN-types 474
 - 13.5.6 APIC-EM-functies 476
 - 13.5.7 APIC-EM Path Trace 476
 - 13.5.8 Test je kennis – Controllers 477
- 13.6 **Opdrachten en quiz 478**
 - 13.6.1 Lab – Installeer Linux op een Virtual Machine en verken de GUI 478
 - 13.6.2 Wat heb je in dit hoofdstuk geleerd? 478
 - 13.6.3 Quiz – Netwerkvirtualisatie 481

- 14 Netwerkautomatisering 485**
- 14.0 **Inleiding 485**
 - 14.0.1 Waarom zou je dit hoofdstuk bestuderen? 485
 - 14.0.2 Wat leer je in dit hoofdstuk? 485
- 14.1 **Overzicht automatisering 485**
 - 14.1.1 Video – Automatisering is overal 485
 - 14.1.2 De toename van automatisering 485
 - 14.1.3 Denkende apparaten 486
 - 14.1.4 Test je kennis – Voordelen van automatisering 486
- 14.2 **Dataformaten 487**
 - 14.2.1 Video – Dataformaten 487
 - 14.2.2 Het dataformaatconcept 487
 - 14.2.3 Dataformaatregels 488
 - 14.2.4 Vergelijking dataformaten 489
 - 14.2.5 JSON-dataformaat 489
 - 14.2.6 JSON-syntaxregels 490
 - 14.2.7 YAML-dataformaat 491
 - 14.2.8 XML-dataformaat 492
 - 14.2.9 Test je kennis – Dataformaten 493
- 14.3 **API's 493**
 - 14.3.1 Video – API's 493
 - 14.3.2 Het API-concept 494
 - 14.3.3 Een API-voorbeeld 494
 - 14.3.4 Open, interne en partner API's 495
 - 14.3.5 Soorten webservice-API's 496
 - 14.3.6 Test je kennis – API's 497
- 14.4 **REST 497**
 - 14.4.1 Video – REST 497
 - 14.4.2 REST en RESTful API 498
 - 14.4.3 RESTful implementatie 498
 - 14.4.4 URI, URN en URL 499
 - 14.4.5 Anatomie van een RESTful-request 500
 - 14.4.6 RESTful API-applicaties 501
 - 14.4.7 Test je kennis – REST 502
- 14.5 **Configuratiemanagementtools 503**
 - 14.5.1 Video – Configuratiemanagementtools 503
 - 14.5.2 Traditionele netwerkconfiguratie 503
 - 14.5.3 Netwerkautomatisering 505
 - 14.5.4 Configuratiemanagementtools 505
 - 14.5.5 Vergelijking van Ansible, Chef, Puppet en SaltStack 506
 - 14.5.6 Test je kennis – Configuratiemanagement 506

- 14.6 IBN en CISCO DNA Center 507
 - 14.6.1 Video – Intent-Based Networking 507
 - 14.6.2 Overzicht van Intent-Based Networking 507
 - 14.6.3 Netwerkinfrastructuur als fabric 508
 - 14.6.4 Cisco Digital Network Architecture (DNA) 509
 - 14.6.5 Cisco DNA Center 511
 - 14.6.6 Video – DNA Center overzicht en platform API's 512
 - 14.6.7 Video – DNA Center design en provision 512
 - 14.6.8 Video – DNA-center policy en assurance 513
 - 14.6.9 DNA Center connectiviteit troubleshooten 513
 - 14.6.10 Test je kennis – IBN en Cisco DNA-center 513
- 14.7 Opdrachten en quiz 514
 - 14.7.1 Wat leerde je in dit hoofdstuk? 514
 - 14.7.2 Quiz – Netwerkautomatisering 515

