Using Routing and Tunnelling to Combat DoS Attacks

Adam Greenhalgh, Mark Handley, Felipe Huici
Dept. of Computer Science
University College London

http://nrg.cs.ucl.ac.uk/mjh/servernets.pdf

Background:

Using Addressing to Combat DoS Attacks

- In previous work, we suggested that many of unwanted modes of operation of the Internet could be prevented by simple changes to the addressing architecture.

  http://www.cs.ucl.ac.uk/staff/M.Handley/papers/dos-arch.pdf

- Unfortunately these changes would be hard to deploy in practice.
  - Needs IPv6, HIP, large-scale agreement on the solution.

Towards deployable solutions.

- To be deployable in the near term, a solution needs to satisfy the following criteria:
  - Feasible with IPv4.
  - Use off-the-shelf hardware.
  - No changes to most Internet hosts.
  - No changes to most Internet routers.
  - Use existing routing protocols.

Towards evolvable solutions

- It is important that in providing short-term solutions we don’t sacrifice the future evolution of the Internet.
- Anything that goes in the middle of the network should be:
  - Application independent.
  - Impose minimal dependencies on transport protocols.

Goals

- Defend servers against DoS attacks.
  - *Opt-in*. Servers have to choose to be defended.
- Shut down unwanted traffic *in the network* as close to the source of that traffic as possible.
  - Server decides certain traffic is unwanted.
  - Requests traffic is shut down.
  - Network filters traffic.

Only network filtering can defend against link-flooding attacks.

Architectural Overview

- Place control points in the network that are capable of performing IP-level filtering.
  - Cause unwanted traffic to our servers to traverse these control points.
  - Provide a signalling mechanism to allow the servers to request certain traffic is filtered.

Problem 1:

How to determine which control point can shut down certain traffic?

Problem 2:

How to ensure that only the recipient of unwanted traffic can request its filtering.

Revised Architectural Overview

- Place control points in the network.
- Cause all traffic to server subnets to traverse at least one control point.
  - Control points mark the traffic with their identity.
- Receivers can see which control points are on the path from sender.
  - Can request correct control point to install filter.

Constraints

- To provide a protocol-independent solution, we must primarily work at the IP layer.
- The main IP-layer tools available to us are:
  - Addressing
  - Routing
  - Encapsulaton

Using these tools...

Addressing

- To identify server subnets.

Routing

- To limit and control the paths to the server subnets.
- To direct traffic through control points near to the source of the traffic.

