

Laborbericht zum Thema

Routing on real hardware with RIP

Von: Arthur Jaks, Ivana Staneva und Emel Altmisoglu
Studiengang: Medieninformatik
Fachsemester: 2

Durchgeführt am Dienstag, den **12. Mai 2015**

Inhaltsverzeichnis

1 Einleitung	- 4 -
2 Versuchsaufbau	- 5 -
3 Versuchsdurchführung, Versuchsergebnisse, Diskussion, Auswertung	- 6 -
4 Zusammenfassung	- 8 -
5 Quellenverzeichnis	- 9 -
6 Anhang - Antworten	- 10 -

Abbildungsverzeichnis

Abbildung 1 - Aufbau der Netzwerke	- 5 -
Abbildung 2 - Konfigurationstabelle.....	- 7 -
Abbildung 3 - ICMP Ping RIPv1	- 8 -
Abbildung 4 - ICMP Ping RIPv2	- 8 -

1 Einleitung

In diesem Versuch sollen mit der Hilfe echter Hardware mehrere Netzwerke erstellt werden, die Unter anderem aus verschiedenen Routern bestehen. Da die einzelnen Router nur die direkt an den jeweiligen Router angeschlossenen Netzwerke kennen, benötigen wir das Routing Information Protocol (RIP). Damit wird uns ermöglicht, dass z.B. der PCs ein anderes, nicht direkt an den Router grenzendes Netzwerk, erreichen kann. Dazu sendet der Router eine Anfrage an alle direkt angrenzenden Router und fragt diese nach deren Routing Tabelle. In dieser Tabelle stehen die Adressen aller direkt verbundener Router. Nachdem die Router sich alle Informationen ausgetauscht haben, kennen sich die Netzwerke untereinander. Somit können auch nicht direkt verbundene Netzwerke miteinander kommunizieren.

Im heutigen Versuch sollen die Router so konfiguriert werden das auch nicht direkt angrenzende Netzwerke miteinander kommunizieren können, in unserem Fall soll PC1 mit PC3 kommunizieren.

2 Versuchsaufbau

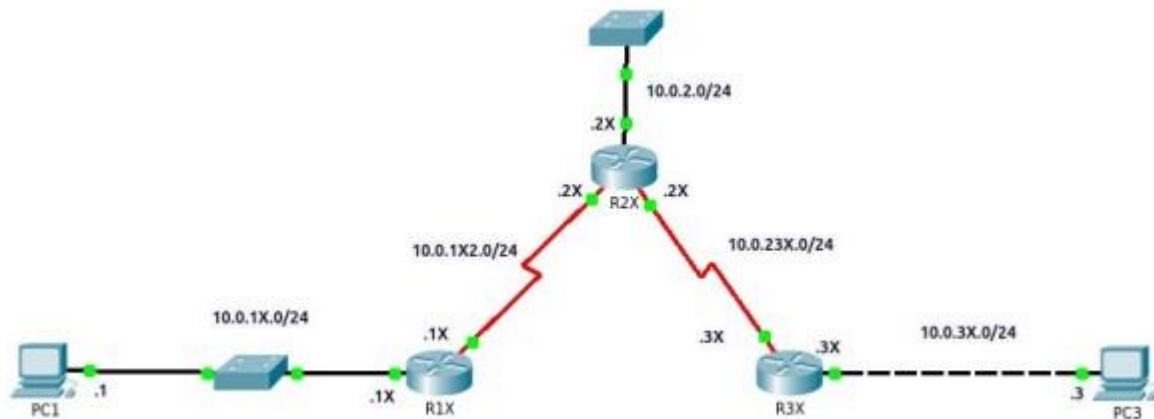


Abbildung 1 - Aufbau der Netzwerke

Der heutige Versuch besteht aus 5 Netzwerken. Dabei gibt es drei Router, „R12“, „R22“ und „R32“, die untereinander mit einem Serial Kabel verbunden sind. Taktgeber ist dabei der Router „R12“.

