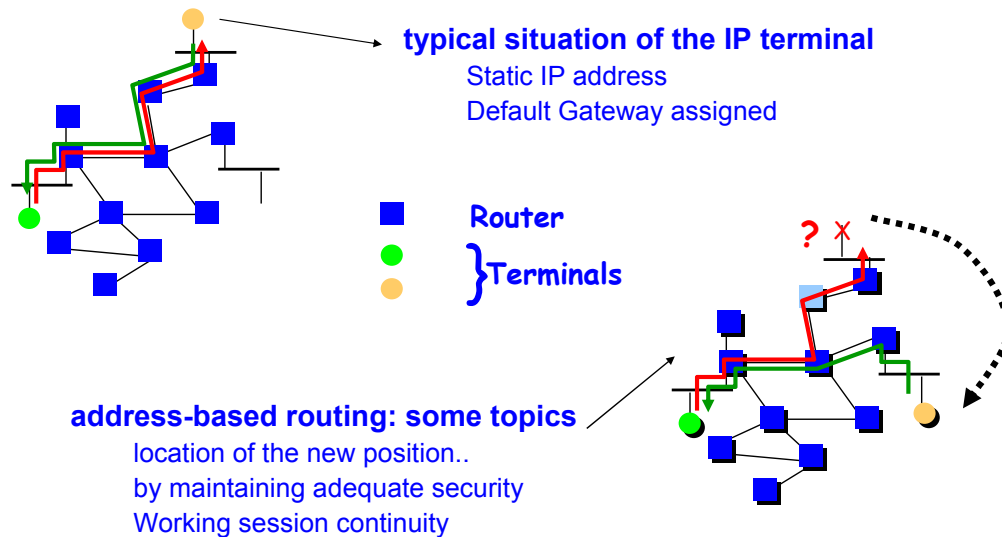


Mobile communications

IP mobility and numbering

**Politecnico di Torino
2006**

IP network – routing and mobility



2



The IP protocols and the relevant services (developed mostly on the fixed network) are assuming a great importance for the mobile context too. Some basic elements of the IP network are recalled in this extension.

The *routing* in the IP networks is performed in function of the *network address* and the *host address* (the address is contained in the header of the IP address).

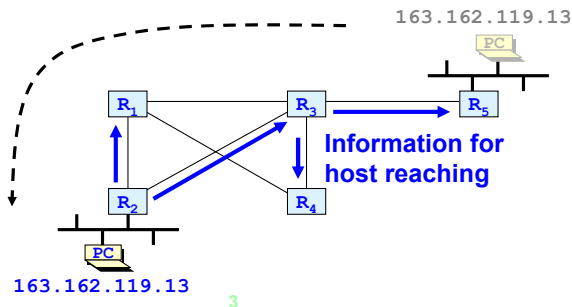
The *router* is the principal element of the IP network. It is a packet switch dealing with the interfaces that connect it with the other (topologically) contiguous routers. Each IP interface is based on a *data link* (Layer 2). Several IP interfaces can use the same *data link*.

The mobility needs in an IP network can occur:

- Within the *Intranet*
- When nomadic events are performed in Internet (access from different sub-networks)
- access to the *Intranet* from a remote point of attachment through the Internet

They are resolved through authentication, security, *tunnelling* and *roaming* processes.

Mobility within Intranet



- Movements within the Intranet:**
- new routing information spread to all the network nodes
 - proprietary solution

3

TELECOM LAB
ITALIA

The IP address (IPv4) is composed by 4 byte x.y.z.w. for instance, in decimal notation: 102.11.3.4. the first part of the address denotes the network (it is used to route the packet between networks) the second part identifies the *host* within the network. There are 3 addressing classes:

- class A assigns 8 bits to the network address (and the remaining 24 to the *hosts*)
- class B assigns 16 bits to the network address
- class C assigns 24 bits to the network address.