o Bedrijfsnetwerken, beveiliging en automatisering

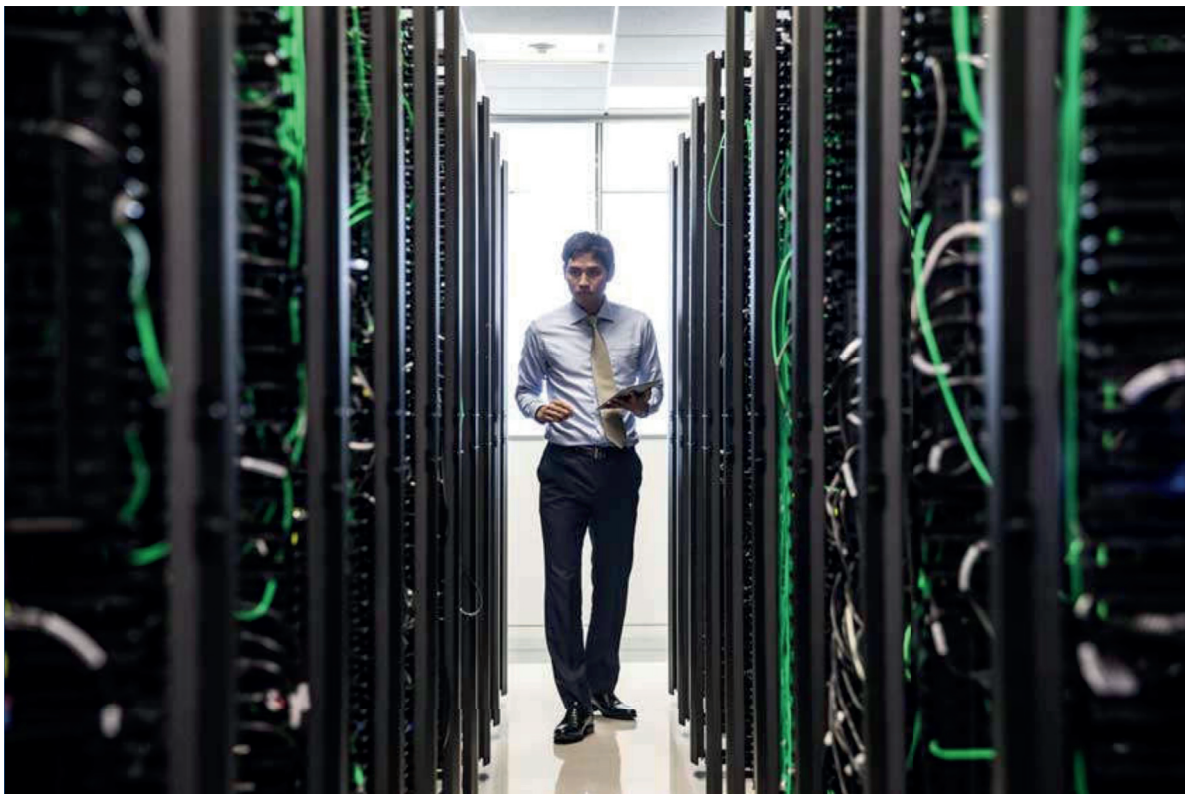
Networking Academy CCNAv7

Welkom bij de laatste cursus van het Cisco Networking Academy CCNAv7-curriculum, *Enterprise Networking, Security en Automation* (ENSA). Dit is de derde van drie cursussen die zijn afgestemd op het CCNA-certificeringsexamen. ENSA bevat 14 modules, elk met een reeks onderwerpen.

In *Bedrijfsnetwerken, beveiliging en automatisering* bouw je voort op de vaardigheden en kennis uit *Netwerken Deel 1* en 2 pas je ze toe op **Wide Area Networks** (WAN's). WAN's zijn grote, complexe netwerken die een geavanceerd begrip van de werking en beveiliging van het netwerk vereisen. ENSA laat je ook kennismaken met twee baanbrekende gebieden van netwerken: virtualisatie en automatisering.

Aan het einde van deze cursus kun je bedrijfsnetwerkapparaten configureren, troubleshooten en beveiligen. Je bent vertrouwd met Application Programming Interfaces (API's) en de tools voor configuratiebeheer die netwerkautomatisering mogelijk maken.

Wanneer je ENSA afgerond hebt, heb je de praktische ervaring opgedaan die je nodig hebt om je op het certificeringsexamen voor te bereiden. Je hebt ook de vaardigheden die nodig zijn voor rollen op associate-niveau in de informatie- en communicatietechnologie (ICT). Laat Cisco Networking Academy je helpen waar je wilt zijn!



LET OP!

Om de Packet-Tracer- en Lab-activiteiten te kunnen uitvoeren heb je de nieuwste versie van Packet Tracer nodig. Hiervoor is een account bij de Cisco Networking Academy nodig.

Ga naar netacad.boomberoepsonderwijs.nl om je aan te melden via je **School-** of **Boom-account** en volg de stappen zoals deze vervolgens op de site aangegeven zijn.

Heb je nog geen account, registreer je dan eerst als gebruiker via **Registreer**.

