Electronics and Computer Science
University of Southampton

CM214-COMP2008
Data Communications and Networks

Network Level Protocols

Karl R. Wilcox
krw@ecs.soton.ac.uk

Objectives

- To consider protocols used in the operation and management of the network itself
  - Naming services
  - Inter-Network Connections

- (Peterson & Davie, Sections 8.4, 9.1)

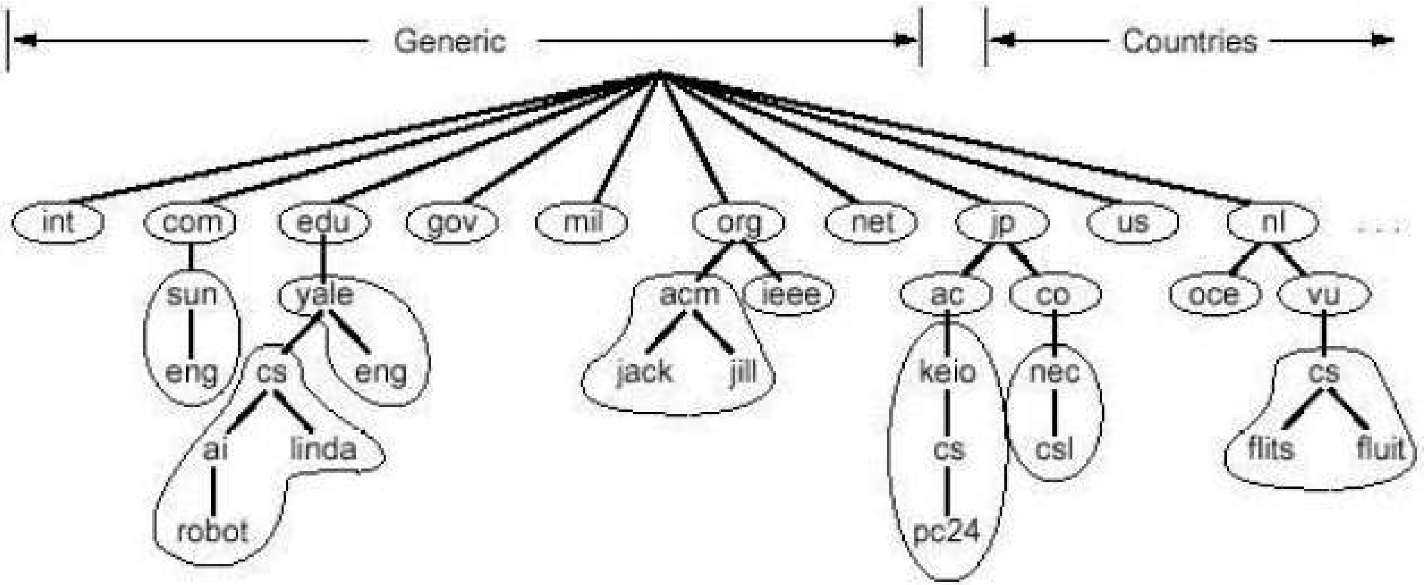
Naming Services

- Naming services provide a layer of abstraction (indirection) in naming “things”
  - DNS: maps IP to readable host names
  - NMB: same for NETBIOS networks
  - LDAP: user and network resources to readable names
  - CORBA INS: distributed objects to names
  - JNDI: Java API for all of the above

Namespaces

- The set of all possible, valid names for a particular naming service
  - May “embed” other namespaces e.g. mail
- Flat namespace e.g. Windows CLSIDs
  - Very large, choose randomly & hope(!)
- Hierarchical e.g. DNS
  - Breakdown into sub-sections

