Het Spanning Tree Protocol (STP)

1. Introductie

In netwerken met switches is het vaak belangrijk om redundantie in te bouwen. Redundante verbindingen zorgen voor fouttolerantie, wat betekent dat het netwerk blijft werken als er één verbinding faalt. Maar deze redundantie kan ook een gevaarlijke situatie creëren: netwerklussen (*loops*). Een loop ontstaat wanneer er meerdere actieve paden zijn tussen netwerkapparaten, wat ervoor zorgt dat datapakketten zich eindeloos in een cirkel blijven verplaatsen. Dit leidt tot congestie, hogere latency en in het ergste geval, volledige netwerkuitval.

Het **Spanning Tree Protocol (STP)** biedt de oplossing voor dit probleem. Het STP voorkomt netwerklussen door een enkele logische route te creëren, zelfs als er meerdere fysieke paden aanwezig zijn. Het protocol zorgt ervoor dat sommige paden tijdelijk worden uitgeschakeld, terwijl andere actief blijven, waardoor een lusvrije topologie ontstaat.

STP maakt deel uit van de **IEEE 802.1D**-specificatie, die het **Spanning Tree Algoritme (STA)** introduceerde om een veilige en efficiënte netwerkinfrastructuur te garanderen. Dit hoofdstuk biedt een diepgaande uitleg van STP en hoe het werkt om netwerklussen te vermijden.

---

2. Werking van het Spanning Tree Protocol

Het Spanning Tree Protocol functioneert door de topologie van het netwerk te analyseren en vervolgens ervoor te zorgen dat er slechts één actief pad bestaat tussen alle netwerkapparaten. Het schakelt automatisch bepaalde verbindingen uit om loops te voorkomen, maar kan ze opnieuw activeren als een andere verbinding uitvalt.

2.1 Root Bridge: De kern van de STP-topologie

Het eerste wat STP doet, is een **Root Bridge** selecteren. Dit is de switch die fungeert als het referentiepunt voor het hele netwerk. Elke switch in het netwerk zal een enkel actief pad hebben naar de Root Bridge, waardoor er geen lussen ontstaan.

Hoe wordt de Root Bridge geselecteerd?

Elke switch in een netwerk heeft een unieke identificatie, het Bridge ID (BID), dat bestaat uit twee componenten:

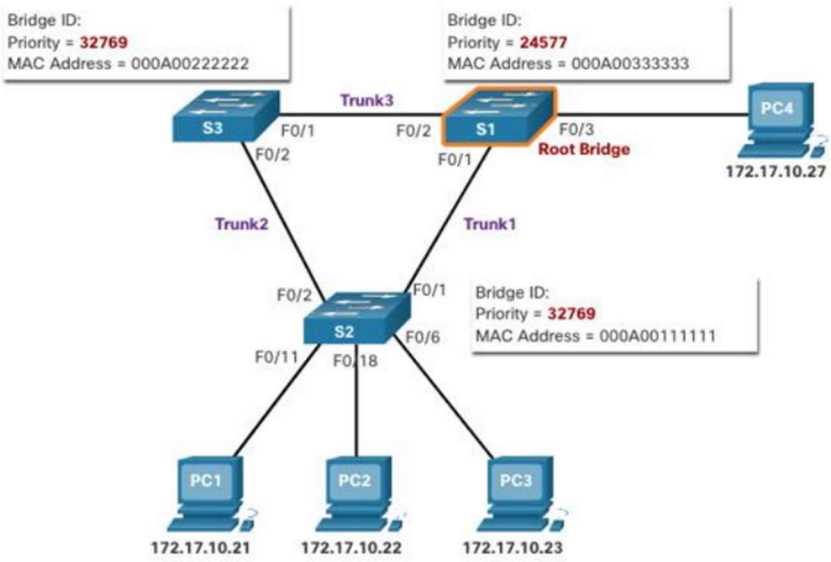
1. Bridge Prioriteit: Dit is een configurabele waarde, met een standaardinstelling van 32.768. Deze waarde kan worden aangepast om voorkeuren in de selectie van de Root Bridge aan te geven.
2. MAC-adres: Het unieke hardware-adres van de switch.

De selectie van de Root Bridge gebeurt op basis van de laagste combinatie van de Bridge Prioriteit en het MAC-adres. De switch met het laagste Bridge ID wordt de Root Bridge. Als de prioriteitswaarden gelijk zijn, wordt de switch met het laagste MAC-adres gekozen.

Toepassing in het voorbeeld

In de afbeelding zien we drie switches:

- S1 met een prioriteit van 24.577 en MAC-adres 000A00333333
- S2 met een prioriteit van 32.769 en MAC-adres 000A00111111
- S3 met een prioriteit van 32.769 en MAC-adres 000A00222222



Omdat S1 een lagere prioriteit heeft (24.577) dan S2 en S3 (beide met de standaardwaarde van 32.769), wordt S1 geselecteerd als de Root Bridge, ondanks dat S1 een hoger MAC-adres heeft dan de andere switches.

In dit scenario kijken de switches primair naar de prioriteitswaarde om de Root Bridge te selecteren.

Waarom is de Root Bridge belangrijk?

De Root Bridge fungeert als het centrum van het netwerk. Elke andere switch bepaalt hoe hij de Root Bridge kan bereiken via het pad met de laagste kosten. Deze kosten worden bepaald door de snelheid van de verbindingen; snellere verbindingen hebben een lagere kost. Alle overige verbindingen worden geblokkeerd om loops te vermijden, maar blijven beschikbaar als back-uproutes.

