

# Network Protocols

## Routing

# One of two critical systems

Routing (BGP) and DNS are, by far, the two most fundamentally critical components of the Internet infrastructure. One big difference is that almost all Internet systems participate in the DNS directly, either as a client, a server or both. In other words, DNS has to be, by definition, one of the most unencumbered protocols in use throughout the Internet.

# Actually, all hosts do routing too

Most hosts have only two forwarding choices to make and they don't participate in a distributed routing system the way most hosts pass around DNS packets. To route, most hosts do one of two things:

- Send a packet directly out an attached interface.
- Send a packet destined for a remote network to a router for forwarding.

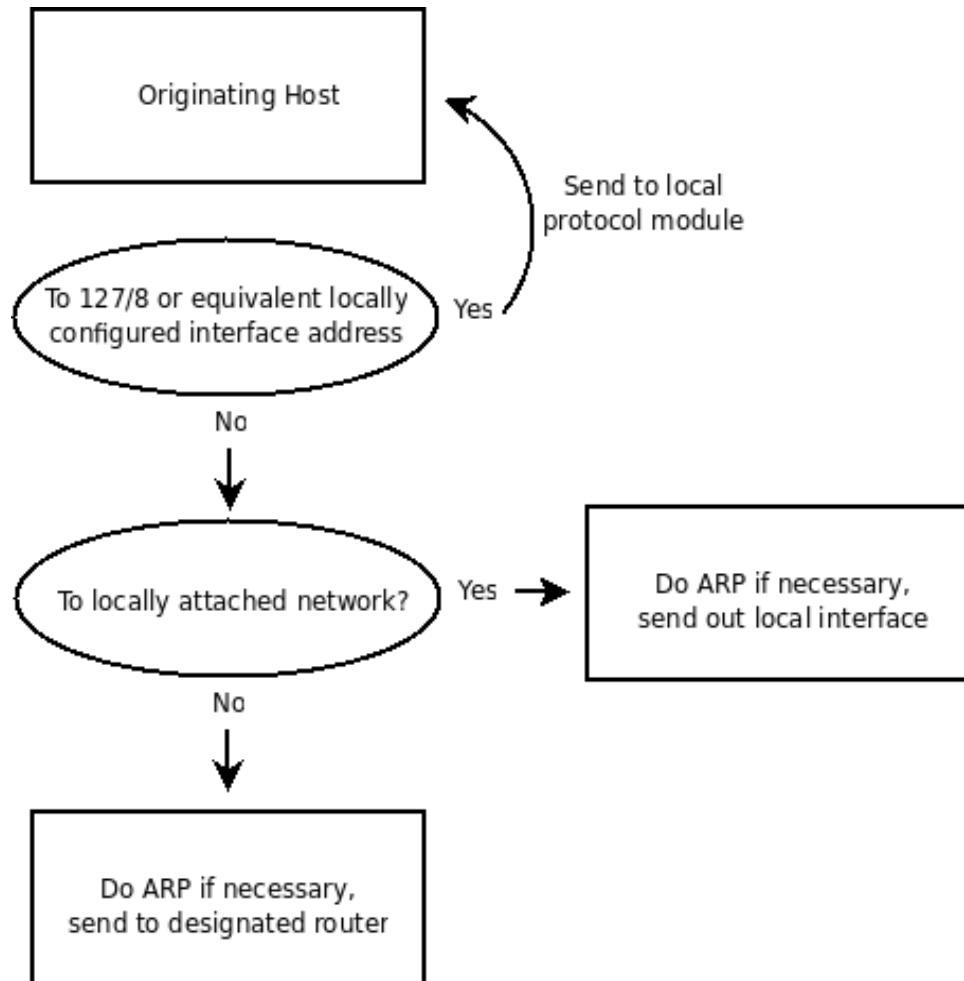
# OK, little more to it than that...

