



U ovom poglavlju su objašnjete sledeće teme koje morate savladati kako biste položili ispit CCNP BCMSN:

- ❑ **Zaštita osnovnog mosta**
U ovom odeljku se objašnjava kako se STP topologija štiti od neočekivanih objava komutatora koji pokušava da postane osnovni most.
- ❑ **Zaštita BPDU poruka**
U ovom odeljku se razmatraju neočekivane STP objave na portovima komutatora koji su konfigurisani za PortFast, kada je priključen samo jedan računar.
- ❑ **Zaštita od petlji premošćavanja**
U ovom odeljku se objašnjava kako zaštititi STP topologiju od prekida pristizanja BPDU poruka sa osnovnog mosta na port komutatora.
- ❑ **UDLD**
U ovom odeljku ću vam objasniti osobinu pomoću koje se otkrivaju jednosmrene veze između komutatora i kako se računarska mreža od tih veza štiti.
- ❑ **Filtriranje BPDU poruka**
U ovom odeljku se objašnjava kako se na portu komutatora filtriraju BPDU poruke kako bi se port sprečio da učestvuje u STP-u. Petlje premošćavanja se ne otkrivaju niti sprečavaju.
- ❑ **Otklanjanje problema vezanih za zaštitu STP-a**
U ovom odeljku se razmatraju komande koje se koriste za dijagnostifikovanje ili proveravanje akcija koje se preduzimaju radi zaštite topologije.

POGLAVLJE 10

Zaštita topologije Spanning Tree Protocol

Postizanje i održavanje Spanning Tree Protocol (STP) topologije bez petlji premošćavnaja zavisi od postupka slanja i primanja jedinica podataka protokola mosta (bridge protocol data unit - BPDU). U normalnim uslovima, kada se svi komutatori ponašaju prema zadatim pravilima, topologija bez petlji premošćavanja se dinamički utvrđuje.

U ovom poglavlju se razmatraju dva osnovna stanja koja mogu narušiti topologiju bez petlji premošćavanja (čak i kada se izvršava protokol STP):

- Na portu koji ne prima BPDU poruke, BPDU poruke se ne očekuju. Pošto se BPDU poruke iznenada pojave iz nekog razloga, STP topologija može ponovo da konvergira i da dovede do neočekivanih rezultata.
- Na portu koji normalno prima BPDU poruke, BPDU poruke se uvek očekuju. Pošto BPDU poruke neočekivano prestanu da pristižu, komutator može da donese pogrešne pretpostavke o topologiji i nenamerno da stvori petlje premošćavanja.

Da li već znate?

Svrha kontrolnih pitanja "Da li već znate?" je da vam pomogne da utvrdite da li treba da pročitate celo poglavlje. Ukoliko odlučite da pročitate celo poglavlje, ne morate na pitanja odmah odgovoriti.

Pitanja koja se odnose na najvažnije delove razrade oblasti će vam pomoći da odlučite kako ćete utrošiti ograničeno vreme koje imate za učenje.

U tabeli 10.1 navedene su glavne oblasti koje su obrađene u ovom poglavlju i kontrolna pitanja "Da li već znate?" koja odgovaraju tim oblastima.

Tabela 10.1. Uporedni prikaz kontrolnih pitanja "Da li već znate?" i oblasti na koje se odnose

Odeljak oblasti	Pitanja koja su obrađena u odeljku	Broj bodova
Root Guard	1-4	
BPDU Guard	5	
Loop Guard	6-8	
UDLD	9-11	
BPDU Filtering	12	
Ukupan rezultat		

UPOZORENJE

Cilj samoocenjivanja je da utvrdite koliko dobro poznajete oblast koja je objašnjena u ovom poglavlju. Ukoliko ne znate odgovor na pitanje ili ste delimično sigurni u odgovor, onda to pitanje treba da obeležite kao pitanje na koje ste dali pogrešan odgovor. Prihvatanje odgovora koji ste pogodili kao odgovor koji ste znali će iskriviti sliku o vašem znanju i verovatno će vam dati lažnu sigurnost.

1. Zbog čega je važno zaštititi mesto osnovnog mosta (Root Bridge)?
 - a. Da bi se sprečilo da dva osnovna mosta (Root Bridge) budu aktivna.
 - b. Da bi STP topologija bila stabilna.
 - c. Da bi svi komutatori imali ispravan mrežni prolaz.
 - d. Da bi osnovni most (Root Bridge) znao kompletnu STP topologiju.
2. Koja od sledećih osobina štiti komutator od primanja superiornih BPDU poruka?
 - a. STP Loop Guard
 - b. STP BPDU Guard
 - c. STP Root Guard
 - d. UDLD
3. Koju od sledećih komandi ćete zadati kako biste na portu komutatora uključili STP Root Guard?
 - a. spanning-tree root guard
 - b. spanning-tree root-guard
 - c. spanning-tree guard root
 - d. spanning-tree rootguard enable

