

Netwerken

Deel 2 – Switching, routing en draadloos

Netwerken

Deel 2 – Switching, routing en draadloos

Versie 7

John Bakker

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

Auteur: John Bakker
Redactie en opmaak: Henk Pel, Zeist
Titel: Netwerken – Deel 2 – Switching, routing en draadloos
ISBN 978 90 372 5909 4
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 **Switching, routing en draadloos 1**
- 1 **Basisapparaatconfiguratie 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 Configureer een switch met de initiële instellingen 3
 - 1.1.1 Switch-boot-sequence 3
 - 1.1.2 Het commando boot system 4
 - 1.1.3 Switch-LED-indicatoren 4
 - 1.1.4 Herstellen van een systeemcrash 6
 - 1.1.5 Toegang tot het switch-beheer 7
 - 1.1.6 Voorbeeld voor het configureren van de SVI van een switch 7
 - 1.1.7 Lab – Basis switch-configuratie 9
- 1.2 Configureer de switch-poorten 9
 - 1.2.1 Duplex-communicatie 9
 - 1.2.2 Configureer switch-poorten op de fysieke laag 9
 - 1.2.3 Auto-MDX 10
 - 1.2.4 Switch-verificatiecommando's 11
 - 1.2.5 Verifieer de switch-poortconfiguratie 11
 - 1.2.6 Netwerk-access-laagproblemen 12
 - 1.2.7 Interface input- en output-errors 14
 - 1.2.8 Netwerk-access-laagproblemen troubleshooten 14
 - 1.2.9 Syntax Checker – Configureer switch-poorten 15
- 1.3 Beveiligde remote access 16
 - 1.3.1 Werking Telnet 16
 - 1.3.2 Werking SSH 16
 - 1.3.3 Controleer of de switch SSH ondersteunt 17
 - 1.3.4 Configureer SSH 17
 - 1.3.5 Controleer of SSH operationeel is 18
 - 1.3.6 Packet Tracer – Configureer SSH 19
- 1.4 Basisrouterconfiguratie 19
 - 1.4.1 Configureer de basisrouterinstellingen 19
 - 1.4.2 Syntax Checker – Configureer de basisrouterinstellingen 20
 - 1.4.3 Dual-stack-topologie 20
 - 1.4.4 Configureer router-interfaces 20
 - 1.4.5 Syntax Checker – Configureer router-interfaces 21
 - 1.4.6 IPv4-loopback-interfaces 21
 - 1.4.7 Packet Tracer – Configureer router-interfaces 22
- 1.5 Verifieer directly connected netwerken 22
 - 1.5.1 Interfaceverificatiecommando's 22
 - 1.5.2 Verifieer de interfacestatus 23
 - 1.5.3 Controleer IPv6 link-local- en multicast-adressen 23
 - 1.5.4 Controleer de interfaceconfiguratie 24
 - 1.5.5 Controleer de routes 24
 - 1.5.6 Filter de uitvoer van show-commando's 25
 - 1.5.7 Syntax Checker – Filter show-commando uitvoer 27
 - 1.5.8 Commando historiefunctie 27

1.5.9	Syntax Checker – Commando historiefuncties	28
1.5.10	Packet Tracer – Controleer directly connected netwerken	28
1.5.11	Test je kennis – Controleer directly connected netwerken	28
1.6	Opdrachten en quiz	29
1.6.1	Packet Tracer – Implementeer een klein netwerk	29
1.6.2	Lab – Configureer basisrouterinstellingen	29
1.6.3	Wat leerde je in dit hoofdstuk?	29
1.6.4	Quiz – Basisapparaatconfiguratie	31
2	Switching-concepten	35
2.0	Inleiding	35
2.0.1	Waarom zou je dit hoofdstuk bestuderen?	35
2.0.2	Wat leer je in dit hoofdstuk?	35
2.1	Frame forwarding	35
2.1.1	Switching in netwerken	35
2.1.2	De MAC-adrestabel van de switch	36
2.1.3	De leer- en forwarding-methode van de switch	36
2.1.4	Video – MAC-adrestabellen op aangesloten switches	37
2.1.5	Switching-forwarding-methoden	37
2.1.6	Store-and-forward-switching	37
2.1.7	Cut-through-switching	38
2.1.8	Activiteit – Switch It!	39
2.2	Switching-domeinen	39
2.2.1	Collision-domeinen	39
2.2.2	Broadcast-domeinen	40
2.2.3	Netwerkcongestie verminderen	41
2.2.4	Test je kennis – Switching-domeinen	41
2.3	Oefeningen en quiz	42
2.3.1	Wat leerde je in dit hoofdstuk?	42
2.3.2	Quiz – Switching-concepten	43
3	VLAN's	45
3.0	Inleiding	45
3.0.1	Waarom zou je dit hoofdstuk bestuderen?	45
3.0.2	Wat leer je in dit hoofdstuk?	45
3.1	Overzicht van VLAN's	45
3.1.1	VLAN-definitie	45
3.1.2	Voordelen van een VLAN-ontwerp	46
3.1.3	Soorten VLAN's	47
3.1.4	Packet Tracer – Wie hoort de broadcasts?	49
3.1.5	Test je kennis – Overzicht van VLAN's	50
3.2	VLAN's in een multi-switch-omgeving	50
3.2.1	VLAN-trunks definiëren	50
3.2.2	Netwerk zonder VLAN's	51
3.2.3	Netwerk met VLAN's	51
3.2.4	VLAN-identificatie met behulp van een tag	52
3.2.5	Native VLAN's en 802.1Q-tagging	53
3.2.6	Voice-VLAN-tagging	54
3.2.7	Voice-VLAN-verificatievoorbeeld	55
3.2.8	Packet Tracer – Onderzoek een VLAN-implementatie	55
3.2.9	Test je kennis – VLAN's in een multi-switch-omgeving	56
3.3	VLAN-configuratie	57
3.3.1	VLAN-ranges op Catalyst-switches	57
3.3.2	VLAN-aanmaakcommando's	58

- 3.3.3 Voorbeeld VLAN aanmaken 58
- 3.3.4 Poorten aan VLAN's toewijzen 59
- 3.3.5 Voorbeeld poorten aan een VLAN toewijzen 59
- 3.3.6 Data- en voice-VLAN's 60
- 3.3.7 Voorbeeld data- en spraak-VLAN 60
- 3.3.8 VLAN-informatie verifiëren 61
- 3.3.9 Wijzig VLAN-poortlidmaatschap 62
- 3.3.10 VLAN's wissen 63
- 3.3.11 Syntax Checker – VLAN-configuratie 63
- 3.3.12 Packet Tracer – VLAN-configuratie 63
- 3.4 VLAN-trunks 64
 - 3.4.1 Trunk-configuratiecommando's 64
 - 3.4.2 Voorbeeld trunk-configuratie 64
 - 3.4.3 Verifieer de trunk-configuratie 65
 - 3.4.4 Reset de trunk naar de default status 65
 - 3.4.5 Packet tracer – Configureer trunks 66
 - 3.4.6 Lab – Configureer VLAN's en trunks 67
- 3.5 Dynamic Trunking Protocol 67
 - 3.5.1 Inleiding in DTP 67
 - 3.5.2 Onderhandelde interface-modes 68
 - 3.5.3 Resultaat van een DTP-configuratie 68
 - 3.5.4 DTP-mode verifiëren 68
 - 3.5.5 Packet Tracer – Configureer DTP 69
 - 3.5.6 Test je kennis – Dynamic Trunking Protocol 69
- 3.6 Opdrachten en quiz 70
 - 3.6.1 Packet Tracer – Implementeer VLAN's en trunking 70
 - 3.6.2 Lab – Implementeer VLAN's en trunking 70
 - 3.6.3 Wat leerde je in dit hoofdstuk? 70
 - 3.6.4 Quiz – VLAN's 71
- 4 Inter-VLAN-routing 75**
 - 4.0 Inleiding 75
 - 4.0.1 Waarom zou je dit hoofdstuk bestuderen? 75
 - 4.0.2 Wat leer je in dit hoofdstuk? 75
 - 4.1 Werking van inter-VLAN-routing 75
 - 4.1.1 Wat is inter-VLAN-routing? 75
 - 4.1.2 Legacy inter-VLAN-routing 76
 - 4.1.3 Router-on-a-stick inter-VLAN-routing 77
 - 4.1.4 Inter-VLAN-routing met een laag-3-switch 78
 - 4.1.5 Test je kennis – Inter-VLAN-routing 79
 - 4.2 Router-on-a-stick inter-VLAN-routing 80
 - 4.2.1 Router-on-a-stick-scenario 80
 - 4.2.2 VLAN- en trunking-configuratie S1 80
 - 4.2.3 VLAN- en trunking-configuratie S2 82
 - 4.2.4 Sub-interfaceconfiguratie R1 83
 - 4.2.5 Verifieer de connectiviteit tussen PC1 en PC2 84
 - 4.2.6 Verificatie router-on-a-stick inter-VLAN-routing 85
 - 4.2.7 Packet Tracer – Configureer router-on-a-stick inter-VLAN-routing 87
 - 4.2.8 Lab – Configureer router-on-a-stick inter-VLAN-routing 87
 - 4.3 Inter-VLAN-routing met laag-3-switches 87
 - 4.3.1 Laag-3-switch inter-VLAN-routing 87
 - 4.3.2 Laag-3-scenario 88
 - 4.3.3 Laag-3-switch-configuratie 88
 - 4.3.4 Laag-3-switch inter-VLAN-routing verifiëren 89
 - 4.3.5 Routing op een laag-3-switch 90

