

TUT Public Access Architecture

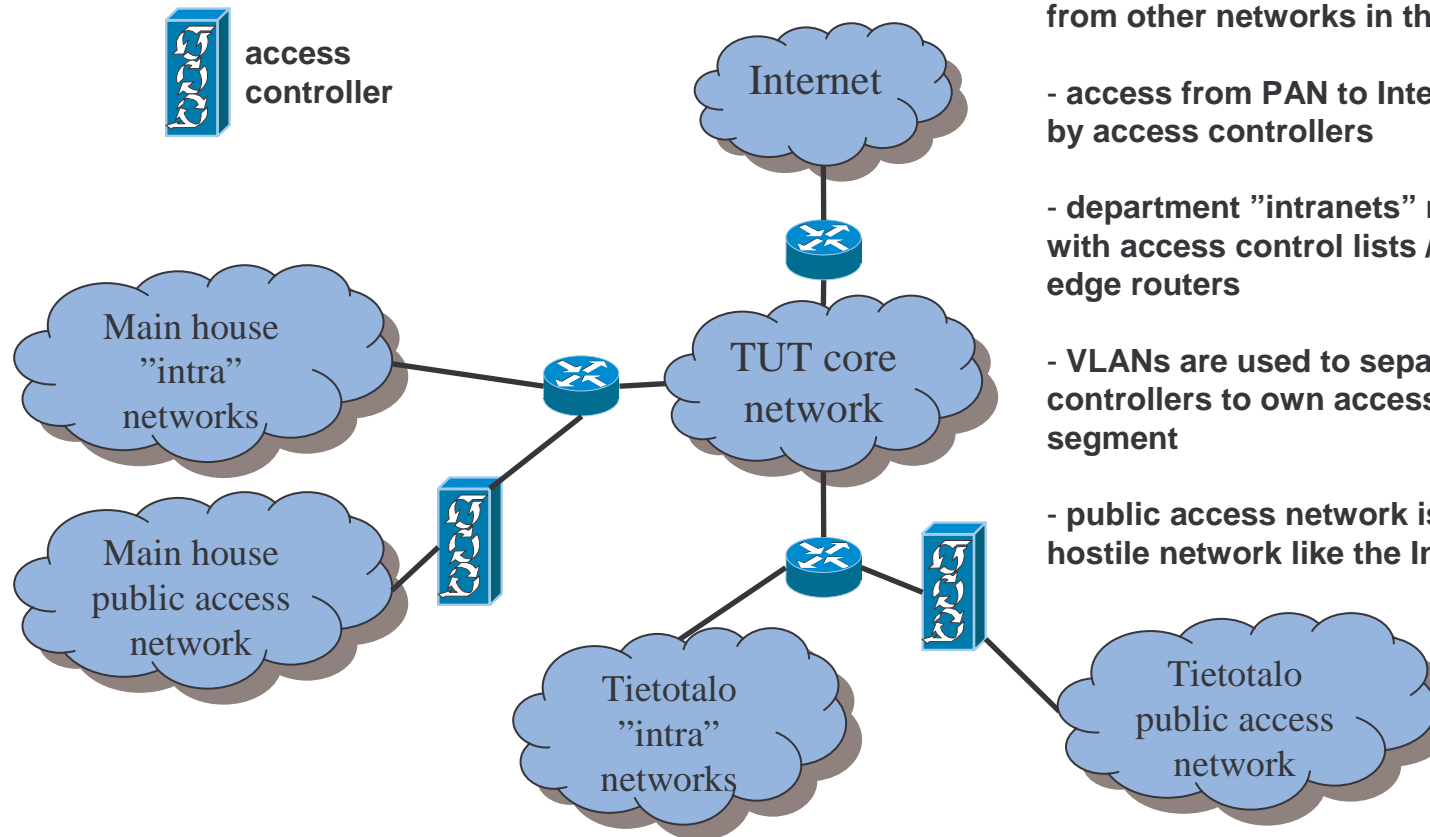
Karri Huhtanen <karrih@cs.tut.fi>

Tampere University of Technology
Institute of Communications Engineering

Architecture Design Principles

- Sufficient Security
 - for employees strongly secured access to department network
 - for students basic authentication and secured limited services
 - for guests an access controlled by host
 - for guests and roaming users ability to use VPN to secure their connection to home network
- Flexibility, Upgradeability, Scalability
 - the architecture should enable introduction of new services, network elements and upgrades flexibly
 - the architecture should not limit the scalability and growth of the network
- Interoperability, Openness, Standards
 - the architecture must support both commercial and non-commercial network elements via standard interfaces
 - open standards and interfaces are preferred
 - closed, proprietary standards and solutions should be avoided
- Usability
 - the basic access should not require any specific client software, hardware or operating system from the user terminal