2.2 Path Cost: Het bepalen van de efficiëntste routes

Nadat de Root Bridge (in dit voorbeeld S1) is geselecteerd, berekenen de andere switches welke route ze moeten gebruiken om de Root Bridge te bereiken. Dit wordt bepaald door de path cost: een numerieke waarde die aangeeft hoe "duur" een bepaald pad is. Hoe lager de path cost, hoe meer kans dat dit pad wordt gekozen als de voorkeursroute naar de Root Bridge.

Path Cost Berekening

De path cost is afhankelijk van de bandbreedte van de verbinding:

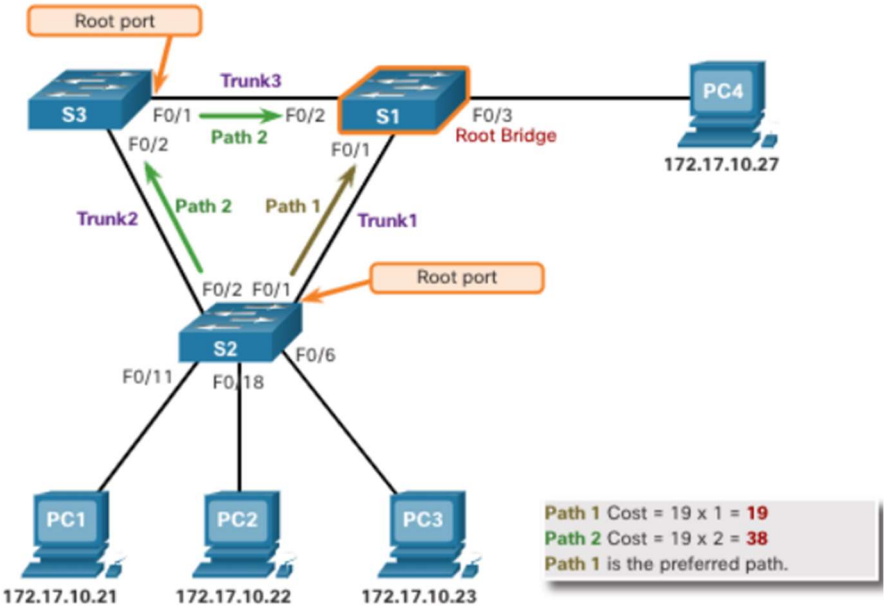
- Een snelle verbinding, zoals een 10 Gbps-link, heeft een lagere path cost (2) in vergelijking met een 100 Mbps-link (19), zoals weergegeven in de tabel.
- STP houdt rekening met de totale kosten van een pad. Hoe lager de cumulatieve path cost, hoe groter de kans dat dit pad de voorkeursroute wordt.

Link Bandwidth	*STP Cos*
4Mbps	250
10Mbps	100
16Mbps	62
45Mbps	39
100Mbps	19
155Mbps	14
622Mbps	6
1Gbps	4
10Gbps	2

Toepassing in het Voorbeeld

In dit netwerk hebben we twee paden van S2 naar de Root Bridge S1:

1. Pad 1 via Trunk1: de kosten zijn 19 (voor de 100 Mbps-link).
2. Pad 2 via Trunk2 en Trunk3: de kosten zijn 19 + 19 = 38, omdat beide verbindingen 100 Mbps zijn en elk een path cost van 19 hebben.



Volgens de STP-regels kiest S2 de route met de laagste cumulatieve path cost. In dit geval heeft Pad 1 de laagste kosten (19), waardoor dit pad de voorkeursroute wordt naar de Root Bridge. De verbinding via Pad 2 wordt geblokkeerd om netwerklussen te vermijden, maar blijft beschikbaar als back-up.

Belang van Path Cost in STP

Door te werken met path costs kiest STP automatisch het snelste en meest efficiënte pad naar de Root Bridge. In situaties waar meerdere paden beschikbaar zijn, zorgt dit mechanisme ervoor dat het netwerk optimaal gebruikmaakt van de beschikbare bandbreedte. De geblokkeerde paden blijven beschikbaar als back-up en kunnen automatisch worden geactiveerd als de actieve verbinding faalt.

---

3. Het Spanning Tree Proces: Stap voor stap

Het Spanning Tree Protocol doorloopt vier hoofdprocessen om loops te vermijden en de netwerkstabiliteit te garanderen.

3.1 Stap 1: Selectie van de Root Bridge

Elke switch in het netwerk stuurt een speciaal bericht genaamd een **BPDU (Bridge Protocol Data Unit)**. Deze BPDU's worden uitgewisseld tussen de switches en bevatten informatie zoals het Bridge ID en de path cost van de zendende switch. Het STP-algoritme vergelijkt deze gegevens om te bepalen welke switch de laagste Bridge ID heeft, die vervolgens wordt geselecteerd als de Root Bridge.

3.2 Stap 2: Bepaling van de Root Port op elke switch

Na de selectie van de Root Bridge bepaalt elke niet-root switch welke van zijn poorten de snelste route naar de Root Bridge biedt. Deze poort wordt de **Root Port** genoemd. Dit is de poort met de laagste cumulatieve path cost naar de Root Bridge, en deze poort blijft actief om verkeer naar de Root Bridge door te sturen.