4.3.6	Routing-scenario op een laag-3-switch	90
4.3.7	Routingconfiguratie op een laag-3-switch	91
4.3.8	Packet Tracer – Configureer laag-3-switching en inter-VLAN-routing	92
4.4	Inter-VLAN-routing troubleshooten	92
4.4.1	Veelvoorkomende inter-VLAN-problemen	92
4.4.2	Inter-VLAN-routing troubleshoot-scenario	93
4.4.3	Ontbrekende VLAN's	94
4.4.4	Trunk-poort-problemen	96
4.4.5	Switch-access-poortproblemen	97
4.4.6	Routerconfiguratieproblemen	98
4.4.7	Test je kennis – Troubleshoot inter-VLAN-routing	100
4.4.8	Packet Tracer – Inter-VLAN-routing troubleshooten	101
4.4.9	Lab – Inter-VLAN-routing troubleshooten	101
4.5	Opdrachten en quiz	101
4.5.1	Packet Tracer – Inter-VLAN-routing challenge	101
4.5.2	Lab – Inter-VLAN-routing implementeren	102
4.5.3	Wat leerde je in dit hoofdstuk?	102
4.5.4	Quiz – Inter-VLAN-routing	103
5	STP-concepten	107
5.0	Inleiding	107
5.0.1	Waarom zou je dit hoofdstuk bestuderen?	107
5.0.2	Wat leer je in dit hoofdstuk?	107
5.1	Doel van STP	107
5.1.1	Redundantie in een laag-2-switched netwerk	107
5.1.2	Spanning Tree Protocol	108
5.1.3	STP-herberekening	108
5.1.4	Problemen met redundante switch-verbindingen	109
5.1.5	Laag-2-loops	109
5.1.6	Broadcast-storm	112
5.1.7	Het Spanning Tree-algoritme	113
5.1.8	Video – Observeer de werking van STP	116
5.1.9	Packet Tracer – Onderzoek STP-loop-preventie	116
5.1.10	Test je kennis – Doel van STP	116
5.2	Werking STP	117
5.2.1	Stappen naar een loop-vrije topologie	117
5.2.2	Verkiezing van de root-bridge	118
5.2.3	Impact van default BID's	118
5.2.4	Het bepalen van de root path cost	119
5.2.5	Verkiezing van de root-poorten	120
5.2.6	Verkiezing van de designated poorten	120
5.2.7	Verkiezing van alternate poorten	122
5.2.8	Verkiezing van een root-poort bij meerdere gelijke padkosten	123
5.2.9	STP-timers en poortstatussen	124
5.2.10	Operationele details van elke poortstatus	125
5.2.11	Per-VLAN-spanning tree	126
5.2.12	Test je kennis – Werking van STP	126
5.3	Evolutie van STP	127
5.3.1	Verschillende versies van STP	127
5.3.2	RSTP-concepten	128
5.3.3	RSTP-poortstatus en -poortrollen	128
5.3.4	PortFast en BPDU-guard	129
5.3.5	Alternatieven voor STP	130
5.3.6	Test je kennis – Evolutie van STP	132

- 5.4 Opdrachten en quiz 133
 - 5.4.1 Wat leerde je in dit hoofdstuk? 133
 - 5.4.2 Quiz – STP 134

- 6 EtherChannel 137**
- 6.0 Inleiding 137
 - 6.0.1 Waarom zou je dit hoofdstuk bestuderen? 137
 - 6.0.2 Wat leer je in dit hoofdstuk? 137
- 6.1 Werking van EtherChannel 137
 - 6.1.1 Linkaggregatie 137
 - 6.1.2 EtherChannel 138
 - 6.1.3 Voordelen van EtherChannel 138
 - 6.1.4 Implementatiebeperkingen 139
 - 6.1.5 Werking van PAgP 139
 - 6.1.6 Voorbeeld van PAgP-mode-instellingen 140
 - 6.1.7 Werking van LACP 141
 - 6.1.8 Voorbeeld van LACP-mode-instellingen 141
 - 6.1.9 Test je kennis – Werking EtherChannel 142
- 6.2 EtherChannel configureren 143
 - 6.2.1 Configuratievoorbeelden 143
 - 6.2.2 LACP-configuratievoorbeeld 144
 - 6.2.3 Syntax Checker – Configureer EtherChannel 144
 - 6.2.4 Packet Tracer – Configureer EtherChannel 145
- 6.3 Verifieer en troubleshoot EtherChannel 145
 - 6.3.1 Verifieer EtherChannel 145
 - 6.3.2 Veelvoorkomende problemen met EtherChannel-configuraties 147
 - 6.3.3 Voorbeeld troubleshooten EtherChannel 147
 - 6.3.4 Packet Tracer – Troubleshoot EtherChannel 149
- 6.4 Opdrachten en quiz 149
 - 6.4.1 Packet Tracer – Implementeer EtherChannel 149
 - 6.4.2 Lab – Implementeer EtherChannel 150
 - 6.4.3 Wat leerde je in dit hoofdstuk? 150
 - 6.4.4 Quiz – EtherChannel 151

- 7 DHCPv4 155**
- 7.0 Inleiding 155
 - 7.0.1 Waarom zou je dit hoofdstuk bestuderen? 155
 - 7.0.2 Wat leer je in dit hoofdstuk? 155
- 7.1 DHCPv4-concepten 155
 - 7.1.1 DHCPv4-server en -client 155
 - 7.1.2 Werking DHCPv4 156
 - 7.1.3 Stappen om een lease te verkrijgen 156
 - 7.1.4 Stappen om een lease te vernieuwen 157
 - 7.1.5 Test je kennis – DHCPv4-concepten 158
- 7.2 Configureer een Cisco IOS-DHCPv4-server 158
 - 7.2.1 Cisco IOS-DHCPv4-server 158
 - 7.2.2 Stappen om een Cisco IOS-DHCPv4-server te configureren 158
 - 7.2.3 Configuratievoorbeeld 160
 - 7.2.4 DHCPv4-verificatiecommando's 160
 - 7.2.5 Verifieer of DHCPv4 operationeel is 160
 - 7.2.6 Syntax checker – Configureer DHCPv4 162
 - 7.2.7 Schakel de Cisco IOS-DHCPv4-server uit 163
 - 7.2.8 DHCPv4-relay 163
 - 7.2.9 Andere service-broadcasts die doorgestuurd worden 165
 - 7.2.10 Packet Tracer – DHCPv4 configureren 165