Network structure



- public access networks (PAN) isolated from other networks in the edge routers

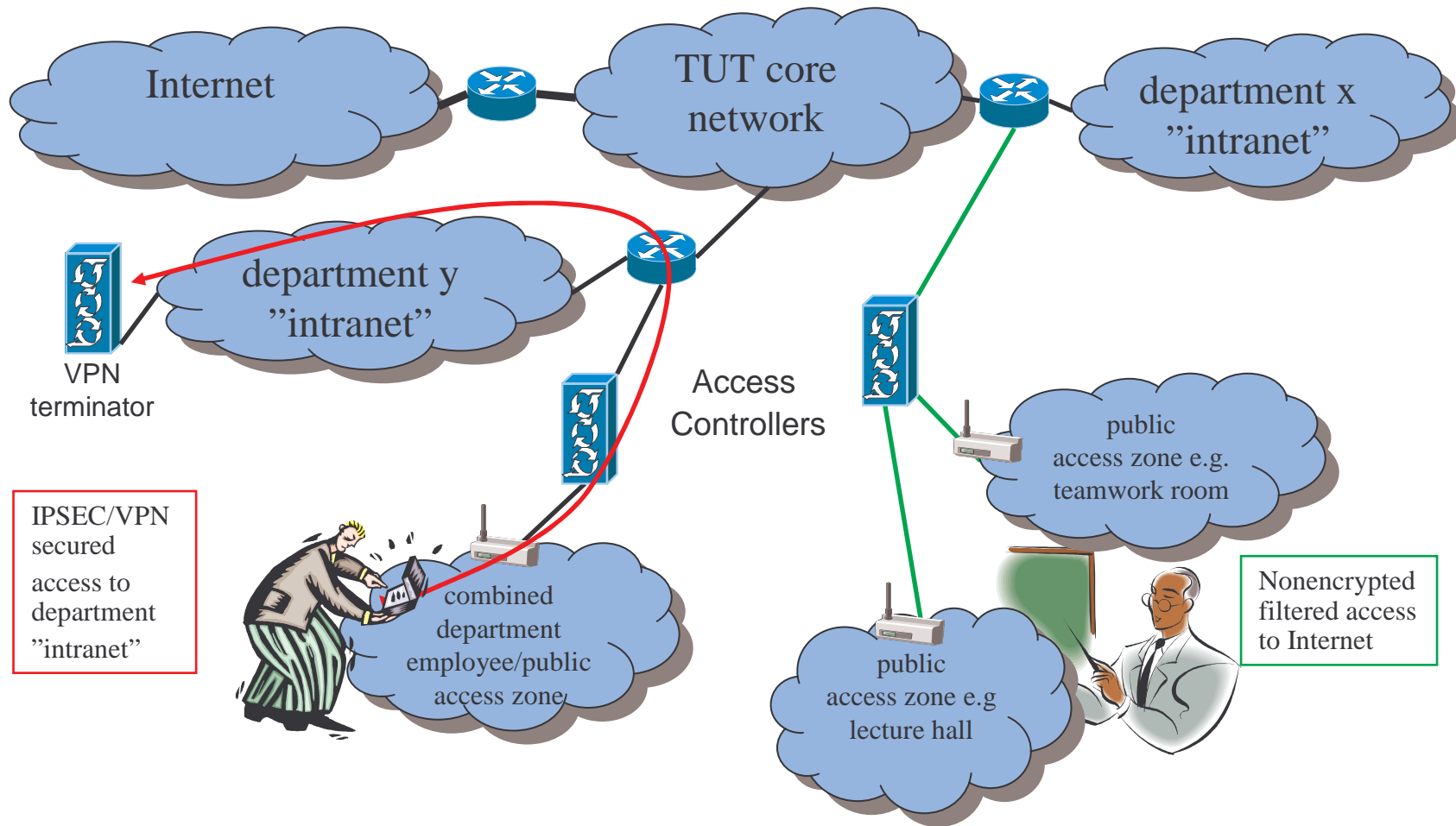
- access from PAN to Internet controlled by access controllers

- department "intranets" may be protected with access control lists / filters in the edge routers

- VLANs are used to separate access controllers to own access controller segment

- public access network is considered a hostile network like the Internet

Network elements



Four ways to access network 1/2

- Student Access:
 - student enters access zone, terminal receives public IP address
 - student starts WWW browser and tries to retrieve WWW page, access controller diverts the request to the SSL protected authentication page
 - student enters his authentication information (username@domain) and password, access controller verifies authentication from roaming proxy or other authentication server
 - student gains possibly limited access to the network
 - if the terminal does not respond to certain number of subsequent pings, it is considered logged out and new authentication is required
- Employee Access
 - employee enters access zone, terminal receives public IP address
 - employee initiates VPN connection to a known VPN terminator and authenticates via means available to VPN solution used
 - employee now gains the secured full access to department "intranet" and possibly also virtual IP which is from trusted network
 - chosen VPN solution may be configured to decide when the user has logged out from the access zone or the employee may logout by terminating VPN connection.

Four ways to access network 2/2

- Guest Access
 - guest enters access zone
 - guest starts WWW browser, on the authentication page there's link and instructions for guest access
 - guest enters guest information on the registration page and receives guest account and generated password
 - the host or some other authorized person approves guest registration and selects the account validity time
 - guest gains access to network with the guest account
 - the rest is similar to student access with the exception of the access revocation when the validity time ends
- Roaming Access
 - roaming user enters access zone
 - roaming user starts WWW browser, access controller captures WWW request and presents authentication page
 - roaming user enters his authentication information (username@domain) and password, access controller verifies authentication from roaming proxy
 - roaming user gains access to the network
 - the roaming user may now use the network like the student or initiate own VPN connection
 - if the terminal does not respond to certain number of subsequent pings, it is considered logged out and new authentication is required

The present status and the future possibilities

- Present status
 - PAC software and device ready, piloting and testing started in Tietotalo, TUT
 - Student access available via pilot before the end of January 2003
 - Employee access under work, evaluation of VPN software starting
 - Combined employee – student –access available as a pilot before the end of February 2003
 - Roaming proxy and roaming tested between WirLab and TUT, looking for other interested Funet organizations
- Future possibilities
 - guest and roaming access
 - Public Access Roaming between Funet organizations
 - Access to PAC as a service and network research and development platform
 - e.g. location dependent services/portal, Mobile-IP, IPv6, seamless roaming, traffic shaping, intrusion detection system etc.
 - PAC and Roaming Proxy software/device "products"
 - Releasing the "product" source code as open source
 - Introduction of new authentication mechanisms