Off by Default!

Hitesh Ballani, Yatin Chawathe, Sylvia Ratnasamy, Timothy Roscoe, Scott Shenker

HotNets-IV, 2005

Internet, then and now

Internet, circa 1975

- Trust in the ends ⇒ Universal reachability
- Routability implies reachability
  - “On” by default

Internet, circa 2005

- Less trust in the ends
  - *every* host is vulnerable to *any* other host(s)
- Firewalls/NATs
  - end-hosts are “Off”, the network is not
  - ad-hoc and not universal

Off by default!

Turn it “Off”

Reachability is “Off” by default

- Hosts turn “On” by explicitly telling the network

Turn it “Off”

Reachability is “Off” by default

- Hosts turn “On” by explicitly telling the network

Issues

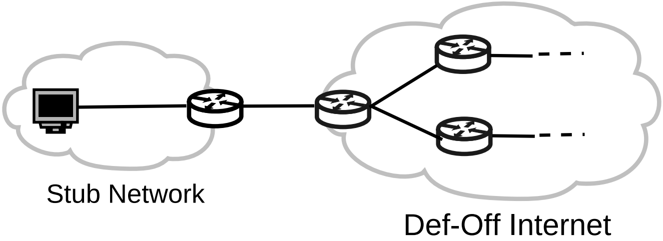
- What are the advantages?
- What are the assumptions?
- What are the incentives?
- . . .

Is it even worth a thought?

Design a Default-Off network

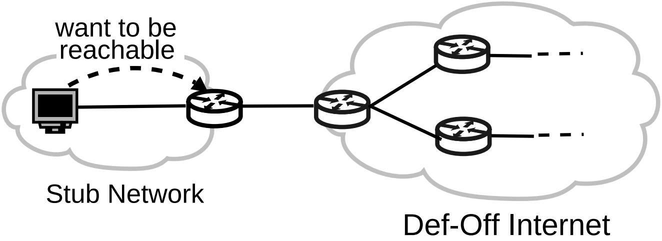
Evaluate its feasibility

Default-Off design



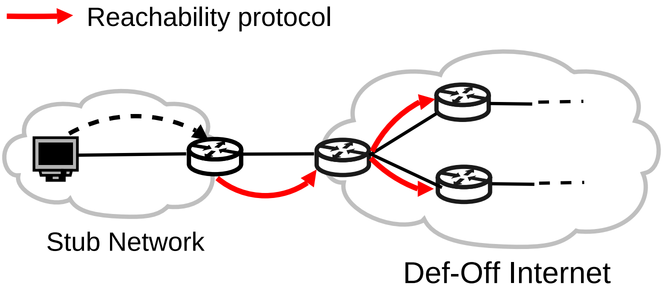
End-hosts are unreachable by default

Default-Off design



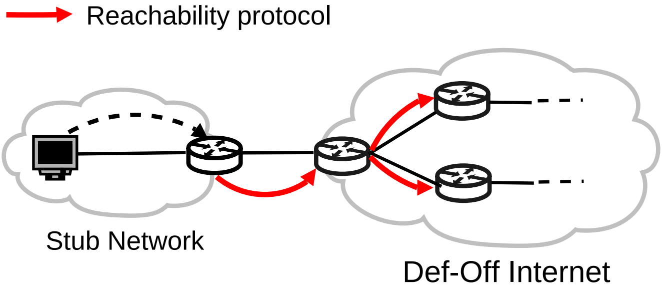
End-hosts signal their intent to turn "On"

Default-Off design



Reachability protocol propagates this intent into the network as *Reachability Advertisements*

Default-Off design

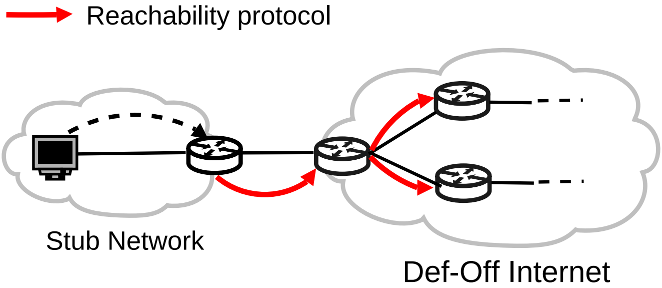


Naïve Approach (not feasible)

