# Domain name-based interface selection

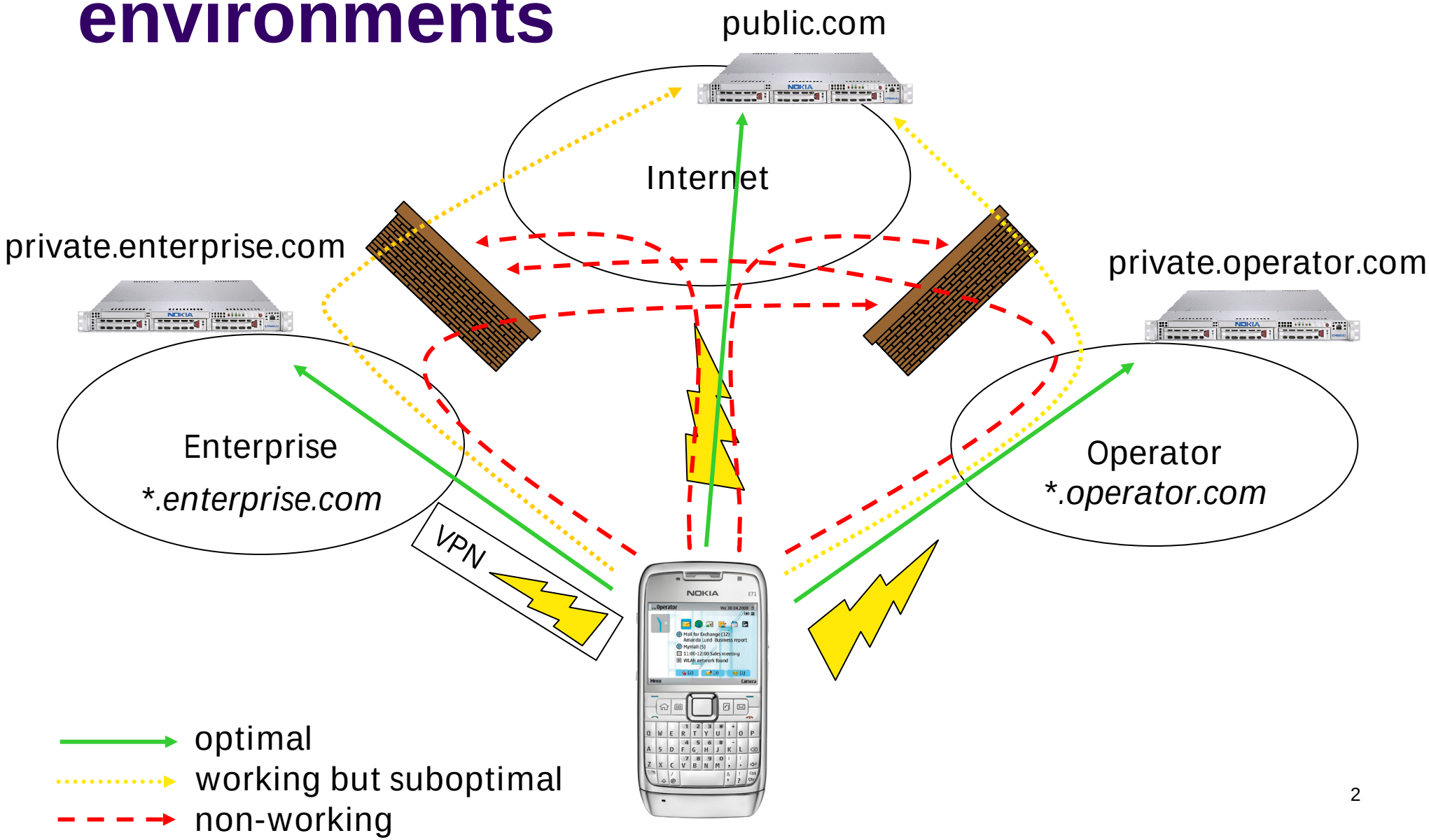
**draft-savolainen-6man-fqdn-based-if-selection**

Teemu Savolainen (Nokia)

6man WG meeting @ IETF#73

17-November-2008

# Network selection in multi-homed environments



# Perceived problems

- IP address based selection needs IP addresses
  - Work is ongoing to improve IPv6 address selection, but for IPv4 similar work is not ongoing (not for this WG to worry about)
- IP addresses are resolved from FQDNs with DNS, but all DNS servers do not have the same information:
  - In split horizon DNS cases some networks, e.g. enterprise, have internal names in use that cannot be resolved elsewhere
- Also all interfaces are not performance-wise equal
  - Connectivity to different destinations may be performance- and cost-wise better via different interfaces
- Existing solutions are not good enough
  - E.g. using just single network interface at a time, (parallel) trial and error, user involvement in network selection

# Proposed solution approach

- In addition to the work already ongoing for improving IPv6 address selection mechanisms

1. Let the network interfaces advertise to hosts what private domain names can be resolved and/or what special services can be connected to via them
   - Also to indicate that a network interface is particularly good for accessing certain destinations (e.g. “*.operator.com”), even if some other network interfaces might also, suboptimally, work
2. Host to pick the network interface that best matches the FQDN host is connecting to
   - I.e. to choose a network interface with “*.operator.com” if connection is requested for “private.operator.com”

# Proposed technical solution for DNS suffix information distribution

- Provide hosts the required DNS suffix information via existing DHCP options
  - DHCPv6 Domain Search List Option number 24, RFC3646
  - DHCPv4 Domain Search Option number 119, RFC3397
- Or design a new DHCP option for this purpose
  - Which possibly would enable more advanced functionalities

# Choosing currently open or closed network interface

- When choosing a network interface to use, a host can choose between currently open network interfaces

  - and/or -

- the host may have stored DNS suffix information into memory, in which case it can consider selecting currently closed, but otherwise available, network interface and opening that on-demand

# Reverse DNS lookup

- For connection requests for IP addresses, a host can
  - use updated IP address selection algorithms and possibly dynamically distributed policies

  - and/or -

  - consult DNS cache for FQDN matching the IP (probably recently resolved), and based on the FQDN pick the network interface having matching DNS suffix
    - Even more useful if dynamic IP address selection policies are not available

# Backwards compatibility

- This proposal allows unmodified hosts and networks to work as currently
- But modified networks can instruct modified and multi-homed hosts for better performance
- If existing DHCP options are used, a network must take into account DNS resolvers using the DNS suffixes also for the original purpose..
  - So only DNS suffixes really belonging to a network should be advertised

# Security implications

- DoS by deliberately advertising target DNS suffixes on wrong interfaces – e.g. “enterprise.com” on unmanaged network
- Risk can be mitigated by prioritizing learned DNS suffixes based on trust level of network interfaces
  - VPN network interfaces trusted over
  - Operator network interfaces trusted over
  - Unmanaged network interfaces

# Comments and next steps

- Do you agree the problem exist?
- Is the proposed solution path feasible?
- Other comments?