The authentication and authorisation mechanisms allow to recognise the user and to authorise its access to the relevant services. The most used protocol is Radius (specified by the IETF).

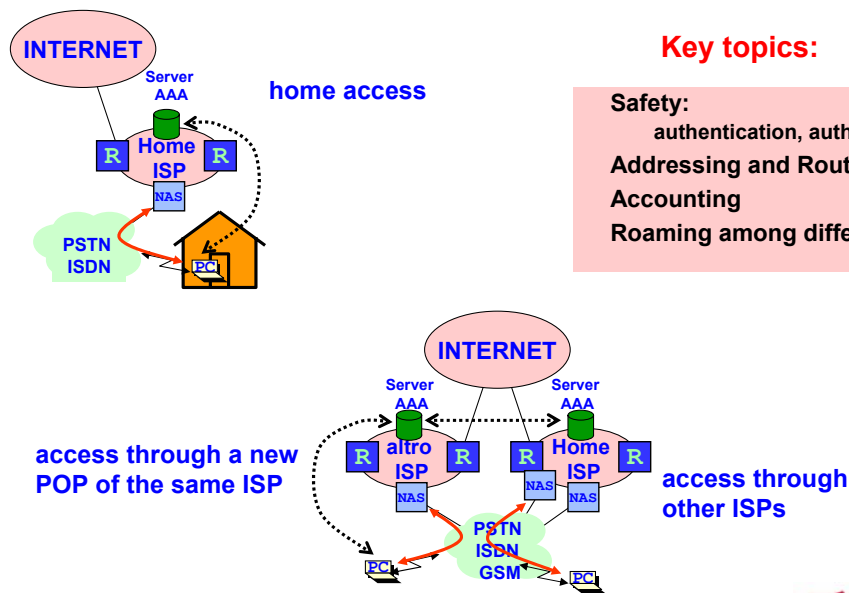
The *tunnelling* mechanisms resolve routing and security problems, also for *Virtual Private Network* configurations.

The *Roaming* between ISPs allows to adapt the global numbering to the needs of a remote access and to supply authentication services among different ISPs (e.g. Ipass).

In case of mobility within the same *Intranet*, the new *host* position is registered by the various nodes by simply registering the info needed to re-route to the new point of attachment the packets generated by any network termination towards the mobile host.

The mobility protocols adopt normally proprietary solutions.

Nomadic behavior in Internet



Some examples of nomadic behaviour in Internet are represents in the figure. The *Server* for *Authorisation, Authentication, Accounting* is queried in any case to resolve the listed functions, all tied to security. When another ISP is involved, an exchange of information is needed between the *AAA servers*.

The *Network Access System* is the ISP access point.

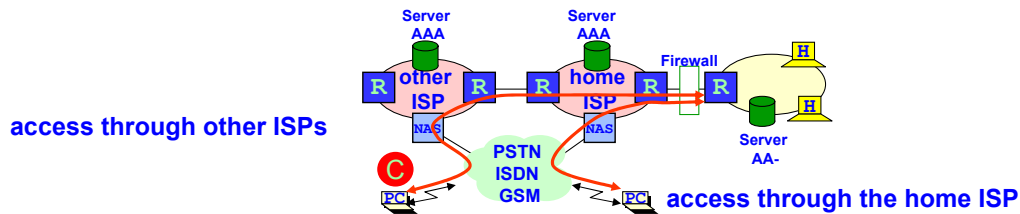
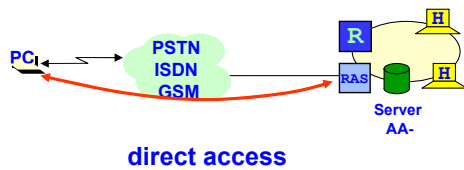
To co-ordinate the offered services through a multiplicity of networks, and administrative contexts, ISPs consortia have been created. They unify the authentication, routing, pricing, and accounting mechanisms.