4. Gde u komutatoru treba uključiti STP Root Guard?
 - a. Svim portovima
 - b. Samo na portovima na kojima nikada ne treba da se vidi osnovni most (Root Bridge)
 - c. Samo na portovima na kojima treba da se nalazi osnovni most (Root Bridge)
 - d. Samo na portovima na kojima je uključen PortFast
5. Koja od sledećih osobina štiti port komutatora od primanja BPDU poruka kada je uključen PortFast?
 - a. STP Loop Guard
 - b. STP BPDU Guard
 - c. STP Root Guard
 - d. UDLD
6. Od čega treba zaštititi izlaznu vezu komutatora da bi se održala STP topologija bez petlji premošćavanja?
 - a. Iznenadnog nestanka BPDU poruka
 - b. Previše BPDU poruka
 - c. Pogrešnih verzija BPDU poruka
 - d. BPDU poruka koje se prenose od osnovnog mosta (Root Bridge)
7. Pomoću koje komande ćete na portu komutatora uključiti STP Loop Guard?
 - a. **spanning-tree loop guard**
 - b. **spanning-tree guard loop**
 - c. **spanning-tree loop-guard**
 - d. **spanning-tree loopguard enable**
8. Koje od sledećih stanja otkriva STP Loop Guard?
 - a. Iznenadno pojavljivanje superiornih BPDU poruka
 - b. Iznenadno nestajanje BPDU poruka
 - c. Pojavljivanje dupliranih BPDU poruka
 - d. Pojavljivanje dva osnovna mosta (Root Bridge)

9. Pomoću koje od sledećih osobina se aktivno može testirati gubitak prihvatne strane veze između komutatora?
- POST
 - BPDU
 - UDLD
 - STP
10. UDLD mora otkriti jednosmernu veze pre nego što?
- Istekne Max Age tajmer.
 - STP prevede vezu u stanje Blocking
 - STP prevede vezu u stanje Forwarding
 - STP prevede vezu u stanje Listening
11. Šta komutator mora da uradi kada preko veze primi UDLD poruku?
- Poruku mora da prosledi drugom komutatoru
 - Mora da pošalje UDLD potvrdu
 - Mora poruku da vrati preko veze
 - Poruku mora da odbaci
12. Koja od sledećih osobina efektivno isključuje operacije obuhvatnog stabla na portu komutatora?
- STP PortFast
 - STP BPDU Filtering
 - STP BPDU Guard
 - STP Root Guard

Odgovore na pitanja ćete pronaći u Dodatku A, "Odgovori na pitanja "Da li ovo već znam?", testove i pitanja u odeljcima "Pitanja i odgovori". Na osnovu osvojenih poena treba da uradite sledeće:

- **10 ili manje poena na celom testu** - Pročitajte celo poglavlje. To obuhvata čitanje razradu teme, zaključak teme i pitanja i odgovore.
- **10 ili 12 poena na celom testu** - Ukoliko želite da unapredite znanje o ovim temama, predite na zaključak teme i potom na pitanja i odgovore na kraju poglavlja. U suprotnom, predite na Poglavlje 11, "Napredni Spanning Tree Protocol".

Razmatranje oblasti

Zaštita od neočekivanih BPDU poruka

Računarska mreža u kojoj se izvršava protokol STP, BPDU poruke koristi za komunikaciju između komutatora (mostova). Komutatori znaju da postoje drugi komutatori i znaju kakvom topologijom su povezani. Pošto se odabere osnovni most (Root Bridge), osnovni most generiše BPDU poruke koje se prenose kroz topologiju obuhvatnog stabla. Svi komutatori u STP domenu dobijaju BPDU poruke koje je poslao osnovni most tako da računarska mreža konvergira i formira se stabilna topologija bez petlji premošćavanja.

Da bi se održala efikasna topologija, mesto osnovnog mosta (Root Bridge) mora biti predvidivo. Srećom, jedan od komutatora možete konfigurisati tako da postane osnovni most (Root Bridge), a drugi komutator možete konfigurisati tako da postane sekundarni osnovni most. Šta će se dogoditi kada se u računarsku mrežu uvede nov komutator, a taj komutator iznenada stekne mogućnost da postane osnovni most (Root Bridge)? Cisco je za protokol STP napravio dve nove osobine koje mogu sprečiti neočekivane rezultate: zaštitu osnovnog mosta (Root Guard) i zaštitu bodu poruka (BPDU Guard).

Zaštita osnovnog mosta

Pošto STP topologija konvergira i nema petlji premošćavanja, portovima komutatora se pridružuju sledeće uloge:

- **Osnovni port (Root Port)** - Port komutatora koji je najbliži (port sa najmanjim troškom osnovne putanje (Root Path Cost)) osnovnom mostu.
- **Namenski port (Designated Port)** - Port na LAN segmentu koji je najbliži osnovnom mostu. Ovaj port prosleđuje, odnosno prenosi, BPDU poruke niže u obuhvatno stablo.
- **Blokirajući port (Blocking port)** - Portovi koji nisu osnovni port ni namenski portovi.
- **Alternativni port (Alternate port)** - Portovi koji su kandidati za osnovne portove (ovi portovi su takođe blizu osnovnog mosta (Root Bridge)), ali se nalaze u stanju Blocking. Ove portove je STP UplinkFast označio kao portove za brzu upotrebu.
- **Portovi za prosleđivanje (Forwarding port)** - Portovi na kojima nije otkrivena nijedna STP aktivnost niti se neka aktivnost očekuje. Ovi portovi se koriste za veze sa korisnicima.

