Nätverkssäkerhet – Lager 2
Storm Control

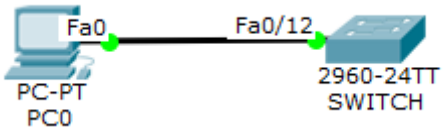
I denna laboration kommer vi att konfigurera *storm control* för att skydda vårt nätverk mot för mycket broadcast- och multicast-trafik. Loopar i vårt nätverk bör *STP* (Spanning Tree Protocol) skydda oss mot men det hjälper inte ifall vi av någon annan anledning får väldigt mycket broadcast-trafik i vårt nätverk (t.ex. p.g.a. felaktig utrustning eller överbelastningsattack).

Antal: Grupper om 2

Material: En dator och en switch. Switchen måste vara *managed*.

Tips: Mer information om fenomenet *broadcast storm* hittar ni i genomgångarna om *STP* och *Nätverkssäkerhet – Lager 2 introduktion* på hemsidan.

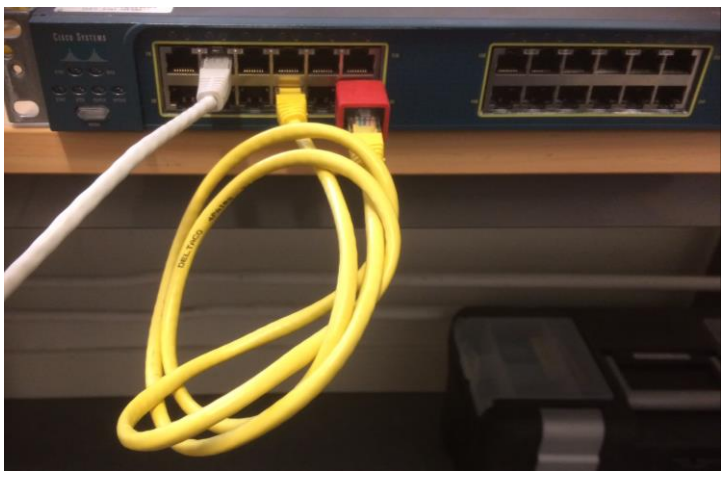
Topologi



Enhet	Gränssnitt	IP-adress	Nätmask	Default-Gateway	Switch port
PC0	Fa0	Spelar ingen roll	Spelar ingen roll	-	valfri

Utförande: Anslut datorn till switchen enligt bilden. Det spelar ingen roll vilka portar ni använder. I instruktionerna så utgår vi ifrån att en CISCO-switch används men principen är densamma även för switchar av andra tillverkare.

1. Anslut datorn till switchen. Datorn ska egentligen bara generera lite trafik så vi behöver ej någon speciell IP-konfiguration.
2. Nästa steg bygger på att ni kan administrera er switch på något sätt och att ni gjort detta tidigare. I detta exempel utgår vi från att det är en CISCO-switch som används.
   Anslut till er switch via console-porten.
3. Vi ska nu inaktivera *STP (Spanning Tree Protocol)*. Kör följande kommandon på switchen:
   enable
   conf t
   no spanning-tree vlan 1
   (Detta förutsätter att switchen är fabriksåterställd eller att VLAN 1 används för aktuella portar).
4. Koppla sedan en loop in switchen (se bild). **OBS** använder ni en äldre Catalyst Switch så kan ni behöva använda en korsad TP-kabel.. Detta gör vi för att enkelt



simulera en broadcast-storm. I normala fall så skyddar STP oss mot loopar i nätverket men inte mot överdriven broadcast-trafik som genereras på annat sätt (vilket vi låtsas sker i denna laboration).

5. Notera att switchen snabbt blir överbelastad och blinkar som ett flipperspel.
6. Koppla ur loopen.
7. Vi ska nu aktivera *storm control* för portarna på switchen. Detta gör vi med följande kommandon:
   (i Global Configuration mode)
   interface range fastEthernet 0/1 – 24
   storm-control broadcast level 0.5
   storm-control multicast level 0.5
   storm-control action shutdown

   Vi har nu konfigurerat alla 24 portar (antal och typ kan såklart variera beroende på vilken switch ni använder) till att stängas ner ifall mer än 50% av bandbredden är broadcast- eller multicast-trafik. Portarna som stängs ner kommer att vara i *error-disable* läge och kräver manuell aktivering igen.
8. Upprepa steg 4 (d.v.s. koppla en loop igen). Vad händer?

9. Hur gör man för att aktivera portarna igen?

Sammanfattning kommandon

Kommando	Beskrivning
enable	Aktivera EXEC-mode
conf t	Aktivera Global Configuration mode
no spanning-tree vlan 1	Inaktiverar STP för VLAN 1
interface range fastEthernet 0/1 – 24	Väljer alla 24 portar
storm-control broadcast level 0.5	Begränsar mängden broadcast-trafik till 50%
storm-control multicast level 0.5	Begränsar mängden multicast-trafik till 50%
storm-control action shutdown	Konfigurerar portarna till att stängas av helt ifall gränsen överskrids

Svart = EXEC kommando, Blå = Global Configuration, Grön = Interface Configuration, Orange = funkar alltid, Rött = Router Configuration

Detta skall du kunna efter genomförd labb:

✓ Konfigurera *Storm Control* för att skydda nätverket mot för mycket broadcast/multicast-trafik