1 Single area OSPFv2-concepten

1.0 Inleiding

1.0.1 Waarom zou je dit hoofdstuk bestuderen?

Welkom bij de single area OSPFv2-concepten! Welkom bij het eerste hoofdstuk van CCNA Enterprise *Bedrijfsnetwerken, beveiliging en automatisering v7.0!*

Stel je voor dat het tijd is dat je familie je grootouders bezoekt. Je pakt je koffers en laadt ze in de auto. Maar dit duurt iets langer dan gepland en nu kom je te laat. Je haalt je wegencartaar tevoorschijn. Er zijn drie verschillende routes. Eén route is niet goed omdat er veel wegwerkzaamheden zijn op de hoofdweg en deze tijdelijk is afgesloten. Een andere route is erg mooi, maar het duurt nog een uur om op je bestemming te komen. De derde route is niet zo mooi, maar er is een snelweg, die veel sneller is. Deze route is zelfs zoveel sneller dat je misschien wel op tijd komt als je deze neemt.

Bij netwerken hoeven packets niet de landschappelijke route te nemen. De snelste beschikbare route is altijd de beste. Open Shortest Path First (OSPF) is ontworpen om het snelste beschikbare pad voor een packet van de source naar de destination te vinden. Dit hoofdstuk behandelt de basisconcepten van OSPFv2 in één gebied (single area). Laten we beginnen!

1.0.2 Wat leer je in dit hoofdstuk?

Er wordt uitgelegd hoe single area OSPFv2 werkt in zowel point-to-point- als in multi-access-netwerken. De paragrafen in dit hoofdstuk zijn:

Onderwerp	Doel
OSPF-functies en eigenschappen	Beschrijving van de basisfuncties en eigenschappen van OSPF.
OSPF-packets	Beschrijving van de OSPF-packet-typen die in een single area OSPF gebruikt worden.
OSPF-werking	Uitleg over hoe single area OSPF werkt.

1.1 OSPF-functies en -eigenschappen

1.1.1 Inleiding in OSPF

Deze paragraaf geeft een kort overzicht van Open Shortest Path First (OSPF), dat single area en multi-area omvat. OSPFv2 wordt gebruikt voor IPv4-netwerken. OSPFv3 wordt gebruikt voor IPv6-netwerken. De primaire focus van dit hele hoofdstuk is OSPFv2 met single area (één gebied).

OSPF is een **Link-state**-routingprotocol dat als alternatief ontwikkeld is voor het **Distance Vector Routing Information Protocol** (RIP). RIP was een acceptabel routingprotocol in de begintijd van netwerken en internet. De RIP-afhankelijkheid van het aantal hops als enige metric voor het bepalen van de beste route werd echter al snel problematisch. Het gebruik van het aantal hops is niet goed schaalbaar in grotere netwerken met meerdere paden met verschillende snelheden. OSPF heeft aanzienlijke voordelen ten opzichte van RIP doordat het snellere convergentie biedt en naar veel grotere netwerkimplementaties opgeschaald kan worden.

OSPF is een **Link-state**-routingprotocol dat gebruikmaakt van het concept van area's (gebieden). Een netwerkbeheerder kan het routingdomein opsplitsen in verschillende gebieden die helpen bij het beheren van routing-updateverkeer. Een link is een interface op een router. Een link is ook een netwerksegment dat twee routers met elkaar verbindt, of een stub-netwerk zoals een Ethernet LAN dat is aangesloten op een enkele router. Informatie over de status van een link wordt een linkstatus genoemd. Alle informatie over de linkstatus omvat het netwerkprefix, de prefixlengte en de costs.

Dit hoofdstuk behandelt eenvoudige OSPF-implementaties en configuraties met één gebied.

1.1.2 Onderdelen van OSPF

Alle routingprotocollen delen vergelijkbare componenten. Ze gebruiken allemaal routingprotocolberichten om route-informatie uit te wisselen. De berichten helpen bij het opbouwen van datastructuren, die vervolgens met behulp van een routingalgoritme verwerkt worden.

Routers met OSPF wisselen berichten uit om routinginformatie over te brengen met behulp van vijf soorten packets. Deze packets zie je in figuur 1-1:

- 1 Hello-packet
- 2 Database description-packet
- 3 Link-state-request-packet
- 4 Link-state-update-packet
- 5 Acknowledgment-packet voor verbindingstoestand

Routingprotocolberichten

Deze pakketten worden gebruikt om naburige routers te ontdekken en ook om routinginformatie uit te wisselen om nauwkeurige informatie over het netwerk bij te houden.



