Übungsprotokoll - NWG2 - Übung 05
Link Aggregation

Thomas Brandstetter (s2210239002) & Jakob Mayr (s2210239021)

8. Juni 2023

1 Konfiguration der Endsysteme

In der folgenden Übung haben wir die PCs 4.1 und 4.2 benutzt, somit sind die Netze 4.x verwendet worden. Die IP-Konfiguration wird folgendermaßen vergeben: Klick auf „Network“ in der Taskleiste → „Network & Internet Settings“ → „Change adapter options“ → gewünschtes Netzwerk Interface auswählen, in diesem Fall Ethernet 2 → „Properties“ → Doppelklick auf „Internet Protocol Version 4“ bzw. „Internet Protocol Version 6“. In den geöffneten Fenstern können wir nun jeweils die IP-Adresse, Subnetzmaske/Präfix und das Gateway eingeben. Folglich sind die Konfigurationen beider PCs zu sehen:

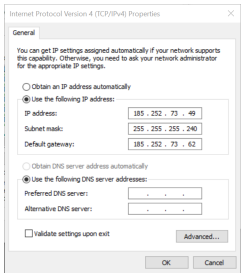

Abbildung 1: PC41 IPv4 config

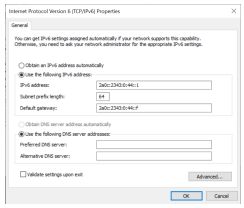

Abbildung 2: PC41 IPv6 config

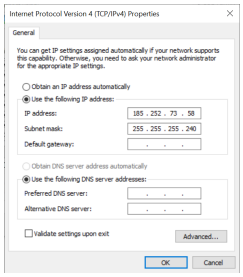

Abbildung 3: PC42 IPv4 config

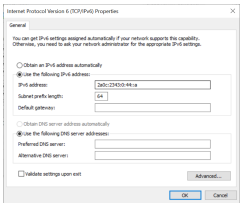

Abbildung 4: PC42 IPv6 config

2 Konfiguration des Gruppenrouters

Für die Konfiguration des Gruppenrouters müssen die Interfaces GigabitEthernet0/0 und GigabitEthernet0/1 mit einer IPv4 und einer IPv6 Adressen versehen werden. Ebenfalls muss dafür ipv6-unicast-routing aktiviert werden.
Als Default-Gateway wird sowohl für IPv4 als auch für IPv6 der Backbone-Router angegeben.

Befehl	**Erklärung**
ip address <ip-address> <ip-address-mask>	Mit diesem Befehl wird auf einem Interface eine IPv4 Adresse mit der zugehörigen Maske konfiguriert.
ipv6 address <ipv6-address/ipv6-address-mask>	Mit diesem Befehl wird auf einem Interface eine IPv6 Adresse mit der zugehörigen Maske konfiguriert.
ip route <network-number> <network-mask> <ip-address|interface>	Mit diesem Befehl wird eine statische IPv4 Route angelegt.
ipv6 route <network-number/network-mask> <ipv6-address|interface>	Mit diesem Befehl wird eine statische IPv6 Route angelegt.
ipv6-unicast-routing	Mit diesem Befehl wird das unicast-routing für IPv6 aktiviert.

Tabelle 1: Verwendete Befehle zur Konfiguration des Gruppenrouters

Als nächstes müssen auf dem Router die notwendigen ACLs (access-control-lists) konfiguriert werden. Hierfür soll sowohl jeder eingehende Trafik von den PCx1's zu PC41, als auch jeder eingehende ICMP Trafik zu PC42 geblockt werden.
Für die ACL der linken PCs werden die Adressen der PCx1's einzeln in einer IPv4 und einer IPv6 ACL geblockt.
Für die ACL des rechten PCs wird jeder ICMP Trafik geblockt.