- 7.3 Een DHCPv4-client configureren 165
 - 7.3.1 Een Cisco router als DHCP-client 165
 - 7.3.2 Configuratievoorbeeld 166
 - 7.3.3 Thuisrouter als DHCP-client 166
 - 7.3.4 Syntax Checker – Configureer een Cisco-router als DHCP-client 167
- 7.4 Opdrachten en quiz 167
 - 7.4.1 Packet Tracer – Implementeer DHCPv4 167
 - 7.4.2 Lab – Implementeer DHCPv4 167
 - 7.4.3 Wat leerde je in dit hoofdstuk? 167
 - 7.4.4 Quiz – DHCPv4 168
- 8 SLAAC en DHCPv6 173**
- 8.0 Inleiding 173
 - 8.0.1 Waarom zou je dit hoofdstuk bestuderen? 173
 - 8.0.2 Wat leer je in dit hoofdstuk? 173
- 8.1 IPv6 GUA-toewijzing 173
 - 8.1.1 IPv6-host configuratie 173
 - 8.1.2 IPv6-link-local-host-adres 174
 - 8.1.3 Toewijzing IPv6-GUA 175
 - 8.1.4 Drie RA-flags 176
 - 8.1.5 Test je kennis – IPv6 GUA-toewijzing 176
- 8.2 SLAAC 177
 - 8.2.1 Overzicht SLAAC 177
 - 8.2.2 SLAAC activeren 177
 - 8.2.3 SLAAC only-methode 178
 - 8.2.4 ICMPv6 RS-berichten 179
 - 8.2.5 Host-proces om een interface-ID te genereren 179
 - 8.2.6 Duplicate Address Detection 180
 - 8.2.7 Test je kennis – SLAAC 180
- 8.3 DHCPv6 181
 - 8.3.1 Werking DHCPv6 181
 - 8.3.2 Werking stateless DHCPv6 184
 - 8.3.3 Stateless DHCPv6 op een interface activeren 184
 - 8.3.4 Werking stateful DHCPv6 185
 - 8.3.5 Stateful DHCPv6 op een interface activeren 185
 - 8.3.6 Test je kennis – DHCPv6 186
- 8.4 DHCPv6-server configureren 186
 - 8.4.1 DHCPv6-routerrollen 186
 - 8.4.2 Een stateless DHCPv6-server configureren 187
 - 8.4.3 Configureer een stateless DHCPv6-client 189
 - 8.4.4 Configureer een stateful DHCPv6-server 190
 - 8.4.5 Configureer een stateful DHCPv6-server 192
 - 8.4.6 DHCPv6-server verificatiecommando's 194
 - 8.4.7 Een DHCPv6-relay-agent configureren 195
 - 8.4.8 De DHCPv6-relay-agent verifiëren 195
 - 8.4.9 Test je kennis – Configureren van een DHCPv6-server 197
- 8.5 Opdrachten en quiz 198
 - 8.5.1 Lab – Configureer DHCPv6 198
 - 8.5.2 Wat leerde je in dit hoofdstuk? 198
 - 8.5.3 Quiz – SLAAC en DHCPv6 199
- 9 FHRP-concepten 203**
- 9.0 Inleiding 203
 - 9.0.1 Waarom zou je dit hoofdstuk bestuderen? 203
 - 9.0.2 Wat leer je in dit hoofdstuk? 203

- 9.1 First Hop Redundancy Protocollen 203
 - 9.1.1 Default gateway-beperkingen 203
 - 9.1.2 Routerredundantie 204
 - 9.1.3 Stappen bij routeruitval 205
 - 9.1.4 FHRP-opties 206
 - 9.1.5 Test je kennis – First Hop Redundancy Protocols 207
- 9.2 HSRP 208
 - 9.2.1 Overzicht HSRP 208
 - 9.2.2 HSRP-prioriteit en preemption 208
 - 9.2.3 HSRP-statussen en timers 209
 - 9.2.4 Test je kennis – HSRP 210
- 9.3 Opdrachten en quiz 210
 - 9.3.1 Wat leerde je in dit hoofdstuk? 210
 - 9.3.2 Quiz – FHRP-concepten 211
 - 9.3.3 Packet Tracer – HSRP-configuratiehandleiding 213

- 10 LAN-beveiligingsconcepten 215**
- 10.0 Inleiding 215
 - 10.0.1 Waarom zou je dit hoofdstuk bestuderen? 215
 - 10.0.2 Wat leer je in dit hoofdstuk? 215
- 10.1 Eindpuntbeveiliging 215
 - 10.1.1 Huidige netwerkattacks 215
 - 10.1.2 Netwerkbeveiligingsapparaten 216
 - 10.1.3 Eindpuntbescherming 217
 - 10.1.4 Cisco Email Security Appliance 217
 - 10.1.5 Cisco Web Security Appliance 218
 - 10.1.6 Test je kennis – Eindpuntbeveiliging 219
- 10.2 Access control 220
 - 10.2.1 Authenticatie met een lokaal wachtwoord 220
 - 10.2.2 AAA-onderdelen 220
 - 10.2.3 Authenticatie 221
 - 10.2.4 Autorisatie 222
 - 10.2.5 Accounting 222
 - 10.2.6 802.1X 223
 - 10.2.7 Test je kennis – Access control 223
- 10.3 Laag-2-security threats 224
 - 10.3.1 Laag-2-vulnerabiliteiten 224
 - 10.3.2 Switch-attack-categorieën 225
 - 10.3.3 Switch-attack-mitigatietechnieken 225
 - 10.3.4 Test je kennis – Laag-2-beveiligings-threats 226
- 10.4 MAC-adrestabel-attacks 226
 - 10.4.1 Overzicht switch-werking 226
 - 10.4.2 MAC-adrestabel-flooding 227
 - 10.4.3 MAC-adrestabel-attack-mitigatie 228
 - 10.4.4 Test je kennis – MAC-adrestabel-attacks 228
- 10.5 LAN-attacks 229
 - 10.5.1 Video – VLAN- en DHCP-attacks 229
 - 10.5.2 VLAN-hopping-attacks 229
 - 10.5.3 VLAN-double-tagging-attack 230
 - 10.5.4 DHCP-berichten 231
 - 10.5.5 DHCP-attacks 232
 - 10.5.6 Video – ARP-attacks, STP-attacks en CDP-reconnaissance 235
 - 10.5.7 ARP-attacks 235
 - 10.5.8 Adres-spoofing-attack 237
 - 10.5.9 ATP-attack 238

- 10.5.10 CDP-reconnaissance (verkenning) 239
- 10.5.11 Test je kennis – LAN-attacks 240
- 10.6 Opdrachten en quiz 241
 - 10.6.1 Wat leerde je in dit hoofdstuk? 241
 - 10.6.2 Quiz – LAN-beveiligingsconcepten 242

- 11 Switch-beveiligingsconfiguratie 245**
- 11.0 Inleiding 245
 - 11.0.1 Waarom zou je dit hoofdstuk bestuderen? 245
 - 11.0.2 Wat leer je in dit hoofdstuk? 245
- 11.1 Port-security implementeren 245
 - 11.1.1 Beveilig ongebruikte poorten 245
 - 11.1.2 Beperk MAC-adrestabel-attacks 246
 - 11.1.3 Port-security activeren 247
 - 11.1.4 MAC-adressen beperken en leren 248
 - 11.1.5 Port-security aging 249
 - 11.1.6 Port-security violation-modes 250
 - 11.1.7 Poorten in error-disabled-status 251
 - 11.1.8 Port-security verifiëren 252
 - 11.1.9 Syntax Checker – Implementeer port-security 254
 - 11.1.10 Packet Tracer – Implementeer port-security 254
- 11.2 Beperk VLAN-attacks 254
 - 11.2.1 Overzicht VLAN-attacks 254
 - 11.2.2 Stappen bij het beperken van VLAN-hopping-attacks 255
 - 11.2.3 Syntax Checker – Beperk VLAN-hopping-attacks 255
- 11.3 Beperk DHCP-attacks 256
 - 11.3.1 Overzicht DHCP-attacks 256
 - 11.3.2 DHCP-snooping 256
 - 11.3.3 Stappen om DHCP-snooping te implementeren 257
 - 11.3.4 Configuratievoorbeeld DHCP-snooping 257
 - 11.3.5 Syntax Checker – DHCP-attacks beperken 258
- 11.4 Beperk ARP-attacks 258
 - 11.4.1 Dynamic ARP Inspection 258
 - 11.4.2 Richtlijnen voor DAI-implementatie 259
 - 11.4.3 Voorbeeld DAI-configuratie 259
 - 11.4.4 Syntax Checker – ARP-attacks beperken 260
- 11.5 Beperk STP-attacks 261
 - 11.5.1 PortFast en BPDU-guard 261
 - 11.5.2 PortFast configureren 261
 - 11.5.3 BPDU-guard configureren 262
 - 11.5.4 Syntax Checker – Beperk STP-attacks 263
- 11.6 Opdrachten en quiz 264
 - 11.6.1 Packet Tracer – Configureer switch-beveiliging 264
 - 11.6.2 Lab – Configureer switch-beveiliging 264
 - 11.6.3 Wat leerde je in dit hoofdstuk? 264
 - 11.6.4 Quiz – Switch-beveiligingsconfiguratie 266