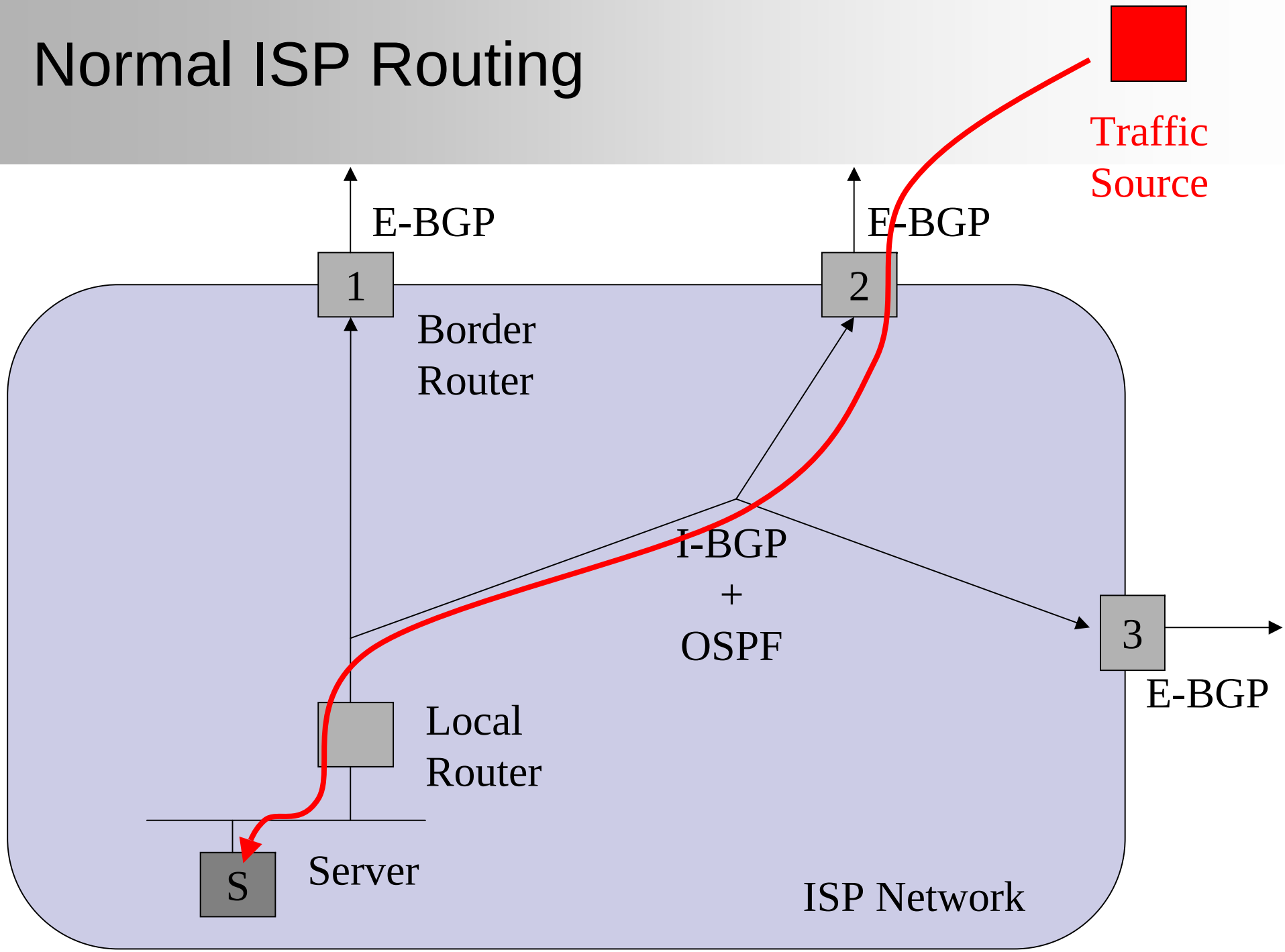
Encapsulation

- To record information about the control points traversed on the path from client to server.