Očekuje se da se osnovni most (Root Bridge) vidi na osnovnom portu i alternativnim portovima jer su ti portovi "najbliži" osnovnom mostu (imaju najmanje troškove putanje).

Pretpostavimo da se u računarsku mrežu uvodi nov komutator čiji je prioritet mosta niži od prioriteta mosta tekućeg osnovnog mosta (Root Bridge). Nov komutator bi u tom slučaju postao osnovni most (Root Bridge), a STP topologija bi verovatno konvergirala u nov oblik. To STP dozvoljava jer komutator sa najnižim identifikatorom mosta (Bridge ID) uvek postaje osnovni most.

Međutim, to nije uvek ono što želite, kao administrator računarske mreže, jer nova STP topologija može biti potpuno neprihvatljiva. Osim toga, dok topologija ponovo konvergira, računarska mreža se verovatno ne može koristiti.

Zaštita osnovnog mosta (Root Guard) je napravljena kao sredstvo za kontrolisanje gde se u računarskoj mreži mogu priključiti kandidati za osnovne mostove (Root Bridge). U osnovi, komutator saznaje identifikator mosta (Bridge ID) *osnovnog mosta* (Root Bridge). Ukoliko drugi komutator pošalje superiornu BPDU poruku, ili poruku sa boljim identifikatorom mosta (Bridge ID), na port komutatora za koji je aktivirana zaštita osnovnog mosta, lokalni komutator neće dozvoliti novom komutatoru da postane osnovni most. Sve dok se superiorne BPDU poruke budu stizale na taj port, port će se nalaziti u STP stanju *root-inconsistent*. U tom stanju se podaci ne mogu slati niti primati, ali port može da osluškuje BPDU poruke koje stižu na port kako bi otkrio novo objavljivanje osnovnog porta.

Zaštita osnovnog mosta, u suštini, određuje da port može samo da prosleđuje BPDU poruke; port se ne može koristiti za primanje BPDU poruka. Zaštita osnovnog mosta sprečava da port da postane osnovni port na koji bi se BPDU poruke osnovnog mosta (Root Bridge) primale.

Zaštitu osnovnog mosta (Root Guard) možete aktivirati za svaki port pojedinačno. Zaštita osnovnog mosta (Root Guard) je, po definiciji, isključena za sve portove komutatora. Da biste je uključili, zadajte sledeću komandu za globalno konfigurisanje komutatora:

```
Switch(config-if)# spanning-tree guard root
```

Pošto se superiorne BPDU poruke više ne budu primale, port prolazi kroz uobičajena STP stanja kako bi ponovo mogao normalno da se koristi.

Zaštitu osnovnog mosta (Root Guard) koristite na portovima na kojima nikada ne očekujete da vidite osnovni most (Root Bridge) za VLAN mrežu. Zaštita osnovnog mosta se odnosi na ceo port, tako da osnovni most (Root Bridge) nikada nije dopušten za *bilo koju* VLAN mrežu na portu. Pošto na port pristigne superiorna BPDU poruka, ceo port se blokira.

SAVET

Portove komutatora koje je Root Guard preveo u stanje root-inconsistent ćete prikazati tako što ćete zadati sledeću komandu:

```
Switch# show spanning-tree inconsistentports
```

Zaštita BPDU poruka

Prisetite se da u tradicionalnom protokolu STP postoji osobina PortFast, koja portovima komutatora omogućava da odmah pređu u stanje Forwarding čim se veza uspostavi. PortFast uređajima korisnika obezbeđuje brz pristup računarskoj mreži u kojoj se ne očekuje formiranje petlji premošćavanja. Čak i kada je PortFast uključen za port komutatora, STP se još uvek izvršava i može da otkrije petlju premošćavanja. Međutim, petlja premošćavanja se može otkriti samo u konačnom vremenskom periodu - to je vreme koje je potrebno da port prođe kroz STP stanja.

NAPOMENA

Upamtite da uključivanje PortFast osobine za port nije isto što i isključivanje protokola STP na istom portu.

Ukoliko uključite PortFast, onda ne očekujete da pronađete bilo šta što može dovesti do petlje premošćavanja - naročito ne drugi komutator ili uređaj koji proizvodi BPDU poruke. Pretpostavimo da je komutator greškom priključen na port za koji je uključen PortFast. U tom slučaju postoji mogućnost formiranja petlje premošćavanja. Veći problem je to što sada postoji mogućnost da novi uređaj šalje objave i postane novi osnovni most (Root Bridge).

Zaštita BPDU poruka (BPDU Guard) je napravljena kako bi se integritet portova za koje je uključen PortFast još više zaštitio. Ukoliko BPDU poruka (bilo superiorna ili inferiorna u odnosu na tekući osnovni most) pristigne na port za koji je uključena zaštita BPDU poruka (BPDU Guard), taj port se odmah prevodi u stanje errdisable. Port se isključuje u stanju greške i mora se ručno uključiti ili automatski oporaviti pomoću errdisable funkcije.

