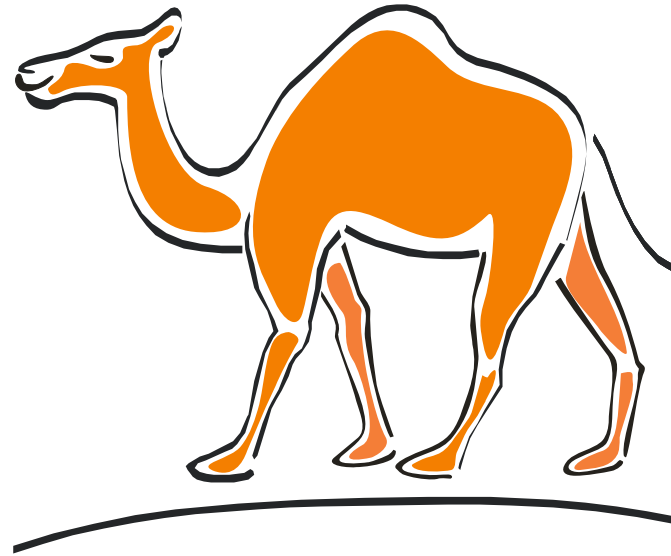


The Nomadic Network



Providing Secure, Scalable and Manageable
Roaming, Remote and Wireless Data Services

Josh Howlett & Nick Skelton
Information Services, University of Bristol

TNC 2003


Background

- 1999-2000: new technologies
 - Ratification of wireless 802.11b standard
 - New broadband technologies (cable, xDSL)
 - Increasing numbers of laptops (students & staff)
- 2001: we wanted to offer
 - Wireless access on campus
 - Wired access on campus
 - VPN access from off campus








Background

- Summary of requirements
 - Integrated (wireless, wired, VPN)
 - Secure (AAA, encryption)
 - Easy for users (many OSes to support)
 - Easy for us to support (not many resources)
 - Good service (does it do what the user wants)?
 - Future proof (bluetooth, etc)
 - Resilient and scaleable (fail-over, load-sharing, etc)
 - Cheap, and preferably free.

Background

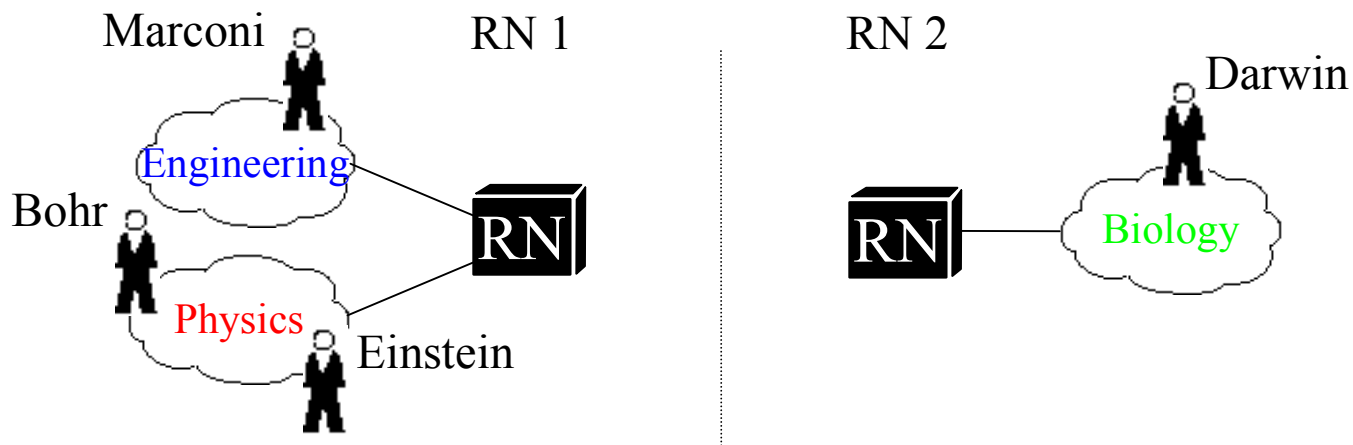
- Decision to develop our own solution
- Linux-based router called a “roamnode” ()
- History
 - Development: started January 2001
 - Pilot service: September 2001 (~100 users)
 - Supported service: September 2002 (now ~910 users)

Theory of operation: network

- All users are assigned to a “home-service”
 - Home-service = an IP network + other info (DNS, WINS...)
 - User “einstein”  Home-service “physics”
 - User “bohr”  Home-service “physics”
 - User “marconi”  Home-service “engineering”
 - User “darwin”  Home-service “biology”
- A home-service is assigned to a “target network”
 - Home-service “physics”  Physics network
 - Home-service “engineering”  Engineering network
 - Home-service “biology”  Biology network

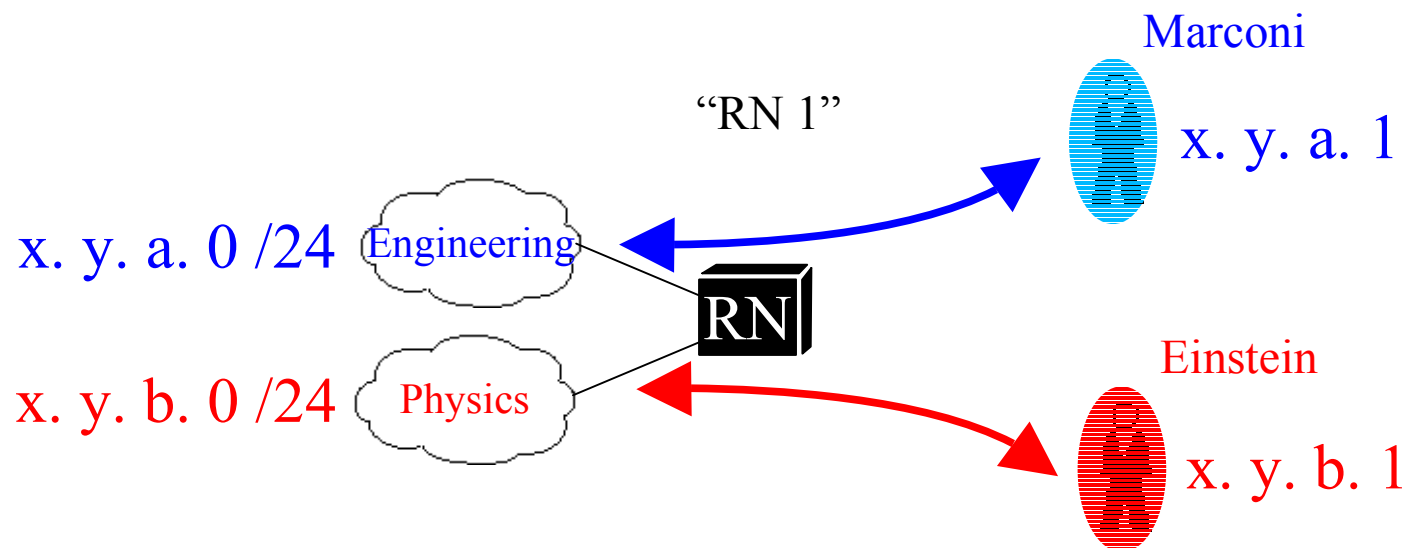
Theory of operation: network

- Each home-service is hosted on a roamnode
 - Home-service “physics”
 - Home-service “engineering”
 - Home-service “biology”
- ➡ Roamnode “RN 1”
- ➡ Roamnode “RN 2”
- Or, diagrammatically:



Theory of operation: network

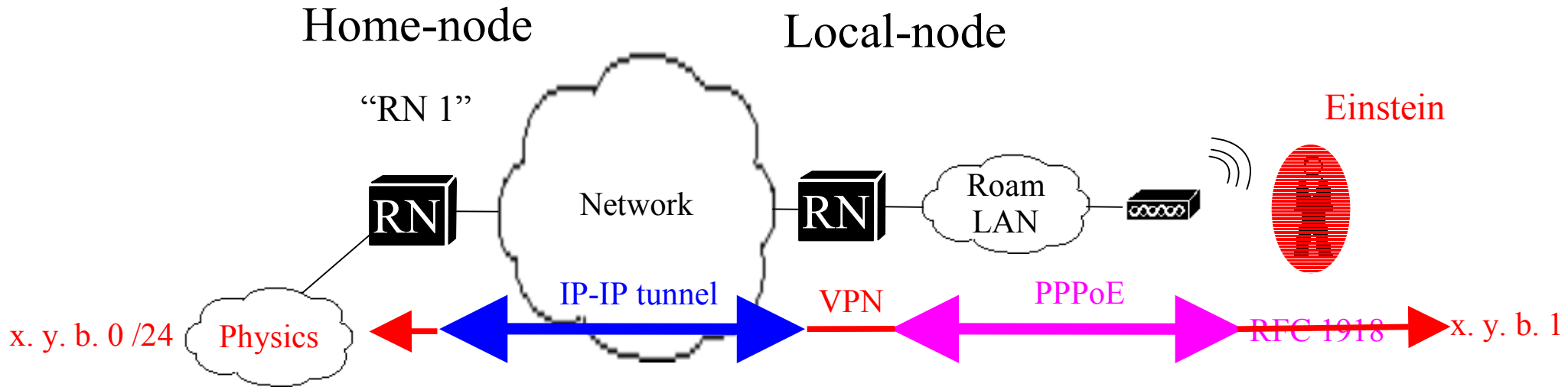
- A user connects to his home-service using a VPN
- A user is allocated an IP address from the user's target network; for example:



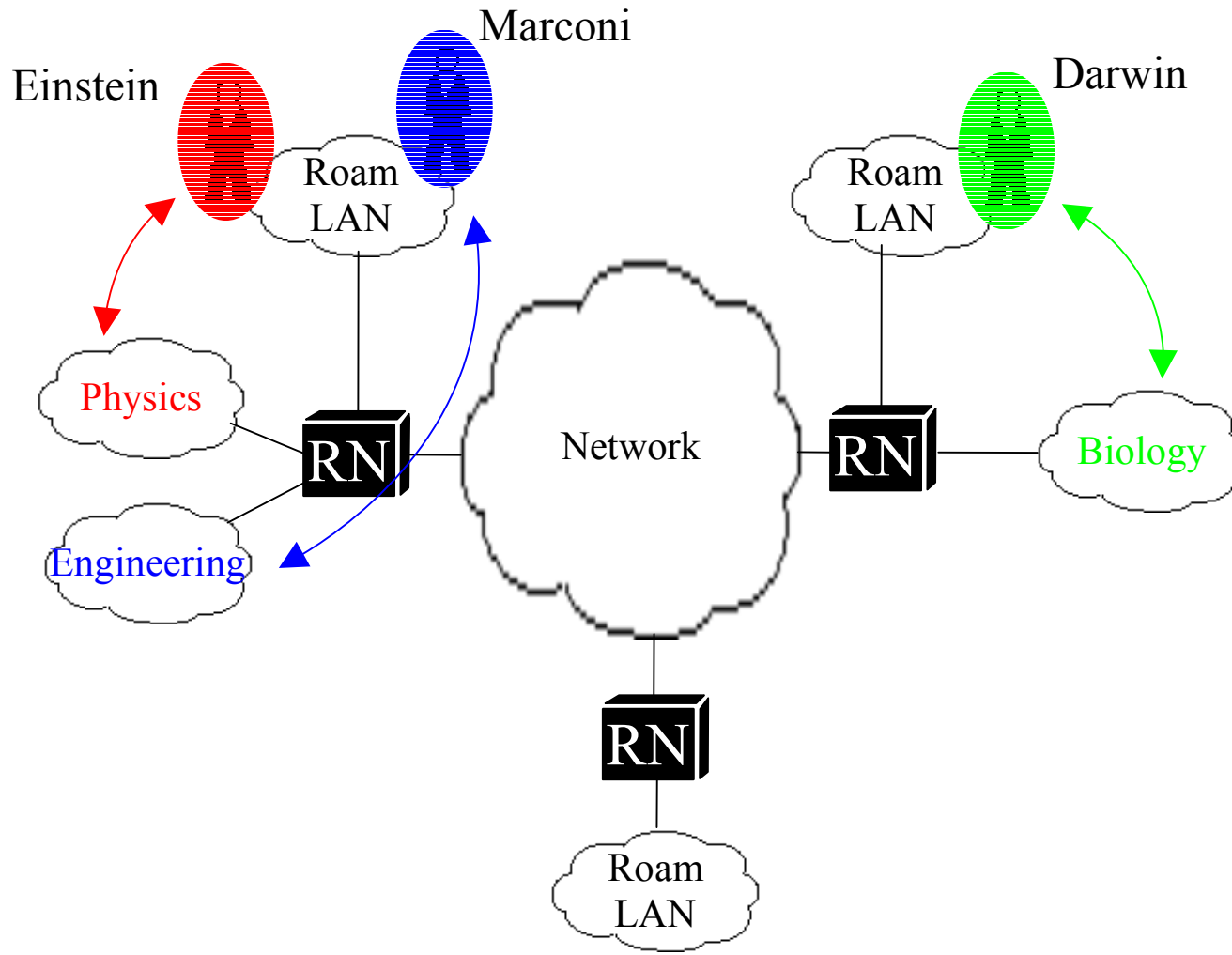
Theory of operation: network

- The user requires an IP address to establish the VPN session
- This IP address is allocated using “PPPoE”
 - The PPPoE session runs across an isolated (logically or physically) network called the “roam LAN”
 - User is allocated an RFC1918 address
 - An overlay network is constructed dynamically using IP-IP tunnels to route user → home-service VPNs
 - Use of PPPoE has several advantages over vanilla 802.3 in wireless (ie. client security and management)