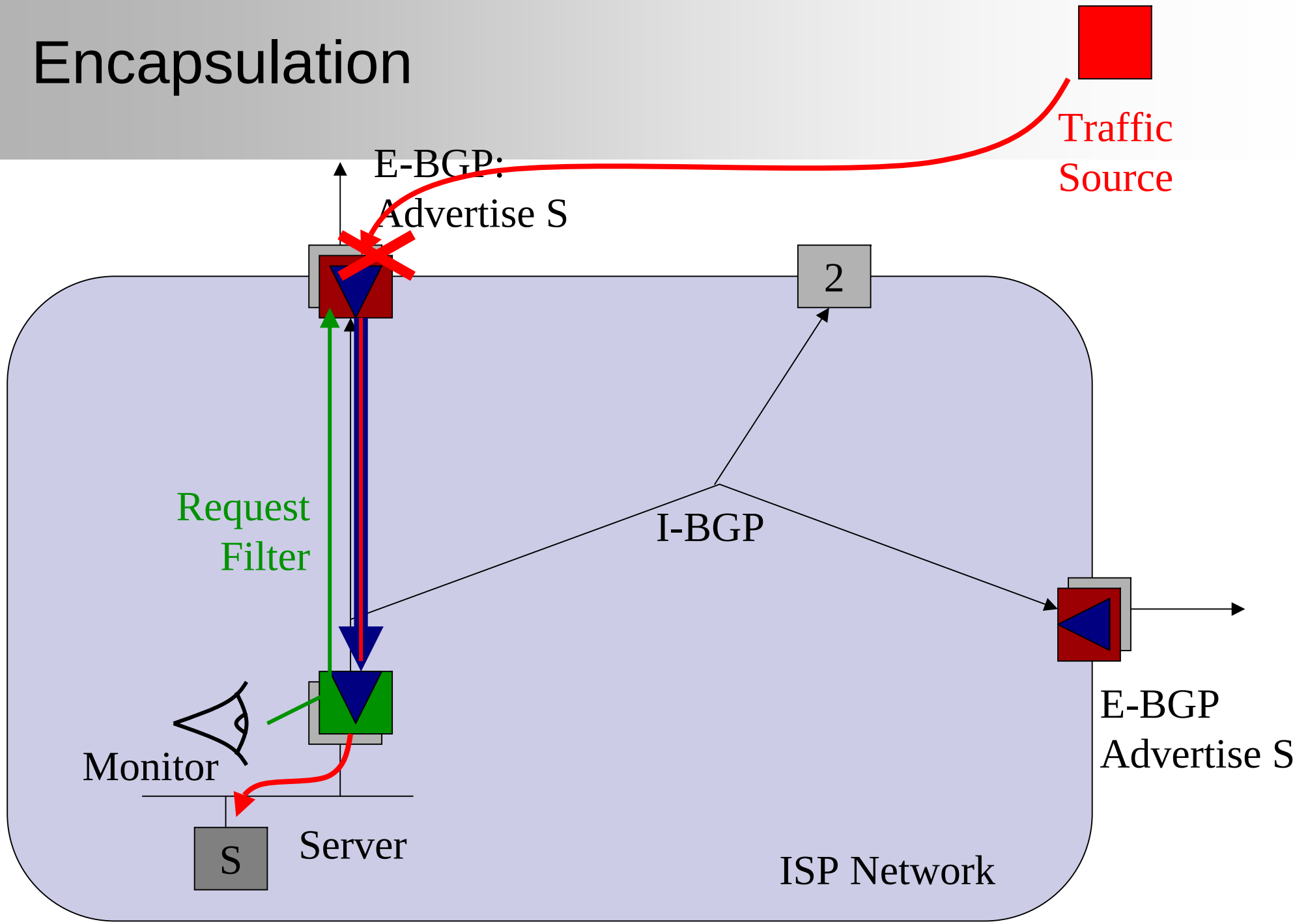
Incremental Deployment

- First we'll sketch out how servernets might be deployed in a single ISP.
  - Can only push back as far as ISP border.
  - Useful for large ISPs with many peering points, as attack has not yet fully converged.
- Next we'll explain how cooperating ISPs can deploy multi-ISP servernets.
  - Greater benefits as pushback can be much closer to attack source.