Routers maintain exact reachability state for all hosts

Instantaneous propagation of advertisements

Default-Off design



Challenges

Router State

Reachability dynamics

Reachability Protocol

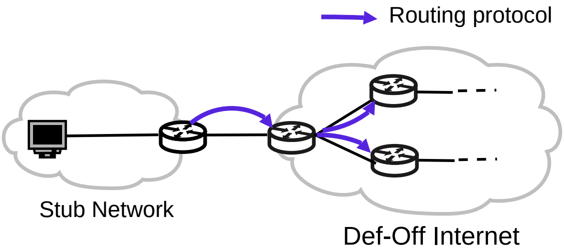
Reachability overlaid on Routing

- Inherit routing trust relationships
- Reachability events $\not\Rightarrow$ Route recalculation

Reachability Protocol

Reachability overlaid on Routing

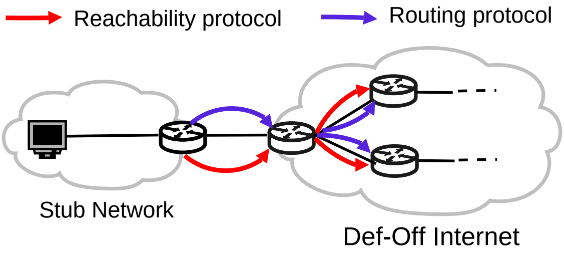
- Inherit routing trust relationships
- Reachability events $\not\Rightarrow$ Route recalculation



Reachability Protocol

Reachability overlaid on Routing

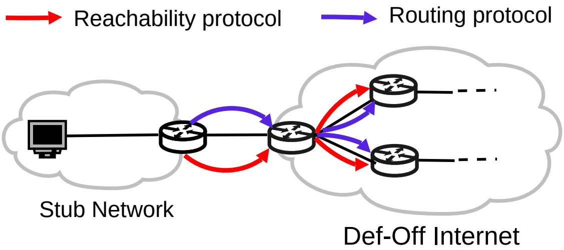
- Inherit routing trust relationships
- Reachability events $\not\Rightarrow$ Route recalculation



Reachability Protocol

Reachability overlaid on Routing

- Inherit routing trust relationships
- Reachability events $\not\Rightarrow$ Route recalculation



Periodic reachability exchanges between domains

- Load due to dynamics Vs Turn-“On” time

Reachability Advertisements

Flexibility : allow for evolution

Reachability Advertisements

Flexibility : allow for evolution

Who?   What?   When?   How much?

Reachability Advertisements

Flexibility : allow for evolution

Who? What? When? How much?

Reachability Advertisement

[prefix, length, RC ... , scope]

Reachability Advertisements

Flexibility : allow for evolution

Who? What? When? How much?

Reachability Advertisement

[prefix, length, RC ... , scope]

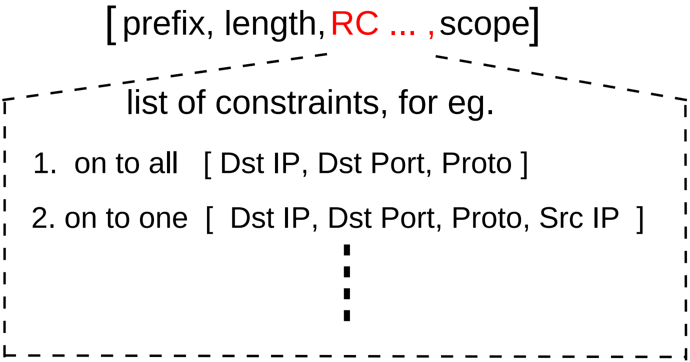
The host whose reachability this advertisement describes

Reachability Advertisements

Flexibility : allow for evolution

Who? What? When? How much?

Reachability Advertisement



[prefix, length, RC ... , scope]

list of constraints, for eg.

1. on to all [Dst IP, Dst Port, Proto]

2. on to one [Dst IP, Dst Port, Proto, Src IP]

⋮

Reachability Advertisements

Flexibility : allow for evolution

Who? What? When? How much?

Reachability Advertisement

[prefix, length, RC ... , scope]

Avoids needless propagation of state

For eg. Limit advertisement in terms of AS

Hops, Set of AS'es, ...