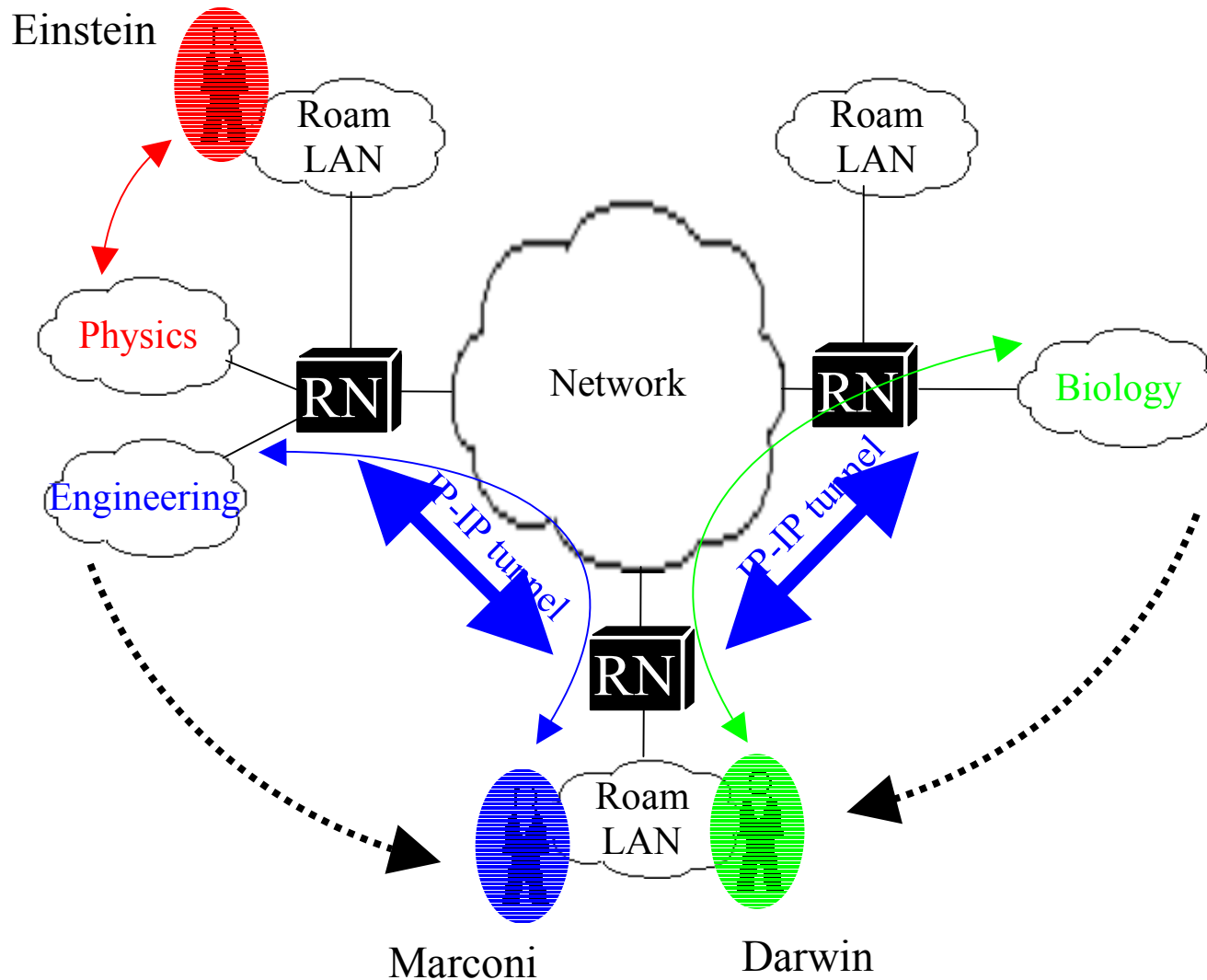
Theory of operation: network



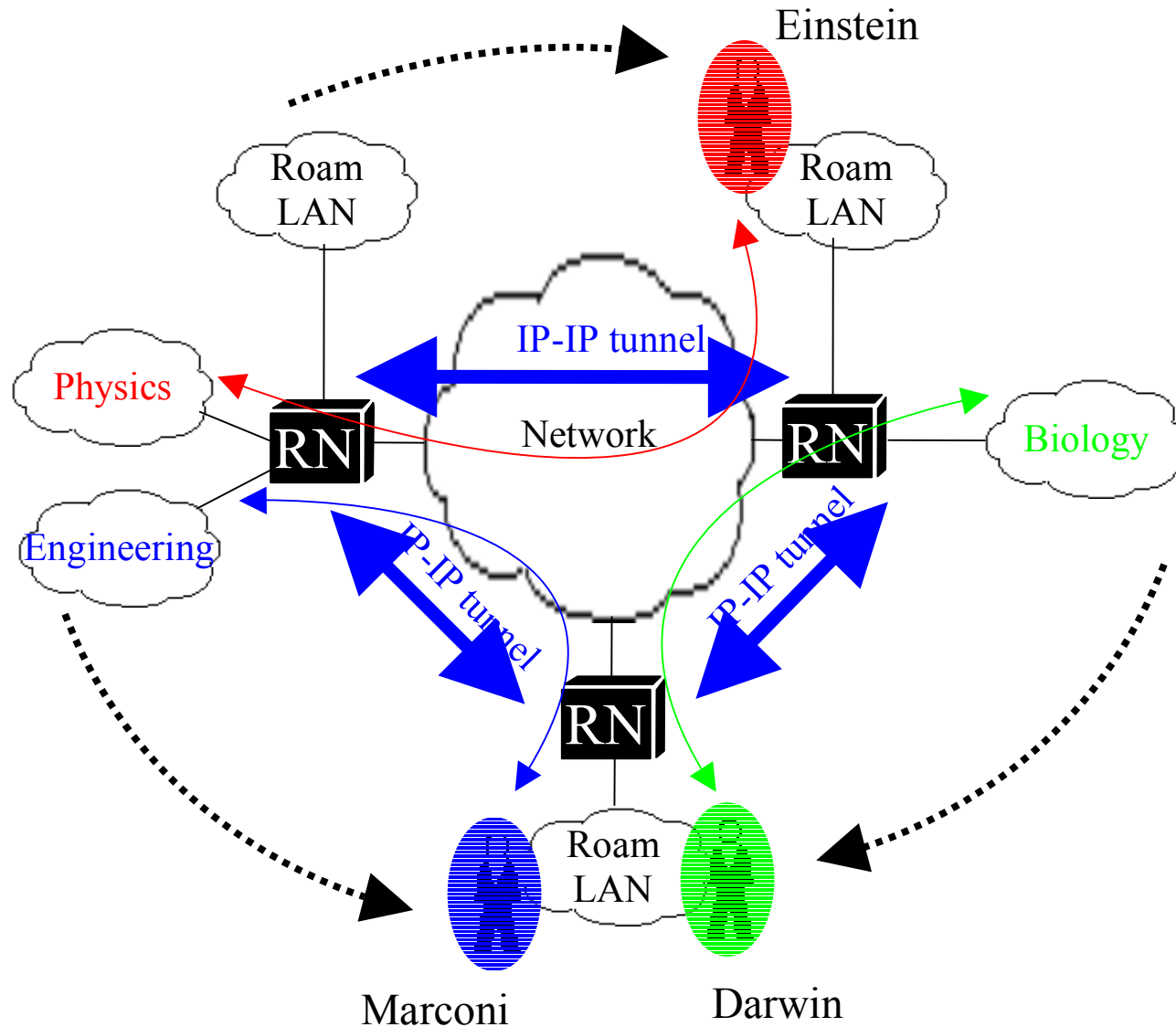
Theory of operation: network



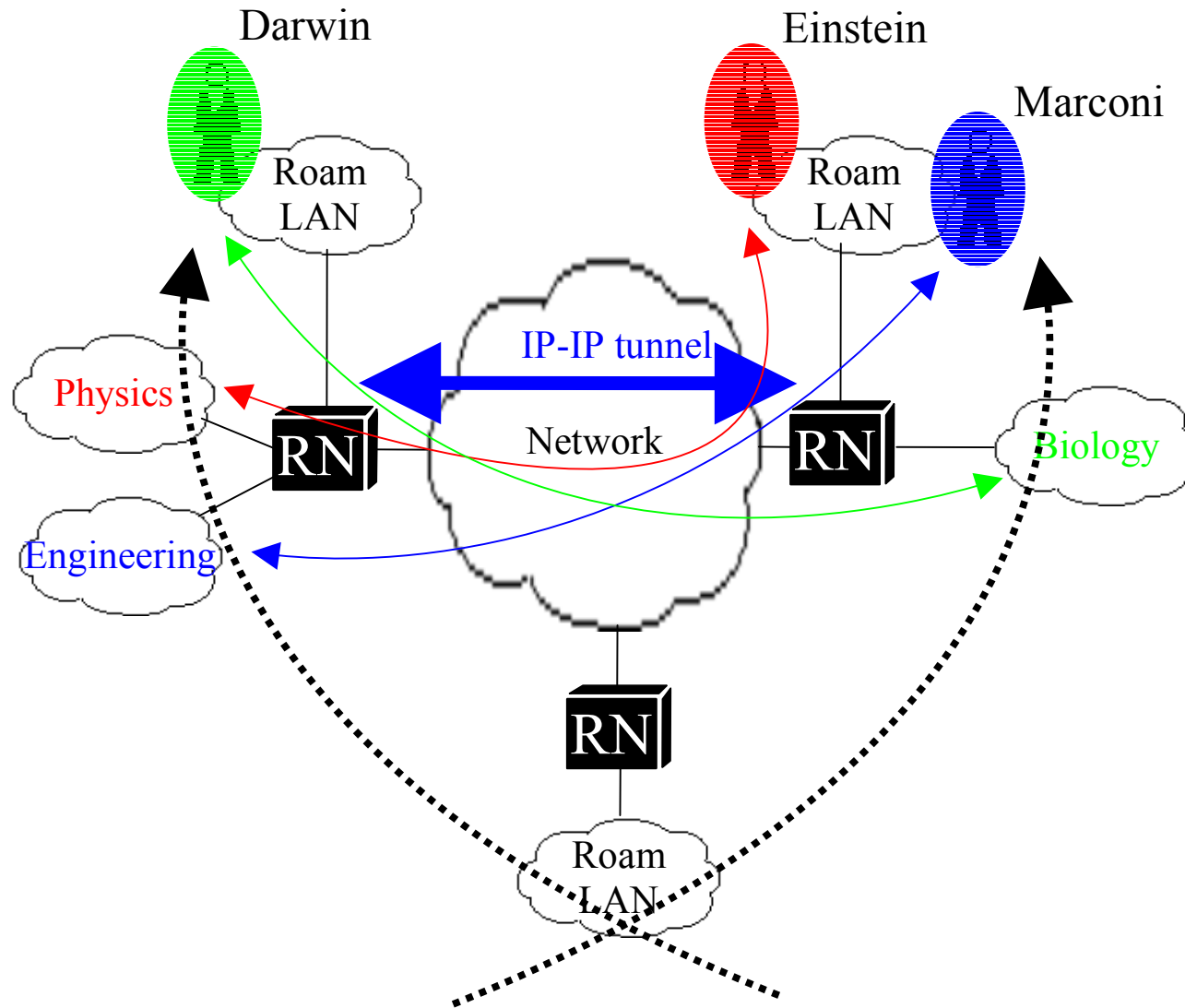
Theory of operation: network



Theory of operation: network



Theory of operation: network



Theory of operation: security

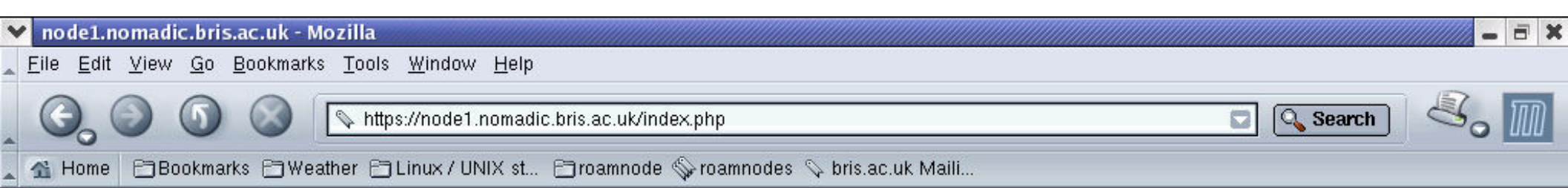
- Authentication & Authorisation
 - User is authenticated twice
 - Localnode: credentials proxied to homenode
 - Homenode: credentials proxied to RADIUS server
 - User is authorised twice
 - Localnode (“is user allowed on this 'roam' network ?”)
 - To control access on basis of physical location
 - Homenode (“is user allowed on this 'target' network ?”)
 - To control access on basis of logical network

Theory of operation: security

- Encryption
 - MPPE at 40 or 128 bits
 - Encryption is performed by the VPN (PPTP)
 - Data encrypted from user to home-node

Implementation

- Roamnode
 - All open-source software
 - Runs on Intel hardware
 - Boots and runs from CD-ROM
 - 8 MB ISO image: download from website
 - Some people are interested in making an “embedded” box
 - All management via secure web interface



node1.nomadic.bris.ac.uk

Current status

[Show users](#) [Show tunnels](#) [Show system status](#)

Configuration

Interface configuration	Host configuration	RLAN configuration	RNET configuration	Peer configuration
802.1D configuration	Reboot configuration	Secure HTTP configuration	Generate new running configuration	Console (only for debug and development)

State

[STANDBY](#) [RUNNING](#) [REBOOT](#) [HALT](#)

Warning - beta quality software and documentation!

1. Read the [manual](#). Even if you're Mr Cisco, there is no way you can configure this without reading the manual.
2. If you have any questions, suggestions, criticisms or run into problems, mail nomadic-general@bris.ac.uk
3. Share and enjoy!