Zaštita BPDU poruka (BPDU Guard) je, po definiciji, uključena za sve portove komutatora. Zaštitu BPDU poruka možete globalno konfigurirati koristeći jednu komandu koja će se odnositi na sve portove komutatora. Za sve portove za koje je uključen PortFast automatski je uključena i zaštita BPDU poruka. Sledeću komandu za globalno konfigurisanje možete zadati kako biste uključili zaštitu BPDU poruka:

```
Switch(config)# spanning-tree portfast bpduguard default
```

Zaštitu BPDU poruka možete uključiti ili isključiti za pojedinačne portove koristeći sledeću komandu za konfigurisanje interfejsa:

```
Switch(config-if)# [no] spanning-tree bpduguard enable
```

Kada se BPDU poruke više ne budu primale, port će ostati u stanju errdisable. Za više informacija o oporavljanju iz errdisable stanja pogledajte Poglavlje 4, "Konfigurisanje portova komutatora".

Zaštitu BPDU poruka (BPDU Guard) treba da koristite na svim portovima komutatora na kojima je uključen PortFast. Na taj način sprečavate da se na port priključi komutator, namerno ili nenamerno. Očigledno je da se zaštita BPDU poruka koristi na portovima komutatora sloja pristupa na koje se mogu priključiti korisnici ili uređaji. Na tim portovima se BPDU poruke ne očekuju, a otkriće se ukoliko se komutator ili razvodni uređaj nenamerno priključe na port.

Zaštita BPDU poruka ne sprečava formiranje petlji premošćavanja ukoliko je Ethernet razvodni uređaj priključen na PortFast port. Razlog je to što razvodni uređaj ne šalje BPDU poruke; razvodni uređaj samo ponavlja Ethernet okvire na drugim portovima. Petlja premošćavanja se može formirati ukoliko se razvodni uređaj priključi na dva mesta u računarskoj mreži i tako stvori put preko kojeg bi se u petlji slali okviri bez ikakve STP aktivnosti.

Zaštitu BPDU poruka (BPDU Guard) nikada ne treba da aktivirate na izlaznoj vezi komutatora na kojoj se nalazi osnovni most (Root Bridge). Ukoliko komutator ima više izlaznih veza, svaki od tih portova može od osnovnog mosta da primi BPDU poruke - čak i kada se portovi, kao rezultat osobine UplinkFast, nalaze u stanju Blocking. Ukoliko je za izlaznu vezu aktivirana zaštita BPDU poruka (BPDU Guard), BPDU poruke će se otkriti i izlazna veza će se prevesti u stanje errdisable. Zbog toga se taj port ne bi mogao koristiti kao izlazna veza u računarsku mrežu.

Zaštita od iznenadnog gubitka BPDU poruka

STP BPDU poruke se koriste kao sonde za istraživanje topologije računarske mreže. Kada komutator koji učestvuje u STP-u konvergira u konzistentnoj topologiji bez petlji premošćavnja, osnovni most (Root Bridge) i dalje mora da šalje BPDU poruke koje svaki drugi komutator u STP domenu mora da prosleđuje. Integritet STP topologije zavisi od stalnog pravilnog slanja BPDU poruka sa osnovnog mosta.

Šta se događa kada komutator redovno ne prima BPDU poruke ili kada uopšte ne prima BPDU poruke? Komutator takvo stanje može da prihvati - možda ne radi odlazni komutator ili izlazna veza. U tom slučaju se topologija mora promeniti, tako da se blokirani portovi ponovo deblokiraju.

Međutim, ukoliko je odsustvo BPDU poruka zapravo greška, a BPDU poruke se ne primaju iako se topologija nije promenila, mogu se formirati petlje premošćavnja.

Cisco je napravio dve STP osobine koje vam pomažu prilikom otkivanja ili sprečavanja neočekivanog gubitka BPDU poruka:

- Zaštita od petlji premošćavanja (Loop Guard)
- Otkrivanje jednosmerne veze (Unidirectional Link detection (UDLD))

Zaštita od petlji premošćavanja

Pretpostavimo da port prima BPDU poruke i da se port nalazi u stanju Blocking. Port pravi redundantnu putanju; nalazi se u stanju Blocking jer nije osnovni port niti je namenski port. Port će ostati u stanju Blocking sve dok redovno prima BPDU poruke.

Ukoliko se BPDU poruke šalju preko veze, ali zbog nekog razloga BPDU poruke prestanu da pristižu, poslednja primljena BPDU poruka se čuva sve dok ne istekne tajmer Max Age. Potom se BPDU poruka uklanja, a komutator više ne vidi razlog da port drži u stanju Blocking. Na kraju krajeva, ukoliko se BPDU poruke ne primaju, onda nije priključen STP uređaj.

