Routing Table Information Gathering

Analysis of possibilities to discover routing tables

Auteurs:	Daniël Sánchez & Marju Jalloh
Opleiding:	System & Network Engineering
Begeleiders:	Marc Smeets (KPMG)
	Hans IJkel (KPMG)
	Cees de Laat (UvA)

Datum:	04-07-2007
Tijd:	15:00 - 15:30

Agenda

- Project introductie
- Achtergrond
- Gerelateerd werk
- Onderzoek
- Conclusie
- Toekomstig werk
- Vragen

Project introductie

- Onderzoeksvraag
- Belang

Project introductie: Onderzoeksvraag

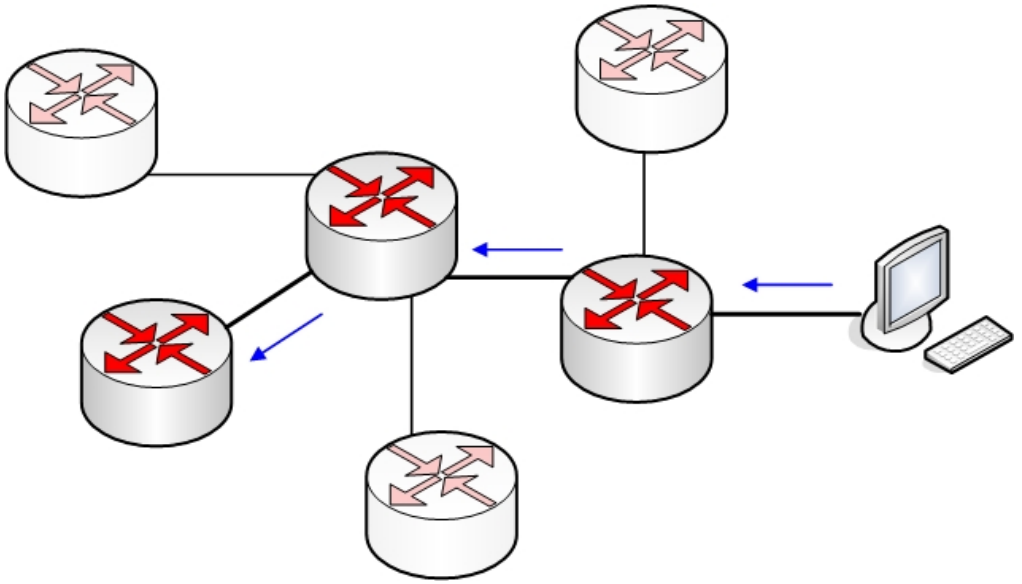
"What are possibilities to discover routing table information from a router, without having authorized access privileges to the router?"

Project introductie:
Belang

- Gevaren
- Netwerk overzicht

Achtergrond

- Routing concept
- Routing algoritme
- Routing database
- Routing protocol



Elke router bepaalt het "beste" pad

Gerelateerd werk

- Router & routing protocol aanvallen
- Topologie discovery
- Backbone data collectors