- 12 WLAN-concepten 269**
- 12.0 Inleiding 269
 - 12.0.1 Waarom zou je dit hoofdstuk bestuderen? 269
 - 12.0.2 Wat leer je in dit hoofdstuk? 269
- 12.1 Inleiding in draadloze netwerken 269
 - 12.1.1 Voordelen van draadloos 269
 - 12.1.2 Soorten draadloze netwerken 270
 - 12.1.3 Draadloze technologieën 271

- 12.1.4 Radiofrequentie 273
- 12.1.5 Wireless-standaardorganisaties 274
- 12.1.6 Test je kennis – Inleiding in draadloos 274
- 12.2 WLAN-componenten 275
 - 12.2.1 Video – WLAN-componenten 275
 - 12.2.2 Draadloze NIC's 275
 - 12.2.3 Draadloze thuisrouters 276
 - 12.2.4 Draadloze access points 277
 - 12.2.5 AP-categorieën 277
 - 12.2.6 Draadloze antennes 278
 - 12.2.7 Test je kennis – WLAN-componenten 279
- 12.3 Werking WLAN 279
 - 12.3.1 Video – Werking WLAN 279
 - 12.3.2 802.11 draadloze topologie-modes 280
 - 12.3.3 BSS en ESS 280
 - 12.3.4 802.11-framestructuur 282
 - 12.3.5 CSMA/CA 282
 - 12.3.6 Draadloze client en AP-associatie 283
 - 12.3.7 Passieve en actieve discover-mode 283
 - 12.3.8 Test je kennis – Werking WLAN 285
- 12.4 Werking CAPWAP 285
 - 12.4.1 Video – CAPWAP 285
 - 12.4.2 Inleiding in CAPWAP 285
 - 12.4.3 Split-MAC-architectuur 286
 - 12.4.4 DTLS-encryptie 286
 - 12.4.5 FlexConnect AP's 287
 - 12.4.6 Test je kennis – Werking CAPWAP 287
- 12.5 Kanaalmanagement 288
 - 12.5.1 Frequentiekanaalverzadiging 288
 - 12.5.2 Kanaalselectie 290
 - 12.5.3 Plan een WLAN-implementatie 292
 - 12.5.4 Test je kennis – Kanaalmanagement 292
- 12.6 WLAN-threats 293
 - 12.6.1 Video – WLAN-threats 293
 - 12.6.2 Overzicht draadloze beveiliging 293
 - 12.6.3 DoS-attacks 294
 - 12.6.4 Rogue access points 294
 - 12.6.5 Man-in-the-middle-attack 295
 - 12.6.6 Test je kennis – WLAN-threats 296
- 12.7 WLAN's beveiligen 296
 - 12.7.1 Video – WLAN-threats 296
 - 12.7.2 SSID-cloaking en MAC-adresfiltering 297
 - 12.7.3 802.11 Oorspronkelijke authenticatiemethoden 297
 - 12.7.4 Shared-key-authenticatiemethoden 298
 - 12.7.5 Authenticatie van een thuisgebruiker 298
 - 12.7.6 Encryptiemethoden 299
 - 12.7.7 Authenticatie in het bedrijf 300
 - 12.7.8 WPA3 301
 - 12.7.9 Test je kennis – Beveiligde WLAN's 301
- 12.8 Oefeningen en quiz 302
 - 12.8.1 Wat leerde je in dit hoofdstuk? 302
 - 12.8.2 Quiz – WLAN-concepten 304

- 13 WLAN-configuratie 307**
 - 13.0 Inleiding 307
 - 13.0.1 Waarom zou je dit hoofdstuk bestuderen? 307
 - 13.0.2 Wat leer je in dit hoofdstuk? 307
 - 13.1 Remote site WLAN-control 307
 - 13.1.1 Video – Configureer een draadloos netwerk 307
 - 13.1.2 De draadloze router 308
 - 13.1.3 Inloggen op de draadloze router 308
 - 13.1.4 Basisnetwerksetup 309
 - 13.1.5 Draadloze basissetup 312
 - 13.1.6 Configureer een draadloos maasnetwerk 315
 - 13.1.7 NAT voor IPv4 316
 - 13.1.8 Quality of Service 316
 - 13.1.9 Port Forwarding 317
 - 13.1.10 Packet Tracer – Configureer een draadloos netwerk 318
 - 13.1.11 Lab – Configureer een draadloos netwerk 318
 - 13.2 Configureer een basis-WLAN op de WLC 318
 - 13.2.1 Video – Configureer een basis-WLAN op de WLC 318
 - 13.2.2 WLC-topologie 318
 - 13.2.3 Login op de WLC 319
 - 13.2.4 Bekijk de AP-informatie 320
 - 13.2.5 Advanced instellingen 321
 - 13.2.6 Een WLAN configureren 322
 - 13.2.7 Packet Tracer – Configureer een basis-WLAN op de WLC 325
 - 13.3 Configureer een WP2-Enterprise-WLAN op de WLC 325
 - 13.3.1 Video – Definieer een SNMP- en RADIUS-server op de WLC 325
 - 13.3.2 SNMP en Radius 326
 - 13.3.3 Configureer de SNMP-serverinformatie 326
 - 13.3.4 Configureer de RADIUS-serverinformatie 327
 - 13.3.5 Video – Configureer een VLAN voor een nieuw WLAN 328
 - 13.3.6 Topologie met VLAN-5-adressering 328
 - 13.3.7 Configureer een nieuwe interface 329
 - 13.3.8 Video – Configureer een DHCP-scope 331
 - 13.3.9 Configureer een DHCP-scope 331
 - 13.3.10 Video – Configureer een WPA2-Enterprise-WLAN 333
 - 13.3.11 Configureer een WPA2-Enterprise-WLAN 333
 - 13.3.12 Packet Tracer – Configureer een WPA2-Enterprise-WLAN op de WLC 335
 - 13.4 WLAN-problemen troubleshooten 335
 - 13.4.1 Aanpak voor troubleshooting 335
 - 13.4.2 Draadloze client krijgt geen verbinding 336
 - 13.4.3 Troubleshooten als het netwerk traag is 338
 - 13.4.4 Firmware updaten 339
 - 13.4.5 Packet Tracer – WLAN-problemen troubleshooten 340
 - 13.5 Opdrachten en quiz 340
 - 13.5.1 Packet Tracer – WLAN-configuratie 340
 - 13.5.2 Wat leerde je in dit hoofdstuk? 340
 - 13.5.3 Quiz – WLAN-configuratie 341
- 14 Routingconcepten 345**
 - 14.0 Inleiding 345
 - 14.0.1 Waarom zou je dit hoofdstuk bestuderen? 345
 - 14.0.2 Wat leer je in dit hoofdstuk? 345
 - 14.1 Paddeterminatie 345
 - 14.1.1 De twee functies van een router 345
 - 14.1.2 Voorbeeld van routerfuncties 346