Komutator potom port provodi kroz STP stanja sve dok ne počne da prosleđuje mrežni saobraćaj - i formira petlju premošćavanja. U poslednjem stanju port postaje namenski port kada počinje da prenosi ili šalje BPDU poruke duž veze, kada bi zapravo trebalo da prima BPDU poruke.

Da biste sprečili takvu situaciju, treba da koristite zaštitu od petlji premošćavanja (Loop Guard). Pošto se aktivira, zaštita od petlji premošćavanja prati BPDU poruke na nenamenskim porotvima. Sve dok se budu primale BPDU poruke, port može normalno da radi. Čim BPDU poruke prestanu da pristižu, zaštita od petlji premošćavanja (Loop Guard) prevodi port u stanje loop-incident. Port je efektivno u stanju Blocking kako bi se sprečilo formiranje petlji premošćavanja i kako bi zadržao ulogu nenamenskog porta.

Pošto BPDU poruke budu ponovo pristizale na port, zaštita od petlji premošćavanja (Loop Guard) omogućava portu da prođe kroz STP stanja i postane aktivan. Na taj način zaštita od petlji premošćavanja automatski upravlja portovima, to jest, ne postoji potreba za intervencijom administratora računarske mreže.

Zaštita od petlji premošćavanja je, po definiciji, aktivirana za sve portove komutatora. Zaštitu od petlji premošćavanja možete da aktivirate za sve portove komutatora tako što ćete zadati sledeću komandu za globalno konfigurisanje komutatora:

```
Switch(config)# spanning-tree loopguard default
```

Zaštitu od petlji premošćavanja možete aktivirati ili deaktivirati za pojedinačne portove komutatora tako što ćete zadati sledeću komandu za konfigurisanje interfejsa:

```
Switch(config-if)# [no] spanning-tree guard loop
```

Iako je zaštita od petlji premošćavanja konfigurisana za port komutatora, akcije blokiranja se preduzimaju nad pojedinačnim VLAN mrežama. Drugim rečima, zaštita od petlji premošćavanja ne blokira ceo port; blokiraju se samo problematične VLAN mreže.

Zaštitu od petlji premošćavanja možete aktivirati za sve portove komutatora, bez obzira na njihove funkcije. Komutator će znati koji portovi nisu namenski portovi i nadgledaće BPDU aktivnost kako bi ti portovi i dalje bili nenamenski. Nenamenski portovi su, u opštem slučaju, osnovni port, alternativni portovi i portovi koji su blokirani.

UDLD

Komutatori su u računarskoj mreži povezani dvosmernim vezama. Jasno je da ukoliko veza ima problem na fizičkom sloju, dva komutatora koja povezuje otkrivaju problem i vezu prikazuju kao vezu koja je prekinuta.

Šta će se dogoditi kada se samo na jednoj strani veze dogodi greška (samo prima ili šalje podatke), kao kada loše radi kolo za prenošenje podataka u GBIC-u ili Small Form-Factor Pluggable (SFP) modulima? U nekim slučajevima će dva komutatora i dalje videti funkcionalnu dvosmernu vezu, iako će se mrežni saobraćaj odvijati samo u jednom smeru. Takva veza se naziva *jednosmerna veza* (unidirectional link).

Jednosmerna veza je potencijalna opasnost za STP topologije jer se BPDU poruke neće primati na jednom kraju veze. Ukoliko bi taj kraj veze bio u stanju Blocking, onda u tom stanju ne bi dugo ostao. Komutator odsustvo BPDU poruka interpretira kao situaciju u kojoj se port može bezbedno provesti kroz STP stanja kako bi mrežni saobraćaj mogao da se prosleđuje. Međutim, ukoliko se to uradi na jednosmernoj vezi, formiraju se petlje premošćavanja, a komutator nikada ne uviđa grešku.

Da biste sprečili nastajanje takve situacije, koristite Ciscovu osobinu za otkrivanje jednosmerne veze (UniDirectional Link Detection - UDLD). Kada je aktivan, UDLD interaktivno nadgleda portove kako bi se uverio da je veza zaista dvosmerna. Komutator šalje specijalne UDLD okvire sloja 2 (Layer 2) pomoću kojih u pravilnim vremenskim razmacima identifikuje port komutatora. UDLD očekuje da komutator na drugom kraju veze vrati okvire preko iste veze i da tim okvirima doda identifikaciju svog porta.

Ukoliko se dobije UDLD okvir i oba susedna porta su identifikovana u okviru, onda veza mora biti dvosmerna. Međutim, ukoliko se ne dobiju povratni okviri, onda je veza, iz nekog razloga, jednosmerna.

Naravno, za slanje odgovora je potrebno da oba *kraja veze* budu konfigurisana za UDLD. U suprotnom, jedan kraj veze neće slati okvire nazad na njihovo izvoriste. Osim toga, komutatori na svakom kraju veze šalju svoje UDLD poruke i očekuju odgovor sa druge strane veze. To znači da se dva procesa slanja i primanja odgovora odvijaju preko jedne veze.