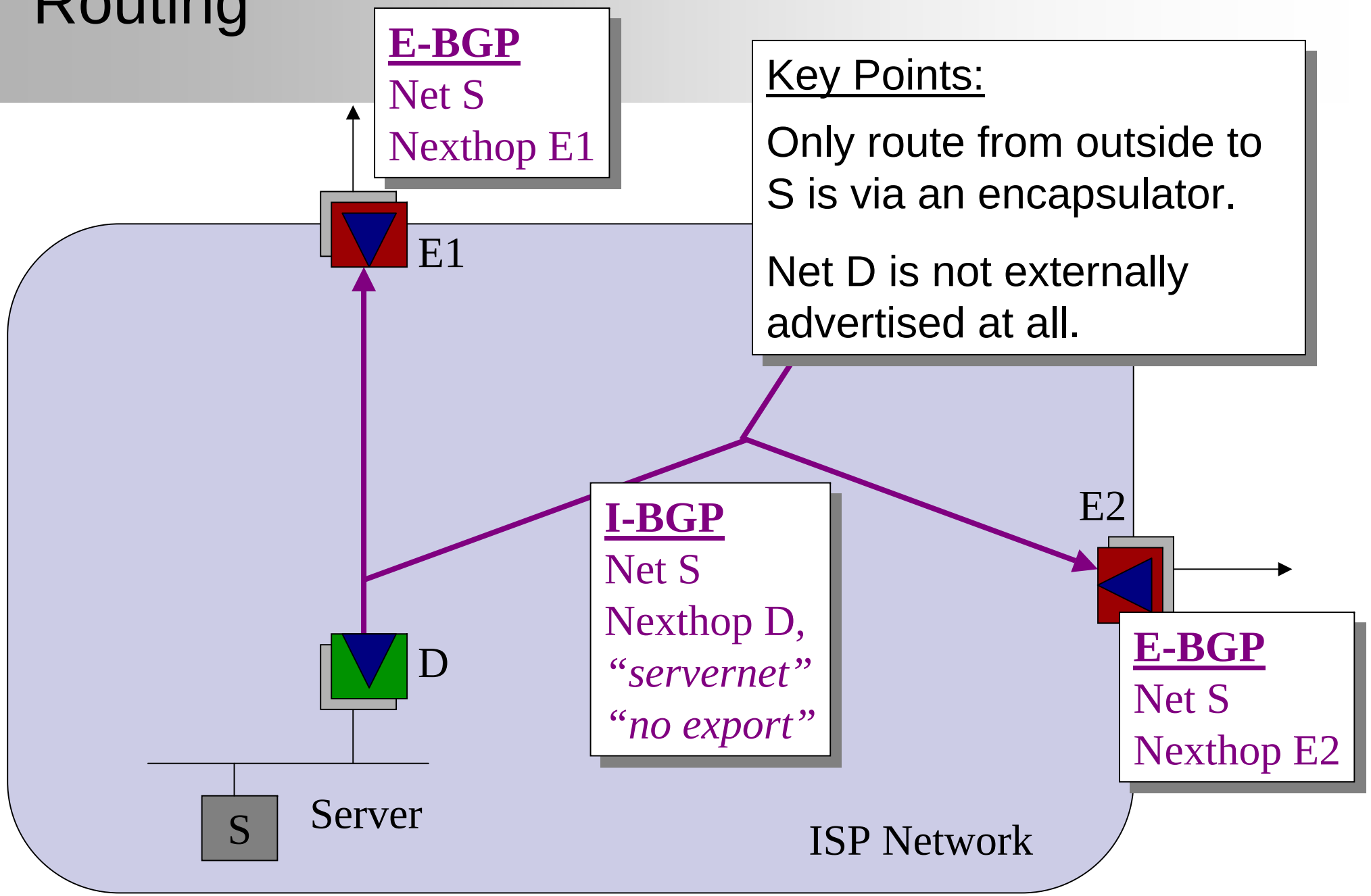
Normal ISP Routing



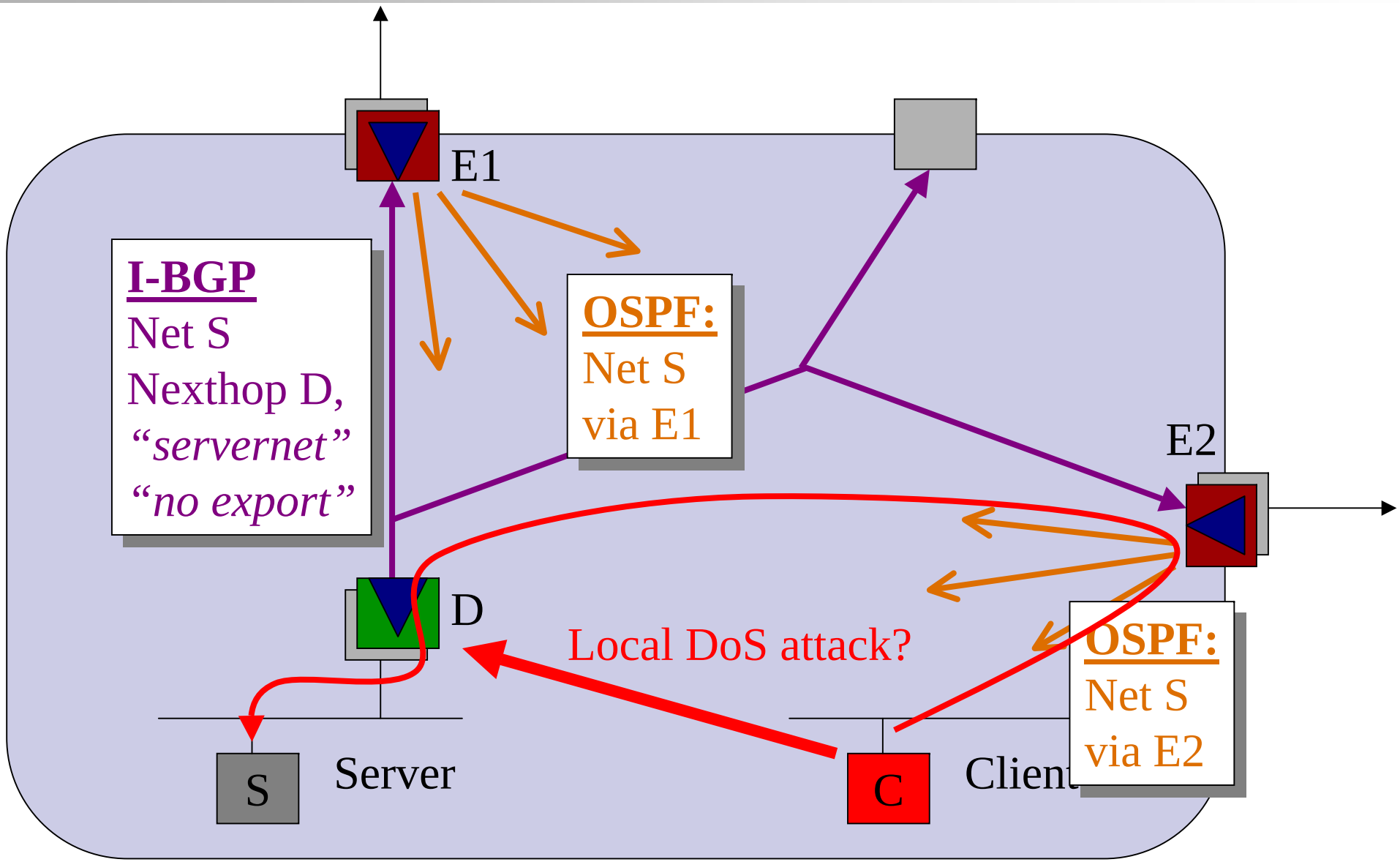
Encapsulation