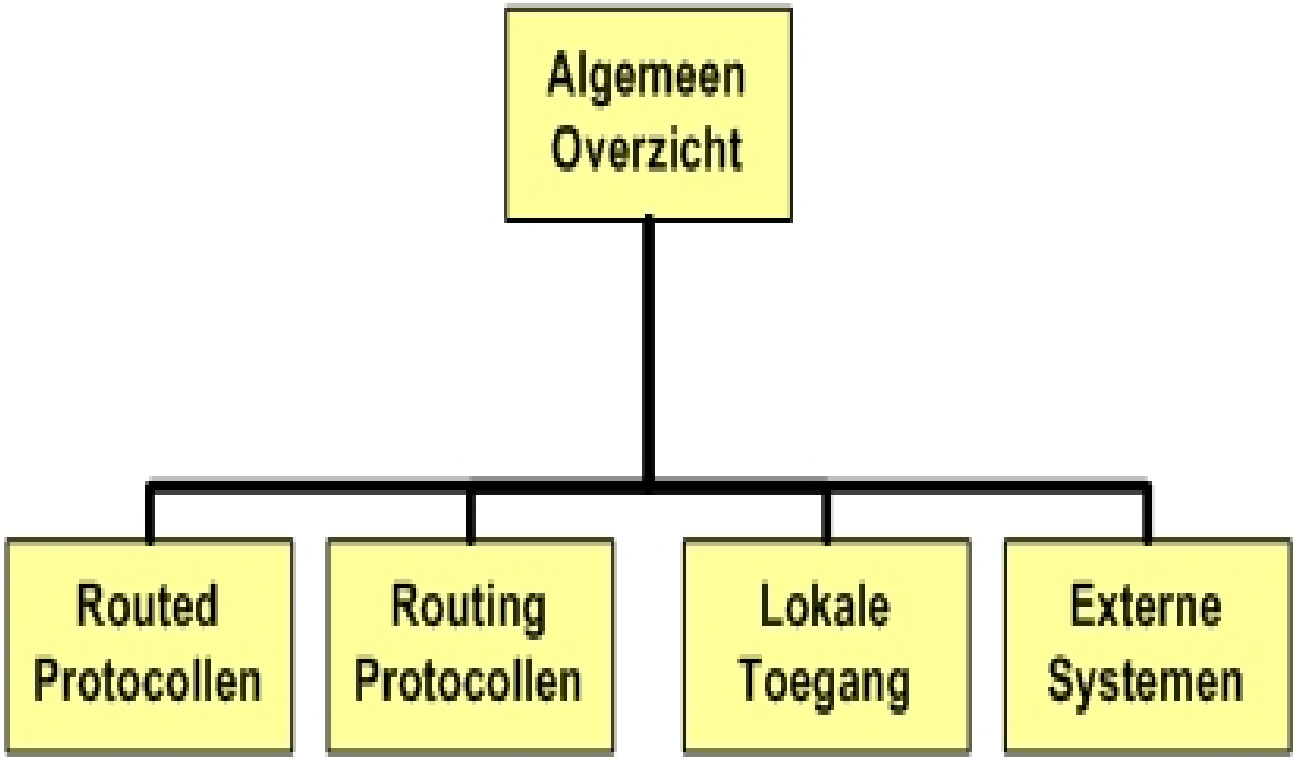
Agenda

- Project introductie
- Onderzoek
- Gerelateerd werk
- Onderzoek
- Conclusie
- Toekomstig werk
- Vragen