Befehl	**Erklärung**
ip access-list extended <ACL-name>	Mit diesem Befehl wird eine ACL für IPv4 angelegt.
ip access-list extended <ACL-name>	Mit diesem Befehl wird eine ACL für IPv6 angelegt.
deny ip host <src-ip-address> host <dest-ip-address>	Mit diesem Befehl wird der Trafik von der src-ip-Adresse zur dest-ip-Adresse geblockt.
deny ipv6 host <src-ipv6-address> host <dest-ipv6-address>	Mit diesem Befehl wird der Trafik von der src-ipv6-Adresse zur dest-ipv6-Adresse geblockt.
deny icmp host <ipv4/ipv6-address> any	Mit diesem Befehl wird jeder eingehende icmp auf die angegebene Adresse geblockt.
permit ip any any / ipv6 permit any any	Diese Befehle müssen am Ende einer ACL hinzugefügt werden, da die Regeln Schritt-für-Schritt abgearbeitet werden und Trafik per-default geblockt wird. Nur mit dieser Regel wird der Trafik welcher von keiner vorherigen Regel geblockt oder speziell erlaubt wird durchgelassen.

Tabelle 2: Verwendete Befehle zum anlegen der ACLs

Damit die ACLs nun auch vom Router verwendet werden können, müssen sie noch den jeweiligen Interfaces hinzugefügt werden.

Befehl	Erklärung
ip access-group <ACL-name> in	Mit diesem Befehl wird eine IPv4-ACL einem Interface hinzugefügt.
ipv6 traffic-filter <ACL-name> in	Mit diesem Befehl wird eine IPv6-ACL einem Interface hinzugefügt.

Tabelle 3: Verwendete Befehle zum hinzufügen der ACLs zu den Interfaces.

3 Konfiguration der Gruppenswitches

Für die Konfiguration der Gruppenswitches ist eine Link-Aggregation zu konfigurieren.
Hierzu müssen zuerst auf beiden Switches ein Port-Channel (1) mit dem load-balancing-mode angelegt werden. Anschließend müssen auf den jeweiligen Interfaces das channel-protocol (lacp) und die channel-group (1) im mode aktiv angelegt werden.

Befehl	Erklärung
port-channel load-balance <load-balancind-mode>	Mit diesem Befehl wird ein Port-Channel mit dem jeweiligen load-balancing-mode konfiguriert. (Für diese Aufgabe funktioniert der „src-dst-ip“ mode, da bei diesem der Trafik der beiden Clients klar von einander getrennt werden kann. Anders könnte der Trafik nicht auf zwei Interfaces aufgeteilt werden.)
channel-protocol <protocol>	Mit diesem Befehl wird auf dem jeweiligen Interface das channel-protocol spezifiziert. (Für diese Aufgabe das lacp - link aggregation control protocol.)
channel-group <number> mode <aktiv/passive>	Mit diesem Befehl wird auf dem jeweiligen Interface die channel-group in dem spezifizierten Modus konfiguriert.

Tabelle 4: Verwendete Befehle zur Konfiguration der Gruppenswitches (Link-Aggregation)

3.1 Mirror-Port

Zuletzt soll auf dem Gruppenswitch GS41 noch ein Mirror-Port eingerichtet werden. Dieser soll als Eingangsport den Port-Channel der zuvor konfigurierten Channel-Group und als Ausgangsport den Port an dem der linke PC41 hängt haben.

Befehl	Erklärung
monitor session <number> source interface <interface-name>	Mit diesem Befehl wird der Eingangsport für den Mirror-Port bestimmt.
monitor session <number> destination interface <interface-name>	Mit diesem Befehl wird der Ausgangsport für den Mirror-Port bestimmt.
channel-group <number> mode <aktiv/passive>	Mit diesem Befehl wird auf dem jeweiligen Interface die channel-group in dem spezifizierten Modus konfiguriert.

Tabelle 5: Verwendete Befehle zur Konfiguration des Mirror-Ports

4 Fragen zur Konfiguration

Frage 5.1 Warum können ohne die Link Aggregation (das Erstellen der Channel Group) nicht beide Links verwendet werden?

Ohne Link Aggregation, auch bekannt als Port Trunking oder EtherChannel, würden die beiden parallelen Fast Ethernet Verbindungen als separate, unabhängige Links betrachtet werden. Dies kann zu mehreren Problemen führen:

- Ungleichmäßige Lastverteilung: Ohne Link Aggregation wäre es schwierig, den Datenverkehr gleichmäßig über die beiden Links zu verteilen. In der Regel würde ein Switch den Datenverkehr über einen Link senden, bis dieser voll ist, und dann erst den anderen Link verwenden. Dies führt zu einer ineffizienten Nutzung der verfügbaren Bandbreite.