An example is offered by the iPass consortium, whose associates are several hundreds of ISPs, with more than 2000 *Point of Presence* (POP) in 750 towns. The consortium members have an iPass *server* and can maintain their authentication mechanism. The service is co-ordinated with the IETF.

Remote access to Intranet

Key topics:

- Safety:
 - » authentication, authorisation
 - » confidentiality, data integrity
 - » firewall barriers
- Addressing and Routing
- Accounting
- Roaming among different ISPs

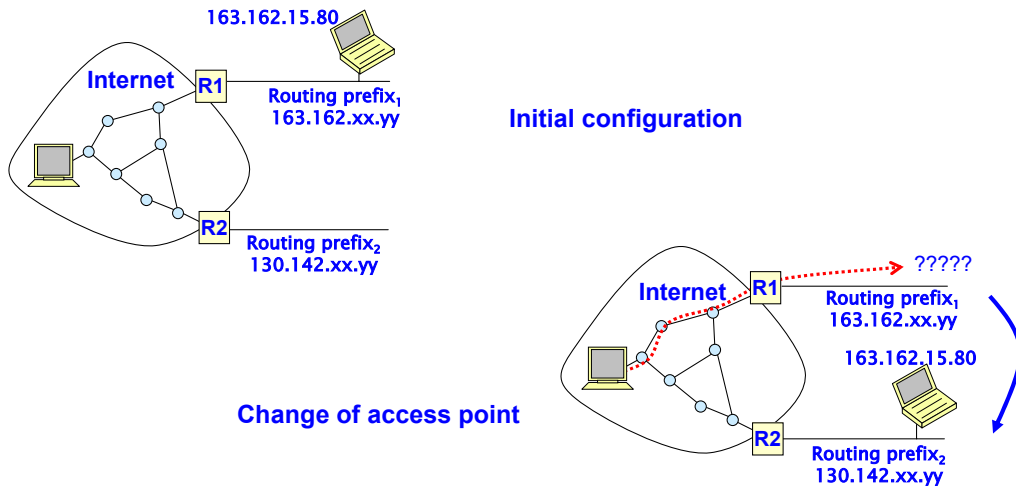


AA - Authorization & Authentication
 AAA - Authorization, Authentication & Accounting

The remote access to Intranet can take place through the *home* network or through other networks. Often, for service pricing issues, (for instance to avoid long distance *dial-up* connections) the local ISP is chosen to access the remote Intranet. This choice poses security problems, addressing and routing.

The *Mobile IP* protocol can help in these cases.

Mobile IP



6

TELECOM LAB
ITALIA

Mobile IP is a protocol defined by IETF for the mobility control at the IP level. It is independent from the layer 2. It makes possible the host movements between different network points of attachments without address changes or modifications of the existing routing schemes. Through *mobile IP* the user can also use with continuity its own *Intranet* services.

The protocol is based on the assignment to the host of two addresses:

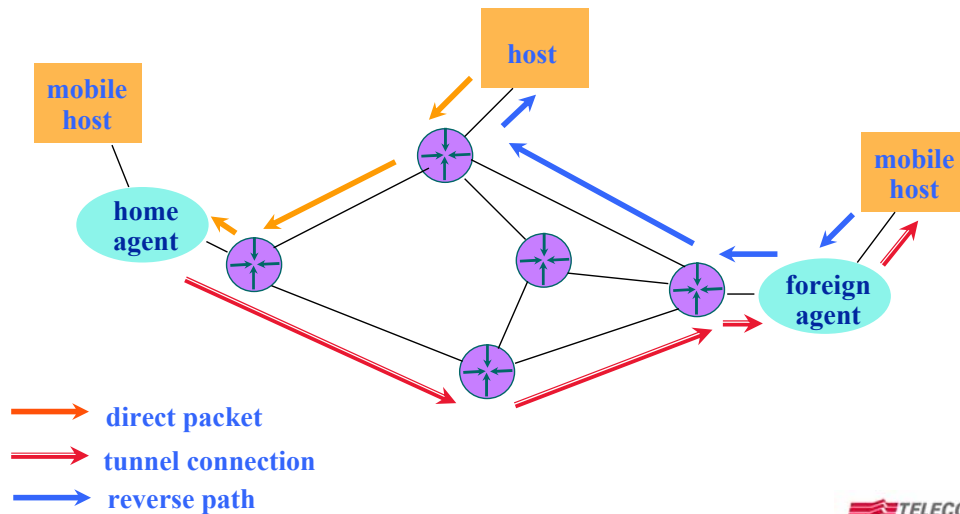
- the *home address* (belongs to the home network of the host)
- the *care-of address*, assigned to the terminal by the visited sub-network (that changes with the host movements)