Onderzoek

- Algemeen overzicht
- Distributed routing table discovery

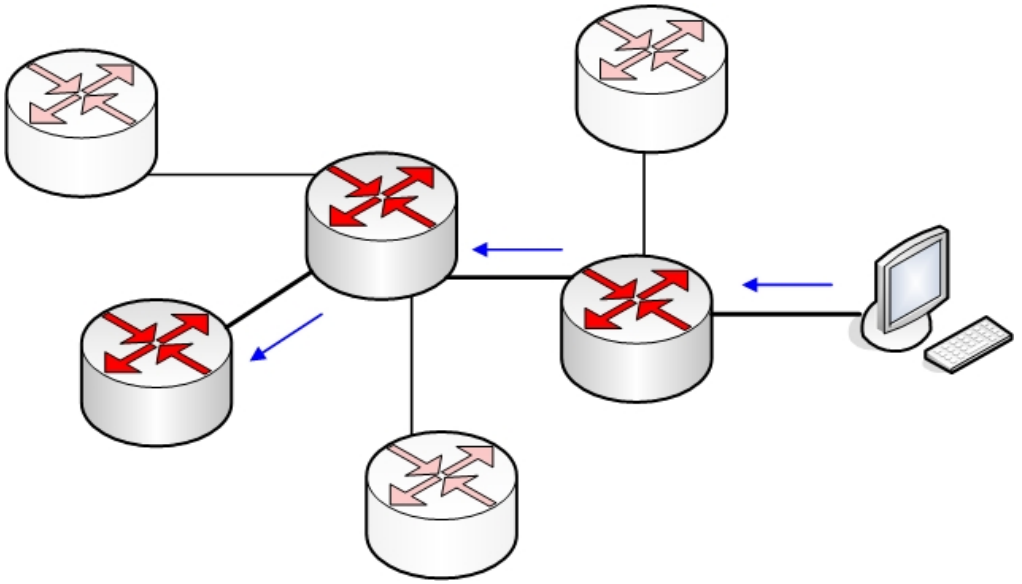
Onderzoek:
Algemeen overzicht



Onderzoek:
Algemeen overzicht

Routed protocollen

- ICMP
- TCP / UDP
- Traceroute en Ping

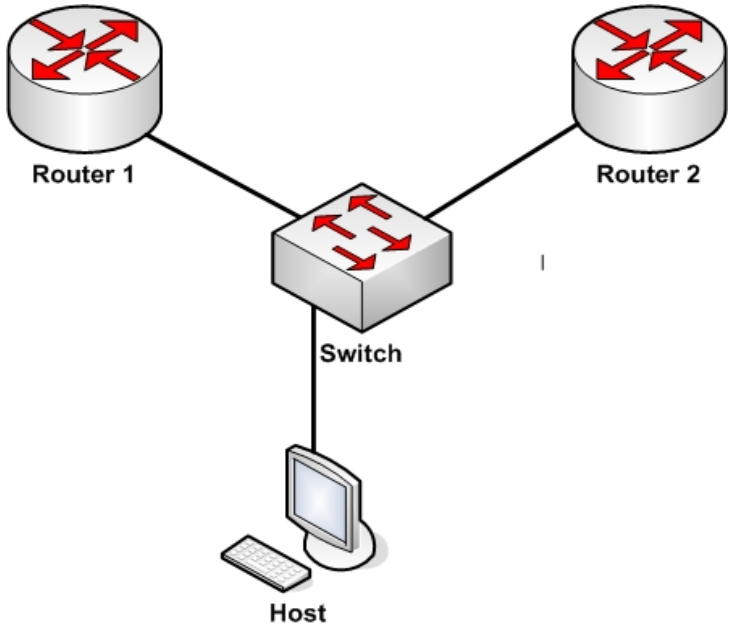


Tracerouten

Onderzoek:
Algemeen overzicht

Routing protocollen

- Deelname aan routing proces
- Zelfde subnet of VLAN
- Zwakheden in protocollen



Informatie verkrijgen via routing protocollen