3.3 Stap 3: Bepaling van Designated Ports

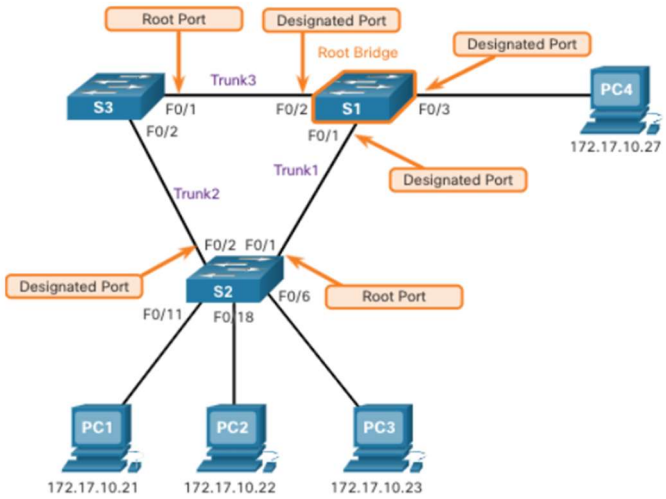
In een netwerk waarin het Spanning Tree Protocol (STP) actief is, speelt de *Designated Port* een essentiële rol in het minimaliseren van lussen en het optimaliseren van dataverkeer naar de Root Bridge.

Designated Port Functie en Selectie:

- Een *Designated Port* is de poort die op een specifieke verbinding of link verantwoordelijk is voor het doorsturen van verkeer richting de Root Bridge.
- Op iedere verbinding tussen switches (zoals tussen S1 en S2, S1 en S3) wordt precies één van de poorten aangewezen als de Designated Port.
- De selectie van de Designated Port gebeurt op basis van de *path cost*. De switch met de laagste cumulatieve path cost naar de Root Bridge wijst zijn poort op die link aan als de Designated Port. Dit betekent dat verkeer altijd de kortste en meest efficiënte route naar de Root Bridge neemt.

Overzicht van Designated Ports in het Voorbeeld: In het netwerkdiagram hierboven zijn de Designated Ports met oranje markeringen aangegeven. Switch S1 is de Root Bridge, dus alle poorten op S1 zijn automatisch Designated Ports. De verbindingen met S2 en S3 hebben elk een Designated Port die verkeer richting de Root Bridge doorstuurt.

1. **Root Bridge Designated Ports**:
    - Aangezien S1 de Root Bridge is, zijn alle poorten op S1 Designated Ports (F0/1, F0/2 en F0/3). Deze poorten sturen verkeer naar andere switches of apparaten en ontvangen terugkoppelingen vanuit de rest van het netwerk.



2. **Designated Port Keuze op Andere Switches**:
    - Voor de verbinding tussen S2 en S3 wordt op elke link bepaald welke poort de Designated Port wordt, afhankelijk van de laagste path cost naar de Root Bridge.
    - Op de verbinding van S2 naar de computers (PC1 en PC2) fungeert de F0/11 poort als de Designated Port richting die eindapparaten, en hetzelfde geldt voor poort F0/6 die verbinding maakt met PC3.

Belang van Designated Ports

De aanwijzing van Designated Ports helpt bij het optimaliseren van de routes door het netwerk. Hierdoor kan STP het verkeer langs de kortste weg naar de Root Bridge leiden en onnodige

vertragingen minimaliseren. Designated Ports werken samen met de Root Ports op andere switches om redundantie in het netwerk mogelijk te maken zonder loops te veroorzaken.

In de configuratie van het netwerk is elke poort zorgvuldig geselecteerd om ervoor te zorgen dat data efficiënt en zonder verstoringen door het netwerk kan bewegen, wat de stabiliteit en prestaties van het netwerk verhoogt.

3.4 Stap 4: Alternate Ports en loop protection

In het Spanning Tree Protocol (STP) worden poorten die niet zijn geselecteerd als Root Ports of Designated Ports automatisch ingesteld als *Alternate Ports*. Deze Alternate Ports spelen een cruciale rol in het voorkomen van netwerkloops en het waarborgen van de stabiliteit van het netwerk.

In het bovenstaande diagram zien we een voorbeeld van een Alternate Port op de link van Switch S3 naar Switch S2, aangeduid door de rode markering op poort F0/1 van S3. Deze Alternate Port blijft inactief totdat deze nodig is, en zorgt ervoor dat er geen netwerkloop ontstaat.

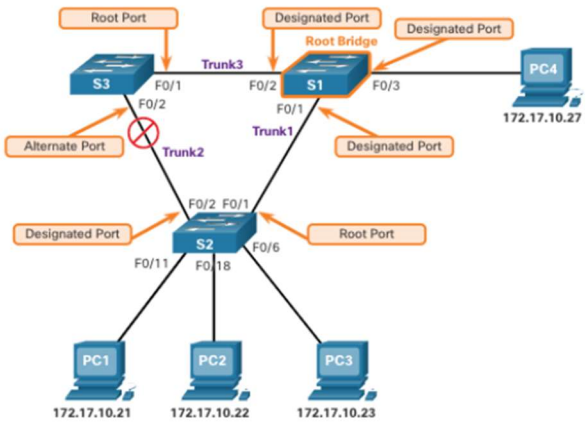
Alternate Ports en Hun Functie:

- *Alternate Ports* blijven in een geblokkeerde staat om te voorkomen dat er loops ontstaan in het netwerk. Dit betekent dat ze geen data doorsturen zolang de belangrijkste route (via de Root en Designated Ports) beschikbaar is.
- In dit voorbeeld is de verbinding tussen S3 en S2 op Trunk2 als Alternate Port ingesteld. Dit is nodig omdat er meerdere verbindingen zijn tussen de switches, wat redundantie creëert. STP blokkeert één van de verbindingen om te zorgen dat het netwerk stabiel blijft en er geen loops ontstaan.