- 14.1.3 Het 'beste pad' is gelijk aan de 'langste match' 346
- 14.1.4 Voorbeeld langste match bij een IPv4-adres 347
- 14.1.5 Voorbeeld langste match bij een IPv6-adres 347
- 14.1.6 Bouw de routetabel op 347
- 14.1.7 Test je kennis – Paddeterminatie 349
- 14.2 Packet-forwarding 349
 - 14.2.1 Beslissingsproces bij packet-forwarding 349
 - 14.2.2 End-to-end packet-forwarding 351
 - 14.2.3 Packet-forwarding-mechanismen 353
 - 14.2.4 Test je kennis – Packet-forwarding 355
- 14.3 Overzicht basisrouterconfiguratie 355
 - 14.3.1 Topologie 355
 - 14.3.2 Configuratiecommando's 356
 - 14.3.3 Verificatiecommando's 357
 - 14.3.4 Filter de commando-uitvoer 361
 - 14.3.5 Packet Tracer – Overzicht basisrouterconfiguratie 362
- 14.4 IP-routetabel 363
 - 14.4.1 Route-sources 363
 - 14.4.2 Routetabelprincipes 364
 - 14.4.3 Routetabel-entries 365
 - 14.4.4 Directly connected netwerken 365
 - 14.4.5 Statische routes 366
 - 14.4.6 Statische routes in de IP-routetabel 367
 - 14.4.7 Dynamische routingprotocollen 368
 - 14.4.8 Dynamische routes in de routetabel 369
 - 14.4.9 Default route 369
 - 14.4.10 Structuur van een IPv4-routetabel 370
 - 14.4.11 Structuur van een IPv6-routetabel 371
 - 14.4.12 Administrative Distance 372
 - 14.4.13 Test je kennis – IP-routetabel 373
- 14.5 Statische en dynamische routing 374
 - 14.5.1 Statisch of dynamisch? 374
 - 14.5.2 Ontwikkeling van dynamische routing 375
 - 14.5.3 Dynamische routingprotocolconcepten 376
 - 14.5.4 Het 'beste pad' 376
 - 14.5.5 Load balancing 378
 - 14.5.6 Test je kennis – Dynamische en statische routing 379
- 14.6 Opdrachten en quiz 379
 - 14.6.1 Wat leerde je in dit hoofdstuk? 379
 - 14.6.2 Quiz – Routingconcepten 381
- 15 Statische IP-routing 385**
 - 15.0 Inleiding 385
 - 15.0.1 Waarom zou je dit hoofdstuk bestuderen? 385
 - 15.0.2 Wat leer je in dit hoofdstuk? 385
 - 15.1 Statische routes 385
 - 15.1.1 Typen statische routes 385
 - 15.1.2 Next-hop-opties 386
 - 15.1.3 Statisch IPv4-routecommando 386
 - 15.1.4 Statisch IPv6-routecommando 387
 - 15.1.5 Dual-stack-topologie 387
 - 15.1.6 IPv4-startroutetabellen 388
 - 15.1.7 IPv6-startroutetabellen 389
 - 15.1.8 Test je kennis – Statische routes 390

- 15.2 Statische IP-routes configureren 390
 - 15.2.1 Statische next-hop-IPv4-route 390
 - 15.2.2 Statische IPv6-next-hop-route 391
 - 15.2.3 Statische directly connected IPv4-route 392
 - 15.2.4 Statische directly connected IPv6-route 393
 - 15.2.5 Statische fully specified IPv4-route 394
 - 15.2.6 Statische fully specified IPv6-route 395
 - 15.2.7 Een statische route controleren 395
 - 15.2.8 Syntax Checker – Configureer statische routes 397
- 15.3 Configureer statische default IP-routes 398
 - 15.3.1 Statisch default route 398
 - 15.3.2 Een statische default route configureren 399
 - 15.3.3 Een statische default route verifiëren 399
 - 15.3.4 Syntax Checker – Statische default route configureren 400
- 15.4 Configureer statische floating routes 401
 - 15.4.1 Statische floating routes 401
 - 15.4.2 Configureren van statische floating IPv4- en IPv6-routes 402
 - 15.4.3 Test de statische floating route 404
 - 15.4.4 Syntax Checker – Configureer statische floating route 405
- 15.5 Configureer statische host-routes 405
 - 15.5.1 Hostroutes 405
 - 15.5.2 Automatisch geïnstalleerde host-routes 405
 - 15.5.3 Statische host-routes 406
 - 15.5.4 Configureer statische host-routes 406
 - 15.5.5 Verifieer statische host-routes 406
 - 15.5.6 Configureer statische IPv6-host-route met link-local-next-hop 407
 - 15.5.7 Syntax Checker – Configureer statische host-routes 407
- 15.6 Opdrachten en quiz 408
 - 15.6.1 Packet Tracer – Configureer IPv4- en IPv6 statische en default routes 408
 - 15.6.2 Lab – Configureer IPv4- en IPv6 statische en default routes 408
 - 15.6.3 Wat leerde je in dit hoofdstuk? 408
 - 15.6.4 Quiz – Statische IP-routing 409
- 16 Troubleshooten van statische en default routes 413**
 - 16.0 Inleiding 413
 - 16.0.1 Waarom zou je dit hoofdstuk bestuderen? 413
 - 16.0.2 Wat leer je in dit hoofdstuk? 413
 - 16.1 Packet-verwerking bij statische routes 413
 - 16.1.1 Statische routes en packet-forwarding 413
 - 16.1.2 Test je kennis – Packet-verwerking met statische routes 414
 - 16.2 Troubleshoot statische en default IPv4-routerconfiguratie 415
 - 16.2.1 Netwerkwijzigingen 415
 - 16.2.2 Veelgebruikte troubleshoot-commando's 416
 - 16.2.3 Een connectiviteitsprobleem oplossen 417
 - 16.2.4 Syntax Checker – IPv4 statische en default routes troubleshooten 420
 - 16.3 Opdrachten en quiz 420
 - 16.3.1 Packet Tracer – Troubleshoot statische en default routes 420
 - 16.3.2 Lab – Troubleshoot statische en default routes 420
 - 16.3.3 Wat leerde je in dit hoofdstuk? 421
 - 16.3.4 Quiz – Statische en default routes troubleshooten 422

o Switching, routing en draadloos

Welkom bij het tweede boek van het Cisco Networking Academy CCNAv7-curriculum, *Switching, routing en draadloos (SRWE)*. Dit is de tweede van drie boeken die op het CCNA-certificeringsexamen afgestemd zijn. Dit boek bevat 16 hoofdstukken met elk een reeks aan onderwerpen.

Switching, routing en draadloos vergroten je kennis van de werking van routers en switches in kleine netwerken. Het boek laat je kennismaken met draadloze lokale netwerken (WLAN's) en netwerkbeveiligingsconcepten.

Aan het einde van dit boek ben je in staat om geavanceerde functionaliteit in routers en switches te configureren. Je kunt ook eenvoudig troubleshooting voor deze componenten uitvoeren. Met behulp van best practices op het gebied van beveiliging zul je veelvoorkomende protocolproblemen in zowel IPv4- als IPv6-netwerken troubleshooten en oplossen.

De vaardigheden en kennis die je in dit boek opdoet, bereiden je voor op het laatste boek in CCNA. Met Cisco Networking Academy is er geen betere tijd dan nu. Aan de slag!



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.boombberoepsonderwijs.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 Basisapparaatconfiguratie

1.0 Inleiding

1.0.1 Waarom zou je dit hoofdstuk bestuderen?

Welkom bij de basisapparaatconfiguratie!

Welkom bij het eerste hoofdstuk van *CCNA Switching, routing en draadloos!* Je weet dat switches en routers een ingebouwde configuratie hebben, dus waarom zou je moeten leren om switches en routers verder te configureren?

Stel dat je een modeltreinenset gekocht hebt. Nadat je de baan gelegd hebt, realiseer je je dat de rails slechts een eenvoudige ovale vorm hebben en dat de treinwagons alleen met de klok mee rijden. Misschien wil je dat de rails een acht vormen met een viaduct. Misschien wil je twee treinen hebben die onafhankelijk van elkaar werken en in verschillende richtingen rijden. Hoe kun je dat bereiken? Je moet het spoor en de bediening opnieuw configureren.

Hetzelfde geldt voor netwerkapparaten. Als netwerkbeheerder heb je gedetailleerde controle over de apparaten in je netwerk nodig. Dit betekent het configureren van de switches en routers zodat je netwerk doet wat je wilt. Dit hoofdstuk bevat meerdere Syntax-Checker- en Packet-Tracer-activiteiten om je te helpen deze vaardigheden te ontwikkelen. Laten we beginnen!