UDLD poruke se šalju u pravilnim vremenskim razmacima sve dok je veza aktivna. Vremenske intervale u kojima se šalju UDLD poruke možete prilagoditi (podrazumevani vremenski interval je 15 sekundi). Cilj UDLD-a je da otkrije jednosmernu vezu pre nego što STP blokirani port prevede u stanje Forwarding. Da bi to uspeo, vremenski interval mora da bude manji od vrednosti tajmera Max Age plus dva intervala tajmera Forward Delay, to jest, 50 sekundi. UDLD može da otkrije jednosmernu vezu pošto isteknu tri vremenska intervala za UDLD poruku (dakle, oko 45 sekundi).

UDLD može da radi u dva režima:

- **Normalan režim (Normal mode)** - Portu je dozvoljeno da, pošto se otkrije jednosmerna veza, nastavi sa radom. UDLD samo obeležava port kao port za koji se stanje ne može utvrditi i generiše syslog poruku.
- **Agresivan režim (Aggressive mode)** - Komutator, pošto se otkrije jednosmerna veza, preduzima akciju kojom se veza ponovo uspostavlja. Poruke se u narednih osam sekundi šalju jednom u sekundi. Ukoliko se ni na jednu od tih poruka ne dobije odgovor, port se prevodi u stanje errdisable, što znači da se ne može koristiti.

UDLD se može konfigurisati za pojedinačne portove, mada se može konfigurisati za sve portove komutatora sa optičkim vlaknom (za GBIC ili SFP module sa optičkim vlaknom). UDLD je, po definiciji, isključen za sve portove komutatora. Da biste UDLD aktivirali za ceo komutator, zadajete sledeću komandu za globalno konfigurisanje komutatora:

```
Switch(config)# udld {enable | aggressive | message time seconds}
```

Da biste UDLD aktivirali u normalnom režimu, koristite rezervisanu reč **enable**; da biste UDLD aktivirali u agresivnom režimu, koristite rezervisanu reč **aggressive**. Rezervisane reči **message time** koristite kako biste zadali interval u kojem se poruke šalju (interval se zadaje u *sekundama*); interval se zadaje u opsegu od 7 do 90 sekundi. (Podrazumevani interval zavisi od komutatora. Na primer, podrazumevani interval na komutatoru Catalyst 3550 je 7 sekundi; na komutatoru Catalyst 4500 je 15 sekundi.)

UDLD možete uključiti ili isključiti za pojedinačne portove, ukoliko je to neophodno, koristeći sledeću komandu za konfigurisanje interfejsa:

```
Switch(config-if)# udld {enable | aggressive | disable}
```

Koristeći rezervisanu reč **disable** možete potpuno isključiti UDLD na optičkom interfejsu.

NAPOMENA

Podrazumevani intervali u kojima se šalju UDLD poruke se razlikuju na raznim Catalyst komutatorima. Iako se na susednim komutatorima intervali za slanje poruka razlikuju, UDLD će ipak pravilno funkcionisati. Razlog je to što dva susedna komutatora UDLD poruke šalju nazad poruke koje su primili, pri čemu ne znaju koliki je vremenski interval za slanje poruka susednog komutatora. Vremenski interval služi samo za donošenje odluke kada treba poslati UDLD poruku i kao osnova za otkrivanje jednosmerne veze na osnovu nepostojanja odgovora na poslatu UDLD poruku.

Ukoliko odlučite da treba da promenite podrazumevani interval za slanje UDLD poruka, učinite to tako da UDLD može da otkrije grešku pre nego što STP odluči da vezu prevede u stanje Forwarding.

UDLD možete bezbedno aktivirati za sve portove komutatora. Komutator aktivira UDLD samo za portove na kojima se koriste optička vlakna. Kablovi sa uporednim paricama i bakarni kablovi ne podležu uzrocima zbog kojih veza postaje jednosmerna. Međutim, ukoliko želite, UDLD možete da aktivirate i za takve veze.

Možda se pitate kako UDLD možete aktivirati na komutatorima na oba kraja veze. Prisjetite se da u agresivnom režimu UDLD isključuje vezu ukoliko susedni komutator ne odgovori na poruku u zadatom vremenskom intervalu. Ukoliko UDLD aktivirate u aktivnoj računarskoj mreži, da li postoji mogućnost da UDLD prekine veze koje funkcionišu pre nego što konfigurišete drugi kraj veze?

Odgovor je negativan. UDLD pravi inteligentne pretpostavke kada se prvi put uključi za port. Prvo, UDLD ne zna da na vezi postoji susedni komutator. UDLD počinje da šalje poruke u nadi da će susedni komutator da ih primi i da na njih odgovori. Očigledno, uređaj na drugom kraju veze mora da podržava UDLD kako bi poruke vratio pošiljaocu.

Ukoliko na susednom komutatoru UDLD još uvek nije aktiviran, neće biti odgovora ni na jednu poruku. UDLD će pokušavati (beskonačno) da otkrije susedni komutator i neće prekinuti vezu. Pošto se na susednom komutatoru konfiguriše UDLD, oba komutatora će saznati da onaj drugi postoji i saznaće da je veza dvosmerna jer će razmenjivati UDLD poruke. Od tog trenutka na dalje, ukoliko se ne dobije odgovor na poruku, veza će biti označena kao jednosmerna veza.