Figuur 1-1 Routers wisselen Hello-packets uit

Datastructuren

Er worden OSPF-berichten gebruikt om de volgende drie OSPF-databases te maken en te onderhouden:

- ▶ **Adjacency-database** – Deze creëert de neighbor-tabel.
- ▶ **Link-state-database** (LSDB) – Hiermee wordt de topologietabel gemaakt.
- ▶ **Forwarding-database** – Deze creëert de routetabel.

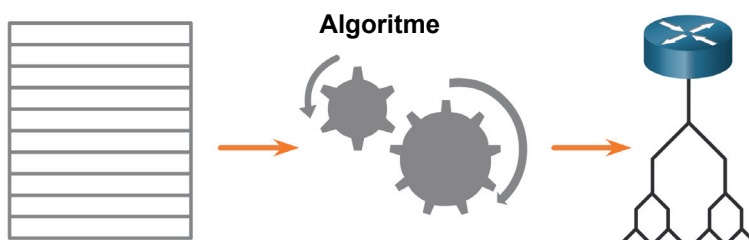
Deze tabellen bevatten een lijst van aangrenzende routers om routinginformatie uit te wisselen. De tabellen worden bewaard en onderhouden in RAM. In de volgende tabel zijn de commando's te zien die gebruikt worden om elke tabel weer te geven.

Database	Tabel	Beschrijving
Adjacency-database	Neighbor-tabel	<ul style="list-style-type: none"> ▶ Lijst met alle neighbor-routers waarmee een router bidirectionele communicatie tot stand heeft gebracht. ▶ Deze tabel is uniek voor elke router. ▶ Kan bekeken worden met het commando <code>show ip ospf neighbor</code>.
Link-state-database	Topologietabel	<ul style="list-style-type: none"> ▶ Geeft informatie over alle andere routers in het netwerk. ▶ Deze database vertegenwoordigt de netwerktopologie. ▶ Alle routers binnen een gebied hebben identieke LSDB. ▶ Kan met het databasecommando <code>show ip ospf</code> bekeken worden.
Forwarding-database	Routetabel	<ul style="list-style-type: none"> ▶ Lijst met routes die gegenereerd worden wanneer een algoritme op de Link-state-database uitgevoerd wordt. ▶ De routetabel van elke router is uniek en bevat informatie over hoe en waar pakketten naar andere routers gestuurd kunnen worden. ▶ Kan met het commando <code>show ip route</code> bekeken worden.

Algoritme

De router stelt de topologietabel samen met behulp van berekeningen op basis van het Dijkstra shortest-path first-algoritme (SPF). Het SPF-algoritme is gebaseerd op de cumulatieve kosten om een bestemming te bereiken.

Het SPF-algoritme maakt een SPF-tree door elke router in de root van de tree te plaatsen en het kortste pad naar elk knooppunt te berekenen. De SPF-tree wordt vervolgens gebruikt om de beste routes te berekenen. OSPF plaatst de beste routes in de forwarding-database, die gebruikt wordt om de routetabel te maken.



Figuur 1-2 Werking algoritme

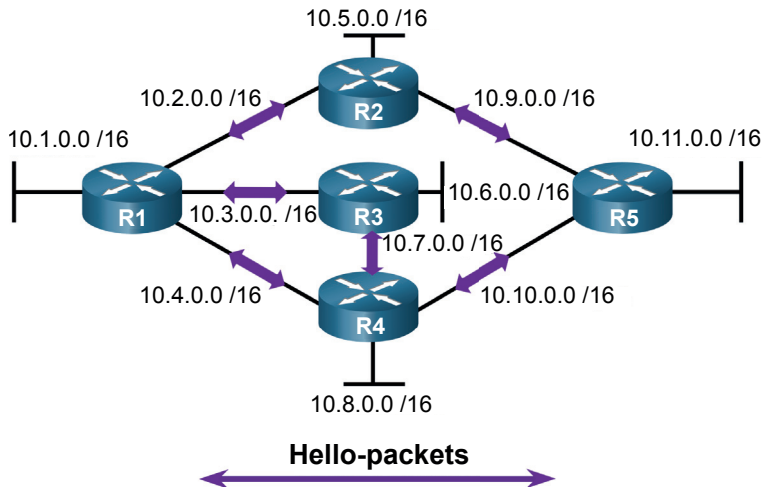
1.1.3 Werking Link-State

Om routinginformatie bij te houden, voeren OSPF-routers een generiek link-state-routingproces uit om een staat van convergentie te bereiken. Figuur 1-3 toont een topologie van vijf routers. Elke link tussen routers is gelabeld met een cost-waarde. In OSPF wordt de cost gebruikt om het beste pad naar de bestemming te bepalen. Hieronder volgen de routingstappen voor de link-status die door een router worden voltooid:

- 1 Bouw neighbor adjacencies op.
- 2 Wissel link-state-advertenties uit.
- 3 Bouw de link-state-database op.
- 4 Voer het SPF-algoritme uit.
- 5 Kies de beste route.

Bouw neighbor adjacencies op

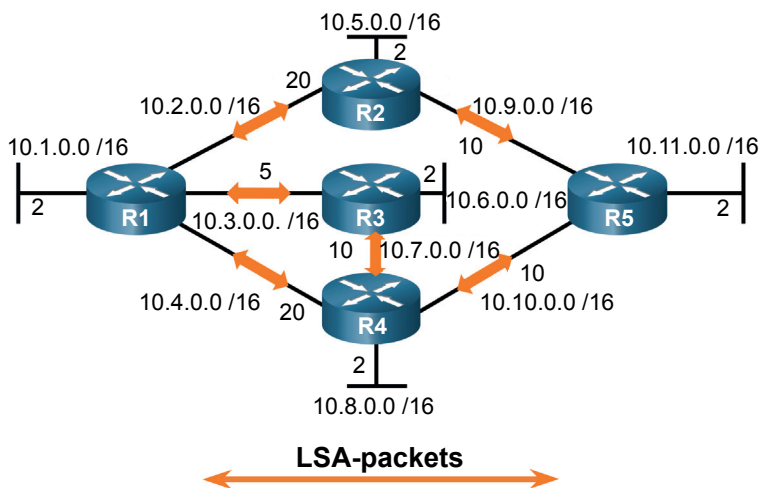
Routers die OSPF ondersteunen, moeten elkaar op het netwerk herkennen voordat ze informatie kunnen delen. Een OSPF-compatibele router verstuurt **Hello**-packets via alle OSPF-compatibele interfaces om te bepalen of er neighbors (buren) aanwezig zijn op die links. Als er een neighbor aanwezig is, probeert de router met OSPF-functionaliteit een adjacency (gemeenschap) met die neighbor tot stand te brengen.



Figuur 1-3 Routers wisselen Hello-packets uit

Wissel link-state-advertenties uit

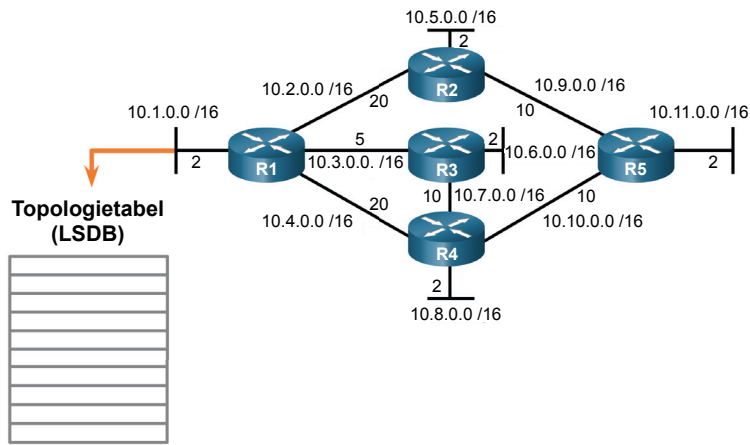
Nadat de adjacencies tot stand gebracht zijn, wisselen routers vervolgens link-state-advertenties (LSA's) uit. LSA's bevatten de status en costs van elke direct verbonden link. Routers versturen hun LSA's naar aangrenzende neighbors. Aangrenzende neighbors die de LSA ontvangen, versturen de LSA onmiddellijk door naar andere direct verbonden neighbors, totdat alle routers in het gebied alle LSA's hebben.