The network access points must be able to send packets and to associate IP addresses. These functions are performed by the *Home Agent* and the *Foreign Agent*.

The *care-of address* can:

- (*co-located care-of address*) be acquired by the mobile host from a *pool* of public addresses (dynamically assigned to the sub-network visiting users); this solution has some limits due to the address restrictions of IPv4
- (*Foreign Agent care-of address*) be assigned directly by the *Foreign Agent*, (in practise, the assigned address belongs to those belonging to the domain of the visited network).

Basic IP routing mechanisms



7

TELECOM LAB
ITALIA

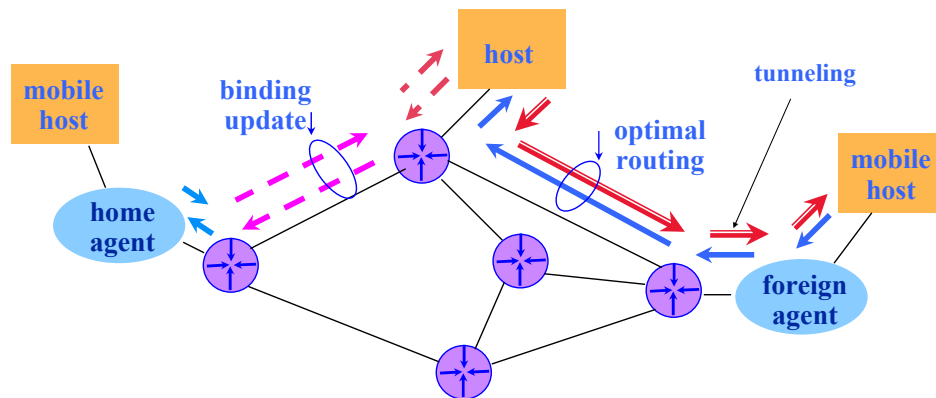
The *Foreign Agent* sends the *care-of address* to the *Home Agent*, which registers it; from that instant on, all the packets sent to the terminal are re-routed by the *Home Agent* consistently with the *care-of address*.

The IPv4 registration messages are transported by the UDP protocol. The *Home Agent* delivers all the packets addressing the terminal in IP packets addressing the *Foreign Agent* with the *care-of address* (tunnelling).

The figure shows the so called triangular routing: all the packets transit always through the *home* network to have the proper header added by the *Home Agent*. This causes an overloading of the network (the *routing* is not optimised). The reverse path is performed directly according to the destination address.

In principle, the TCP session is not affected by the host movements, which are recovered at the level of IP *networking* IP.

Mobile IP - optimised routing



8

TELECOM LAB
ITALIA

The routing is not optimised in the general case. To improve this mechanism, the protocol can set-up more efficient connections (from a routing viewpoint). They base on the capability of the sending *host* to *acquire care-of address* of the mobile terminal along the data transfer session, hence on the possibility of addressing directly the destination host, without passing through the *Home Agent*.