Router State : “Off” hosts

“Off” hosts do not incur state

Router State : “Off” hosts

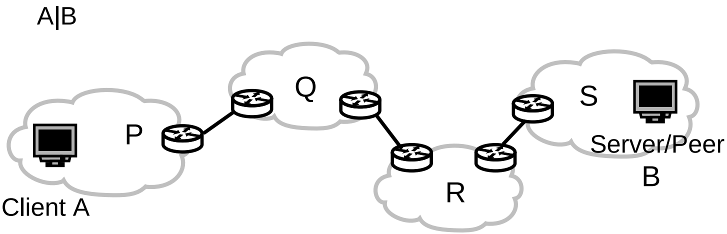
“Off” hosts do not incur state

- Clients are “Off” [Handley FDNA’04]
- “Off” hosts accessed using path-based addresses (address gives path back to the “Off” host)

Router State : “Off” hosts

“Off” hosts do not incur state

- Clients are “Off” [Handley FDNA’04]
- “Off” hosts accessed using path-based addresses (address gives path back to the “Off” host)

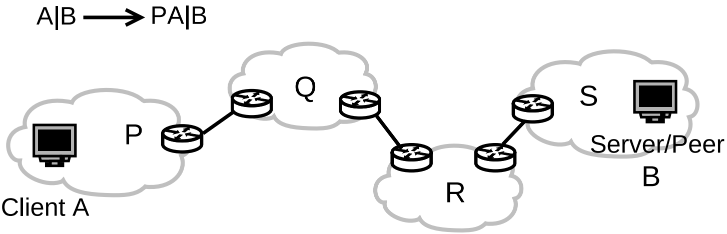


“Off” host A wants to communicate with “On” host B (A|B)

Router State : "Off" hosts

"Off" hosts do not incur state

- Clients are "Off" [Handley FDNA'04]
- "Off" hosts accessed using path-based addresses (address gives path back to the "Off" host)

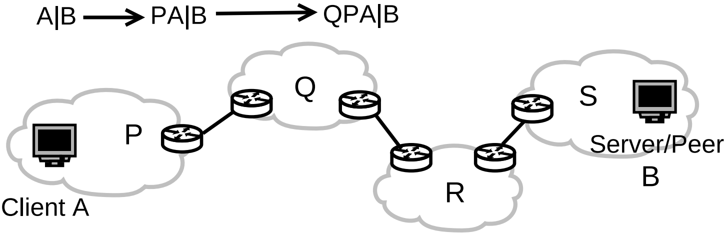


Host B is "On" so domain P forwards it; but also adds itself into the source (PA)

Router State : “Off” hosts

“Off” hosts do not incur state

- Clients are “Off” [Handley FDNA’04]
- “Off” hosts accessed using path-based addresses (address gives path back to the “Off” host)

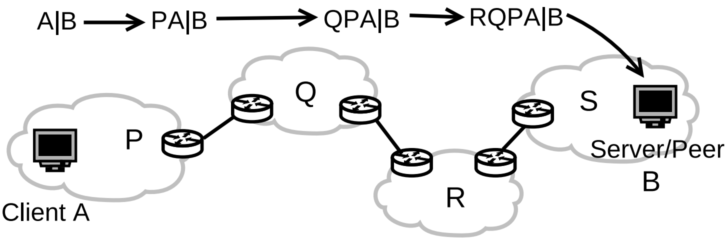


At the egress of domain Q, Q is added to the source (QPA)

Router State : “Off” hosts

“Off” hosts do not incur state

- Clients are “Off” [Handley FDNA’04]
- “Off” hosts accessed using path-based addresses (address gives path back to the “Off” host)

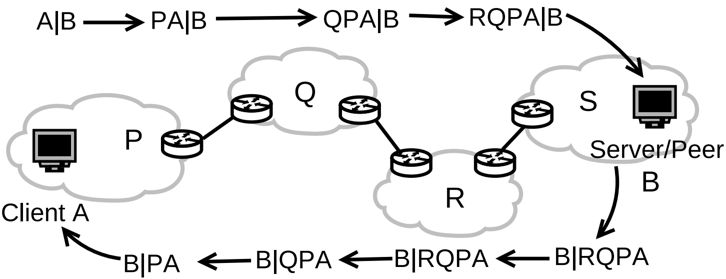


Host B can use the path (RQPA) to get to “Off” host A

Router State : “Off” hosts

“Off” hosts do not incur state

- Clients are “Off” [Handley FDNA’04]
- “Off” hosts accessed using path-based addresses (address gives path back to the “Off” host)