1.0.2 Wat leer je in dit hoofdstuk?

Er wordt uitgelegd hoe je apparaten met beveiligings-‘best practices’ configureert. De paragrafen in dit hoofdstuk zijn:

Onderwerp	Doel
Configureer een switch met de initiële instellingen	Configureer de initiële instellingen op een Cisco-switch
Switch-poorten configureren	Configureer de switch-poorten om aan de netwerkeisen te voldoen
Beveilig de externe toegang	Configureer de beveiligde beheertoegang voor een switch
Basisrouterconfiguratie	Configureer, met behulp van de CLI, de basisinstellingen op een router om tussen twee direct aangesloten netwerken te routeren
Verifieer directly connected netwerken	Controleer de connectiviteit tussen twee netwerken die direct met een router verbonden zijn

1.1 Configureer een switch met de initiële instellingen

1.1.1 Switch-boot-sequence

Voordat je een switch kunt configureren, moet je hem inschakelen en de vijf stappen van de opstartvolgorde laten doorlopen. Deze paragraaf behandelt de basisprincipes van het configureren van een switch en heeft aan het einde een Lab-activiteit.

Nadat een Cisco-switch ingeschakeld is, doorloopt hij de volgende vijf stappen:

- 1 Eerst laadt de switch een **POST**-programma (Power-ON Self Test) dat in **ROM** opgeslagen is. POST controleert het CPU-subsysteem. Het POST-programma test CPU, DRAM en het gedeelte van het flash-systeem waaruit het flash-bestandssysteem bestaat.

- 2 Vervolgens laadt de switch de boot-loader-software. De boot-loader is een klein programma dat in ROM opgeslagen is en onmiddellijk nadat de POST met succes voltooid is, uitgevoerd wordt.
- 3 De boot-loader voert een low-level CPU-initialisatie uit. De CPU-registers, die bepalen waar het fysieke geheugen toegewezen wordt, de hoeveelheid geheugen en de snelheid, worden geïnitieerd.
- 4 De boot-loader initialiseert het flash-bestandssysteem op het moederbord.
- 5 Tenslotte lokaliseert en laadt de boot-loader een standaard IOS-image in het geheugen en geeft de besturing van de switch over aan het IOS.

1.1.2 Het commando boot system

De switch probeert met behulp van de informatie in de **BOOT**-omgevingsvariabele automatisch op te starten. Als deze variabele niet ingesteld is, probeert de switch het eerste uitvoerbare bestand dat het kan vinden te laden en uit te voeren. Op Catalyst 2960-serie-switches bevindt het image-bestand zich normaal gesproken in een map met dezelfde naam als het imagebestand (met uitzondering van de .bin-bestandsextensie).

Het IOS-besturingssysteem initialiseert vervolgens met behulp van de IOS-commando's in het startup-config-bestand de interfaces. Het startup-config-bestand heet **config.text** en bevindt zich in flash.

In het voorbeeld wordt de **BOOT**-omgevingsvariabele met het globale configuratiecommando **boot system** ingesteld. Je ziet dat het IOS zich in een afzonderlijke map bevindt en dat het pad naar de map opgegeven is. Gebruik het commando **show boot** om te zien wat het huidige IOS-boot-bestand is.

S1(config)#

boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin

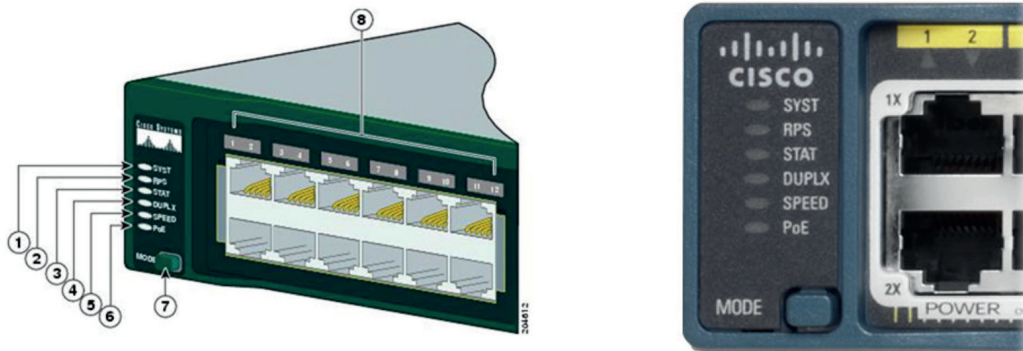
De tabel definieert elk deel van het **boot system**-commando.

Commando	Definitie
boot system	Het hoofdcommando
flash:	De locatie waar het bestand opgeslagen is
c2960-lanbasek9-mz.150-2.SE/	Het pad naar het bestandsysteem
c2960-lanbasek9-mz.150-2.SE.bin	De IOS-bestandsnaam

1.1.3 Switch-LED-indicatoren

Cisco Catalyst-switches hebben verschillende status-LED's. Je kunt de switch-LED's gebruiken om de activiteit en prestaties van de switch snel te controleren. Switches van de verschillende modellen en functiesets hebben verschillende LED's en de plaatsing op het frontpaneel van de switch kan eveneens variëren.

In figuur 1-1 zijn de switch-LED's en de mode-knop van de Cisco Catalyst 2960-switch te zien.



Figuur 1-1 Indicatie-LED's van de Catalyst 2960-switch

De mode-knop (7 in figuur 1-1) wordt gebruikt om tussen poortstatus, poortduplex, poortsnelheid en, als dat ondersteund wordt, de **Power over Ethernet** (PoE)-status van de poort-LED's (8 in de figuur) te schakelen.

Hieronder staat het doel van de LED's (1 t/m 6 in figuur 1-1) en de betekenis van de kleuren.

System-LED (1)

Geeft aan dat het systeem spanning heeft en naar behoren functioneert. Als de LED uit is, betekent dit dat het systeem niet ingeschakeld is. Als de LED groen is, werkt het systeem normaal. Als de LED oranje is, heeft het systeem spanning maar werkt het niet goed.

Redundant Power System (RPS) LED (2)

Geeft de RPS-status weer. Als de LED uit is, is het RPS uit of is dit niet correct aangesloten. Als de LED groen is, is het RPS aangesloten en gereed om back-up-voeding te leveren. Als de LED groen knippert, is het RPS aangesloten maar niet beschikbaar omdat dit een ander apparaat van spanning voorziet. Als de LED oranje is, bevindt het RPS zich in de standby-mode of heeft het een storing. Als de LED oranje knippert, is de interne voeding van de switch defect en levert het RPS de spanning.

Poortstatus-LED (3)

Geeft aan dat de poortstatus geselecteerd is wanneer de LED groen is. Dit is de standaard mode. Als deze mode geselecteerd is, geven de poort-LED's kleuren met verschillende betekenissen weer. Als de poort-LED uit is, is er geen verbinding of is de poort administratief uitgeschakeld (**shutdown**). Als de poort-LED groen is, is er een verbinding aanwezig. Als de poort-LED groen knippert, is er een activiteit en verstuurt of ontvangt de poort data. Als de poort-LED groen/oranje wisselt, is er een verbindingfout. Als de poort-LED oranje is, is de poort geblokkeerd om ervoor te zorgen dat er geen loop ontstaat in het forwarding-domein en stuurt het geen data door (poorten blijven meestal de eerste 30 seconden na activering in deze status). Als de poort-LED oranje knippert, is de poort geblokkeerd om een mogelijke loop in het forwarding-domein te voorkomen.

Poort-duplex-LED (4)

Geeft aan dat de poort-duplex-mode geselecteerd is wanneer de LED groen is. Als deze mode geselecteerd is, bevinden de poorten waarvan de poort-LED's uit zijn zich in half-duplex-mode. Als de poort-LED groen is, bevindt de poort zich in full-duplex-mode.