Die zweite Schnittstelle von Router R12 führt zu einem Switch, beide Geräte sind dabei mit einem Straight Through Kabel verbunden. Von diesem Switch führt ein weiteres Straight Through Kabel zum PC1.

Von Router R22 führt ein Straight Through Kabel zu einem Switch. An diesem Switch ist kein weiteres Gerät angeschlossen.

Router R32 ist mit PC3 direkt über ein Crossover Kabel verbunden.

Die Aufgabe besteht zum einen daraus dieses Netzwerk nachzubauen und zum anderen es mit Hilfe von RIP so zu konfigurieren, dass die PCs miteinander kommunizieren können.

3 Versuchsdurchführung, Versuchsergebnisse, Diskussion, Auswertung

In diesem Versuch soll mit Hilfe von echter Hardware das in der Abbildung 1 abgebildete Netzwerk nachgebaut werden. Dazu stehen zwei Computer, ein Rechnerschränk mit allen Routern und Switches und Straight Through sowie Crossover Kabel zur Verfügung.

Als Erstes muss der PC1 mit dem Switch verbunden werden. Dazu nimmt man ein Straight Through Kabel und verbindet am Rechnerschränk den PC1 mit dem Switch.

Als Nächstes verbindet man den Switch mit dem Router R12, dazu nimmt man ebenso ein Straight Through Kabel und verbindet den Switch mit dem Router R12.

Damit der PC1 den Router R12 konfigurieren kann, ist es nötig den PC und den Router mit einem Straight Through Kabel an der Konsolen Schnittstelle zu verbinden.

Als Nächstes verbindet man den PC3 mit dem Router R32. Da der PC direkt mit dem Router verbunden wird, benötigt man ein Crossover Kabel und verbindet beide Geräte.

Ist der PC mit dem Router verbunden, muss genau so wie bei PC1 und Router R12 der PC mit dem Router über ein Straight Through an der Konsolen Schnittstelle verbunden werden.

Sobald beide Router über die Konsolen Schnittstelle mit dem Router verbunden sind, muss man die Router an dem jeweiligen PC konfigurieren.

Dazu benutzt man die auf beiden PCs vorinstallierte VMware. Die VMware verfügt über ein Programm, mit dem man den verbundenen Router konfigurieren kann.

Sobald alles geklappt hat und man auf den Router Zugriff hat, ändert man zunächst den Hostnamen des Routers. Dazu gibt man zuerst **enable** ein, um in den privilegierten Modus des Routers zu wechseln und gibt anschließend **configure terminal** ein, um in den globalen Konfigurationsmodus zu wechseln. Dort angekommen gibt man nur **hostname R12** ein um den Hostnamen des Routers zu ändern.

Nachdem der Hostname geändert wurde, setzt man das Konsolen und Telnet Passwort des Routers. Dazu bleibt man im globalen Konfigurationsmodus und gibt dort als erstes **line console 0** ein. Damit wechseln man zum Konsolenzugang und kann von hier aus **password cisco** eingeben, um das Passwort zu setzen. Um das Passwort zu aktivieren, muss man im Anschluss noch **login** schreiben.

Um nun das Telet-Passwort zu setzen muss man erst mal den Konsolenzugang mit der Eingabe von **exit** verlassen. Befindet man sich nun im globalen Konfigurationsmodus, kann man **line vty 0 4** eingeben, um zu den Telnet Lines 0 bis 4 zu wechseln. Dort angekommen setzt man genauso wie im Konsolenzugang, das Telnet Passwort mit **password cisco** und anschließend **login** um es zu aktivieren.

Im nächsten Schritt wird das secret des Routers gesetzt. Dazu muss man zuerst wieder in den globalen Konfigurationsmodus wechseln. Sobald man sich dort befindet, kann man mit dem Befehl **enable secret class** das verschlüsselte Enable Secret setzen.

Als Nächstes wird ein Banner mit einer Willkommensnachricht gesetzt. Dazu muss man wieder in den globalen Konfigurationsmodus wechseln. Sobald man sich in diesem Modus befindet, kann man mit **banner motd # Nachricht #** eine beliebige Willkommensnachricht setzen.