- Hosts have to learn the netmask and relay router
- This isn't so much a routing system issue
- Its in practice a bootstrap issue
- This is where DHCP, ARP, ICMP redirects, etc. come in

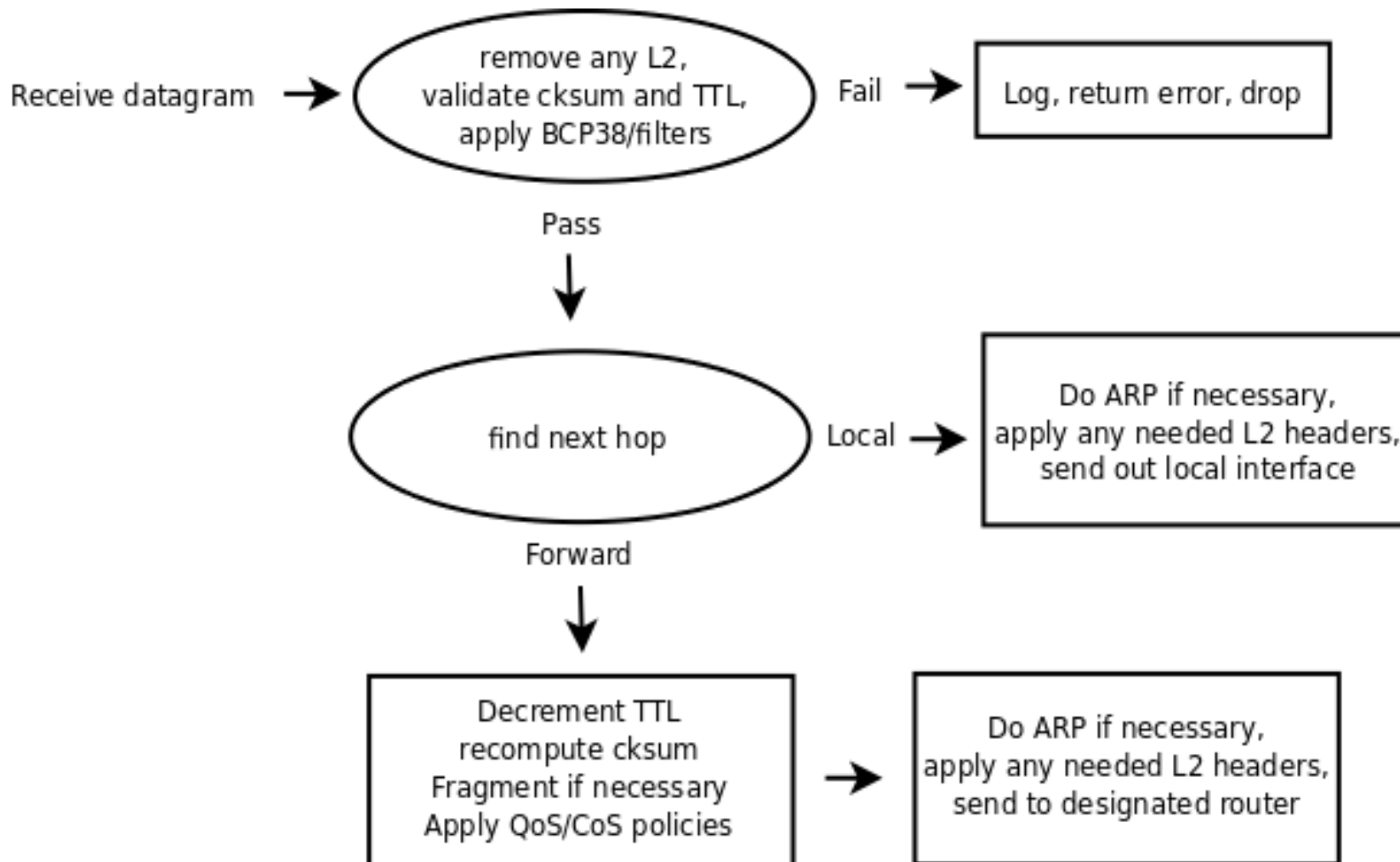
# IPv4 unicast routing

- All Internet hosts perform basic routing
  - for local net destinations, send to local net
  - for non-local nets, send to router
- Dedicated routers often used between networks
- Routing tables maintain next hop information
- Forwarding decision based on destination address
  - routers can use other info to influence decision
- Routers forward to next-hop if not locally attached

# Simplified routing decision tree



# Real routers work more like this



# Best match forwarding

- So the routing decision goes kind of like this:
  - Is this packet for me?
  - Is this packet for an attached interface?
  - What is the most specific network route I have?
    - Host (/32) route, /31, /30, /29, ... default (/0)?
    - Send to the best one
  - If no route, drop and return ICMP error to source