[Return to the main page](#); View connected users - node1.nomadic.bris.ac.uk

Current RoamLAN users

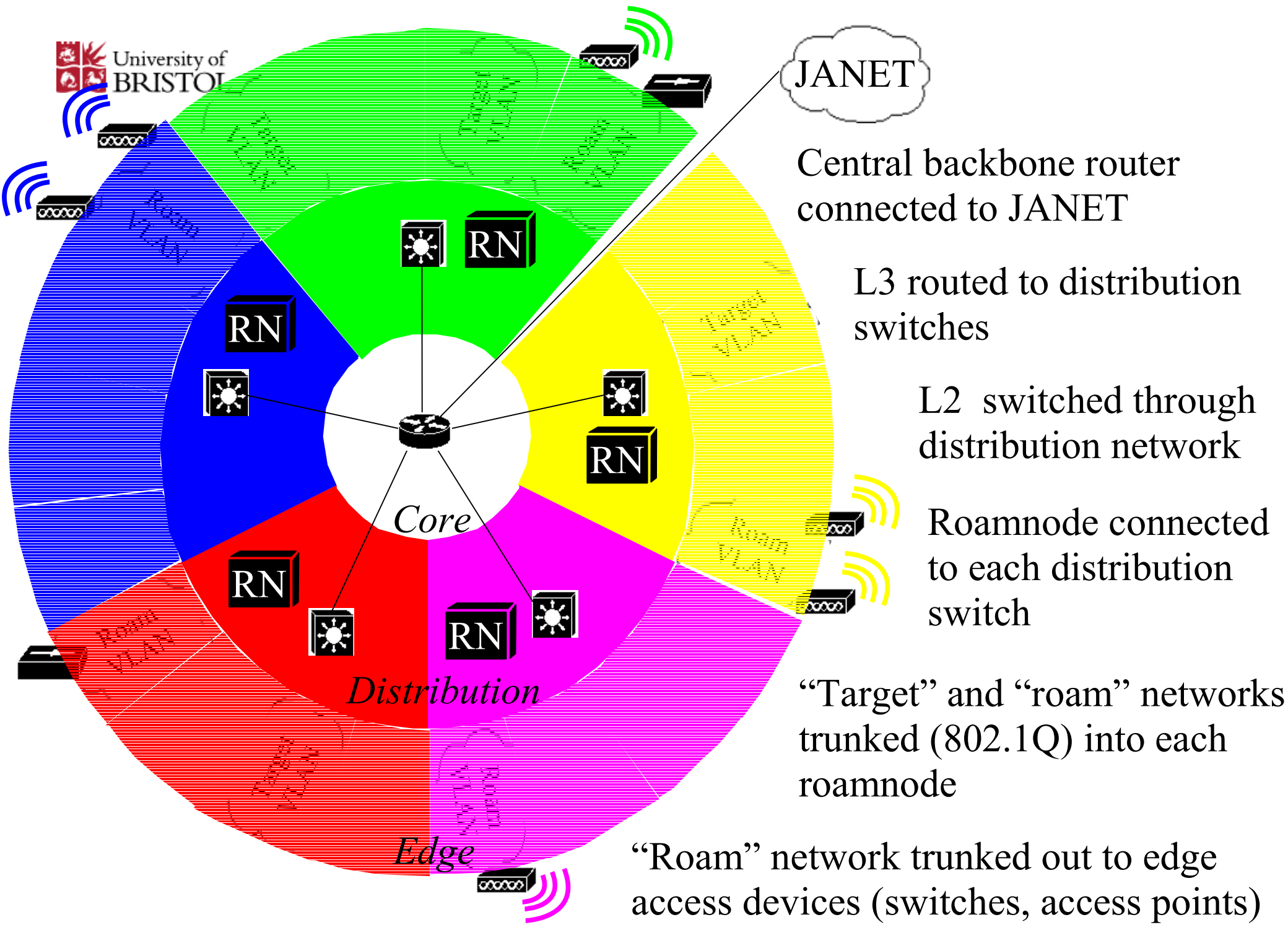
Start of session	Username	Homeservice	MAC address	Location	Recv (MB)	Sent (MB)	Total (MB)	Rate (Kb/s)
12:06:53 1/5/03 UTC	cg7751		00:03:93:1e:30:c4	Arts & Social Sciences Library	0.01	0.01	0.02	1.93
10:20:35 1/5/03 UTC	cmpjs		00:02:2d:23:56:b2		0.26	0.76	1.02	1.29
11:02:19 1/5/03 UTC	ms2876		d2:e8:0a:c9:fa:97		0.11	0.21	0.32	0.66
11:06:52 1/5/03 UTC	ns2032		00:90:99:5d:22:c2		0.37	3.28	3.65	8.11
11:54:16 1/5/03 UTC	rc8299		00:30:ab:0e:6c:5b		0.26	0.76	1.02	9.92
11:44:09 1/5/03 UTC	wz2941		00:08:02:62:39:c6		3.43	15.83	19.26	108.89

Current RoamNET users

Start of session	Username	RoamNET	IP address	Recv (MB)	Sent (MB)	Total (MB)	Rate (Kb/s)
11:05:43 1/5/03 UTC	bzims	ilrt-vpn.nomadic.bris.ac.uk	137.222.34.230	1.1	2.86	3.96	8.64
09:51:50 29/4/03 UTC	cdams	staff-vpn.nomadic.bris.ac.uk	137.222.86.4	0.05	0.05	0.1	0
12:06:58 1/5/03 UTC	cg7751	student-vpn.nomadic.bris.ac.uk	137.222.83.9	0	0.01	0.01	1.02
10:21:17 1/5/03 UTC	cmpjs	ilrt-vpn.nomadic.bris.ac.uk	137.222.34.229	0.16	0.63	0.79	1.01
12:01:58 1/5/03 UTC	cw0944	student-vpn.nomadic.bris.ac.uk	137.222.83.8	0.16	1.12	1.28	27.59
09:30:49 1/5/03 UTC	isxel	staff-vpn.nomadic.bris.ac.uk	137.222.86.2	0.88	11.02	11.9	10.32
23:02:15 30/4/03 UTC	jb0309			0	0	0	0
09:36:31 1/5/03 UTC	jh1761	student-vpn.nomadic.bris.ac.uk	137.222.83.4	0.24	0.29	0.53	0.48
00:14:55 1/5/03 UTC	jh1977	student-vpn.nomadic.bris.ac.uk	137.222.83.4	2.33	1.11	3.44	0.66
11:03:23 1/5/03 UTC	ms2876	student-vpn.nomadic.bris.ac.uk	137.222.83.7	0.11	0.11	0.22	0.46
11:07:01 1/5/03 UTC	ns2032	student-vpn.nomadic.bris.ac.uk	137.222.83.3	0.22	3	3.22	7.17
09:40:08 1/5/03 UTC	pearc	staff-vpn.nomadic.bris.ac.uk	137.222.86.6	0.31	1.72	2.03	1.87
09:38:58 1/5/03 UTC	pypdl	staff-vpn.nomadic.bris.ac.uk	137.222.86.5	8.86	23.77	32.63	29.83
11:55:38 1/5/03 UTC	rc8299	student-vpn.nomadic.bris.ac.uk	137.222.83.5	0.12	0.7	0.82	8.84
11:44:50 1/5/03 UTC	wz2941	student-vpn.nomadic.bris.ac.uk	137.222.83.2	2.82	14.80	17.71	102.7

Implementation

- University of Bristol
 - Network
 - Non-contiguous network at L2 across the Campus (legacy due to previous ATM back-bone)
 - Therefore five roamnodes required
 - Authentication / Authorisation
 - Microsoft Active Directory stores all users' credentials
 - Roamnodes authenticate against MS RADIUS server (IAS)
 - Roamnode is vendor neutral!



JANET

Central backbone router connected to JANET

L3 routed to distribution switches

L2 switched through distribution network

Roamnode connected to each distribution switch

“Target” and “roam” networks trunked (802.1Q) into each roamnode

“Roam” network trunked out to edge access devices (switches, access points)

University of BRISTOL

Core

Distribution

Edge

RN

RN

RN

RN

RN

Roam VLAN

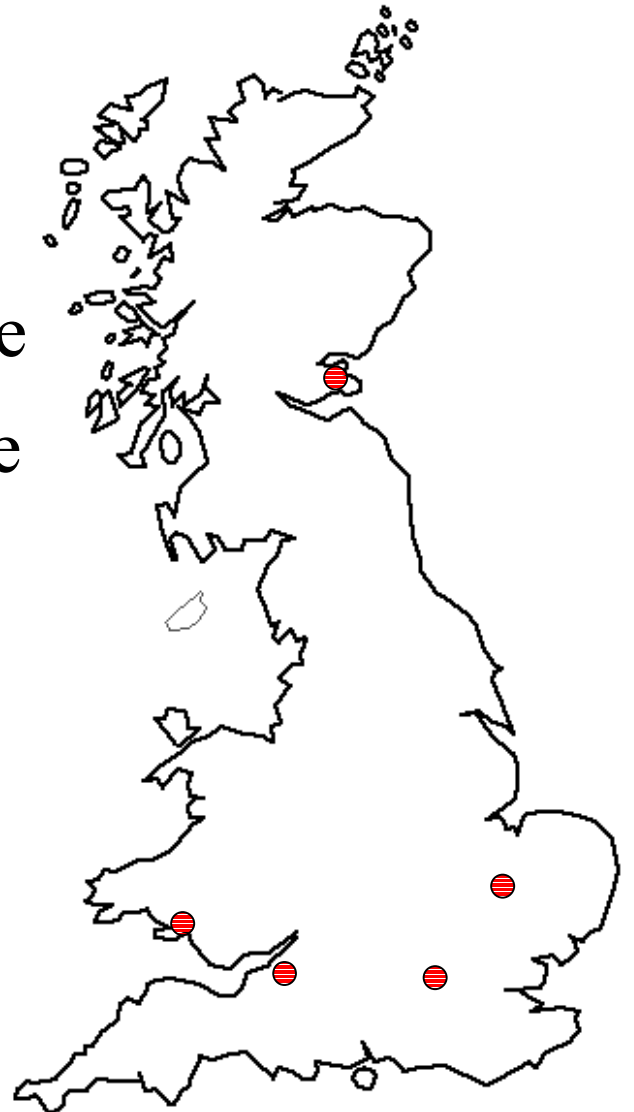
Roam VLAN

Target VLAN

Roam VLAN

Implementation

- Other implementations
 - 5 Universities in the UK known to be piloting or implementing the roamnode
 - Main reasons given for interest
 - Proven solution
 - Flexible
 - Free