Najzad, upamtite da ukoliko UDLD otkrije da je veza jednosmerna, preduzeće akciju samo nad tom vezom. To je važno kada se radi o kanalu EtherChannel: ukoliko jedna veza kanala postane jednosmerna, UDLD označava, odnosno prekida, samo vezu koja je jednosmerna, a ne ceo kanal EtherChannel. UDLD šalje i odgovara na poruke na svakoj vezi koja je deo kanala EtherChannel.

Isključivanje protokola STP na portu filtriranjem BPDU poruka

Protokol STP se izvršava na svim portovima komutatora kako bi se sprečilo formiranje petlji premošćavanja. BPDU poruke se šalju na sve portove komutatora - čak i na portove na kojima je uključen PortFast. BPDU poruke se mogu primiti i obraditi ukoliko ih pošalje bilo koji susjedni komutator.

Da biste sprečili formiranje petlji premošćavanja, uvek treba da omogućite izvršavanje protokola STP. Međutim, u posebnim slučajevima u kojima treba da sprečite slanje i obrađivanje BPDU poruka na jednom ili više portova komutatora, koristite filtriranje BPDU poruka kako biste na tim portovima efikasno isključili protokol STP. Filtriranje BPDU poruka je, po definiciji, isključeno za sve portove komutatora. Filtriranje BPDU poruka možete globalno konfigurirati za sve portove komutatora tako što ćete zadati sledeću komandu:

```
Switch(config)# spanning-tree portfast bpdupfilter default
```

Na svim portovima na kojima je uključen PortFast će automatski biti uključeno filtriranje BPDU poruka. Takođe, filtriranje BPDU poruka možete uključiti za pojedinačne portove komutatora tako što ćete zadati sledeću komandu:

```
Switch(config-if)# spanning-tree bpdupfilter {enable | disable}
```

Filtriranje BPDU poruka uključujete samo u kontrolisanim uslovima kada ste potpuno sigurni da je na port komutatora priključen samo jedan računar i da se petlje premošćavanja ne mogu formirati. Filtriranje BPDU poruka uključite samo onda kada uređaj ne može da primi ili pošalje BPDU poruke. U suprotnom, kao meru predostrožnosti, na portovima komutatora treba da se izvršava protokol STP.

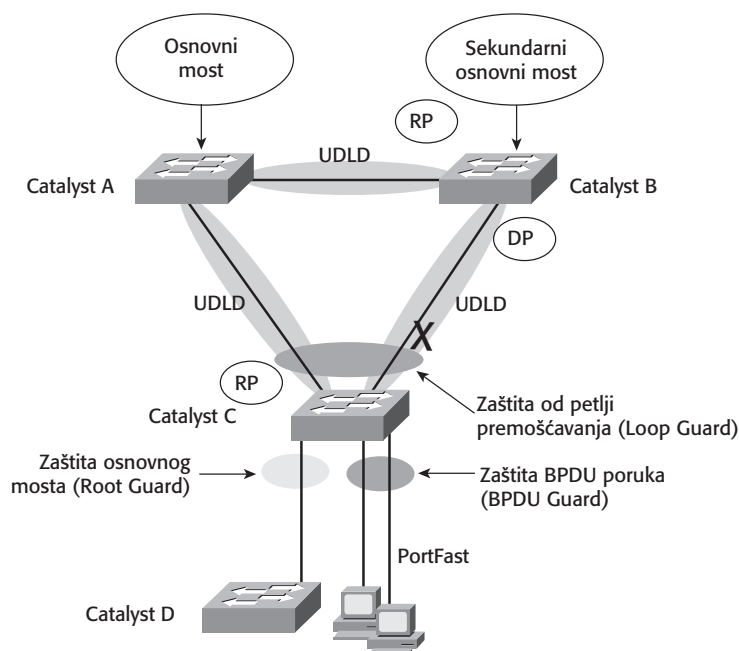
Otklanjanje problema vezanih za zaštitu STP-a

Pošto možete da koristite nekoliko vrsta zaštite protokola STP, morate da znate koja (ako je ijedna) od tih zaštita konfigurisana za port komutatora. U tabeli 10.2 su navedene i opisane EXEC komande pomoću kojih proveravate osobine koje su u ovom poglavlju objašnjene.

Tabela 10.2. Komande za proveravanje zaštite protokola STP i otklanjanje problema

Funkcija	Sintaksa komande
Prikazuje portove koji su označeni kao portovi u nekonzistentnom stanju.	Switch# show spanning-tree inconsistentports
Prikazuje detaljne informacije o nekonzistentnosti.	Switch# show spanning-tree interface type mod/num [detail]
Prikazuje globalno stanje zaštite BPDU poruka (BPDU Guard), filtriranja BPDU poruka (BPDU Filtering) i zaštite od petlji premošćavanja (Loop Guard).	Switch# show spanning-tree summary
Prikazuje UDLD status na jednom ili svim portovima.	Switch# show udld [type num/mod]
Ponovo uključuje portove koje je UDLD u agresivnom režimu isključio.	Switch# udld reset

Pošto možete koristiti mnogo sličnih i međusobno isključivih zaštita protokola STP, možda teže pamтите gde se neka od zaštita koristi. Sliku 10.1 možete koristiti kao kratko uputstvo.