Nun geht es darum die Router zu konfigurieren. Dazu wird RIPv1 und die folgende Konfigurationstabelle genutzt:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1X	Fa0/0	10.0.1X.1X	255.255.255.0	N/A
	S0/2/0	10.0.1X2.1X	255.255.255.0	N/A
R2X	S0/2/0	10.0.1X2.2X	255.255.255.0	N/A
	Fa0/0	10.0.2.2X	255.255.255.0	N/A
	S0/2/1	10.0.23X.2X	255.255.255.0	N/A
R3X	Fa0/0	10.0.3X.3X	255.255.255.0	N/A
	S0/2/?	10.0.23X.3X	255.255.255.0	N/A
PC1	FastEthernet 0	10.0.1X.1	255.255.255.0	10.0.1X.1X
PC3	FastEthernet 0	10.0.3X.3	255.255.255.0	10.0.3X.3X

Abbildung 2 - Konfigurationstabelle

Mithilfe dieser Tabelle weist man jetzt jeder Schnittstelle die dazugehörige IP Adresse zu. Dazu geht man in den globalen Konfigurationsmodus, wechseln von dort aus zu der entsprechenden Schnittstelle also z.B. **interface fa0/0** und gibt dort die zugehörige IP Adresse und Subnetz Maske an, in diesem Fall wäre es **ip address 10.0.12.12 255.255.255.0**. Nachdem man die IP-Adresse vergeben hat, ist es sehr wichtig diese Schnittstelle hochzufahren, dies macht man mit **no shutdown**. Diesen Vorgang wiederholt man für alle Schnittstellen eines Routers.

Im nächsten Schritt kann man nun dem Router mittels RIP die anliegenden Netzwerke mitteilen. Dazu geht man in den globalen Konfigurationsmodus und gibt danach **router rip** ein um RIP auf dem Router zu aktivieren und um in den Router Modus zu wechseln. Hier gibt man jetzt die anliegenden Netzwerke an. Dies wird mit dem Befehl **network 10.0.12.0** gemacht, dabei muss jedes anliegende Netzwerk mit der IP Adresse angegeben werden.

Alle Schritte der Konfiguration wiederholt man nun für Router R32 und R22. Dabei muss bedacht werden, dass der Router R22 erst konfiguriert werden kann wenn man einen der beiden PCs von der aktuellen Konsolen Schnittstelle entfernt und in den Router R22 steckt. Danach kann wie gewohnt konfiguriert werden.

Nachdem alles konfiguriert wurde, prüft man nun ob PC1 mit PC3 Kommunizieren kann.

Dazu wird Wireshark auf PC1 geöffnet. Danach macht man einen Ping von PC1 zu PC3, wenn dies klappen sollte, wurde alles richtig konfiguriert.

Man kann nun das Protokoll von RIPv1 auf RIPv2 ändern. Dazu geht man in die Konfiguration der Router und gibt im globalen Konfigurationsmodus **router rip** ein. Um RIPv2 zu aktivieren gibt man **version 2** ein.

Die ICMP Ausgabe des Pings in Wireshark mit RIPv1 und RIPv2 ist in der folgenden Abbildung zu sehen:

Source	Destination	Protocol	Length	Info
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 24)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=125 (request in 23)
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 27)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=125 (request in 26)
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 31)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=125 (request in 30)
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 33)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=125 (request in 32)

Abbildung 3 - ICMP Ping RIPv1

Source	Destination	Protocol	Length	Info
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 17)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=125 (request in 16)
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 21)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=125 (request in 20)
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 24)
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=125 (request in 23)
10.0.12.1	10.0.32.3	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128
10.0.32.3	10.0.12.1	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=125 (request in 27)

Abbildung 4 - ICMP Ping RIPv2

Um zu sehen, welche Verbindungen nun in der Routing Tabelle sind, kann man den Befehl **show ip route** aufrufen.