Implementation

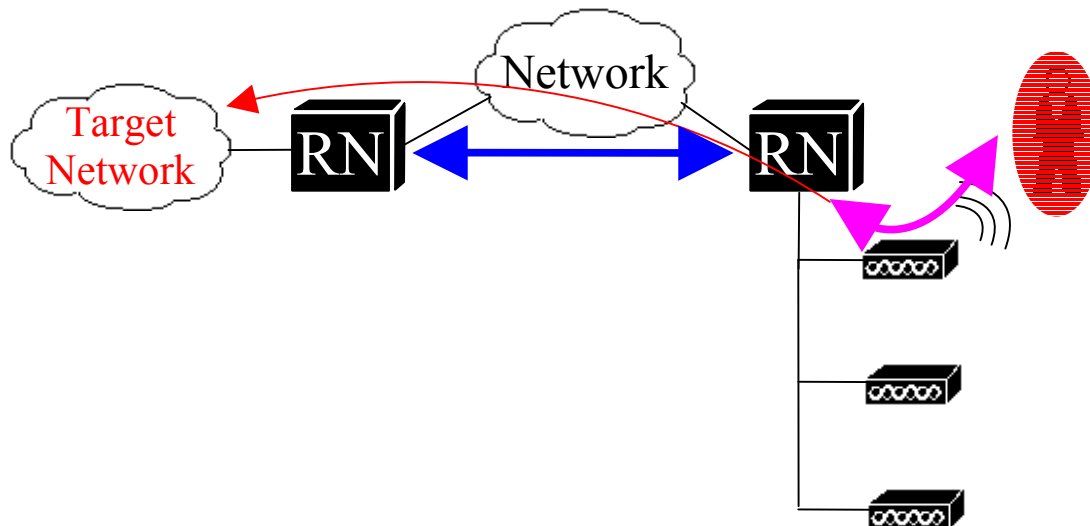
- University of Wales Swansea (implementing)
 - Outside of Bristol, the most advanced implementation
 - Main differences
 - Contiguous network at L2, therefore only 1 roamnode
 - Multiple authentication databases (NT domain, Novell, etc)

Implementation

- Genome Campus, Cambridge (piloting)
 - Consists of three separate institutions
 - Sanger Institute
 - European Bioinformatics Institute
 - Human Genome Project Resource Centre
 - Researchers need to be able to roam between each institution, as well as shared facilities (libraries, canteens, etc)

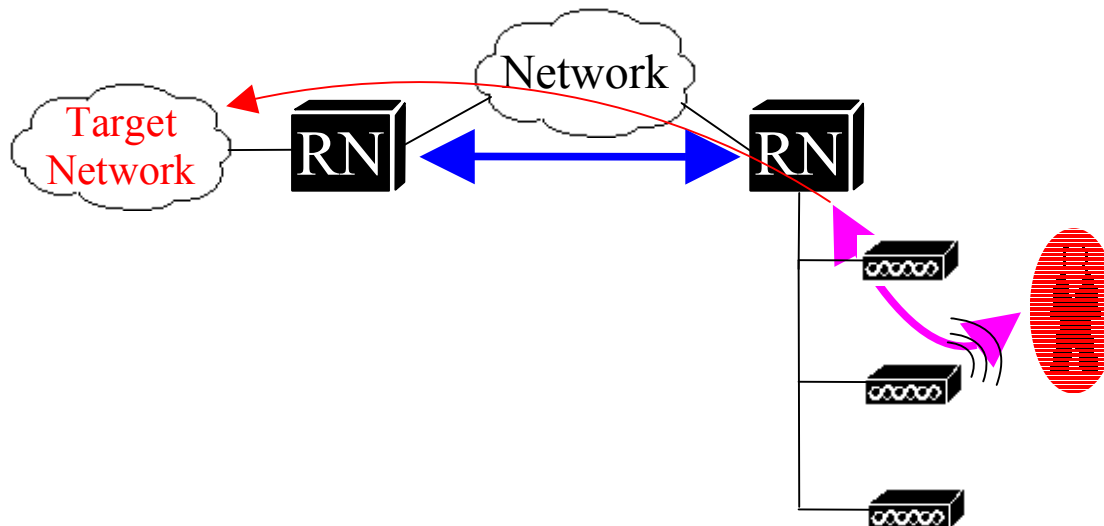
Mobility

- Roaming
 - Different access points
 - Handled transparently at L2 if APs on same network



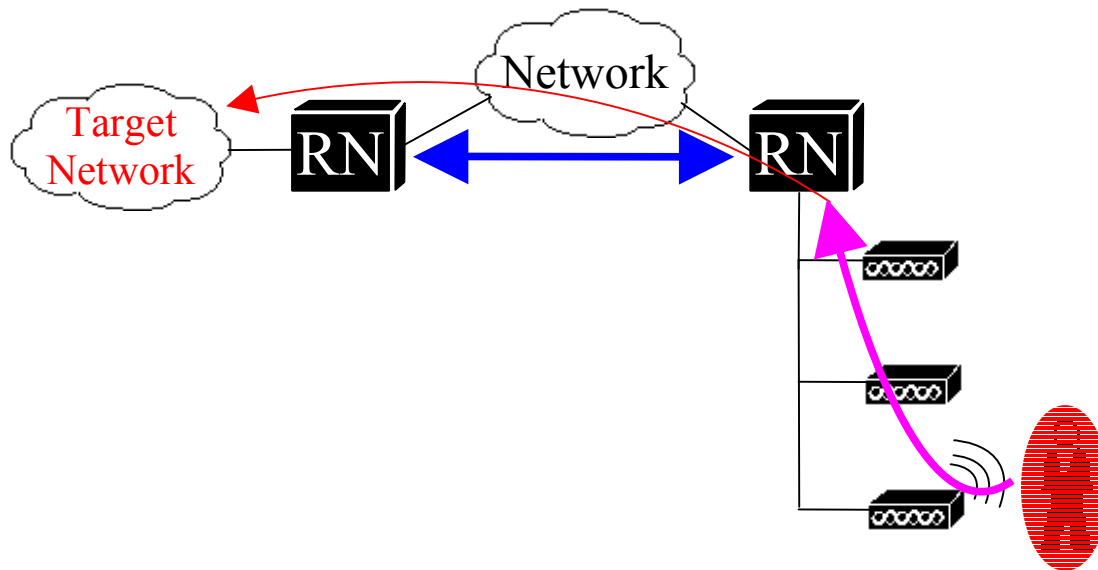
Mobility

- Roaming
 - Different access points
 - Handled transparently at L2 if APs on same network



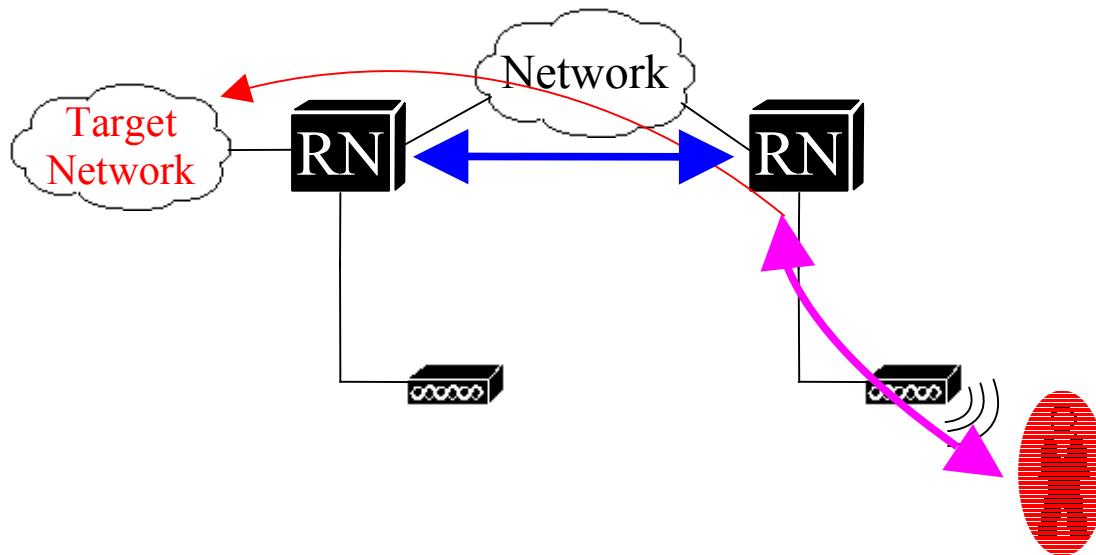
Mobility

- Roaming
 - Different access points
 - Handled transparently at L2 if APs on same network