- Fehlende Redundanz und Ausfallsicherheit: Ohne Link Aggregation, wenn ein Link ausfällt, würde der Datenverkehr, der über diesen Link fließt, unterbrochen werden, bis der Switch den Ausfall erkennt und auf den anderen Link umschaltet. Mit Link Aggregation würde der Datenverkehr einfach über den verbleibenden Link weitergeleitet werden, wenn ein Link ausfällt, was zu einer höheren Ausfallsicherheit führt.

Frage 5.2 Wie kann durch ein geeignetes Load Balancing sichergestellt werden, dass beide Rechner mit voller Geschwindigkeit bedient werden?

Dies kann erreicht werden, indem man beispielsweise das Load Balancing so konfiguriert, dass es auf der Basis der Quell- und Ziel-IP-Adressen und/oder Portnummern arbeitet. Auf diese Weise würde der Verkehr von und zu den beiden verschiedenen Rechnern wahrscheinlich auf die beiden verschiedenen Links verteilt werden, was dazu beitragen würde, dass beide Rechner mit voller Geschwindigkeit bedient werden.

Frage 5.3 Wenn Gruppe A die ACLs bereits fertig konfiguriert hat, Gruppe B aber nicht, wie wirkt sich das auf Ping zwischen den linken PCs aus? Falls es nicht geht, welche Fehlermeldungen erscheinen wann?

In diesem Szenario, wenn Gruppe A ihre ACLs so konfiguriert hat, dass jeglicher Trafic von den anderen linken PCs (PCx1) auf den eigenen linken PC am Routerinterface Gi0/0 eingehend geblockt wird, und jeglicher ICMP Trafic (Ping) vom eigenen rechten PC auf alle anderen Geräte am Routerinterface Gi0/1 eingehend geblockt wird, dann wird jeglicher Ping-Verkehr, der von den PCs der Gruppe A ausgeht, blockiert.

Wenn Gruppe B ihre ACLs jedoch nicht konfiguriert hat, dann gibt es auf ihrer Seite keine Beschränkungen für den Netzwerkverkehr. Das bedeutet, dass Ping-Verkehr von den PCs der Gruppe B zu den PCs der Gruppe A möglich ist, aber die Antworten von den PCs der Gruppe A werden aufgrund der ACLs der Gruppe A blockiert.

In Bezug auf Fehlermeldungen, wenn ein Ping-Versuch durchgeführt wird und die Antwort blockiert wird, wird in der Regel eine „Request timed out“ oder „Destination host unreachable“ Nachricht angezeigt. Dies zeigt an, dass der Ping-Request nicht erfolgreich war, weil keine Antwort vom Ziel-PC empfangen wurde.

Frage 5.4 Wie wirken sich die ACLs auf den Kontakt zum FTP Server aus, und warum?

Da die ACL einerseits den Trafik von anderen Clients (PCx1) und andererseits ICMP Trafik sperren, haben sie keine Auswirkung auf den Kontakt zum FTP Server. Wichtig ist dafür jedoch die „permit ip any any“ regel am Ende der ACL.

Frage 5.5 Was bedeutet es für den linken PC, dass er an einem Mirror Port hängt? Wie wirkt sich das auf seine Kommunikationsfähigkeit aus? Welche ports sollten für einen Mirror Port verwendet werden und warum?

Wenn der linke PC an einem Mirror Port hängt, bedeutet das, dass er eine Kopie des Netzwerkverkehrs von den Quellports empfängt. Dies sollte seine normale Kommunikationsfähigkeit nicht beeinflussen - er kann immer noch Netzwerkverkehr senden und empfangen wie gewohnt. Der Unterschied ist, dass er zusätzlich eine Kopie des Netzwerkverkehrs von den Quellports empfängt.