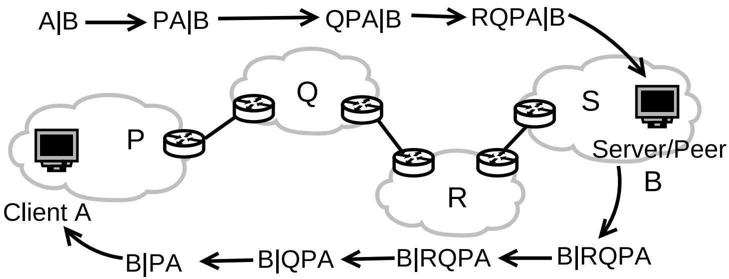


Destination field is stripped off, source field accumulates the path

Router State : "Off" hosts

"Off" hosts do not incur state

- Clients are "Off" [Handley FDNA'04]
- "Off" hosts accessed using path-based addresses (address gives path back to the "Off" host)



Issues and advantages associated with path-based addresses

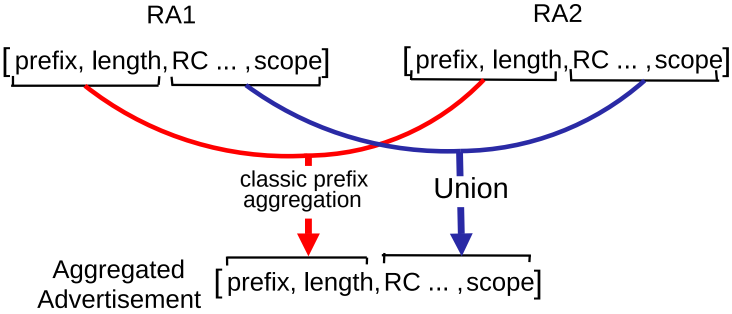
Router State : “On” hosts

Routers don’t keep exact reachability state

Router State : “On” hosts

Routers don’t keep exact reachability state

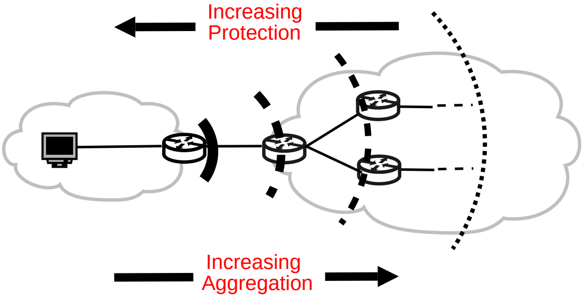
- Aggregation according to router memory


RA1
[prefix, length, RC ... , scope]
RA2
[prefix, length, RC ... , scope]
classic prefix aggregation
Union
Aggregated Advertisement
[prefix, length, RC ... , scope]

Router State : “On” hosts

Routers don’t keep exact reachability state

- Aggregation according to router memory
- Introduces false-positives
- Default-Off offers best-effort protection to “Off” hosts



How effective is Default-Off at limiting unwanted traffic?

Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

- H - hosts per prefix that are “On”
- T - amount of router memory available

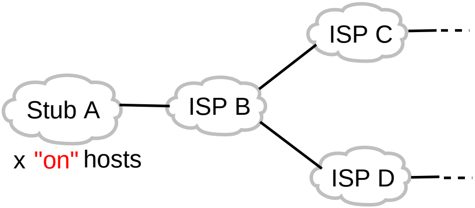
Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

- H - hosts per prefix that are "On"
- T - amount of router memory available



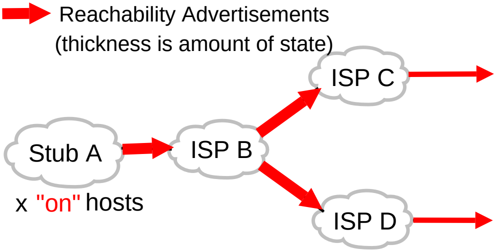
Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

- H - hosts per prefix that are "On"
- T - amount of router memory available



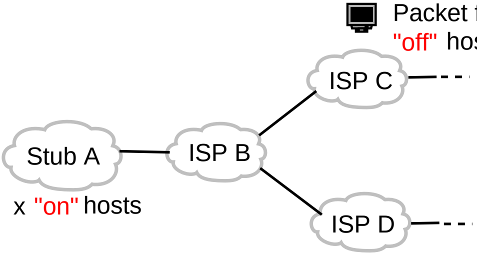
Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