Figuur 1-4 Routers wisselen LSA's uit

Bouw de link-state-database op

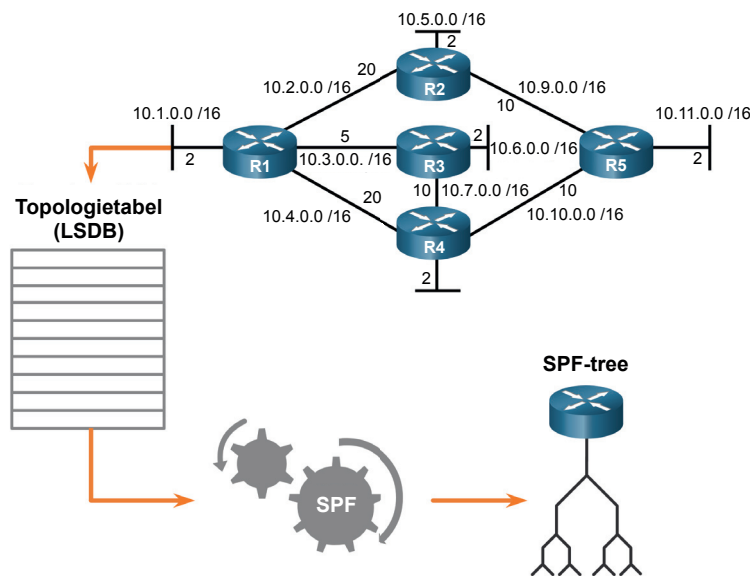
Nadat de LSA's ontvangen zijn, bouwen OSPF-compatibele routers de topologietabel (LSDB) op basis van de ontvangen LSA's op. Deze database bevat uiteindelijk alle informatie over de topologie van de area.



Figuur 1-5 R1 bouwt zijn topologietabel op

Voer het SPF-algoritme uit

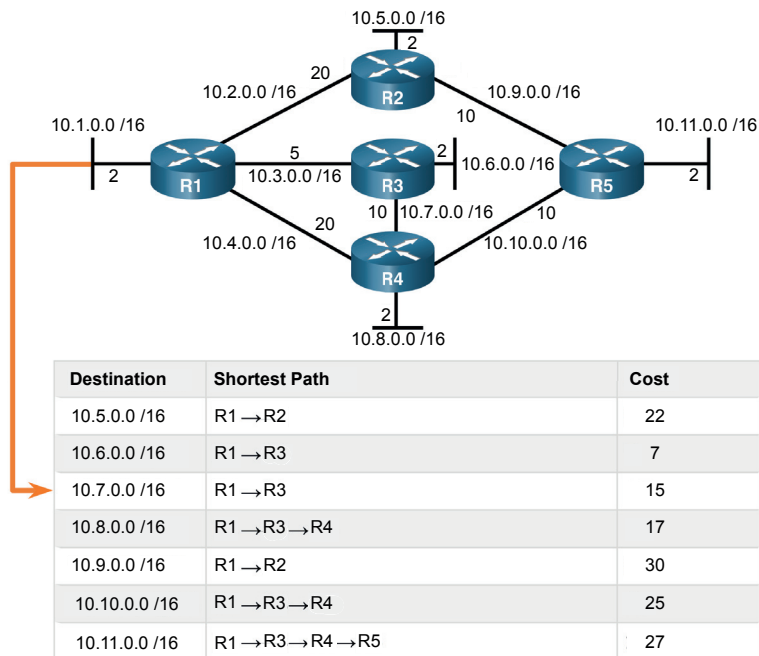
Routers voeren vervolgens het SPF-algoritme uit. De tandwielen in figuur 1-6 voor deze stap worden gebruikt om de uitvoering van het SPF-algoritme weer te geven. Het SPF-algoritme bouwt de SPF-tree op.



Figuur 1-6 R1 stelt de SPF-tree samen

Kies de beste route

Nadat de SPF-tree opgebouwd is, worden de beste paden naar elk netwerk aan de IP-routetabel aangeboden. De route wordt in de routetabel ingevoegd, tenzij er een route-source naar hetzelfde netwerk is met een lagere administratieve afstand (AD), zoals een statische route. Routebeslissingen worden op basis van de data in de routetabel genomen.