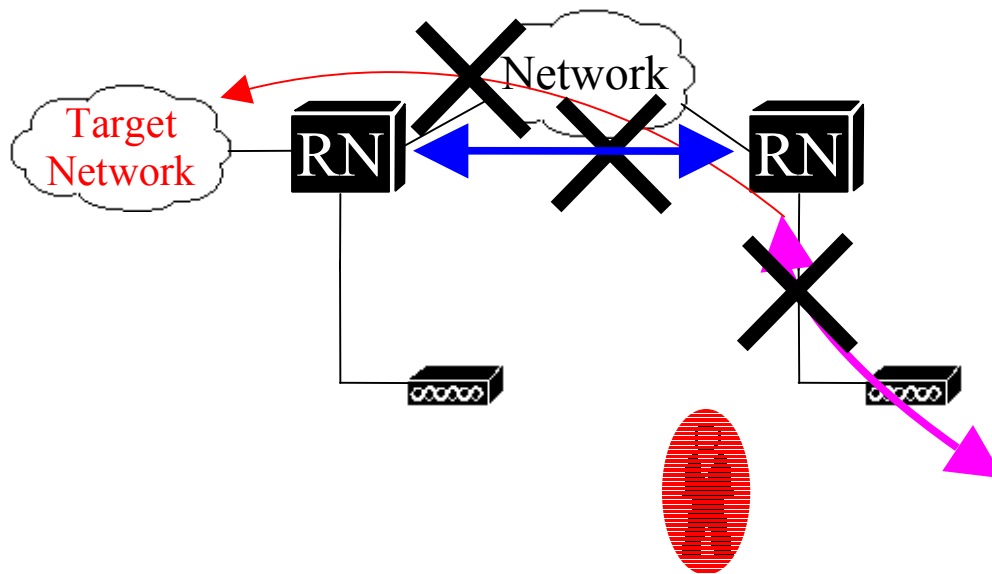
Mobility

- Roaming
 - Different roamnodes on same Nomadic network
 - PPPoE & VPN sessions active



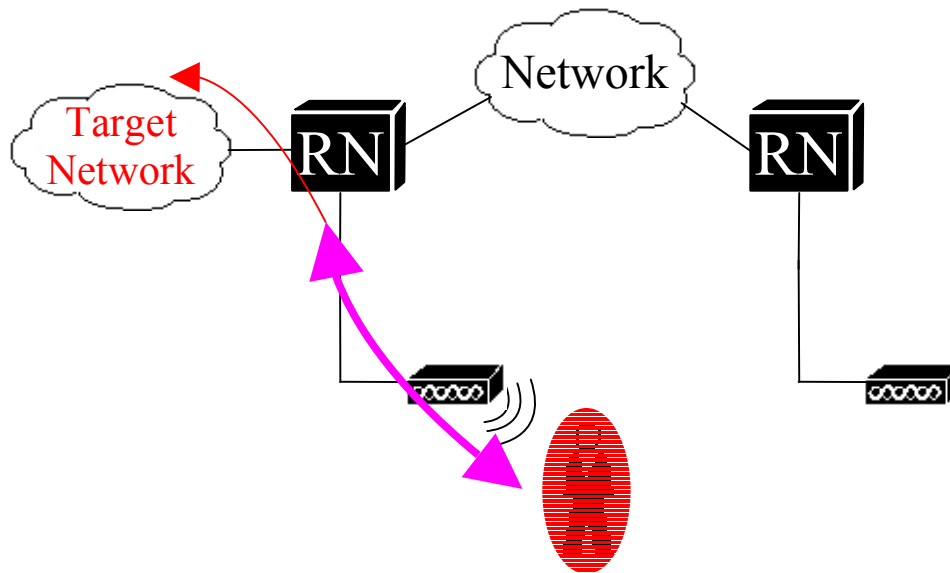
Mobility

- Roaming
 - Different roamnodes on same Nomadic network
 - PPPoE & VPN sessions terminated, and IP-IP tunnel down



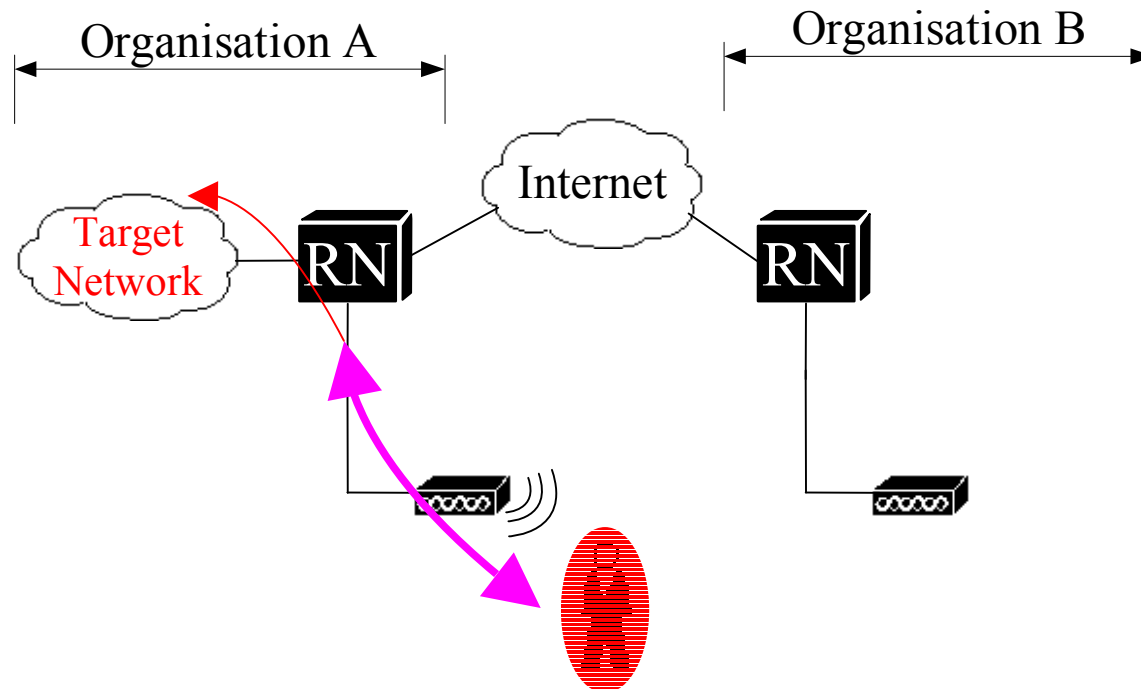
Mobility

- Roaming
 - Different roamnodes on same Nomadic network
 - PPPoE & VPN sessions re-started