Loopbescherming en Herstel bij Storing:

- Alternate Ports blijven inactief, maar staan klaar om geactiveerd te worden bij een storing. Mocht een actieve poort, zoals een Root Port of Designated Port, uitvallen door bijvoorbeeld een kabelbreuk of hardwarestoring, zal STP automatisch de Alternate Port activeren.
- STP detecteert de verandering in de netwerkstructuur en herberekent de topologie om de Alternate Port (in dit geval F0/1 van S3) te activeren. Hierdoor kan het verkeer via deze poort doorgaan, waardoor de netwerkconnectiviteit behouden blijft zonder loops.

Voordelen van Alternate Ports: Het hebben van Alternate Ports verhoogt de betrouwbaarheid en veerkracht van het netwerk, omdat het netwerk zichzelf snel kan aanpassen aan veranderingen of storingen. Door Alternate Ports te activeren bij een storing, hoeft er geen handmatige configuratie plaats te vinden om het netwerk weer operationeel te maken. Dit zorgt voor een hoge beschikbaarheid van het netwerk, wat vooral belangrijk is in kritieke omgevingen waar downtime minimaal moet zijn.



De Alternate Port is dus een essentieel onderdeel van STP, omdat het netwerk hiermee redundant en betrouwbaar blijft, zelfs bij storingen of veranderingen in de netwerkstructuur.

---

4. Soorten Spanning Tree Protocols

Door de jaren heen zijn er verschillende versies van STP ontwikkeld om beter in te spelen op de behoeften van moderne netwerken.

4.1 Oorspronkelijke STP (IEEE 802.1D)

De eerste versie van STP, zoals gedefinieerd door **IEEE 802.1D**, was de standaard voor veel netwerken. Deze versie hield echter geen rekening met VLAN's (Virtual Local Area Networks) en was relatief traag. Als een link faalde, kon het soms tientallen seconden duren voordat een nieuw pad werd berekend.

4.2 Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)

Om de beperkingen van de oorspronkelijke STP te verhelpen, werd het **Rapid Spanning Tree Protocol (RSTP)** geïntroduceerd. Deze versie, vastgelegd in **IEEE 802.1w**, biedt een snellere convergentie. Wanneer een verbinding uitvalt, berekent RSTP de nieuwe paden aanzienlijk sneller dan het originele STP, waardoor de impact op het netwerk wordt verminderd.

4.3 Per VLAN Spanning Tree (PVST+ en RPVST+)

Per VLAN Spanning Tree (PVST+), ontwikkeld door Cisco, voegt ondersteuning toe voor VLAN's. Dit betekent dat voor elk VLAN een afzonderlijk STP-proces wordt uitgevoerd. Hierdoor kan een poort bijvoorbeeld geblokkeerd zijn voor verkeer van één VLAN, maar actief blijven voor verkeer van een ander VLAN. **Rapid PVST+** combineert de voordelen van RSTP met VLAN-ondersteuning, wat zorgt voor snellere en efficiëntere failover in omgevingen met meerdere VLAN's.

---

5. Uitdagingen en Overwegingen

Hoewel STP een krachtig middel is om netwerklussen te vermijden, brengt het enkele uitdagingen en configuratiecomplexiteit met zich mee:

1. **Configuratiecomplexiteit**: STP vereist zorgvuldige configuratie op alle switches in het netwerk. Een verkeerd geconfigureerde switch kan leiden tot netwerklussen of prestatieproblemen.
2. **Prestatie-impact**: Het constant versturen van BPDU's zorgt voor extra netwerkverkeer. Hoewel dit meestal niet significant is, kan het in grote netwerken leiden tot hogere netwerkbelasting en verminderde prestaties.
3. **Single point of failure**: De Root Bridge is het referentiepunt van het netwerk. Als deze switch faalt, moet STP snel een nieuwe Root Bridge kiezen. Hoewel dit meestal automatisch gebeurt, kan het netwerk tijdelijk instabiel zijn tijdens de herberekening.

---

6. Conclusie

Het Spanning Tree Protocol is een essentieel onderdeel van elke netwerkconfiguratie die redundantie vereist. Door loops te voorkomen en alleen de meest efficiënte routes te activeren, zorgt STP voor een stabiele en fouttolerante netwerkarchitectuur. De moderne varianten zoals RSTP en PVST+ bieden verbeterde prestaties en functionaliteit, waardoor STP nog steeds een fundamenteel protocol is in veel netwerkinfrastructuren.

Als netwerkbeheerder is het belangrijk om STP zorgvuldig te configureren en te begrijpen hoe het protocol de netwerktopologie beïnvloedt. Samen met extra mechanismen zoals **BPDU Guard** en **PortFast**, biedt STP een krachtige oplossing om netwerken te beveiligen en te optimaliseren.

Hoe kan je dit beter beveiligen

BPDU Guard en PortFast: Beveiliging en optimalisatie van netwerkpoorten

In netwerken met switches kunnen enkele configuratiefouten of ongewenste apparaten die aan het netwerk worden gekoppeld, netwerkstoringen veroorzaken. Om deze situaties te voorkomen, bieden BPDU Guard en PortFast een extra laag beveiliging en prestatieoptimalisatie. Beide functies worden vaak toegepast op *edge*-poorten, die doorgaans niet zijn aangesloten op andere netwerkapparaten zoals switches, maar op eindgebruikersapparatuur zoals pc's, printers of VoIP-telefoons.

1. Wat is PortFast?

PortFast is een functie die wordt gebruikt op switchpoorten die zijn aangesloten op eindapparaten zoals computers en servers, niet op andere switches. Standaard doorloopt elke poort die op een switch is aangesloten verschillende Spanning Tree Protocol-stadia, waaronder **Blocking**, **Listening**, **Learning**, en uiteindelijk **Forwarding**. Dit zorgt ervoor dat de poort niet direct data doorstuurt na de activatie van de verbinding, wat tot 30 seconden kan duren. Dit is een veiligheidsmaatregel om loops in het netwerk te voorkomen.