4 Zusammenfassung

Nachdem man diesen Versuch erfolgreich beendet hat, ist man ist der Lage mehrere Netzwerke eigenständig zu verbinden. Außerdem hat man gelernt wie man die Schnittstellen und RIP konfiguriert, den Hostnamen eines Routers ändert, eine Willkommensnachricht generiert, ein Konsolen und Telnet Passwort setzt, das Secret eines Routers setzt, zwischen zwei PCs pingt und wie man sich die Routing Tabelle angucken kann. Zudem hat man mit dem Wireshark Programm gearbeitet und die Ruten verfolgen können.

5 Quellenverzeichnis

Lab 4 - Aufgabenzettel (vom 18.05.2015)

https://www.aulis.hs-bremen.de/goto.php?target=file_535667_download&client_id=hsbremen

Cisco IOS Kommandos (vom 18.05.2015)

https://www.aulis.hs-bremen.de/goto.php?target=file_524292_download&client_id=hsbremen

Configuring a Cisco Router (vom 18.05.2015)

https://www.aulis.hs-bremen.de/goto.php?target=file_535698_download&client_id=hsbremen

Wikipedia – Routing Information Protocol (vom 18.05.2015)

http://de.wikipedia.org/wiki/Routing_Information_Protocol

6 Anhang - Antworten

ICMP ECHO REQUEST – ECHO REPLY (PING):

- 1.) ICMPv4 ist im RFC 792 definiert.
- 2.) Die MAC Adresse des Routers zu dem das Packet zurückgesendet wurde.
- 3.) Nein, da sie nicht in einem Netz sind.
- 4.) In dem es 0x0800 in das Typ-Feld schreibt.
- 5.) In dem es in die Protokollnummer eine 1 reinschreibt.
- 6.) Der Typ eines ICMP Pakets ist 8 Bit lang.
- 7.) Ein Echo Request hat die Typ Nummer 8.
- 8.) Eine Echo Antwort hat die Typ Nummer 0.
- 9.) Optional kann eine Echo Reply Nachricht in dem Data Block mit verschickt werden, z.B. Fehler Meldungen

TRACEROUTE

- 10.) Das ICMP benutzt Traceroute.
- 11.) Die Portnummer 33434.
- 12.) Gib die Anzahl an Hops des Datenpakets an. Wenn es das Ziel nach den angegebenen Hops nicht erreicht hat wird es verworfen.
- 13.) Traceroute beginnt seine Time To Live mit einer 1.
- 14.) Weil das Paket sein Ziel nicht mit einem Hop erreichen konnte.
- 15.) Das Time To Live wird so oft vom nächsten Router um eins Hochgezählt bis die gesamt Anzahl an Hops erreicht wurde.
- 16.) Ein ICMP Echo Reply.
- 17.) In dem Typ Feld steht eine 3, wenn das Ziel nicht erreichbar ist.

RIPv1 and RIPv2:

19. 1111
21. RIP nutzt User Datagram Protocol (UDP) als Transport Protocol
22. Destination port 520.
23. RFC 1058

RIPv2:

24. Die Ziel ist das nächste Gerät zum host MAC-Address
 25. IPv4 destination address
 26. MAC addresses for multicasting as Ethernet
 27. IPv4 reserviert einige Adressen für spezielle Zwecke wie private Netzwerke oder Multicast Adressen.
 28. Über RIP werden die Daten über UDP übertragen.
 29. RIPv2 ist klassenlos Routing Protocol und unterstützt VLSM (Variable Length Subnet Masking).
- RIPv2 unterstützt die Authentisierung zwischen Routers.
- RIPv1 ist klassenvoll Routing Protocol und unterstützt nicht VLSM.

30. Die Angabe eines Wert von 0.0.0.0 in dem Next-Hop Field zeigt, dass Routing sollte die Urheber der RIP Anzeige sein. Eine Adresse die spezifiziert sich als Next-Hop muss direkt erreichbar sein auf der logischen Subnetz, über die die Anzeige gemacht wird.

31. IP multicast address 224.0.0.9 wird wie periodic broadcasts benutzt um zu die unnötige Ladungen auf diesen Host zu reduzieren.