Onderzoek:
Algemeen overzicht

Lokale toegang

- Fysieke toegang
- Zwakheden in configuraties

Onderzoek: Algemeen overzicht

Externe systemen

- DNS
- Configuratie opslag
- Backbone data collectors

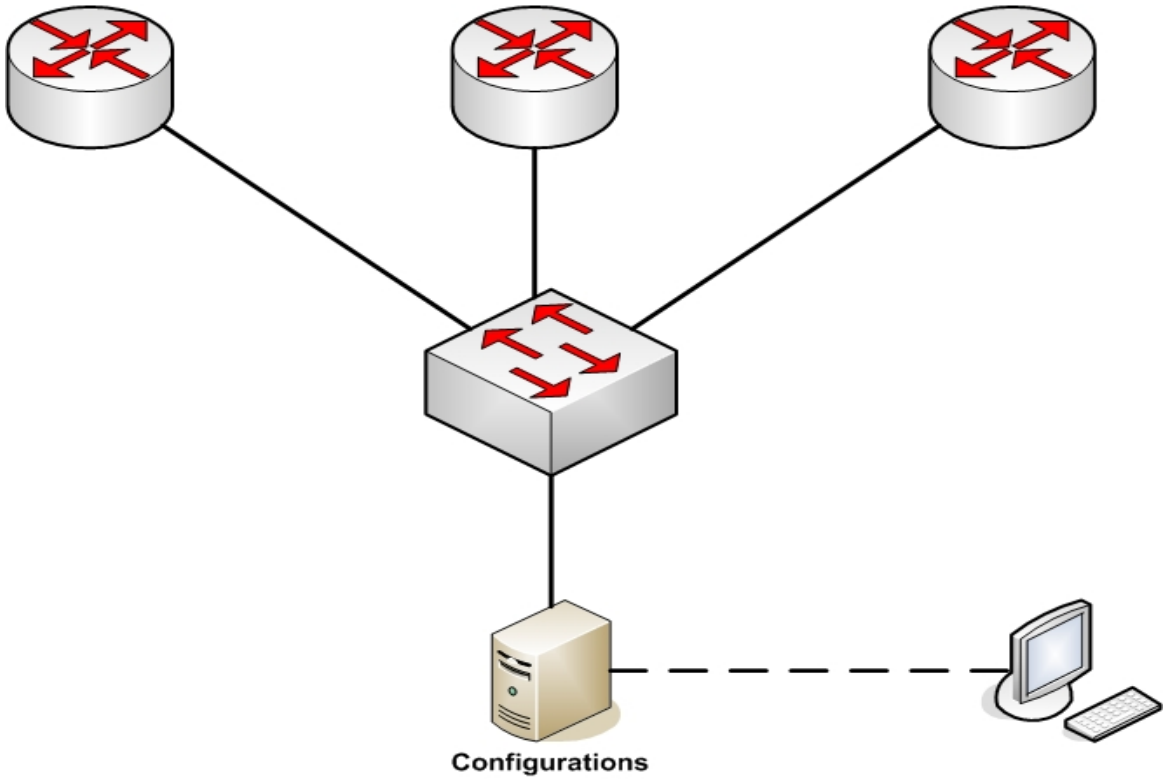
Onderzoek:
Algemeen overzicht

Externe systemen: DNS

- Nslookup
- IP adressen behorende bij router

Onderzoek:
Algemeen overzicht

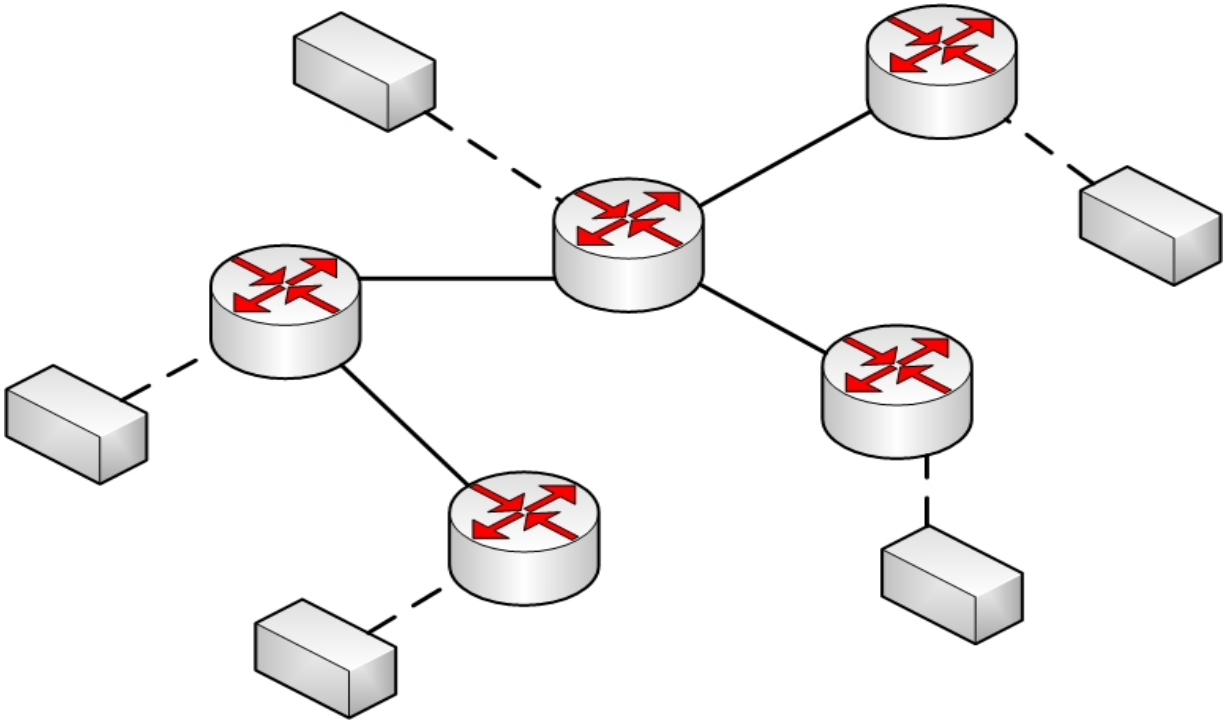
Externe systemen: configuratie opslag



