APNIC eLearning: Routing Basics

Contact: training@apnic.net
Overview

• What does a router do?
• Routing vs. Forwarding
• IP Route Lookup
• RIB and FIB
• Explicit and Default Routing
• Autonomous Systems
• Routing Policy
• Routing Protocols
• IGP and EGP
What does a router do?
A day in a life of a router

- find path
- forward packet, forward packet, forward packet, forward packet...
- find alternate path
- forward packet, forward packet, forward packet, forward packet…
- repeat until powered off
Routing versus Forwarding

- Routing = building maps and giving directions
- Forwarding = moving packets between interfaces according to the “directions”
IP Routing – finding the path

- Path derived from information received from a routing protocol
- Several alternative paths may exist
  - best path stored in forwarding table
- Decisions are updated periodically or as topology changes (event driven)
- Decisions are based on:
  - topology, policies and metrics (hop count, filtering, delay, bandwidth, etc.)
IP route lookup

• Based on destination IP address
• “longest match” routing
  – More specific prefix preferred over less specific prefix
  – Example: packet with destination of 10.1.1.1/32 is sent to the router announcing 10.1/16 rather than the router announcing 10/8.
IP route lookup

- Based on destination IP address

Packet: Destination IP address: 10.1.1.1

R2’s IP routing table:
- 10/8 → R3
- 10.1/16 → R4
- 20/8 → R5
- 30/8 → R6
- ....

10/8 announced from here

10.1/16 announced from here
IP route lookup: Longest match routing

- Based on destination IP address

Packet: Destination IP address: 10.1.1.1

10/8 → R3
10.1/16 → R4
20/8 → R5
30/8 → R6

R2’s IP routing table

10.1.1.1 && FF.0.0.0 vs. 10.0.0.0 && FF.0.0.0

Match!

10/8 announced from here
10.1/16 announced from here
IP route lookup:
Longest match routing

• Based on destination IP address

Packet: Destination
IP address: 10.1.1.1

R2’s IP routing table

10/8 → R3
10.1/16 → R4
20/8 → R5
30/8 → R6

...
IP route lookup: Longest match routing

- Based on destination IP address

Packet: Destination IP address: 10.1.1.1

10/8 → R3
10.1/16 → R4
20/8 → R5
30/8 → R6

.....

R2’s IP routing table

10/8 announced from here
10.1/16 announced from here

10.1.1.1 & FF.0.0.0
vs.
20.0.0.0 & FF.0.0.0

Does not match!
IP route lookup: Longest match routing

• Based on destination IP address

Packet: Destination IP address: 10.1.1.1

10/8 → R3
10.1/16 → R4
20/8 → R5
30/8 → R6

10.1.1.1 && FF.0.0.0 vs. 30.0.0.0 && FF.0.0.0

Does not match!
IP route lookup: Longest match routing

- Based on destination IP address

Packet: Destination IP address: 10.1.1.1

R2’s IP routing table:
- 10/8 → R3
- 10.1/16 → R4
- 20/8 → R5
- 30/8 → R6
- .....
RIBs and FIBs

• FIB is the Forwarding Table
  – It contains destinations and the interfaces to get to those destinations
  – Used by the router to figure out where to send the packet
  – Careful! Some people still call this a route!

• RIB is the Routing Table
  – It contains a list of all the destinations and the various next hops used to get to those destinations – and lots of other information too!
  – One destination can have lots of possible next-hops – only the best next-hop goes into the FIB
Explicit versus Default Routing

• Default:
  – simple, cheap (cycles, memory, bandwidth)
  – low granularity (metric games)

• Explicit (default free zone)
  – high overhead, complex, high cost, high granularity

• Hybrid
  – minimise overhead
  – provide useful granularity
  – requires some filtering knowledge
Egress Traffic

• How packets leave your network
• Egress traffic depends on:
  – route availability (what others send you)
  – route acceptance (what you accept from others)
  – policy and tuning (what you do with routes from others)
  – Peering and transit agreements
Ingress Traffic

• How packets get to your network and your customers’ networks

• Ingress traffic depends on:
  – what information you send and to whom
  – based on your addressing and AS’s
  – based on others’ policy (what they accept from you and what they do with it)
Autonomous System (AS)

- Collection of networks with same routing policy
- Single routing protocol
- Usually under single ownership, trust and administrative control
Definition of terms

• Neighbours
  – AS’s which directly exchange routing information
  – Routers which exchange routing information

• Announce
  – send routing information to a neighbour

• Accept
  – receive and use routing information sent by a neighbour

• Originate
  – insert routing information into external announcements (usually as a result of the IGP)

• Peers
  – routers in neighbouring AS’s or within one AS which exchange routing and policy information
Routing flow and packet flow