Probleem: In bepaalde gevallen, zoals bij apparaten die gebruikmaken van DHCP (Dynamic Host Configuration Protocol), kan deze wachttijd van 30 seconden leiden tot problemen. Een computer die wordt ingeschakeld en snel een IP-adres probeert te verkrijgen, kan in deze periode een time-out krijgen voordat de poort actief is, wat resulteert in netwerkproblemen of mislukte verbindingen.

Oplossing: **PortFast** versnelt dit proces door de poort direct in de **Forwarding**-status te zetten zodra de verbinding actief is. Dit betekent dat apparaten onmiddellijk verbinding kunnen maken met het netwerk zonder te wachten op de gebruikelijke STP-vertraging.

Gebruik: PortFast wordt alleen ingeschakeld op poorten die zijn verbonden met eindgebruikersapparaten. Het moet nooit worden ingeschakeld op poorten die zijn aangesloten op andere switches, omdat dit kan leiden tot netwerkloops – precies wat STP probeert te voorkomen.

Voordelen van PortFast:

- Snellere activatie van poorten na het opstarten of aansluiten van een apparaat.
- Vermijdt DHCP time-outs en problemen met netwerkverbindingen bij het opstarten.
- Geschikt voor omgevingen waar snelle connectiviteit van apparaten vereist is, zoals in kantoren met veel gebruikersapparaten.

---

2. Wat is BPDU Guard?

Hoewel PortFast de wachttijd bij edge-poorten wegneemt, introduceert het ook een risico: als een PortFast-poort per ongeluk wordt aangesloten op een ander netwerkapparaat, zoals een switch, kan dit leiden tot loops in het netwerk. Om dit risico te beperken, wordt **BPDU Guard** gebruikt.

BPDU's (Bridge Protocol Data Units) zijn de speciale berichten die switches uitwisselen om de netwerkstructuur te leren kennen en loops te detecteren. Een poort waarop PortFast is ingeschakeld, zou normaal gesproken geen BPDU's moeten ontvangen, omdat hij niet verbonden zou moeten zijn met een andere switch. **BPDU Guard** zorgt ervoor dat een poort die PortFast gebruikt, onmiddellijk in een *error-disabled* status wordt geplaatst als er onverwacht een BPDU binnenkomt. Dit voorkomt dat een verkeerd aangesloten switch een loop creëert.

Functie van BPDU Guard:

- Wanneer BPDU Guard is ingeschakeld en een PortFast-poort een BPDU ontvangt, wordt de poort direct uitgeschakeld (*error-disabled* status).
- Dit voorkomt dat apparaten zoals mini-switches of verkeerd aangesloten apparatuur het STP-proces verstoren en loops in het netwerk veroorzaken.
- De netwerkbeheerder moet handmatig ingrijpen om de poort opnieuw te activeren nadat deze door BPDU Guard is uitgeschakeld.

Voordelen van BPDU Guard:

- Beschermt het netwerk tegen onverwachte loops door direct in te grijpen bij een mogelijk gevaarlijke situatie.
- Verhoogt de veiligheid van edge-poorten die normaal gesproken niet betrokken zouden moeten zijn bij het STP-proces.
- Helpt voorkomen dat eindgebruikers of niet-beheerde apparaten het netwerk onbedoeld verstoren door foutieve verbindingen.

---

3. Wanneer BPDU Guard en PortFast gebruiken?

- **PortFast** wordt gebruikt op *edge*-poorten, oftewel poorten die rechtstreeks verbonden zijn met eindgebruikersapparaten zoals desktops, laptops, printers en IP-telefoons.
- **BPDU Guard** wordt meestal samen met PortFast geconfigureerd om ervoor te zorgen dat een poort, ondanks zijn snelle forwarding-configuratie, wordt uitgeschakeld als hij toch wordt aangesloten op een ander netwerkapparaat dat BPDU's verstuurt.

---

4. Praktijkvoorbeeld

Stel je voor dat in een kantoorgebouw een schoonmaker per ongeluk een patchkabel tussen twee netwerkpoorten steekt die verbonden zijn met dezelfde switch. Zonder bescherming zou dit een loop veroorzaken die het netwerk ernstig zou verstoren. Met BPDU Guard en PortFast ingeschakeld, zal het netwerk dit direct detecteren. Zodra een BPDU wordt gedetecteerd op een poort waar het niet zou moeten zijn (bijvoorbeeld op een PortFast-poort), schakelt BPDU Guard de poort onmiddellijk uit. Dit voorkomt dat de netwerkloop daadwerkelijk ontstaat.

---

5. Conclusie

Samen zorgen **PortFast** en **BPDU Guard** ervoor dat edge-poorten sneller en veiliger functioneren in een netwerk. PortFast biedt eindgebruikersapparaten een snelle verbinding zonder de gebruikelijke STP-vertragingen, terwijl BPDU Guard zorgt voor een beschermingsmechanisme dat voorkomt dat onverwachte loops optreden. Deze functies spelen een cruciale rol in het stabiel en veilig houden van moderne netwerken, met name in omgevingen waar snelheid en betrouwbaarheid essentieel zijn.