Poortsnelheid-LED (5)

Geeft aan dat de poortsnelheids-mode geselecteerd is. Als deze mode geselecteerd is, geven de poort-LED's kleuren met verschillende betekenissen weer. Als de poort-LED uit is, werkt de poort op 10 Mb/s. Als de poort-LED groen is, werkt de poort op 100 Mb/s. Als de LED groen knippert, werkt de poort op 1000 Mb/s.

Power over Ethernet (PoE) mode LED (6)

Als PoE ondersteund wordt, is een PoE-mode-LED aanwezig. Als de LED uit is, geeft dit aan dat de PoE-mode niet geselecteerd is en dat geen van de poorten spanning geweigerd is of in storing staat. Als de LED oranje knippert, is de PoE-mode niet geselecteerd, maar is aan ten minste één poort spanning geweigerd of is een poort in storing. Als de PoE-LED groen is, geeft dit aan dat de PoE-mode geselecteerd is en geven de poort-LED's kleuren met verschillende betekenis weer. Als de poort-LED uit is, is de PoE uit. Als de poort-LED groen is, is de PoE aan. Als de poort-LED groen/oranje afwisselt, wordt PoE geweigerd omdat de stroomvoorziening van de switch door het gevoede apparaat te zwaar belast wordt. Als de poort-LED oranje knippert, is de PoE vanwege een fout uitgeschakeld. Als de poort-LED oranje is, is PoE voor de poort uitgeschakeld.

1.1.4 Herstellen van een systeemcrash

De boot-loader biedt toegang tot de switch als het besturingssysteem vanwege ontbrekende of beschadigde systeembestanden niet gebruikt kan worden. De boot-loader heeft een command-line die toegang tot de bestanden geeft die in het flashgeheugen opgeslagen zijn.

De boot-loader is via een consoleverbinding toegankelijk door de volgende stappen te volgen:

- 1 Sluit een PC met een consolekabel op de switch-console-poort aan. Configureer de terminal-emulatiesoftware om verbinding met de switch te maken.
- 2 Koppel het netsnoer van de switch af.
- 3 Sluit het netsnoer van de switch weer aan en druk binnen 15 seconden op de mode-knop en houd deze ingedrukt terwijl de systeem-LED nog groen knippert.
- 4 Houd de mode-knop ingedrukt totdat de systeem-LED kort oranje en vervolgens ononderbroken groen wordt. Laat vervolgens de mode-knop los.
- 5 De boot-loader-prompt **switch:** verschijnt in de terminal-emulatiesoftware op de switch.

Typ **help** of **?** op de boot-loader-prompt om een overzicht van de beschikbare commando's te bekijken.

De switch probeert standaard automatisch met behulp van de informatie in de **BOOT**-omgevingsvariabele op te starten.

```
switch: set
BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin
(output omitted)
switch: flash_init
Initializing Flash...
flashfs[0]: 2 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11838464
flashfs[0]: Bytes available: 20675584
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.
```

Nadat flash geïnitieerd is, kun je het commando **dir flash:** invoeren om de mappen en bestanden in flash te bekijken, zoals hieronder te zien is.

```
switch: dir flash:
Directory of flash:/
  2  -rwx  11834846          c2960-lanbasek9-mz.150-2.SE8.bin
  3  -rwx   2072           multiple-fs
```

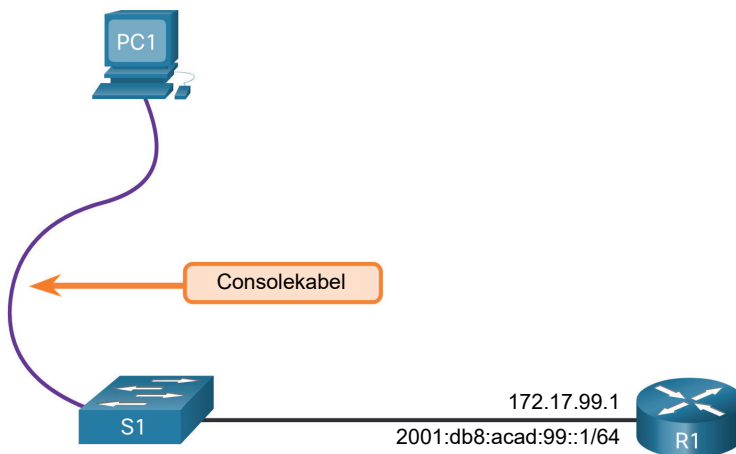
Voer het commando **BOOT=flash** in om het pad van de **BOOT**-omgevingsvariabele te wijzigen dat de switch gebruikt om het nieuwe IOS in flash te laden. Voer opnieuw het commando **set** in om het nieuwe pad van de **BOOT**-omgevingsvariabele te verifiëren. Tenslotte typ je het **boot**-commando zonder argumenten in om het nieuwe IOS te laden, zoals hieronder te zien is.

```
switch: BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
switch: set
BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
(output omitted)
switch: boot
```

De boot-loader-commando's ondersteunen het initialiseren van flash, het installeren van een nieuw IOS, het wijzigen van de BOOT-omgevingsvariabele en het herstellen van verloren of vergeten wachtwoorden.

1.1.5 Toegang tot het switch-beheer

Om een switch op remote beheer voor te bereiden, moet de switch met een IP-adres en een subnetmasker geconfigureerd worden. Houd er rekening mee dat op de switch een default gateway geconfigureerd moet worden om de switch vanaf een extern netwerk te kunnen beheren. Dit lijkt erg op het configureren van de IP-adresinformatie voor host-apparaten. In figuur 1-2 moet aan de **Switch Virtual Interface (SVI)** van S1 een IP-adres toegewezen worden. De SVI is een virtuele interface, geen fysieke poort op de switch. Een consolekabel wordt gebruikt om verbinding met een PC te maken, zodat de switch geconfigureerd kan worden.



Figuur 1-2 PC-aansluiting om de switch te configureren

1.1.6 Voorbeeld voor het configureren van de SVI van een switch

Standaard is de switch zo geconfigureerd dat het beheer ervan via VLAN 1 gecontroleerd wordt. Alle poorten zijn standaard aan VLAN 1 toegewezen. Om veiligheidsredenen wordt het als **best practice** gezien om een ander VLAN dan VLAN 1 te gebruiken voor het beheer-VLAN, zoals VLAN 99 in het voorbeeld.

De stappen voor het configureren van de toegang voor het switch-beheer zijn:

Configureer de beheerinterface

In de VLAN-interfaceconfiguratie-mode wordt een IPv4-adres en subnetmasker aan de beheer-SVI van de switch toegewezen.

Opmerking De SVI van VLAN 99 verschijnt niet ‘up/up’ totdat VLAN 99 aangemaakt is en er een apparaat op een switch-poort aangesloten is dat aan VLAN 99 gekoppeld is.

Opmerking De switch moet misschien ook voor IPv6 geconfigureerd worden. Voordat je een IPv6-adres op bijvoorbeeld een Catalyst 2960-switch met IOS-versie 15.0 kunt configureren, moet je het globale configuratiecommando **sdm prefer dual-ipv4-and-ipv6 default** invoeren en de switch opnieuw opstarten (reload).

IOS-commando's	Taak
S1# configure terminal	Ga naar de globale configuratie-mode.
S1(config)# interface vlan 99	Ga naar de interfaceconfiguratie-mode voor de SVI.
S1(config-if)# ip address 172.17.99.11 255.255.255.0	Configureer het beheer-interface-IPv4-adres.
S1(config-if)# ipv6 address 2001:db8:acad:99::1/64	Configureer het beheer-interface-IPv6-adres.
S1(config-if)# no shutdown	Activeer de beheer-interface.
S1(config-if)# end	Ga naar de privileged-EXEC-mode.
S1# copy running-config startup-config	Bewaar de running-config in de startup-config.

Configureer de default gateway

De switch moet met een default gateway geconfigureerd worden als deze op afstand vanuit netwerken beheerd wordt, die niet direct verbonden zijn.

Opmerking Omdat de default gateway-informatie van een Router-Advertisement-bericht (RA-bericht) ontvangen wordt, heeft de switch geen IPv6-default gateway nodig.