The Domain Name System



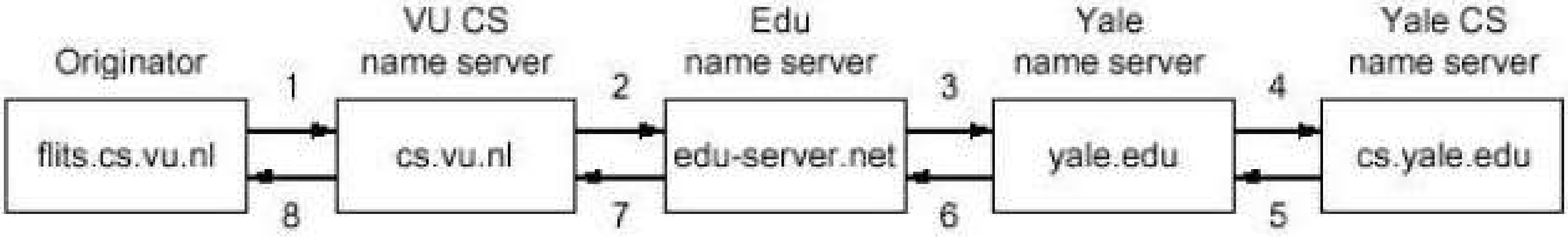
- Divided into zones
  - Authoritative primary nameserver
  - Usually also secondary nameserver

DNS Name Resolution

- Each name server is responsible for:
  - Mapping IP address to names in own domain
  - Forwarding resolution requests to “somebody else”
  - Accepting requests from (some) other name servers
  - Caching resolved names