# Key IP field for routing: TTL

- More apt name today would be hop count
  - In fact, that is just what it is called in IPv6 now
- This field prevents packets looping forever
- Other uses are secondary to this
  - traceroute
  - Source OS fingerprint and distance detection
  - BGP peering hack (aka GTSM, RFC 3682)

# Key IP field for routing: Source Address

- Consists of both a...
  - host/interface identifier (usually unique) and
  - a network identifier (also usually unique)
- Combined, the saddr helps hosts and routers
  - get the packet to the correct network
  - and to the specific host on the correct network

# BGP Overview

- The routing protocol for connecting *domains*
- Besides the *network prefix* the path is the key component of a BGP route
- Autonomous system numbers (ASNs) define path
  - generally an ASN == domain
    - NOTE: this is not a reference to DNS!
- Even if you don't use it for actual Internet routing, it might be handy for other things (e.g Team Cymru bogon route server, IP addr to ASN mapping)

# IS-IS/OSPF Overview

- Widely used *intradomain* routing protocols
- *Link state* database of entire routed network built by all routers
- Each router can make an optimal forwarding decision, because it has a complete view of all the routers and their attached networks
- Relatively simple idea, but is a bit more complex to implement – e.g. database synchronization issues

# A real Internet BGP route entry

```
route-views.oregon-ix.net>sh ip bgp 68.22.187.0/24
BGP routing table entry for 68.22.187.0/24, version 543323
Paths: (34 available, best #7, table Default-IP-Routing-Table)
  Not advertised to any peer
  8075 2828 23028
    207.46.32.34 from 207.46.32.34 (207.46.32.34)
      Origin IGP, localpref 100, valid, external
  3333 3356 2828 23028
    193.0.0.56 from 193.0.0.56 (193.0.0.56)
      Origin IGP, localpref 100, valid, external
  4513 13789 3561 23028 23028 23028 23028
    209.10.12.125 from 209.10.12.125 (209.10.12.125)
      Origin IGP, metric 4103, localpref 100, valid, external
```

# An example routing table

```
route-views.oregon-ix.net>show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF
```

```
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
```

```
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
```

```
       E2 - OSPF external type 2, E - EGP i - IS-IS
```

```
       su - IS-IS summary, L1 - IS-IS level-1
```

```
       L2 - IS-IS level-2, ia - IS-IS inter area
```

```
       * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 128.223.51.1 to network 0.0.0.0
```

```
B       216.221.5.0/24 [20/489] via 208.51.134.254, 18:06:49
```

```
B       210.51.225.0/24 [20/0] via 12.0.1.63, 18:07:52
```

```
B       210.17.195.0/24 [20/0] via 216.218.252.164, 18:08:11
```

```
B       209.136.89.0/24 [20/0] via 216.218.252.164, 18:08:21
```

```
B       209.34.243.0/24 [20/0] via 157.130.10.233, 17:59:49
```

```
B       205.204.1.0/24 [20/0] via 157.130.10.233, 18:00:57
```

```
B       204.255.51.0/24 [20/0] via 157.130.10.233, 17:59:44
```

```
B       204.238.34.0/24 [20/0] via 157.130.10.233, 18:00:28
```

# Want router access?

- Telnet to route-views.routeviews.org
- Browse to <http://routerproxy.grnoc.iu.edu/>
- Go easy, don't ruin it for the rest of us please
  - Notwithstanding potential bugs or attacks, by default access it intended to be limited (sorry, no “enable”), but they can still be **very** helpful for remote analysis and troubleshooting

# You do have enable, kind of

- On Unix, Linux, Mac OS X
  - `netstat -arn`
- On Microsoft Windows
  - `route print`

# There is router security and there is route security

- Few serious network engineers use HTTP
  - “That's probably a good thing!” you say
- Many Cisco networks still use Telnet
  - This is where you security people go “WTF!?!?”
- Many networks have SNMPv1 write enabled
  - Then you go “OMFG!?!?”
- Almost nobody watches out for more specifics
  - “Specifics smurifics, whoop-dee \$#!&@”

# Au contraire

- Router security
  - Authentication, filtering, crypto... DONE!
  - Eh, no.
- Route security
  - This is the old, “my security, depends on your ability to do security” problem
  - Say you have and announce a /16
  - Someone announces /24's in that /16.
  - Uh-oh.

# FYI...

- Stay tuned for...
  - BGP
  - OSPF
  - Blackholes, data and routing plane security
  - The routing process
  - Peering
  - And much, much more
- After the mid-term exam... phew!