Configuratie bestanden opgeslagen op een extern systeem

Onderzoek:
Algemeen overzicht

Externe systemen: Backbone data collectors

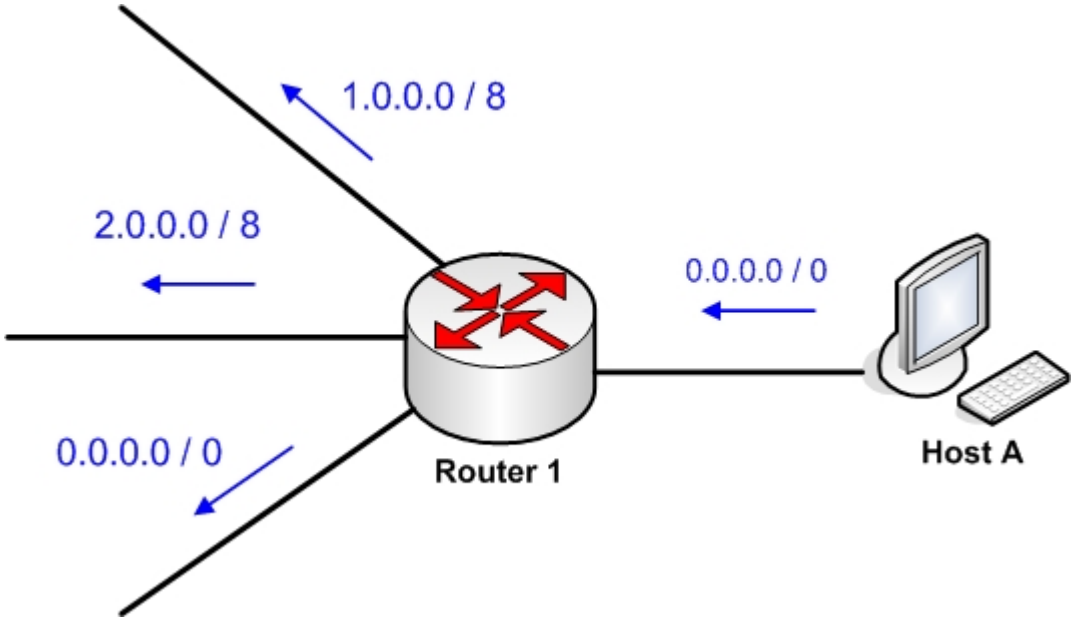


Onderzoek:
Distributed routing table discovery

- Concept
- Mogelijke implementatie
- Implementatie issues
- Proof of concept

Onderzoek:
Distributed routing table discovery

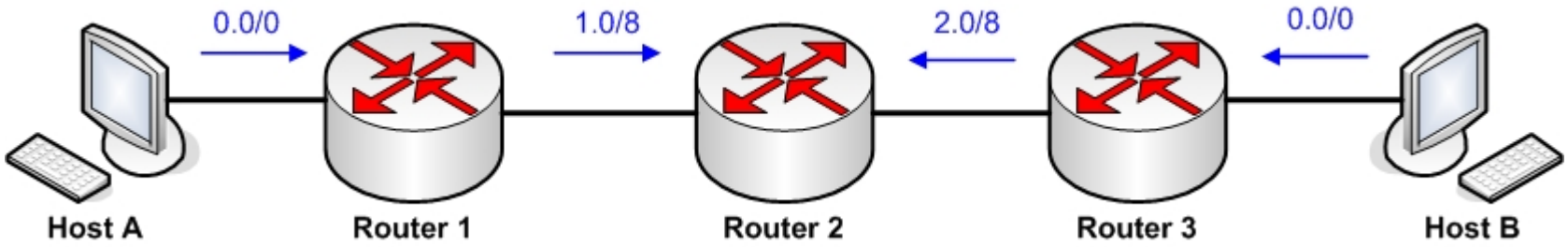
Concept



Concept van routing tabellen verkrijgen

Onderzoek:
Distributed routing table discovery