Misbruiken van STP protocol

Inleiding tot Misbruik van STP

Het **Spanning Tree Protocol** is ontworpen om netwerkloops te voorkomen door een enkele, lusvrije pad te creëren in netwerken met redundante verbindingen. STP selecteert automatisch een **Root Bridge** en bepaalt de beste paden naar deze brug om een stabiele en lusvrije topologie te garanderen. Hoewel het een effectief protocol is voor netwerktopologiebeheer, is STP niet zonder beveiligingsrisico's. Kwaadwillenden kunnen STP-aanvallen uitvoeren om het netwerk te destabiliseren, netwerkverkeer te onderscheppen, of zichzelf ongeautoriseerde toegang te verschaffen tot bepaalde netwerksegmenten.

Waarom STP kwetsbaar is voor misbruik

STP is kwetsbaar voor misbruik om de volgende redenen:

1. **Gebrek aan Authenticatie**: STP-berichten worden doorgaans zonder encryptie of authenticatie verstuurd. Dit betekent dat elke switch of apparaat STP-berichten kan verzenden zonder dat het netwerk deze kan verifiëren.
2. **Root Bridge-selectie**: Omdat STP de switch met het laagste Bridge ID selecteert als Root Bridge, kunnen aanvallers met een lagere prioriteitswaarde of een lager MAC-adres proberen om deze positie over te nemen.
3. **Ontbreken van Bescherming tegen Spoofing**: Kwaadwillende apparaten kunnen zich voordoen als een vertrouwde switch en het STP-verkeer manipuleren door bijvoorbeeld **Bridge Protocol Data Units (BPDU's)** te vervalsen.

Technieken voor Misbruik van STP

Hieronder worden enkele veelvoorkomende technieken beschreven waarmee kwaadwillenden STP kunnen misbruiken.

1. Root Bridge Spoofing

In een **Root Bridge Spoofing**-aanval probeert de aanvaller de rol van de Root Bridge over te nemen door zichzelf te presenteren met een lager Bridge ID. Door een lagere prioriteitswaarde of een laag MAC-adres te gebruiken, kan een aanvallend apparaat een bestaande Root Bridge "verslaan" en zichzelf als de nieuwe Root Bridge laten erkennen door het netwerk.

Doel: Zodra de aanvaller Root Bridge is, heeft deze meer controle over de topologie. Dit kan leiden tot netwerkstoringen, omdat de aanvaller gegevensverkeer via zijn apparaat kan laten lopen, wat een beveiligingsrisico vormt en tot prestatieproblemen kan leiden.

Voorbeeld van Impact:

- Verlies van netwerksegmenten die tijdelijk geen connectiviteit hebben tijdens de herconfiguratie.

- Verhoogde kans op netwerkloops als de nieuwe "Root Bridge" onjuiste configuraties heeft.

2. BPDU Flooding Attack

Bij een **BPDU Flooding**-aanval stuurt de aanvaller een grote hoeveelheid BPDU-pakketten naar het netwerk. Het doel van deze aanval is om de switches te overweldigen met STP-updates, wat kan leiden tot instabiliteit en een herconfiguratie van de STP-topologie.

Doel: Door het netwerk te laten overspoelen met BPDU's, kunnen switches zich constant opnieuw moeten configureren, wat kan leiden tot een tijdelijke uitval van het netwerk of vertraagde netwerkresponsen.

Voorbeeld van Impact:

- Continue wijzigingen in de topologie leiden tot latentieproblemen.
- Verhoogde kans op netwerkloops en verlies van gegevens door instabiliteit.

3. Man-in-the-Middle via STP Manipulatie

Een aanvaller kan STP manipuleren om zichzelf in een positie te plaatsen waar hij dataverkeer kan onderscheppen, manipuleren of afluisteren. Dit kan door zichzelf strategisch te positioneren als een Root Bridge of door zich op een kritieke verbinding tussen twee switches te plaatsen.

Doel: De aanvaller wil ongeautoriseerde toegang krijgen tot gevoelige gegevens of verkeer tussen twee netwerksegmenten onderscheppen.

Voorbeeld van Impact:

- Vertrouwelijke informatie kan worden blootgesteld aan de aanvaller.
- De integriteit van het netwerk wordt in gevaar gebracht, omdat de aanvaller mogelijk verkeer kan manipuleren.

Beschermingsmaatregelen tegen STP-misbruik

Het is mogelijk om de STP-beveiliging te versterken met een reeks beveiligingsmaatregelen die helpen om netwerkcomponenten te beschermen tegen ongeautoriseerde toegang en STP-aanvallen.

1. BPDU Guard

BPDU Guard is een STP-beveiligingsfunctie die ervoor zorgt dat poorten die zijn geconfigureerd voor **PortFast** automatisch worden uitgeschakeld als ze een BPDU ontvangen. BPDU Guard voorkomt dat ongeautoriseerde apparaten of switches zich als Root Bridge presenteren op poorten die zijn bedoeld voor eindapparaten (zoals computers).

Hoe het werkt: BPDU Guard schakelt de poort uit (zet deze in de foutstatus) als er een BPDU-pakket wordt ontvangen, wat betekent dat de poort niet meer actief is totdat de beheerder de situatie oplost.

2. Root Guard

Root Guard voorkomt dat ongeautoriseerde switches een poort overnemen om Root Bridge te worden. Als een switch-poort die is beveiligd met Root Guard een superieure BPDU ontvangt (een BPDU met een lager Bridge ID), blokkeert Root Guard de poort tijdelijk om te voorkomen dat een kwaadwillende switch de Root Bridge-status kan claimen.

Hoe het werkt: Root Guard plaatst de poort in een “gedwongen” status totdat er geen superieure BPDU’s meer worden ontvangen. Zodra de bedreiging is weggenomen, herstelt de poort zich.