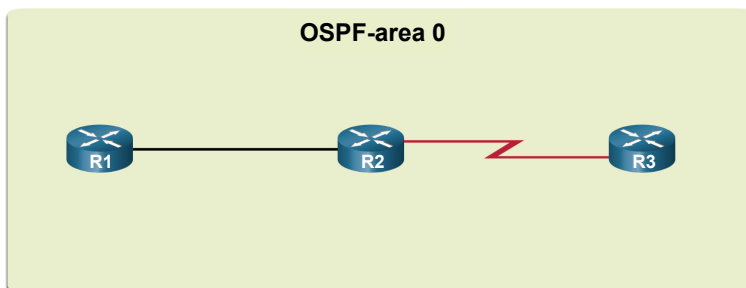
Figuur 1-7 Inhoud van de SPF-tree van R1

1.1.4 Single area en multi-area OSPF

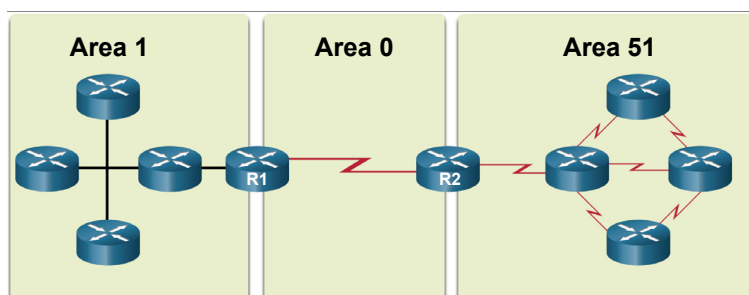
Om OSPF efficiënter en schaalbaarder te maken, ondersteunt OSPF hiërarchische routing met behulp van area's. Een OSPF-area is een groep routers die dezelfde link-statusinformatie in hun LSDB's delen. OSPF kan op twee manieren geïmplementeerd worden:

- ▶ **Single area OSPF** – Alle routers bevinden zich in één area. Je kunt het beste **area 0** gebruiken.
- ▶ **Multi-area OSPF** – OSPF wordt in meerdere area's geïmplementeerd, op een hiërarchische manier. Alle area's moeten verbinding met de backbone-area (area 0) maken. Routers die area's met elkaar verbinden, worden **Area Border Routers** (ABR's) genoemd.

De focus van dit hoofdstuk ligt op OSPFv2 met één area.



Figuur 1-8 Single area OSPF



Figuur 1-9 Multi-area OSPF

1.1.5 Multi-area OSPF

Bij multi-area OSPF kan één groot routingdomein in kleinere area's onderverdeeld worden om hiërarchische routing te ondersteunen. Routing vindt nog steeds plaats tussen de gebieden (inter-area-routing), terwijl veel van de processor-intensieve routingbewerkingen, zoals het herberekenen van de database, binnen één area gehouden worden.

Elke keer dat een router bijvoorbeeld nieuwe informatie ontvangt over een topologieverandering binnen de area (inclusief het toevoegen, verwijderen of wijzigen van een link), moet de router het SPF-algoritme opnieuw uitvoeren, een nieuwe SPF-tree maken en de routetabel bijwerken. Het SPF-algoritme is CPU-intensief en de tijd die nodig is voor de berekening is afhankelijk van de grootte van de area.

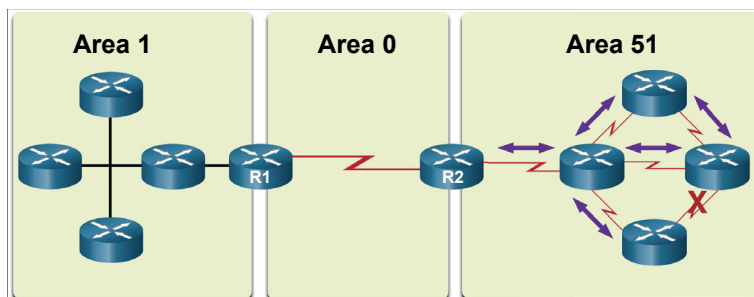
Opmerking Routers in andere area's ontvangen updates met betrekking tot wijzigingen in de topologie, maar deze routers werken alleen de routetabel bij en voeren het SPF-algoritme niet opnieuw uit.

Te veel routers in één area zouden de LSDB's erg groot maken en de belasting van de CPU vergroten. Daarom verdeelt het rangschikken van routers in area's een potentieel grote database effectief in kleinere en beter beheersbare databases.

De ontwerptopties voor hiërarchische topologie met OSPF met meerdere area's kunnen de volgende voordelen bieden:

- ▶ **Kleinere routetabellen** – Tabellen zijn kleiner omdat er minder route-entries zijn. Dit komt omdat netwerkadressen tussen area's samengevoegd kunnen worden. Route-summary is niet standaard ingeschakeld.
- ▶ **Verminderde overhead bij het bijwerken van de link-status** – Het ontwerpen van OSPF met meerdere area's met kleinere area's minimaliseert de verwerkings- en geheugeneisen.
- ▶ **Verminderde frequentie van SPF-berekeningen** – Multi-area OSPF beperkt de impact van een topologieverandering tot één area. Het minimaliseert bijvoorbeeld de impact op het bijwerken van routing, omdat LSA-berichten bij de area-grens stoppen.