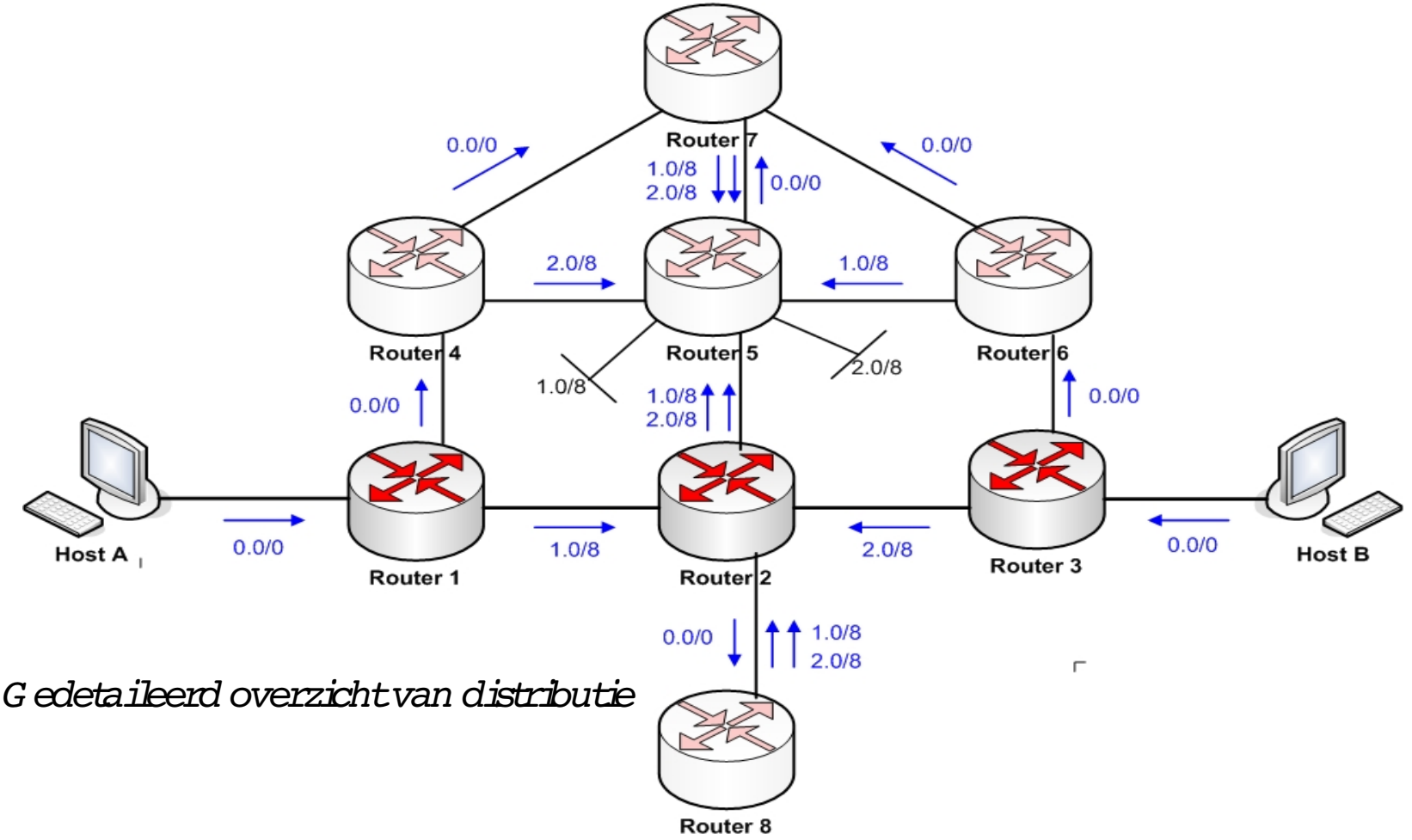
Concept



Concept van distributed routing table discovery

Onderzoek:
Distributed routing table discovery

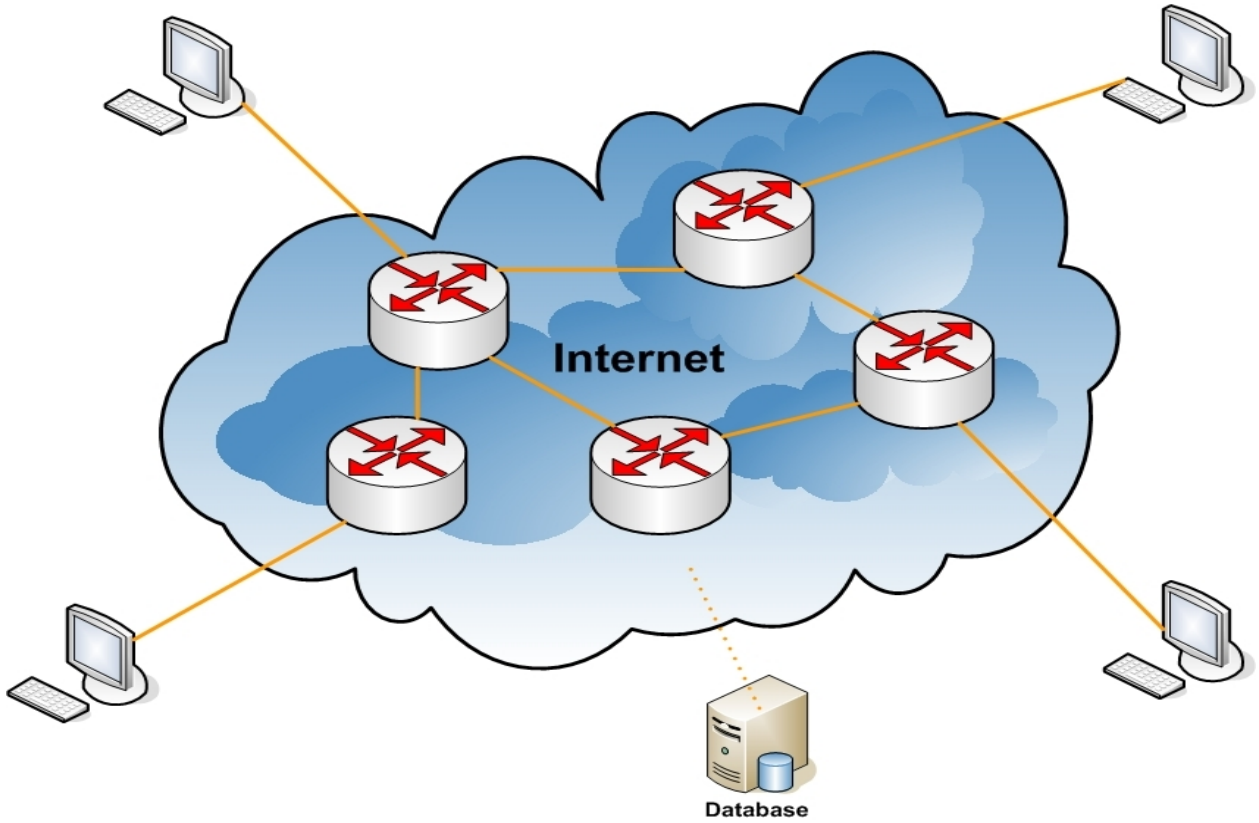
Concept



Gedetailleerd overzicht van distributie

Onderzoek:
Distributed routing table discovery

Mogelijke implementatie



Distributed routing table discovery

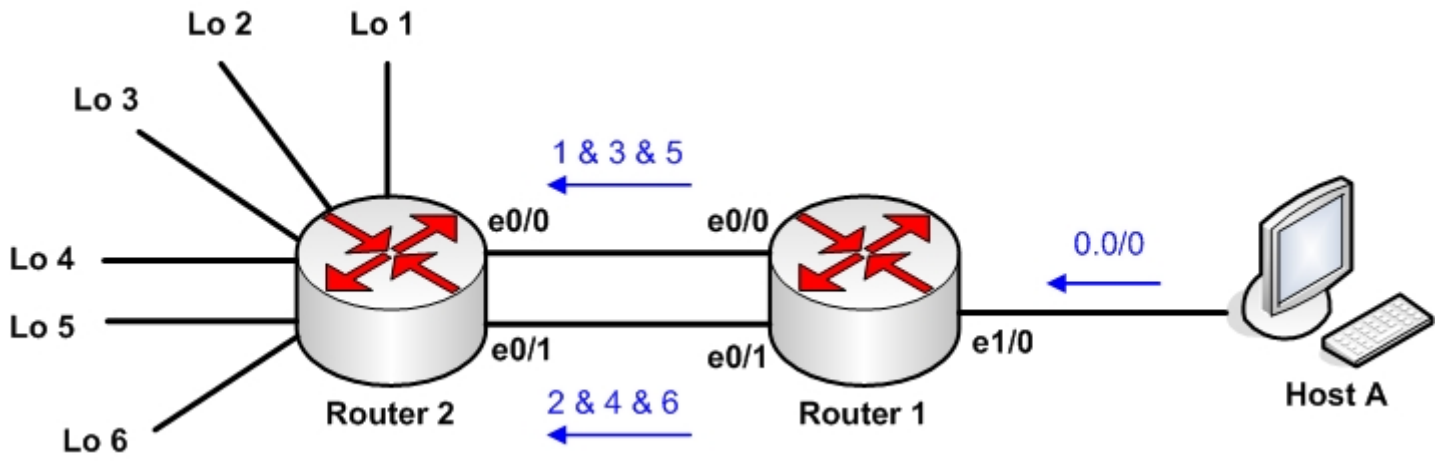
Onderzoek:
Distributed routing table discovery

Implementatie issues:

- ICMP is geblokt