3. PortFast

PortFast is een STP-optie die is bedoeld voor poorten die zijn verbonden met eindapparaten, zoals computers. Door PortFast in te schakelen, overslaan de poorten bepaalde STP-stadia, waardoor ze direct actief worden. Dit kan het risico op STP-misbruik verminderen, omdat eindapparaten normaal gesproken geen BPDUs verzenden.

Hoe het werkt: PortFast-poorten gaan direct naar de forwarding-modus, wat nuttig is voor poorten waar geen switches op zijn aangesloten.

Conclusie

Het **Spanning Tree Protocol** is cruciaal voor het beheer van netwerktopologieën met redundante verbindingen, maar het kent ook kwetsbaarheden die door kwaadwillenden kunnen worden uitgebuit. Aanvallen zoals **Root Bridge Spoofing**, **BPDU Flooding**, en **Man-in-the-Middle-aanvallen** tonen aan dat STP zonder extra beveiliging onvoldoende bescherming biedt. Gelukkig kunnen functies zoals **BPDU Guard**, **Root Guard** en **PortFast** helpen om het netwerk te beveiligen en de kans op STP-misbruik te verminderen.

Het is essentieel voor netwerkbeheerders om deze beveiligingsopties te configureren en regelmatig te controleren om te voorkomen dat kwaadwillenden het netwerk destabiliseren of vertrouwelijke gegevens onderscheppen. Met de juiste voorzorgsmaatregelen kan STP veilig en effectief blijven functioneren in netwerkomgevingen.

STP mangling

Root Bridge Spoofing, of **STP Mangling**, is een krachtige aanvalstechniek die specifiek gericht is op het manipuleren van het Spanning Tree Protocol (STP) om zichzelf als de centrale **Root Bridge** te positioneren. Door de Root Bridge te worden, dwingt een aanvaller al het verkeer door zijn eigen apparaat. Hierdoor kan de aanvaller effectief een **Man-in-the-Middle (MitM)**-positie verkrijgen, waarbij het verkeer over alle VLANs door hem heen gaat. Dit creëert een unieke kans om netwerkverkeer op grote schaal te onderscheppen en mogelijk te manipuleren zonder dat de eindgebruikers of netwerkapparatuur dit opmerken.

Hoe werkt de Root Bridge in STP?

Om te begrijpen hoe Root Bridge Spoofing werkt, is het belangrijk om de rol van de Root Bridge in STP te begrijpen.

1. **Root Bridge in Spanning Tree Protocol**: STP is een protocol dat gebruikt wordt om **loops** in een netwerk met redundante verbindingen te voorkomen. Dit gebeurt door één enkele switch aan te wijzen als de **Root Bridge**. De Root Bridge fungeert als het centrale referentiepunt in het netwerk en vormt de basis voor de best mogelijke paden naar andere switches in het netwerk.
2. **Bridge ID (BID)**: Elke switch in een netwerk heeft een uniek **Bridge ID** (BID) dat bestaat uit een **prioriteitswaarde** en het **MAC-adres** van de switch. De switch met het laagste BID wordt automatisch de Root Bridge. In situaties waar de prioriteit van alle switches hetzelfde is, wordt het MAC-adres als beslissende factor gebruikt.
3. **Padberekening en root-padselectie**: Wanneer een Root Bridge is gekozen, berekent STP de kortste paden naar de Root Bridge vanuit elk ander netwerkapparaat. Het verkeer wordt zo geleid dat elke switch een enkele, lusvrije route naar de Root Bridge heeft. Door zichzelf als Root Bridge te presenteren, kan een aanvaller invloed uitoefenen op al deze routes.

Hoe Root Bridge Spoofing (STP Mangling) wordt uitgevoerd

Bij een **STP Mangling**-aanval probeert een aanvaller de rol van Root Bridge over te nemen door een lager BID te presenteren dan de huidige Root Bridge. Dit kan worden bereikt door een lagere **prioriteitswaarde** in te stellen of door een **MAC-adres te vervalsen**. Hier zijn de stappen die een aanvaller volgt:

1. **Configureren van een lager Bridge ID**: De aanvaller past de prioriteitswaarde van zijn apparaat aan, zodat deze lager is dan die van de huidige Root Bridge. Door de prioriteitswaarde te verlagen, wordt het BID van de aanvaller lager, wat hem aantrekkelijker maakt voor andere switches om als de Root Bridge te beschouwen.
2. **Vervalsen en verzenden van BPDU's**: Zodra de aanvaller het Bridge ID heeft verlaagd, begint hij **Bridge Protocol Data Units (BPDU's)** te verzenden die de nieuwe prioriteitswaarde communiceren naar de rest van het netwerk. Andere switches die deze BPDU's

ontvangen, herconfigureren hun STP-topologie om de aanvaller als de nieuwe Root Bridge te accepteren.

3. **Herconfiguratie van netwerktopologie**: Door de aanvaller als Root Bridge te accepteren, herconfigureren de switches hun paden om verkeer via de aanvaller te sturen. Dit betekent dat al het verkeer in het netwerk, inclusief verkeer dat via VLANs loopt, nu via het apparaat van de aanvaller gaat.
4. **Volledige MitM-positie in het netwerk**: Als nieuwe Root Bridge bevindt de aanvaller zich in een unieke positie waarin hij al het verkeer tussen netwerksegmenten, over alle VLANs heen, kan onderscheppen. Dit biedt mogelijkheden voor het onderscheppen, wijzigen, of zelfs blokkeren van netwerkverkeer.