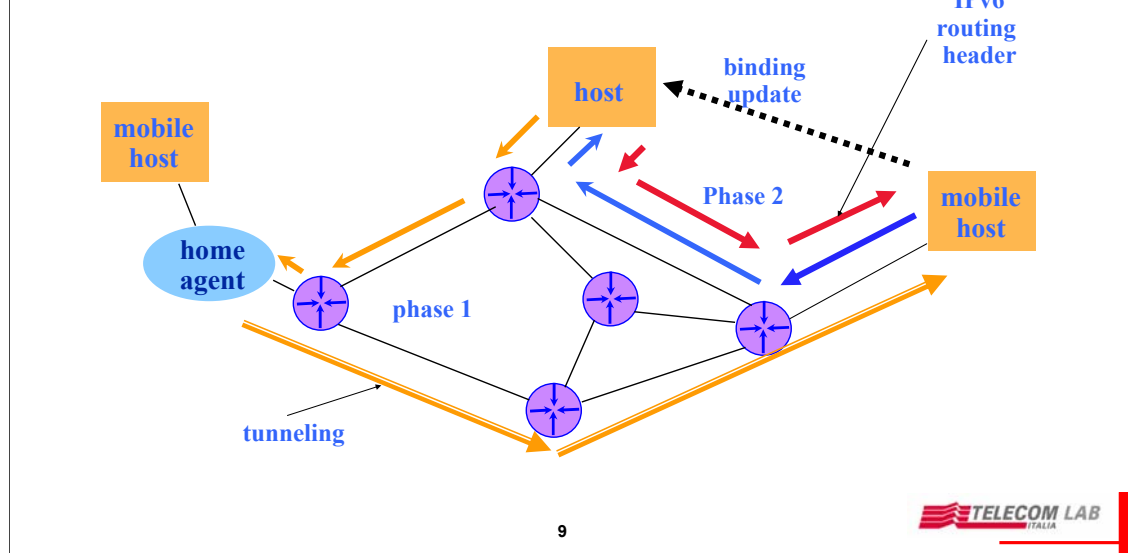
To realise the new mechanism, the *Home Agent* sends to the sending host the *care-of address* (*binding update* procedure). From that instant on, the terminal is directly performing the *tunnelling* of all the packets addressed to the mobile host (*optimised routing*).

If the mobile host still moves within another sub-network, the new *Foreign Agent* must update with a new *care-of address* not only its *Home Agent* but also the *Foreign Agent* previously visited.

Then, if the *Home Agent* (or the *sending host* directly when the *routing is optimised*) before assuming the new *care-of address*, should send packets to the mobile host, the *Foreign Agent* previously visited, could take the role of sending them to the proper address (new *tunnelling*). After the transient phase, the routing assumes its final configuration.

The above procedure can also be performed by avoiding the update of the old *Foreign Agent* with the new *care-of address*: it will take care of re-route the packets towards the *Home Agent* which will, by turn, update the sending host.

Mobile IP - optimised routing - IPv6 case



The routing optimisation protocol is much more effective when IPv6 is used. Here, the host is directly able to send the *care-of address* to the sending host in correspondence to each change of its point of attachment.

This is made possible thanks to the greater transport capability of the IP packet: the *binding update* message can be directly encoded in the *extension header* of the IPv6 within a canonical data packet. The signalling traffic is then minimised.

Besides, IPv6 can avoid the *tunnelling* mechanism, in fact, the *routing header* can be utilised. The latter forces the IP packets to follow a pre-assigned path: that specified by the *care-of address*.

The use of the IPv6 *routing header* (figure) is obviously much more efficient compared with the *tunneling* mechanism.

The mobility within Internet poses several security problems:

- the registration messages must be authenticated by the *Home Agent* (to avoid wrong delivery and third party intrusions, able to divert the mobile-terminated messages)
- the authentication is relatively simple when it can take place between the MS and its *Home Agent*: both belong to the same administrative domain hence they can share the same security mechanisms
- in case of optimal routing, the *Home Agent* may be not included in the optimal routing path: each sending terminal should be able to authenticate the *binding update* messages; this is obviously impossible if a *Public Key Infrastructure* able to guarantee a neutral procedure is not available.