- Rate limiting
- Proces erg langzaam
- Software distributie

Onderzoek:
Distributed routing table discovery

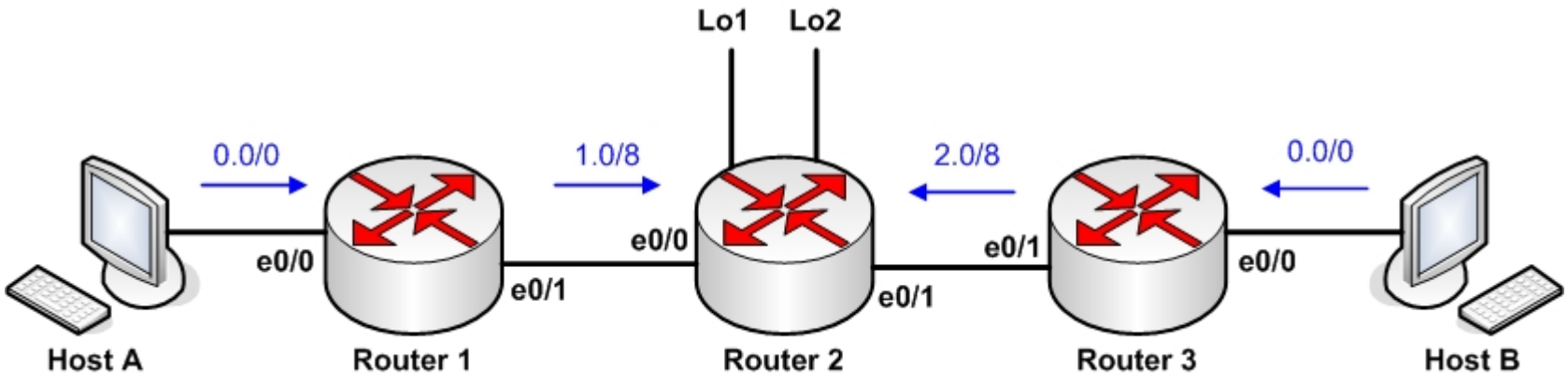
Proof of concept



Test1

Onderzoek:
Distributed routing table discovery

Proof of concept



Test 2

Agenda

- Project introductie
- Onderzoek
- Gerelateerd werk
- Onderzoek
- Conclusie
- Toekomstig werk
- Vragen

Conclusie

Onderzoeksvraag:

“What are possibilities to discover routing table information from a router, without having authorized access privileges to the router?”

Conclusie

Algemeen overzicht:

- Routed protocollen
- Routing protocollen
- Lokale toegang
- Externe systemen

Conclusie

Distributed routing table discovery:

- Concept
- Mogelijke implementatie
- Implementatie issues
- Proof of concept

Toekomstig werk

- Software ontwikkeling van het concept
- Graphische representatie
- Topologie tool gebaseerd op routing
- Verder onderzoek naar routed protocollen

Vragen