- H - hosts per prefix that are "On"
- T - amount of router memory available



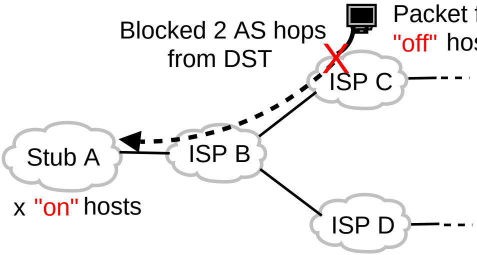
Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

- H - hosts per prefix that are "On"
- T - amount of router memory available



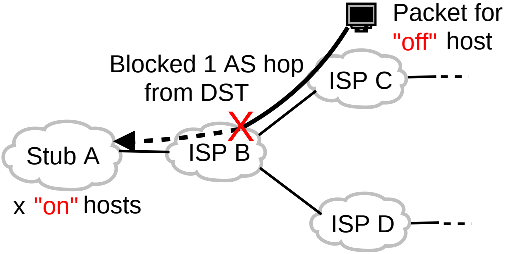
Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

- H - hosts per prefix that are "On"
- T - amount of router memory available



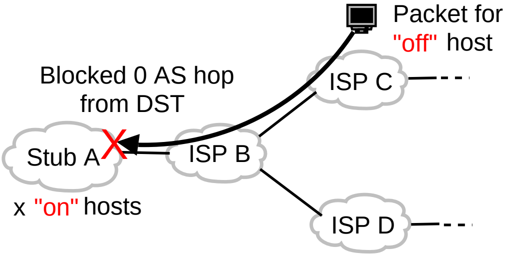
Feasibility : Router State

Simulated Default-Off operation

- AS-level internet topology [Subramanian '05]
- 200,000 routable prefixes [Route-Views '05]

Parameters of interest

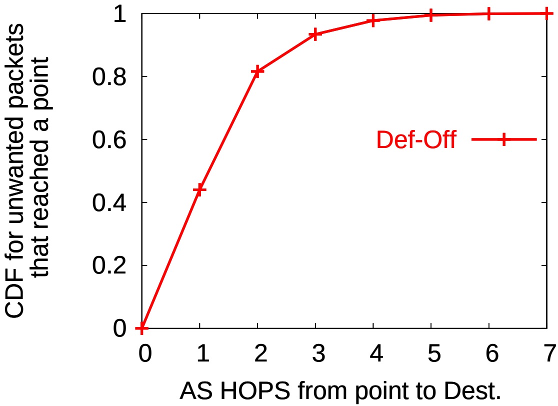
- H - hosts per prefix that are "On"
- T - amount of router memory available



Feasibility : Router State

H : 45 “On” hosts per prefix [Surveys; Karagiannis ’04]

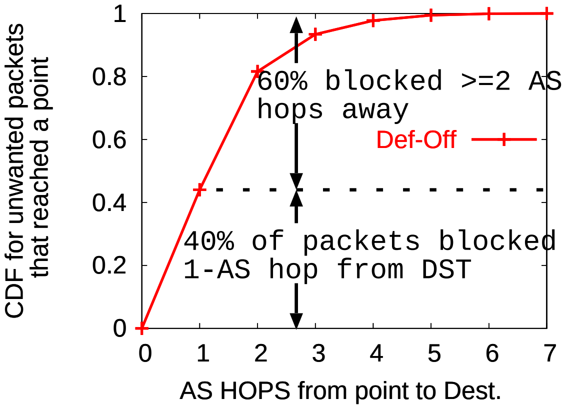
T : 7 MB per line card [Surveys; Keshav ’98]



Feasibility : Router State

H : 45 "On" hosts per prefix [Surveys; Karagiannis '04]

T : 7 MB per line card [Surveys; Keshav '98]



∼60% packets blocked ≥2 AS-hops away from DST

Can routers handle the dynamics of hosts turning "Off" / "On"?

Can routers handle the dynamics of hosts turning “Off”/“On”?