In figuur 1-10 is R2 bijvoorbeeld een ABR voor area 51. Een topologieverandering in area 51 zal ertoe leiden dat alle routers van area 51 het SPF-algoritme opnieuw uitvoeren, een nieuwe SPF-tree maken en hun IP-routetabellen bijwerken. De ABR, R2, zal een LSA sturen naar routers in het gebied 0, die uiteindelijk naar alle routers in het OSPF-routingdomein doorgestuurd worden. Dit type LSA zorgt ervoor dat routers in andere gebieden het SPF-algoritme niet opnieuw uitvoeren. Ze hoeven alleen hun LSDB en routetabel bij te werken.



Figuur 1-10 Link-wijzigingen hebben alleen impact op de lokale area

- ▶ Het uitvallen van de link heeft alleen invloed op de lokale area (area 51).
- ▶ De ABR (R2) isoleert de flooding van een specifieke LSA tot area 51.
- ▶ Routers in de area's 0 en 1 hoeven het SPF-algoritme niet uit te voeren.

1.1.6 OSPFv3

OSPFv3 is de OSPFv2-tegenhanger voor het uitwisselen van IPv6-prefixes. Zoals je weet wordt bij IPv6 het netwerkadres het prefix en het subnetmasker de prefixlengte genoemd.

Net als zijn IPv4-tegenhanger wisselt OSPFv3 routinginformatie uit om de IPv6-routetabel met externe prefixes te vullen.

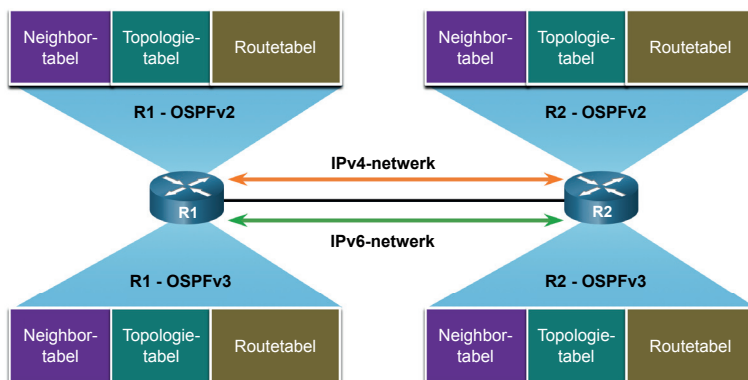
Opmerking Met de OSPFv3 Address Families-functie biedt OSPFv3 ondersteuning voor zowel IPv4 als IPv6. OSPF Address Families vallen buiten de scope van dit curriculum.

OSPFv2 draait op de IPv4-netwerklaag, communiceert met andere OSPF IPv4-peers en adverteert alleen IPv4-routes.

OSPFv3 heeft dezelfde functionaliteit als OSPFv2, maar gebruikt IPv6 als transport op de netwerklaag, communiceert met OSPFv3-peers en adverteert IPv6-routes. OSPFv3 gebruikt ook het SPF-algoritme als de reken-engine om de beste paden door het routingdomein te bepalen.

OSPFv3 heeft andere processen dan zijn IPv4-tegenhanger. De processen en bewerkingen zijn in principe hetzelfde als in het IPv4-routingprotocol, maar werken onafhankelijk. OSPFv2 en OSPFv3 hebben elk aparte adjacency-tabellen, OSPF-topologietabellen en IP-routetabellen, zoals in figuur 1-11 te zien is.

De OSPFv3-configuratie- en verificatiecommando's zijn vergelijkbaar met die van OSPFv2.



Figuur 1-11 OSPFv2- en OSPFv3-datastructuren

i 1.1.7 Test je kennis – OSPF-functies en -eigenschappen

Test je kennis van de OSPF-functies en -eigenschappen door het beste antwoord op de volgende vragen te kiezen.

- 1 Welke van de volgende OSPF-componenten is aan de neighbor-tabel gekoppeld?
 - a Dijkstra's algoritme
 - b Link-state-database
 - c Routingprotocolberichten
 - d Adjacency-tabel
 - e Forwarding-database