In Bezug auf die Auswahl der Ports für einen Mirror Port, sollte der Mirror Port in der Regel an einen dedizierten Überwachungs- oder Analysegerät angeschlossen werden, wie z.B. einen PC mit Netzwerkanalyse-Software (wie Wireshark). Der Quellport (oder die Quellports) sollte derjenige sein, dessen Verkehr Sie überwachen oder analysieren möchten. Es ist wichtig zu beachten, dass der Mirror Port nur eine Kopie des Verkehrs empfängt - er kann nicht auf diesen Verkehr antworten oder interagieren. Daher ist es in der Regel nicht sinnvoll, einen Mirror Port für normale Netzwerkkommunikation zu verwenden.

5 Tests und Interpretation ihrer Resultate

5.1 GS41 & GS42

Verwendete „Load-Balancing“ Konfiguration auf des Switchtes GS41 und GS42:

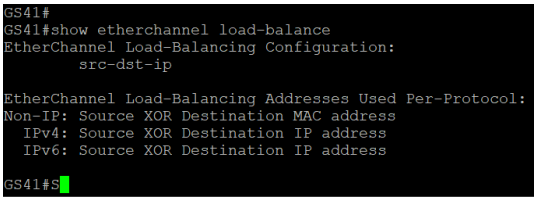

Abbildung 5: GS41 EtherChannel Load-Balancing Configuration

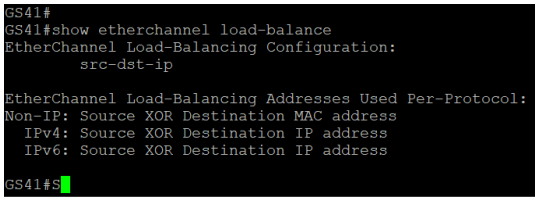

Abbildung 6: GS41 EtherChannel Load-Balancing Configuration

5.2 PC41

Ping von PC41 zu PC42, Ping zu Netz 8 - PC81 (fehlgeschlagen da ACL) und FTP-Verbindung

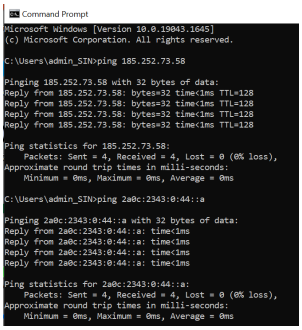

Abbildung 7: PC41 ping PC42

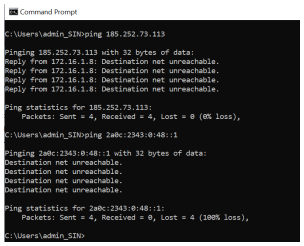

Abbildung 8: PC41 Ping zu Netz 8 - PC81 (fehlgeschlagen da ACL)
Dieser fehlgeschlagene ping zum Gruppenrouter von Gruppe 8 zeigt, dass die ACL von Gruppe 8 korrekt umgesetzt wurde.

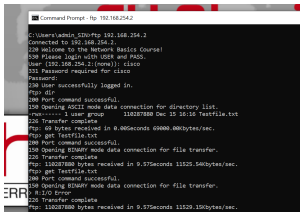

Abbildung 9: PC41 FTP-Verbindung

5.3 PC42

Ping von PC42 zu PC41, Ping zu Netz 8 - PC82 (fehlgeschlagen da ACL) und FTP-Verbindung

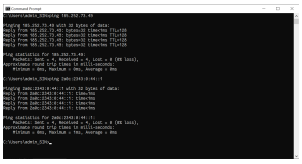

Abbildung 10: PC42 ping PC41

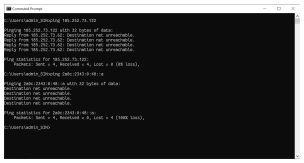

Abbildung 11: PC42 Ping zu Netz 8 - PC82 (fehlgeschlagen da ACL)
Dieser fehlgeschlagene Ping zu PC82 zeigt, dass die ACL von Gruppe 8 korrekt umgesetzt wurde.

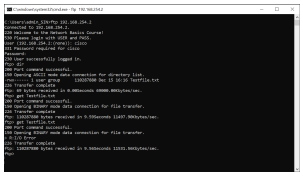

Abbildung 12: PC42 FTP-Verbindung