Zaštita osnovnog mosta (Root Guard) i zaštita BPDU poruka (BPDU Guard)

255

Na slici 10.1 vidite dva komutatora na sloju jezgra (Catalyst A i Catalyst B), kao i komutator na sloju pristupa (Catalyst C) koji ima redundantne izlazne veze. Korisnici su povezani na komutator na sloju pristupa. Na tom komutatoru je uključen PortFast. Još jedan komutator na sloju pristupa (Catalyst D) ima izlaznu vezu do komutatora Catalyst C na sloju pristupa. Sve veze između komutatora su Gigabit Ethernet optička vlakna. Očigledno je da se osnovni most (Root Bridge) nikada ne sme videti sa komutatora Catalyst D.

Tabela 10.3. Komande za konfigurisanje zaštite protokola STP

Namena	Sintaksa komande za globalno konfigurisanje komutatora	Sintaksa komande za konfigurisanje interfejsa
Uključivanje zaštite osnovnog mosta		Switch(config-if)# spanning-tree guard root
Uključivanje zaštite BPDU poruka	Switch(config)# spanning-tree portfast bpduguard default	Switch(config-if)# spanning-tree bpduguard enable
Uključivanje zaštite od petlji premošćavanja	Switch(config)# spanning-tree loopguard default	Switch(config-if)# spanning-tree guard loop
Uključivanje UDLD-a	Switch(config)# udld {enable aggressive message time seconds}	Switch(config-if)# udld {enable aggressive disable }
Uključivanje filtriranja BPDU poruka	Switch(config)# spanning-tree bpdufilter default	Switch(config-if)# spanning-tree bpdufilter enable

Tabela 10.4. Komande za aktivnost zaštite protokola STP

Namena	Sintaksa komande
Pronalazi portove koji su u nekonzistentnom stanju.	Switch# show spanning-tree inconsistentports
Prikazuje globalno stanje zaštite BPDU poruka (BPDU Guard), filtriranja BPDU poruka (BPDU Filtering) i zaštite od petlji premošćavanja (Loop Guard).	Switch# show spanning-tree summary
Prikazuje UDLD status na jednom ili svim portovima.	Switch# show udld [type num/mod]
Ponovo uključuje portove koje je UDLD u agresivnom režimu isključio.	Switch# udld reset

Pitanja i odgovori

Pitanja i scenariji koji su dati u ovoj knjizi mnogo su teži od pitanja i scenarija na ispitu. Pitanjima se ne pokušava obuhvatiti više gradiva nego na ispitu; međutim, napisana su tako da budete sigurni da znate odgovor. Umesto da imate mogućnost da pogodite odgovor na osnovu skrivenih naznaka u pitanjima, ispituje se vaše razumevanje i znanje o nekoj oblasti. Nadam se da će ova pitanja ograničiti broj ispitnih pitanja na koja ćete odgovor dati odabiranjem jednog od dva ponuđena odgovora.

Odgovore na ova pitanja ćete pronaći u Dodatku A.

1. Zbog čega je jednosmerna veza loša?
2. Koji uslovi treba da budu ispunjeni kako bi port komutatora ostao u stanju Blocking?
3. Šta se dogodilo na portu komutatora ukoliko je port u nekonzistentnom stanju?
4. Šta morate uraditi da biste ponovo uključili port komutatora pošto se na portu aktivira zaštita osnovnog mosta (Root Guard)?
5. Pošto se aktivira zaštita BPDU poruka (BPDU Guard), u kom stanju će biti port komutatora, ukoliko se na portu otkriju BPDU poruke?
6. Šta morate uraditi da biste ponovo uključili port komutatora pošto se na portu aktivira zaštita BPDU poruka (BPDU Guard)?
7. Pošto se aktivira zaštita od petlji premošćavanja, u kom stanju će biti port komutatora, ukoliko se na tom portu otkriju BPDU poruke?
8. Da li se STP zaštita od petlju premošćavanja može aktivirati za sve portove komutatora?
9. Pošto se UDLD aktivira na portu komutatora, šta se još mora uraditi kako bi se na portu otkrila jednosmerna veza?
10. Objasnite razliku između UDLD normanog i agresivnog režima?
11. Pomoću koje komande aktivirate agresivan UDLD režim za interfejs komutatora?
12. Ukoliko je UDLD aktiviran za portove komutatora koji su međusobno povezani, da li vreme za slanje UDLD poruka treba da se poklapa?
13. UDLD treba da koristite na portovima na kojima se koristi koji tip medija?
14. Da li se UDLD bez problema može koristiti na svim portovima komutatora?
15. Da li je moguće isključiti protokol STP na jednom portu komutatora, a da pri tom ne isključite celu instancu protokola STP?
16. Dovršite sledeću komandu tako da prikaže sve portove koji su isključeni zbog zaštite protokola STP:

show spanning-tree _____