For networks in AS1 and AS2 to communicate:

AS1 must announce to AS2
AS2 must accept from AS1
AS2 must announce to AS1
AS1 must accept from AS2
Routing flow and Traffic flow

- Traffic flow is always in the opposite direction of the flow of Routing information
  - Filtering outgoing routing information inhibits traffic flow inbound
  - Filtering inbound routing information inhibits traffic flow outbound
Routing Flow/Packet Flow: With multiple ASes

• For net N1 in AS1 to send traffic to net N16 in AS16:
  – AS16 must originate and announce N16 to AS8.
  – AS8 must accept N16 from AS16.
  – AS8 must forward announcement of N16 to AS1 or AS34.
  – AS1 must accept N16 from AS8 or AS34.

• For two-way packet flow, similar policies must exist for N1
Routing Flow/Packet Flow: With multiple ASes

As multiple paths between sites are implemented it is easy to see how policies can become quite complex.
Routing Policy

• Used to control traffic flow in and out of an ISP network

• ISP makes decisions on what routing information to accept and discard from its neighbours
  – Individual routes
  – Routes originated by specific ASes
  – Routes traversing specific ASes
  – Routes belonging to other groupings
    • Groupings which you define as you see fit
Routing Policy Limitations

- AS99 uses red link for traffic to the red AS and the green link for remaining traffic.

- To implement this policy, AS99 has to:
  - Accept routes originating from the red AS on the red link
  - Accept all other routes on the green link
Routing Policy Limitations

- AS99 would like packets coming from the green AS to use the green link.
- But unless AS22 cooperates in pushing traffic from the green AS down the green link, there is very little that AS99 can do to achieve this aim.

packet flow

- AS99 would like packets coming from the green AS to use the green link.
- But unless AS22 cooperates in pushing traffic from the green AS down the green link, there is very little that AS99 can do to achieve this aim.
Routing Protocols

- Routers use “routing protocols” to exchange routing information with each other
  - IGP is used to refer to the process running on routers inside an ISP’s network
  - EGP is used to refer to the process running between routers bordering directly connected ISP networks
What Is an IGP?

- Interior Gateway Protocol
- Within an Autonomous System
- Carries information about internal infrastructure prefixes
- Two widely used IGPs in service provider network:
  - OSPF
  - ISIS
Why Do We Need an IGP?

- ISP backbone scaling
  - Hierarchy
  - Limiting scope of failure
  - Only used for ISP’s *infrastructure* addresses, not customers or anything else
  - Design goal is to *minimise* number of prefixes in IGP to aid scalability and rapid convergence
What Is an EGP?

- Exterior Gateway Protocol
- Used to convey routing information between Autonomous Systems
- De-coupled from the IGP
- Current EGP is BGP
Why Do We Need an EGP?

- Scaling to large network
  - Hierarchy
  - Limit scope of failure

- Define Administrative Boundary

- Policy
  - Control reachability of prefixes
  - Merge separate organisations
  - Connect multiple IGPs
Interior versus Exterior Routing Protocols

• Interior
  – Automatic neighbour discovery
  – Generally trust your IGP routers
  – Prefixes go to all IGP routers
  – Binds routers in one AS together
  – Carries ISP infrastructure addresses only
  – ISPs aim to keep the IGP small for efficiency and scalability

• Exterior
  – Specifically configured peers
  – Connecting with outside networks
  – Set administrative boundaries
  – Binds AS’s together
  – Carries customer prefixes
  – Carries Internet prefixes
  – EGPs are independent of ISP network topology
Hierarchy of Routing Protocols

- BGP4
- BGP4 and OSPF/ISIS
- Other ISPs
- Static/BGP4
- IXP
- Customers
## FYI: Cisco IOS Default Administrative Distances

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Interface</td>
<td>0</td>
</tr>
<tr>
<td>Static Route</td>
<td>1</td>
</tr>
<tr>
<td>Enhanced IGRP Summary Route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal Enhanced IGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>IS-IS</td>
<td>115</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>EGP</td>
<td>140</td>
</tr>
<tr>
<td>External Enhanced IGRP</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>
Questions

• Please remember to fill out the feedback form
  – <survey-link>

• Slide handouts will be available after completing the survey
APNIC Helpdesk Chat

Services

Helpdesk
Monday - Friday
09:00 to 21:00 (UTC +10)

Email
helpdesk@apnic.net

Phone
+61 7 3858 3188

VoIP
helpdesk@voip.apnic.net

Fax
+ 61 7 3858 3199

Multi-language phone support
Bansan Indonesian, Bengali, Cantonese, English, Filipino (Tagalog), Hindi, and Mandarin.

Frequently asked questions
Thank You!

End of Session