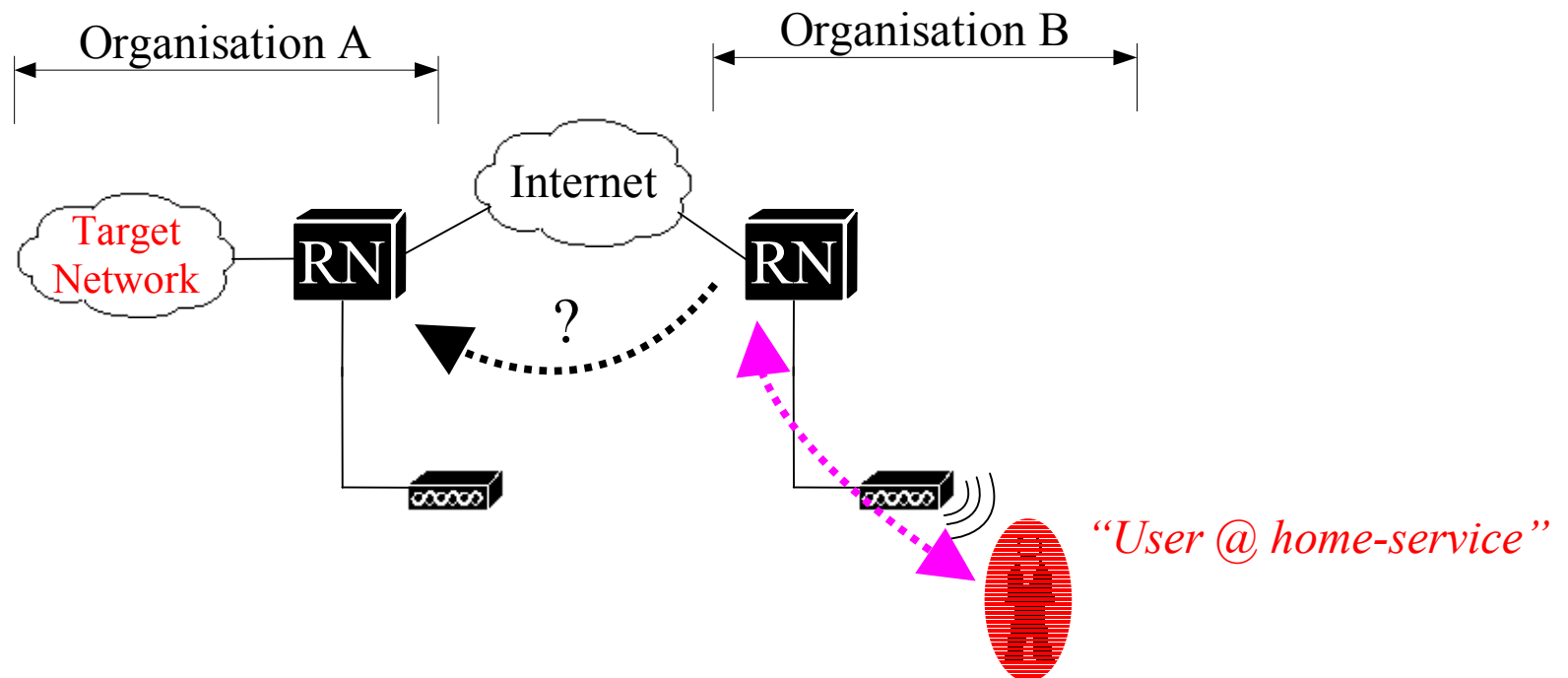
Mobility

- Roaming
 - Different Nomadic networks
 - Roaming on “home” organisation



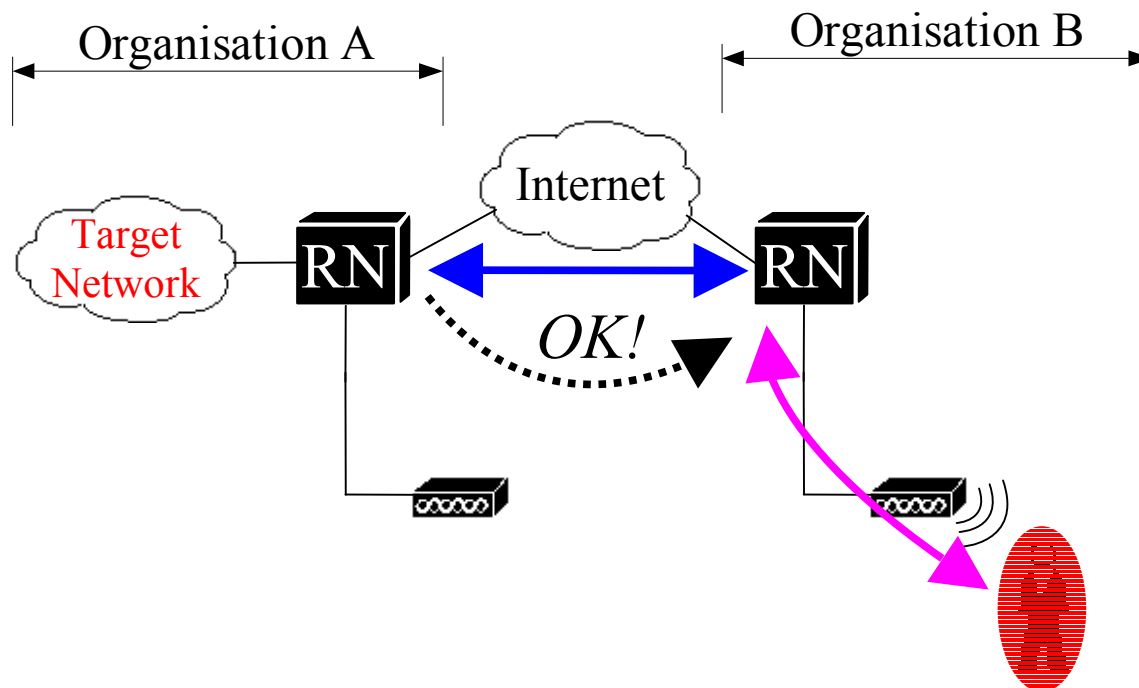
Mobility

- Roaming
 - Different Nomadic networks
 - Authentication request forwarded via RADIUS



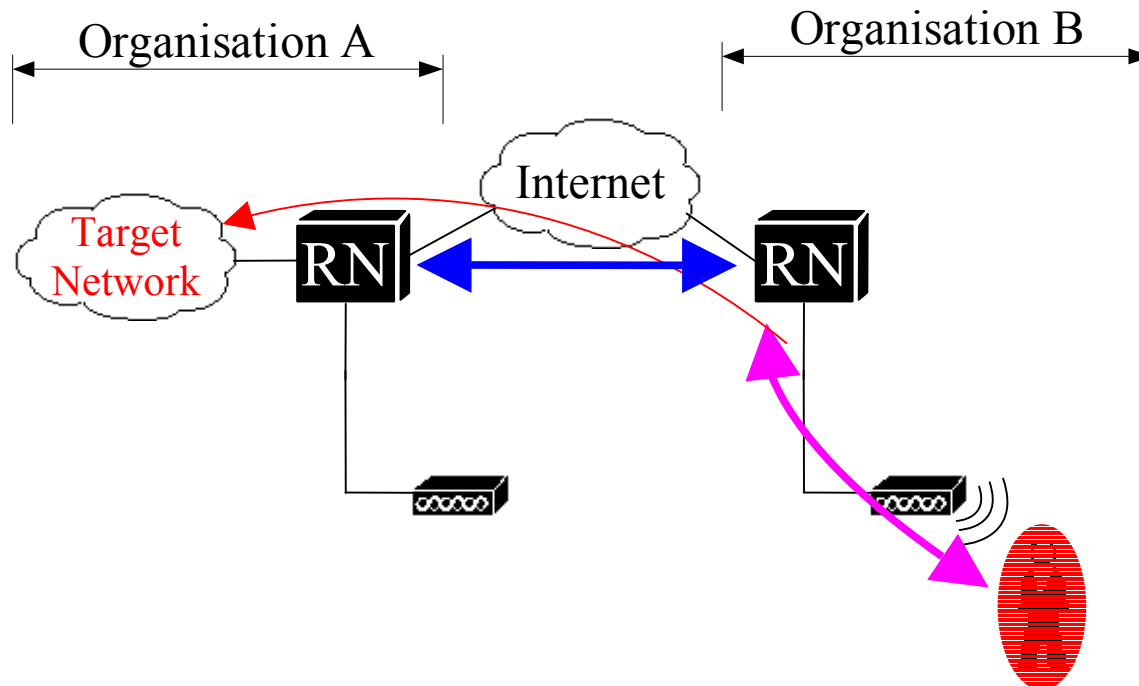
Mobility

- Roaming
 - Different Nomadic networks
 - PPPoE session accepted & IP-IP tunnel up