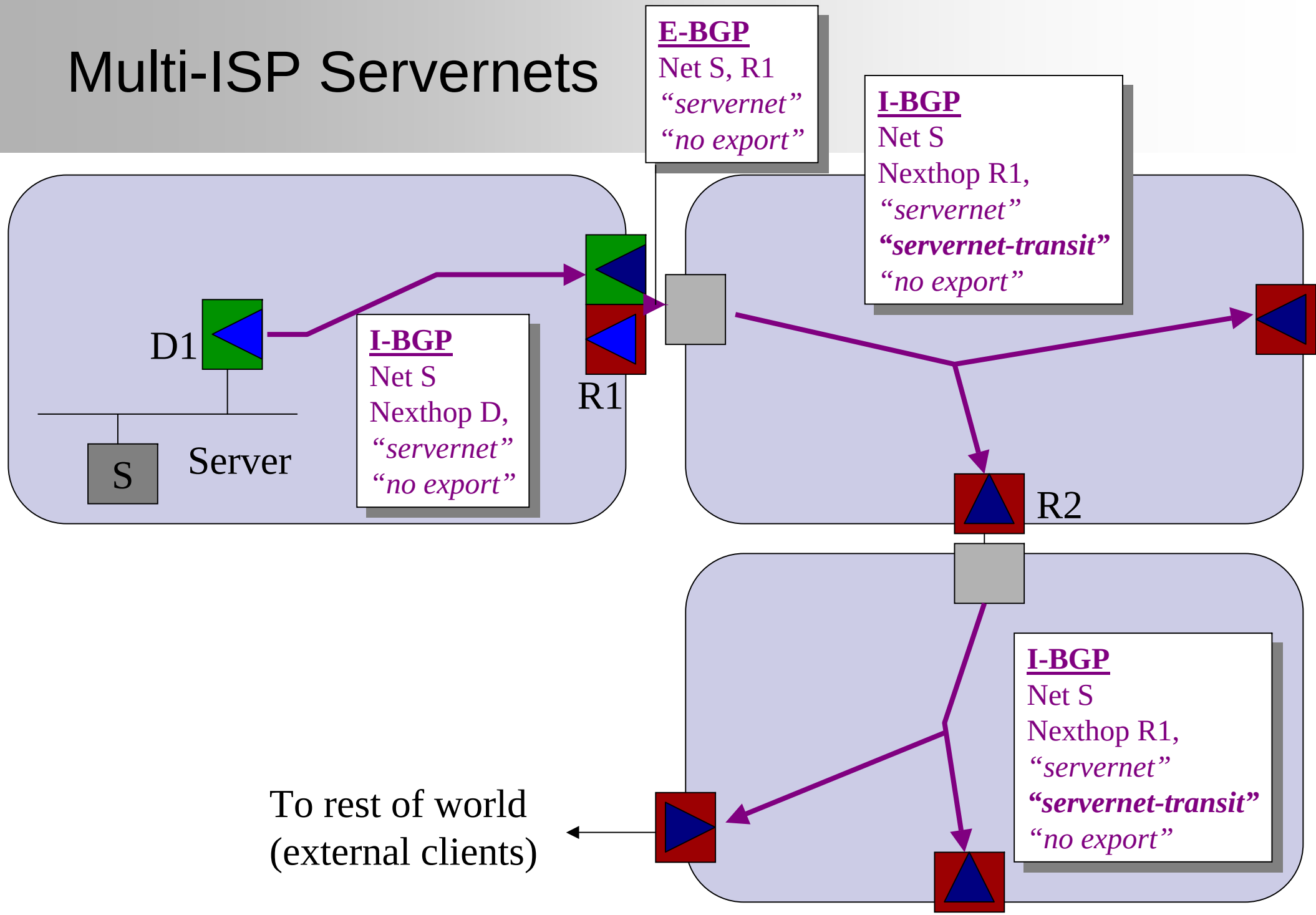
Routing


E-BGP
Net S
Nexthop E1
Key Points:
Only route from outside to S is via an encapsulator.
Net D is not externally advertised at all.
E1
I-BGP
Net S
Nexthop D,
"servernet"
"no export"
E2
D
E-BGP
Net S
Nexthop E2
S
Server
ISP Network