DNS Resolution Example

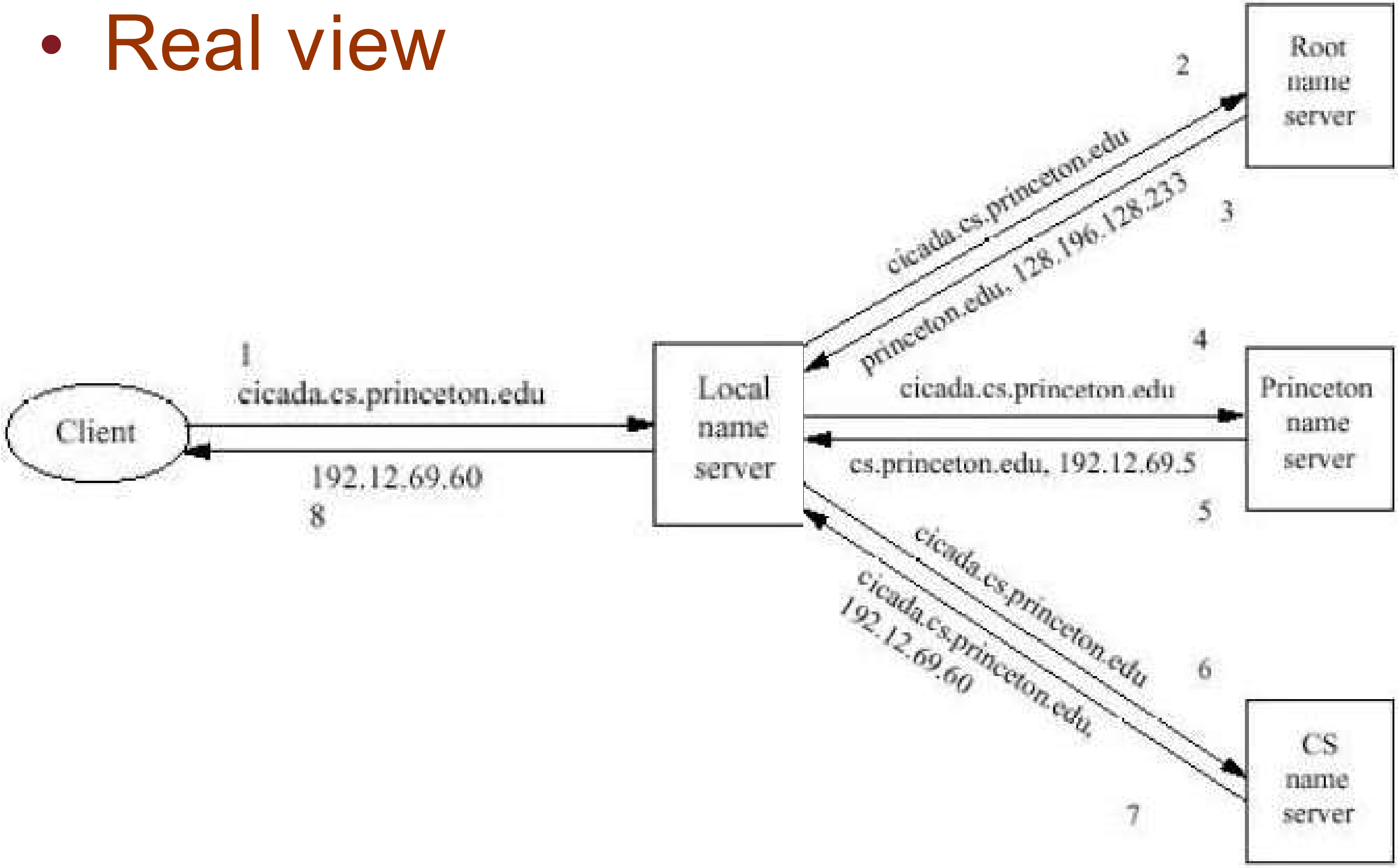
- Logical view



- Analogy – finding a phone number by phoning someone you know and asking them!

DNS Resolution Example

- Real view



DNS Records

DOMAIN-NAME

TIME-TO-LIVE

CLASS

TYPE

VALUE

Types are:

SOA - Start of Authority

A - IP Address

MX - Mail Exchange

NS - Name server

CNAME - Canonical name

PTR - Pointer (Alias)

HINFO - Host Description

```
$TTL 86400
@ IN SOA ns0.ecs.soton.ac.uk
hostmaster.ecs.soton.ac.uk (
20010501.1358 ; time in GMT
7200 ; Refresh time
3600 ; Retry time
604800 ; Expire time
3600 ) ; minimum TTL
ecs.soton.ac.uk IN MX 5 hawk
gatekeeper IN A 152.78.175.8
hawk IN A 152.78.69.21
thrush IN A 152.78.69.29
; + all other internal hosts
```

Inter-Network Connections

- So far, we have assumed inter-networking is open and transparent
  - Not usually the case
- Some level of control is desirable over the form and content of the connection
  - Firewalls
  - Proxies
  - Network Address Translation

Firewalls

- Protect internal network from insecure external network
  - Can be software (e.g. Windows XP)
  - Or separate host with two network interfaces, internal + external
  - Or special purpose router

Firewall Actions

- IP packet filtering
  - Rules based on IP address & port
    - E.g. inbound access to web(80), mail(25) etc.
    - How Windows XP firewall works
- Stateful filters
  - Maintain knowledge per connection
    - Can spot IP spoofing attacks

Firewall Problems

- TCP headers only in first fragment of each connection
- Internal IP addresses and other information visible to outside world
  - Monitor HTTP requests (especially PUT with user IDs)
  - Gives idea of network topology

Firewall Limitations

- Do **NOT** protect against
  - Forged e-mail addresses
  - Redirected web pages
  - Trojans, viruses and other application level vulnerabilities
  - Users installing modems on their PCs
  - Wireless network “leakage”

Firewall Setup

- Firewalls need to be set up
  - They are not “off-the-shelf” products
- The set up needs to match the needs of the organisation
  - Required inbound and outbound connections
  - Needs to be kept up to date

Network Address Translation

- Addition to a firewall or router
- Allows firewall to:
  - Hide internal IP addresses
  - Map multiple internal addresses to a single internet registered address
- NAT is a “fundamental proxy”
  - Works at IP level, uses TCP port number to track packet destinations

Other Proxies

- Unlike NAT, most proxies work at application level
  - E.g. HTTP proxy server
  - Makes requests on behalf of all clients
- Need one proxy for each application
- May be transparent (captures packets at firewall / router)
- May need explicit set up

Virtual Private Networks

- Also known as encrypted tunnels
- Links two networks across an insecure network (e.g. the internet)
  - One network may be a “dial-in” laptop
- Encapsulates “internal” IP packets inside encrypted “public” packets
- At IP level, therefore application independent

Summary

- DNS – maps names to resources
- Firewalls – filter packets between networks
- NATs – share IP addresses
- Proxies – run application protocols on behalf of clients
- VPNs – secure IP level connection over insecure network