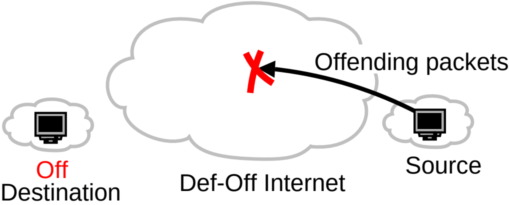
Load due to dynamics Vs Turn-“On” time
controlled using the exchange period

Can routers handle the dynamics of hosts turning "Off" / "On"?

Load due to dynamics Vs Turn-"On" time

controlled using the exchange period

Quality of protection Vs Load due to dynamics

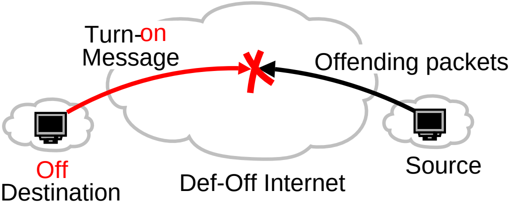


Can routers handle the dynamics of hosts turning "Off" / "On"?

Load due to dynamics Vs Turn-"On" time

controlled using the exchange period

Quality of protection Vs Load due to dynamics



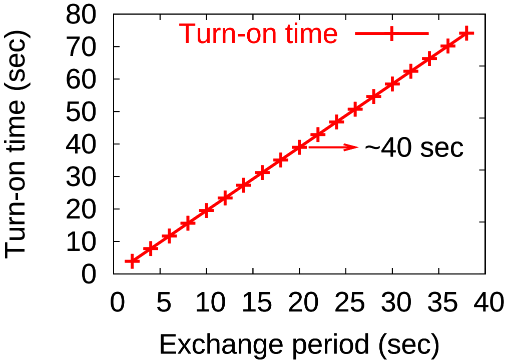
Knob

Router Memory

Feasibility : Reachability dynamics

H : 45 “On” hosts per prefix

T : 7 MB per line card

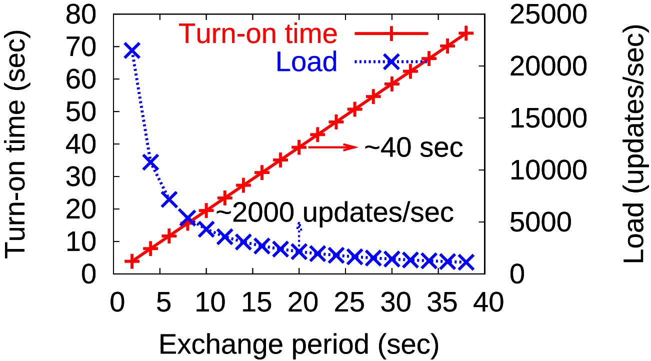


Exchange Period = 20 sec ⇒ Turn-on time ≈40 sec

Feasibility : Reachability dynamics

H : 45 "On" hosts per prefix

T : 7 MB per line card

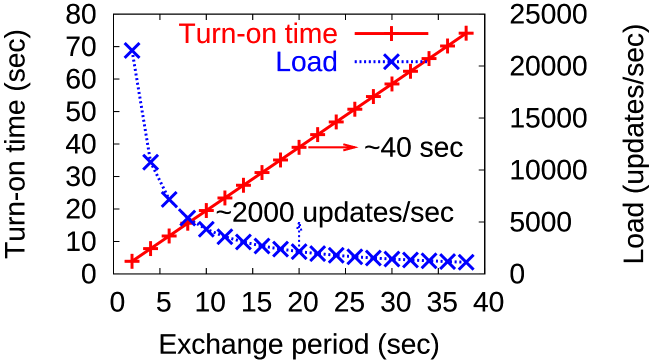


Exchange Period = 20 sec ⇒ Load ≈ 2000 updates/sec

Feasibility : Reachability dynamics

H : 45 "On" hosts per prefix

T : 7 MB per line card



Actual updates per second << 2000 updates/sec

“Take Home Message”

First-cut analysis shows that Default-Off might be feasible!

Issues

Advantages

[Handley FDNA'04]

Incentives

Existing ISP solutions

Usage

decision to switch on

Richness of reachability protocol

Stable (and secure) indentifiers for end-hosts, applications etc.

Issues

Advantages

[Handley FDNA'04]

Incentives

Existing ISP solutions

Usage

decision to switch on

Richness of reachability protocol

Stable (and secure) indentifiers for end-hosts, applications etc.