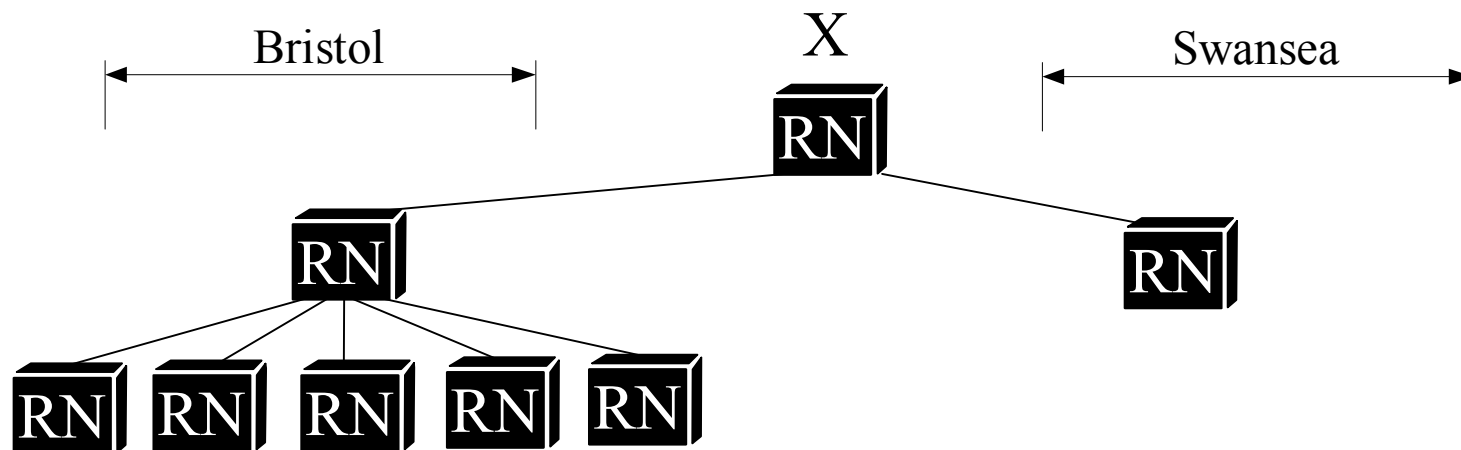
Mobility

- Roaming
 - Different Nomadic networks
 - VPN session started



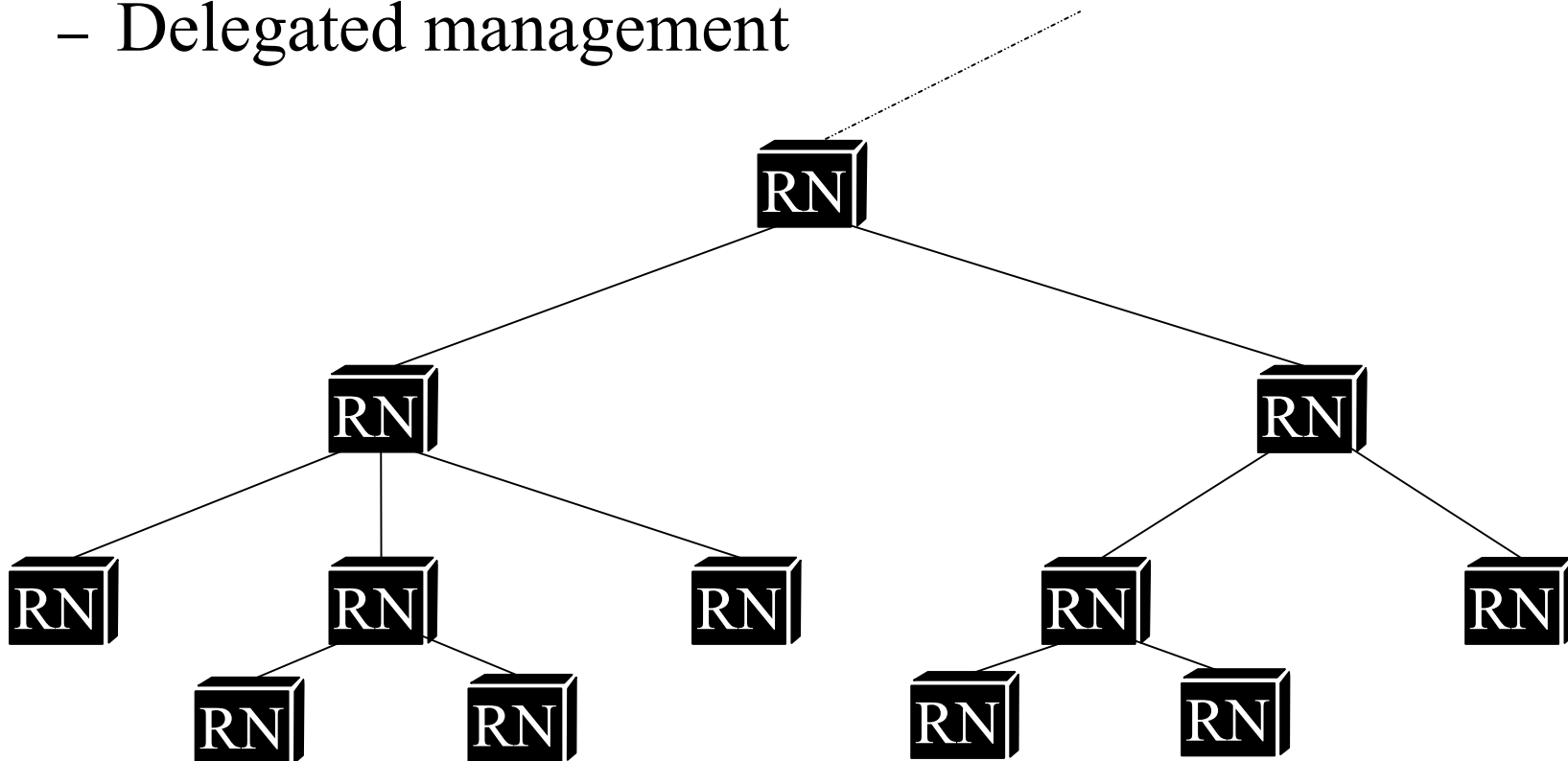
Mobility

- Roaming between Bristol & Swansea campuses
 - Based on trust relationships
 - Bristol trusts node “X”
 - Swansea trusts node “X”
 - Thus, they will accept each others' users



Mobility

- Hierarchical design
 - Scales well
 - Delegated management

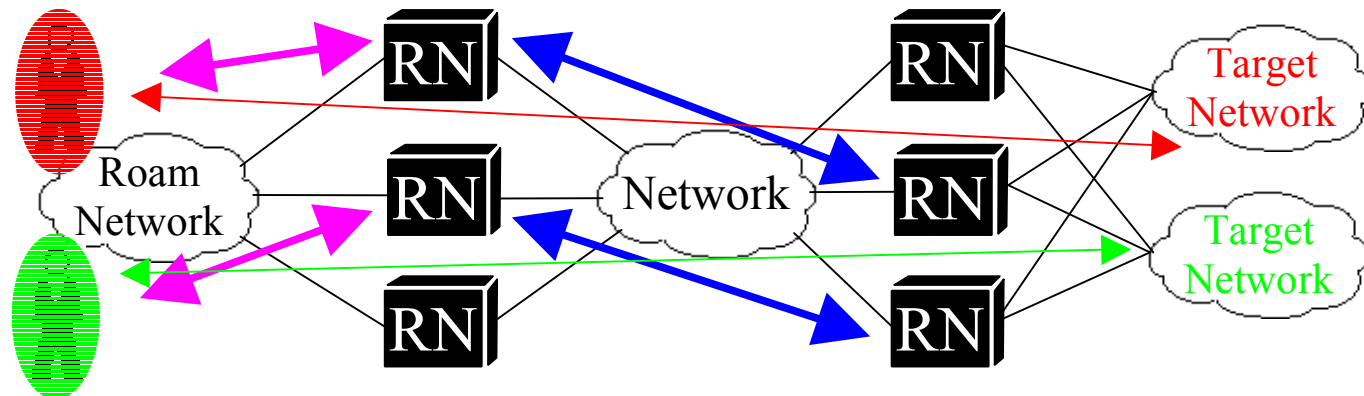


Current development

- Roaming between institutions
 - Allows users to roam between networks that share a trust relationship
 - Same user identity (username) and network identity (IP address) across different networks
 - The only management task that must be centralised is IP space allocation for “roam LANs”
 - IP space allocations can also be arbitrary
 - No need for management of overlay network; created “on demand” (or “on-the-fly”) as users change location

Current development

- Resilience
 - Resilient roamnode clusters
 - Redundant roamnodes within a cluster
 - Load-sharing and fail-over
 - Mostly complete



Current development

- Locating users
 - Where is a user connected?
 - Many potential applications:
 - Provisioning: “where do we need more access points?”
 - Web: ie. <http://www.bristol.ac.uk/where-am-i>
 - Re-directs web browser to “nearest” web-site (ie. Library catalogue, if user is in the library)
 - Automatic selection of the nearest network printer
 - More than 30 public printers, some 20 kilometers apart

Future proof ?

- Any media that supports ethernet encapsulation
 - Copper / wireless ethernet; Bluetooth (BNEP); etc.
- VPN is currently PPTP but could support others
- Dynamic overlay network will move to IPv6
 - IPv4 and/or IPv6 VPN tunnels over IPv6 and/or IPv4 overlay network
 - RFC1918 is “untidy”
 - IPv6 provides more address space

Client-side Requirements

- Support a broad range of platforms
 - Win95 – XP, Apple Mac OS 10.2, Linux
- No licensing costs
 - Use built-in or free software
- Minimise support effort required
 - Self-registration, self-connection
- As easy to install as possible
 - Provide instructions, software

Network Stack

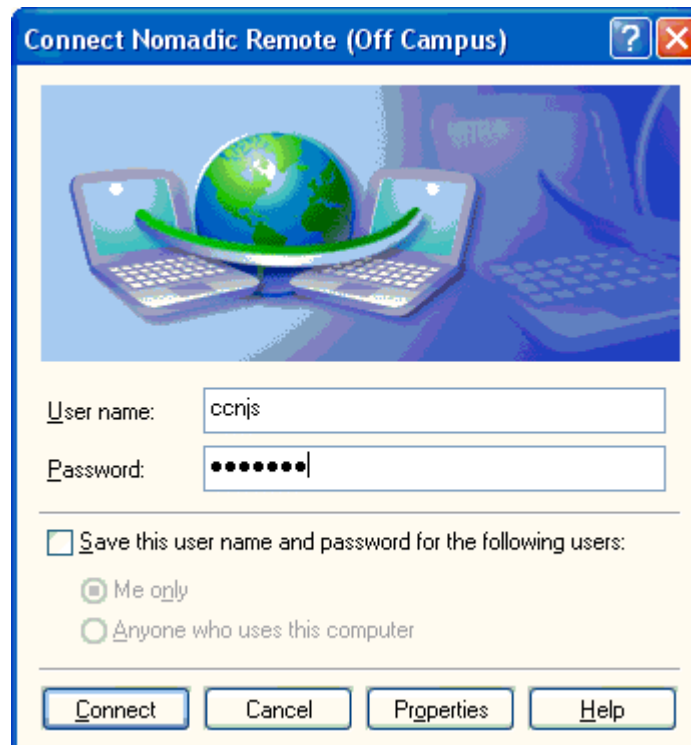
- Requirements in the client OS vary:
 - Remote off-campus service (VPN)
 - PPTP (Point to Point Tunnelling protocol) support
 - Roaming on campus service (Wireless and wired)
 - PPTP (Point to Point Tunnelling protocol) support
 - PPPoE (PPP over Ethernet) support

Software Required

- PPPoE stack
 - Built-in to latest OSes (WinXP, MacOS 10.2)
 - Free third-party client (RASPPPoE) for older Windows versions
- PPTP stack
 - Built-in (but needs patches for older Windows versions)

User Interface

- Looks like a dialup networking connection
 - Familiar
 - Doesn't disrupt other network services on system



Resources

- Web site
- Online registration form
- Step-by-step connection guide for each OS
- CD with software and OS patches
- Support from existing ResNet team

User Procedure

- Register using online form
- Print out documentation
- Pick up software CD (if required)
- Follow step by step connection guide
- Consult support if necessary

Installation Usability

- Most users connect successfully
- Minority of users had problems connecting
 - old systems with Win95/98
 - non-English Windows versions
(need different patches)
- How long does it take to set up?
 - Win 95/98 ~ 30-60 minutes
 - WinXP ~ 5-10 minutes

Current status

- 910 users after nine months
- 50-80 distinct users each day
- About 20 sign up each week
- 5-10% don't self connect and need installation support
 - Comparable to other services such as ResNet

Who uses the service and why?

- Remote VPN service popular with staff
 - Access your files anywhere
- Roaming service popular with students
 - More convenient and personal than public computer rooms

Remote users and home working

- Too far to visit
 - Telephone and email support
- Large range of operating systems
- Users expect support for applications on top
 - Manage expectations
 - Lower level of support for more diverse systems
 - Provide good 'self-support' resources

Future client support

- Support new platforms
 - PDAs (Palm, PocketPC...)
 - No PPPoE support on these platforms yet
- Short-term visitors
 - Quicker registration and configuration with existing service
 - Considering a complementary and restricted web only service

Summary

- Popular with users, fills definite needs
- Support requirements in line with other services
- Low cost
- Low management overheads
- Secure
- Scalable

To find out more...

- Web:
 - Documentation & software (8MB iso image)
 - Go to www.nomadic.bristol.ac.uk
and click 'Roamnode software'
- Or email josh.howlett@bristol.ac.uk