Doel van de STP Mangling-aanval: Man-in-the-Middle over alle VLANs

In netwerken met meerdere **Virtual LANs (VLANs)** kan STP Mangling ook worden gebruikt om verkeer van meerdere VLANs tegelijk te onderscheppen. Omdat de Root Bridge een centrale rol speelt in het bepalen van de netwerkpaden, wordt verkeer in alle VLANs door de nieuwe Root Bridge geleid. Hierdoor kan een aanvaller met Root Bridge Spoofing eenvoudig een MitM-aanval uitvoeren op verkeer van verschillende VLANs, wat bijzonder schadelijk kan zijn in netwerken met gevoelige informatie.

Voordelen voor de aanvaller:

1. **Inzicht in netwerkverkeer**: Omdat al het verkeer door de aanvaller loopt, kan deze netwerkpakketten analyseren en gevoelige informatie zoals wachtwoorden, gebruikersnamen, e-mails en andere vertrouwelijke gegevens onderscheppen.
2. **Data Manipulatie**: De aanvaller kan niet alleen verkeer onderscheppen, maar ook de inhoud manipuleren. Dit kan bijvoorbeeld worden gebruikt voor **session hijacking** of om onjuiste informatie in te voegen.
3. **Brede controle over netwerksegmenten**: Door de Root Bridge te zijn, kan de aanvaller potentieel invloed uitoefenen op de route van data door het hele netwerk, wat hem volledige zichtbaarheid en controle geeft over meerdere VLANs.
4. **Stealth en Persistente Aanval**: Omdat het STP-protocol dynamisch is en regelmatig BPDUs uitwisselt om de topologie up-to-date te houden, is het moeilijk voor beheerders om subtiele wijzigingen op te merken zonder nauwkeurige monitoring. De aanvaller kan relatief onopgemerkt blijven zolang er geen STP-beschermingsmaatregelen zijn geconfigureerd.

Gevolgen van STP Mangling in Netwerken

1. **Grote kwetsbaarheid voor gegevenslekken**: Een MitM-aanval die alle VLANs beïnvloedt, creëert een aanzienlijke kans op datalekken. Vertrouwelijke informatie die binnen een VLAN blijft, kan door deze aanval worden blootgesteld.
2. **Verhoogde kwetsbaarheid voor andere aanvallen**: Met controle over het netwerk kan een aanvaller extra aanvallen lanceren, zoals **ARP spoofing** of **DNS spoofing**, waardoor hij de kans op het verkrijgen van gevoelige gegevens verder vergroot.

3. **Uitval of prestatieverlies**: De netwerkherconfiguratie en mogelijk extra hops kunnen leiden tot prestatieproblemen of zelfs netwerkuitval als de configuratie overbelast raakt.
4. **Ongeautoriseerde toegang tot andere VLANs**: VLAN-scheiding wordt vaak gebruikt om gevoelige segmenten in een netwerk te beveiligen. Root Bridge Spoofing kan echter leiden tot ongeautoriseerde toegang, waardoor verkeer van beveiligde VLANs door de aanvaller kan worden onderschept.

Preventieve Maatregelen tegen Root Bridge Spoofing

Het voorkomen van Root Bridge Spoofing vereist het instellen van effectieve beveiligingsmaatregelen binnen het netwerk:

1. **BPDU Guard**: Schakel BPDU Guard in op poorten die niet zijn bedoeld voor switches, zodat eindgebruikers geen BPDUs kunnen verzenden en dus niet de Root Bridge-status kunnen claimen. BPDU Guard schakelt automatisch de poort uit wanneer een BPDU wordt gedetecteerd op een eindapparaatpoort.
2. **Root Guard**: Schakel Root Guard in op poorten die zijn bedoeld om verbinding te maken met andere switches. Root Guard voorkomt dat een andere switch een Root Bridge-status kan claimen. Als een switch probeert Root Bridge te worden, wordt de poort in een **"root-inconsistent"** status geplaatst totdat de dreiging is verdwenen.
3. **Vaste Prioriteitswaarden voor Root Bridge**: Beheerders kunnen prioriteitswaarden expliciet instellen voor belangrijke switches om te voorkomen dat kwaadwillenden eenvoudigweg een lager Bridge ID configureren.
4. **Regelmatige Monitoring**: Door het monitoren van STP-logs en het detecteren van wijzigingen in de Root Bridge, kunnen netwerkbeheerders verdachte activiteiten sneller opmerken.
5. **Netwerksegmentatie en ACLs**: Door strikte toegangscontrolelijsten (ACLs) en netwerksegmentatie toe te passen, kan het risico van onbevoegde toegang tot verschillende VLANs worden beperkt, zelfs als een aanvaller Root Bridge wordt.

Conclusie

STP Mangling of **Root Bridge Spoofing** is een krachtige aanval die gebruikmaakt van het Spanning Tree Protocol om zichzelf als Root Bridge te positioneren. Hierdoor kan de aanvaller effectief een **Man-in-the-Middle**-positie verkrijgen, waarin hij al het verkeer, inclusief dat van verschillende VLANs, kan onderscheppen en manipuleren.

Deze aanval vormt een groot risico in netwerken waar segmentatie en beveiliging essentieel zijn. Met controle over meerdere VLANs kan de aanvaller gevoelige gegevens bekijken, wijzigen, en zelfs aanvullende aanvallen uitvoeren. Om zich tegen deze bedreiging te beschermen, moeten netwerkbeheerders maatregelen nemen zoals BPDU Guard, Root Guard, en het instellen van vaste prioriteitswaarden. Daarnaast is regelmatige monitoring essentieel om een STP Mangling-aanval tijdig op te merken en te blokkeren.

Door het bewustzijn en de beveiligingsmaatregelen rondom Root Bridge Spoofing te verhogen, kan een netwerk aanzienlijk veiliger worden gemaakt tegen deze subtiele, maar effectieve aanvalstechniek.

Yersinia op kali