Issues

Advantages

[Handley FDNA'04]

Incentives

Existing ISP solutions

Usage

decision to switch on

Richness of reachability protocol

Stable (and secure) indentifiers for end-hosts, applications etc.

Issues

Advantages

[Handley FDNA'04]

Incentives

Existing ISP solutions

Usage

decision to switch on

Richness of reachability protocol

Stable (and secure) indentifiers for end-hosts, applications etc.

Issues

Advantages

[Handley FDNA'04]

Incentives

Existing ISP solutions

Usage

decision to switch on

Richness of reachability protocol

Stable (and secure) indentifiers for end-hosts, applications etc.

Issues

Advantages

[Handley FDNA'04]

Incentives

Existing ISP solutions

Usage

decision to switch on

Richness of reachability protocol

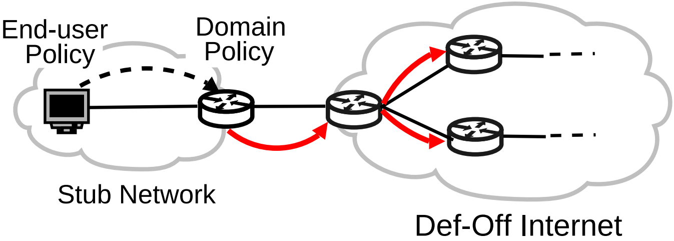
Stable (and secure) indentifiers for end-hosts, applications etc.

. . . should all this be pushed into the network?

Backup slides

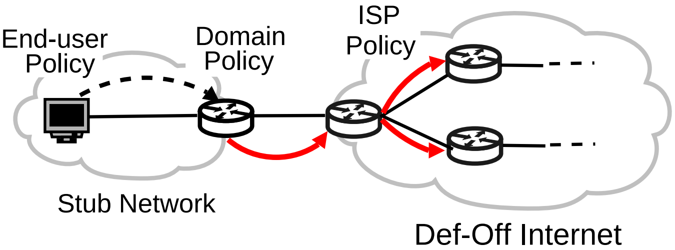
Conducive for policy enforcement

- User policy (administrator)
- Organization policy



Conducive for policy enforcement

- User policy (administrator)
- Organization policy



Threat Model

Compromise attacks

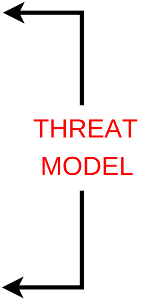
- Scanning worms
- Other worms (human activity based)
- Viruses, Spy-ware

Resource exhaustion attacks

- Flooding (Bandwidth/Processing)
- Single packet attacks

And others

- Spam, Phishing, . . .



THREAT MODEL

Reachability Protocol : the bigger picture

- Design space for access-control based solutions

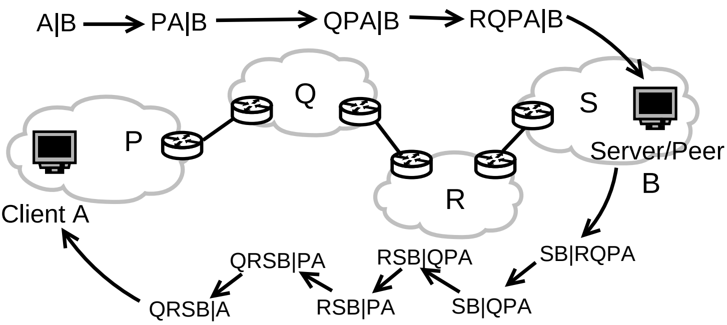
	at Ends	in Network
Proactive	Firewalls	Mayday, i3, SOS
Reactive	Reactive Firewalls	Pushback, AITF

- Reachability protocol in a Default-Off network
  - Encompasses several such proposals
  - Intrinsically less trusting network
- Feasibility check for the extreme design point
  - Caveat - Do not claim sufficiency or optimality

Actual use of path-based addresses

“Off” hosts do not incur state

- Clients are “Off” [Handley FDNA’04]
- “Off” hosts accessed using path-based addresses


A|B
PA|B
QPA|B
RQPA|B
Q
S
P
Server/Peer
B
R
Client A
QRSB|PA
RSB|QPA
SB|RQPA
QRSB|A
RSB|PA
SB|QPA