IOS-commando's	Taak
S1# configure terminal	Ga naar de globale configuratie-mode.
S1(config)# ip default-gateway 172.17.99.1	Configureer de default gateway voor de switch.
S1(config-if)# end	Ga naar de privileged-EXEC-mode.
S1# copy running-config startup-config	Bewaar de running-config in de startup-config.

Verifieer de connectiviteit

De commando's **show ip interface brief** en **show ipv6 interface brief** zijn handig om de status van zowel de fysieke als virtuele interfaces te bepalen. De onderstaande uitvoer bevestigt dat de interface VLAN 99 met een IPv4- en IPv6-adres geconfigureerd is.

Opmerking Een IP-adres dat op de SVI toegepast wordt, is alleen voor externe toegang tot de switch, hiermee kan de switch geen laag-3-packets routeren.

```
S1# show ip interface brief
Interface    IP-Address      OK? Method   Status    Protocol
Vlan99      172.17.99.11   YES manual   down      down
(output omitted)
S1# show ipv6 interface brief
Vlan99      [down/down]
FE80::C27B:BCFF:FEC4:A9C1
2001:DB8:ACAD:99::1
(output omitted)
```


➔ 1.1.7 Lab – Basis switch-configuratie

In dit Lab voer je de volgende opdrachten uit:

- ▶ Sluit het netwerk aan en controleer de default configuratie van de switch.
- ▶ Configureer de basisinstellingen van het netwerkapparaat.
- ▶ Controleer en test de connectiviteit.
- ▶ Beheer de MAC-adrestabel.

Download de opdracht in pdf-formaat in de NetAcad-omgeving.

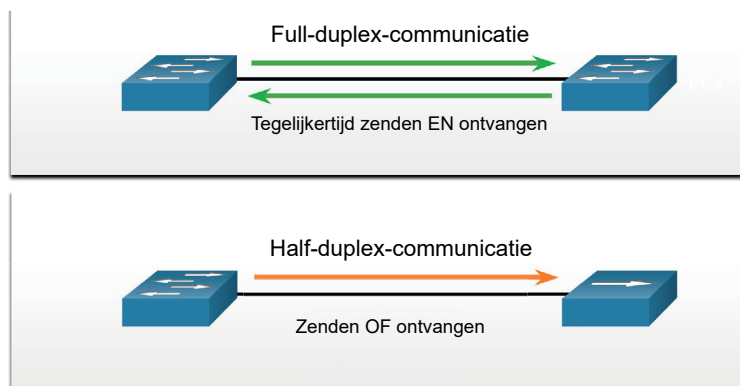
1.2 Configureer de switch-poorten

1.2.1 Duplex-communicatie

De poorten van de switch kunnen onafhankelijk van elkaar voor verschillende behoeften geconfigureerd worden. In deze paragraaf wordt uitgelegd hoe je switch-poorten configureert, hoe je de configuraties verifieert, welke fouten veel voorkomen en hoe je problemen met switch-configuraties troubleshoot.

Full-duplex-communicatie verhoogt de efficiëntie van de bandbreedte doordat beide uiteinden van een verbinding tegelijkertijd data kunnen verzenden en ontvangen. Dit wordt bidirectionele communicatie genoemd en vereist microsegmentatie. Een micro-gesegmenteerd LAN ontstaat wanneer er slechts één apparaat op een switch-poort aangesloten is en in full-duplex-mode werkt. Er is geen collision-domein geassocieerd met een switch-poort die in full-duplex-mode werkt.

In tegenstelling tot full-duplex-communicatie is half-duplex-communicatie unidirectioneel. Half-duplex-communicatie veroorzaakt prestatieproblemen omdat data slechts in één richting tegelijk kunnen stromen, wat vaak tot collisions (botsingen) leidt. Half-duplex-verbindingen zijn meestal te vinden bij oudere hardware, zoals hubs. Full-duplex-communicatie heeft bij de meeste hardware half-duplex vervangen.

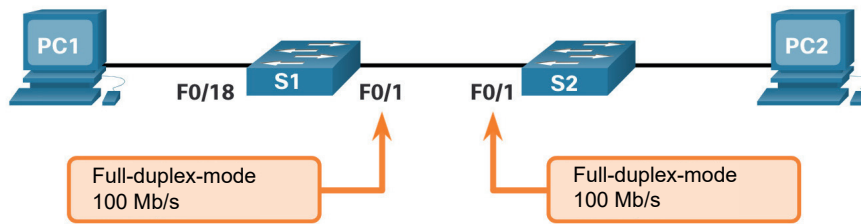


Figuur 1-3 *Verskil tussen full- en half-duplex*

GigabitEthernet en 10 Gb NIC's vereisen full-duplexverbindingen om te kunnen functioneren. In full-duplex-mode is het collision-circuit van de NIC uitgeschakeld. Full-duplex biedt 100 procent efficiëntie in beide richtingen (verzenden en ontvangen). Dit resulteert in een verdubbeling van het potentiële gebruik van de opgegeven bandbreedte.

1.2.2 Configureer switch-poorten op de fysieke laag

Switch-poorten kunnen handmatig met specifieke duplex- en snelheidsinstellingen geconfigureerd worden. Gebruik het interfaceconfiguratiecommando **duplex** om de duplex-mode voor een switch-poort handmatig op te geven. Gebruik het interfaceconfiguratiecommando **speed** om de snelheid handmatig op te geven. Beide switches in de topologie moeten bijvoorbeeld altijd in full-duplex met 100 Mb/s functioneren.



Figuur 1-4 Switch-poort-instellingen moeten aan beide zijden gelijk zijn

De tabel geeft de commando's voor S1. Dezelfde commando's kunnen op S2 toegepast worden.

IOS-commando's	Taak
S1# <code>configure terminal</code>	Ga naar de globale configuratie-mode.
S1(config)# <code>interface FastEthernet 0/1</code>	Ga naar de interfaceconfiguratie-mode.
S1(config-if)# <code>duplex full</code>	Configureer de interface-duplex.
S1(config-if)# <code>speed 100</code>	Configureer de interfacesnelheid.
S1(config-if)# <code>end</code>	Ga naar de privileged-EXEC-mode.
S1# <code>copy running-config startup-config</code>	Bewaar de running-config in de startup-config.

De standaardinstelling voor zowel duplex als snelheid voor switch-poorten op Catalyst 2960- en 3560-switches is **auto**. De 10/100/1000-poorten werken in half- of full-duplex-mode wanneer ze ingesteld zijn op 10 of 100 Mb/s en werken alleen in full-duplex-mode wanneer ze op 1000 Mb/s (1 Gb/s) ingesteld zijn. Autonegotiation is handig wanneer de snelheid en duplexinstellingen van het apparaat dat met de poort verbinding maakt onbekend zijn of kunnen veranderen. Als je verbinding met bekende apparaten maakt, zoals servers, speciale werkstation of netwerkapparaten, is het een goed idee om de instellingen voor snelheid en duplex handmatig in te stellen.

Bij het troubleshooten van switch-poortproblemen is het belangrijk dat de instellingen voor duplex en snelheid gecontroleerd worden.

Opmerking Niet-overeenkomende instellingen voor duplex-mode en snelheid van switch-poorten kunnen verbindingproblemen veroorzaken. Autonegotiation-storingen zorgen voor niet-overeenkomende instellingen.

Alle glasvezelpoorten, zoals 1000BASE-SX-poorten, werken alleen met één vooraf ingestelde snelheid en zijn altijd full-duplex.

1.2.3 Auto-MDX

Tot voor kort waren bepaalde kabeltypen (straight-through of crossover) nodig voor het aansluiten van apparaten. Switch-to-switch- en switch-to-router-verbindingen hadden verschillende Ethernet-kabels nodig. Het gebruik van **Automatic Medium-Dependent Interface crossover** (auto-MDIX) op een interface lost dit probleem op. Wanneer auto-MDIX ingeschakeld is, detecteert de interface automatisch het vereiste type kabelverbinding (straight-through of crossover) en configureert de verbinding op de juiste wijze. Wanneer je een verbinding met switches zonder auto-MDIX-functie maakt, moeten straight-through-kabels gebruikt worden om verbinding met apparaten zoals servers, werkstations of routers te maken. Crossover-kabels moeten gebruikt worden om verbinding met andere switches of repeaters te maken.