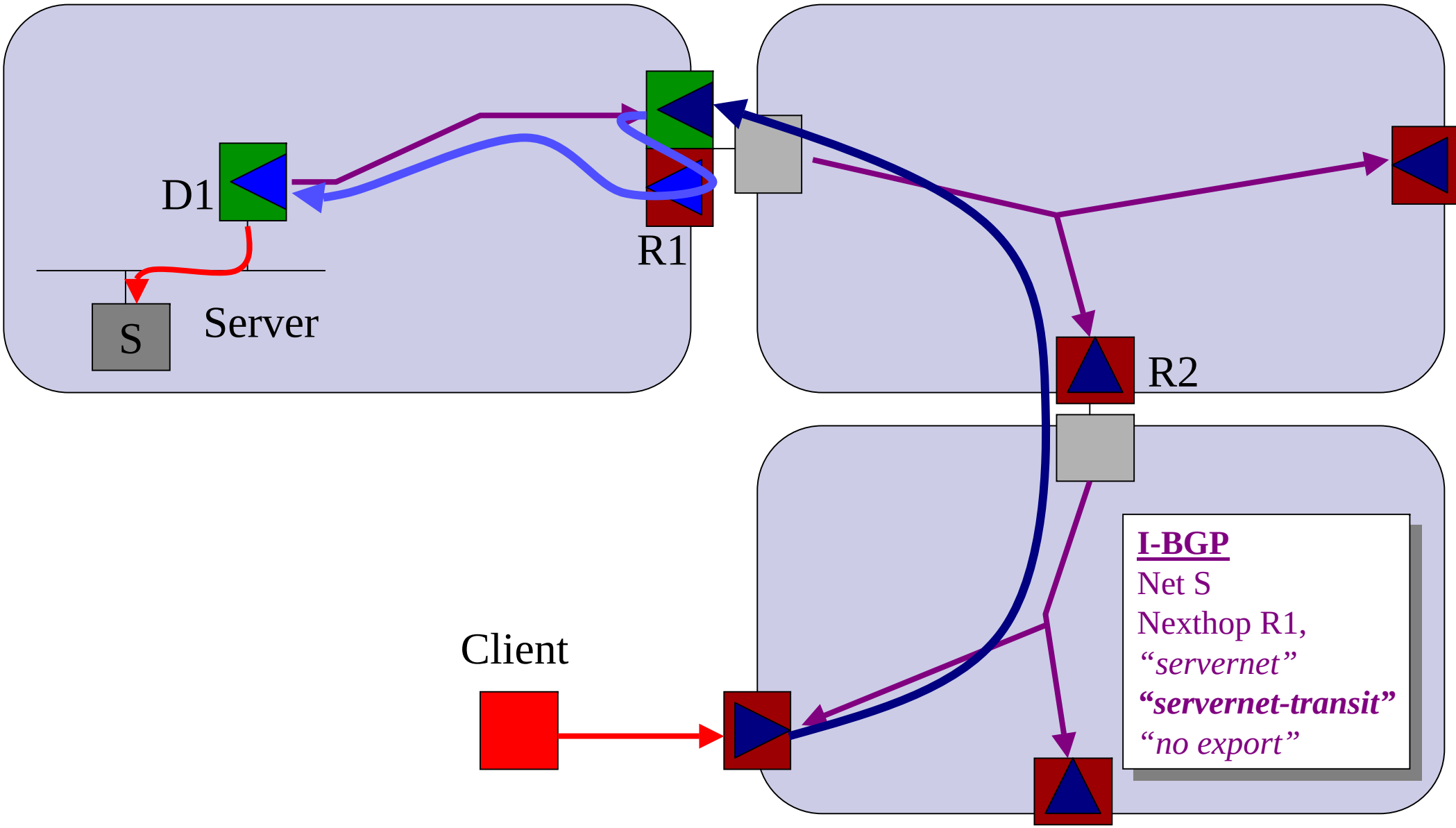
Routing for Internal Clients



Multi-ISP Servernets



Multi-ISP Servernets



Protection

- Provide defense against non-spoofed traffic for servers that opt-in.
  - Automatic mechanism reduces costs for ISP.
  - Lower collateral damage for ISP.

- Assumes a detection mechanism exists that can identify bad traffic sources.
- What about spoofed traffic?

Attack landscape

- Currently most DoS attacks are not spoofed.
  - No need to!
- Servernets change the landscape. Attackers will then need to:
  - Spoof source addresses.
  - Disguise their attack traffic to fly below the detection threshold.

Spoofing

- The existence of servernets would provide stronger motivation for deployment of ingress filtering.
  - Currently there's limited gain from doing so.

- Servernet encapsulators are a natural place to perform source address validation.
  - Only current ways to do this are hacks, but future extensions to protocol stack could provide simple address authentication.
  - Eg. ICMP nonce-exchange.
  - This is a longer-term solution.

Future work

- Implement and test the scheme in the lab.
  - Software implementation on fast PC hardware.
  - Goal is to encap/decap and firewall at 1Gb/s.
  - Already in progress (3 to 6 months).
- Deploy the scheme in the wild.
  - Industrial collaborators are most welcome.