Accessing Network File System (NFS) from Linux* Laptop

Gregory Touretsky

Senior Systems Engineer

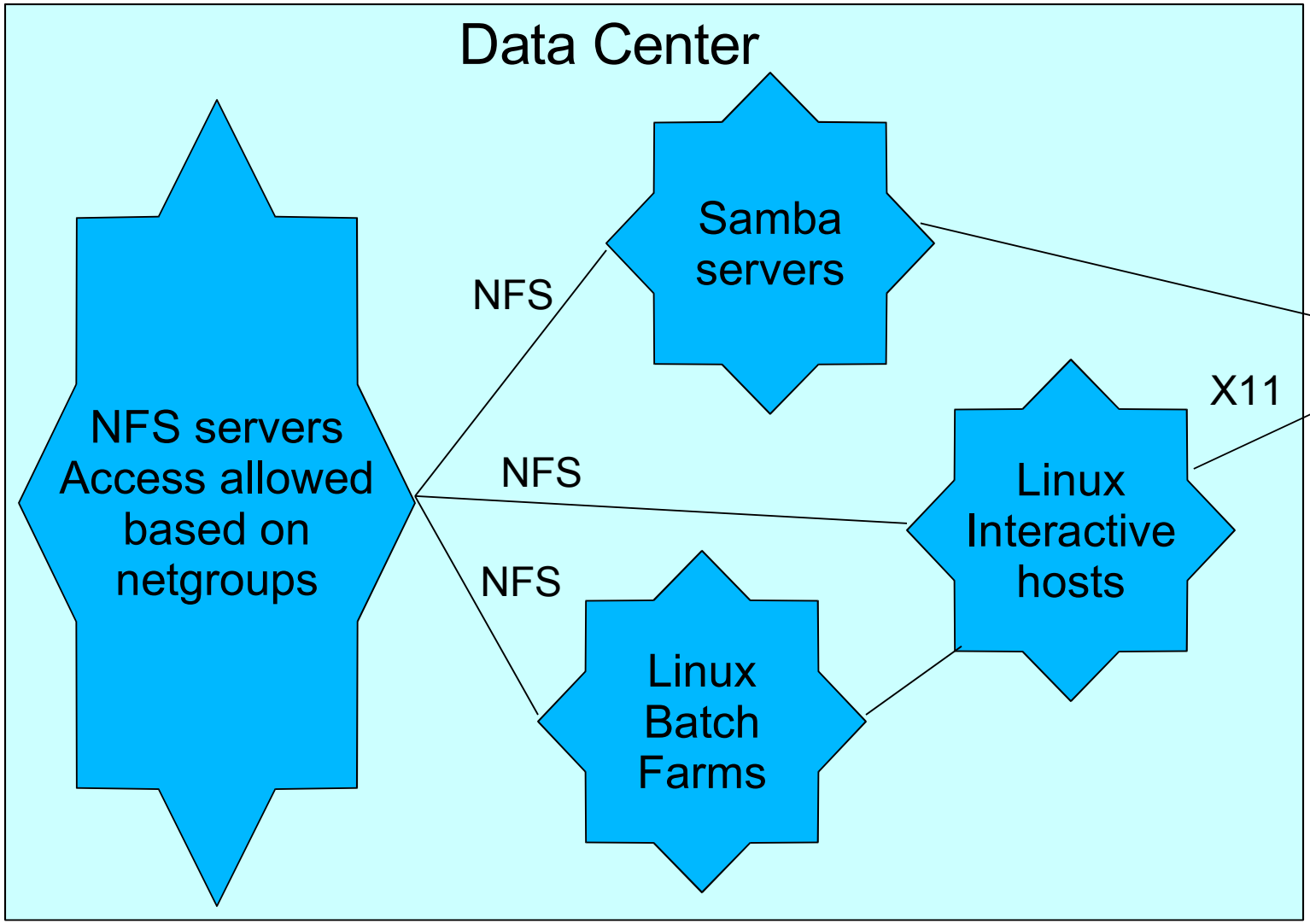
Intel Corporation

gregory.touretsky@intel.com

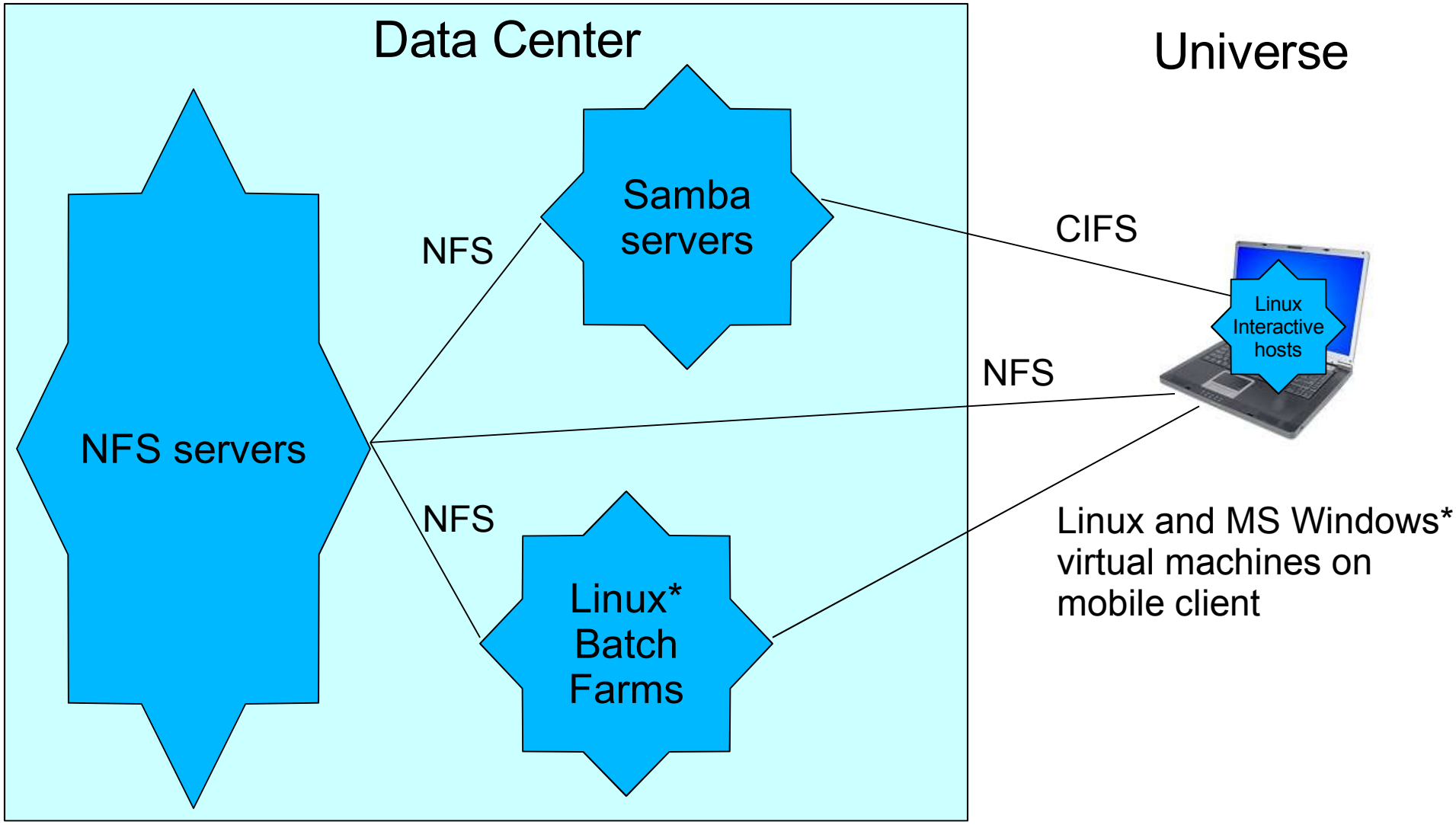
Intel's Engineering Environment

- Around 70 design centers worldwide
- Hardware/Software development, mostly Unix*-based
  - Large design projects span multiple sites
- Large farms of data-less Linux* compute servers used for batch and interactive jobs
- NFS is used for data sharing within data centers

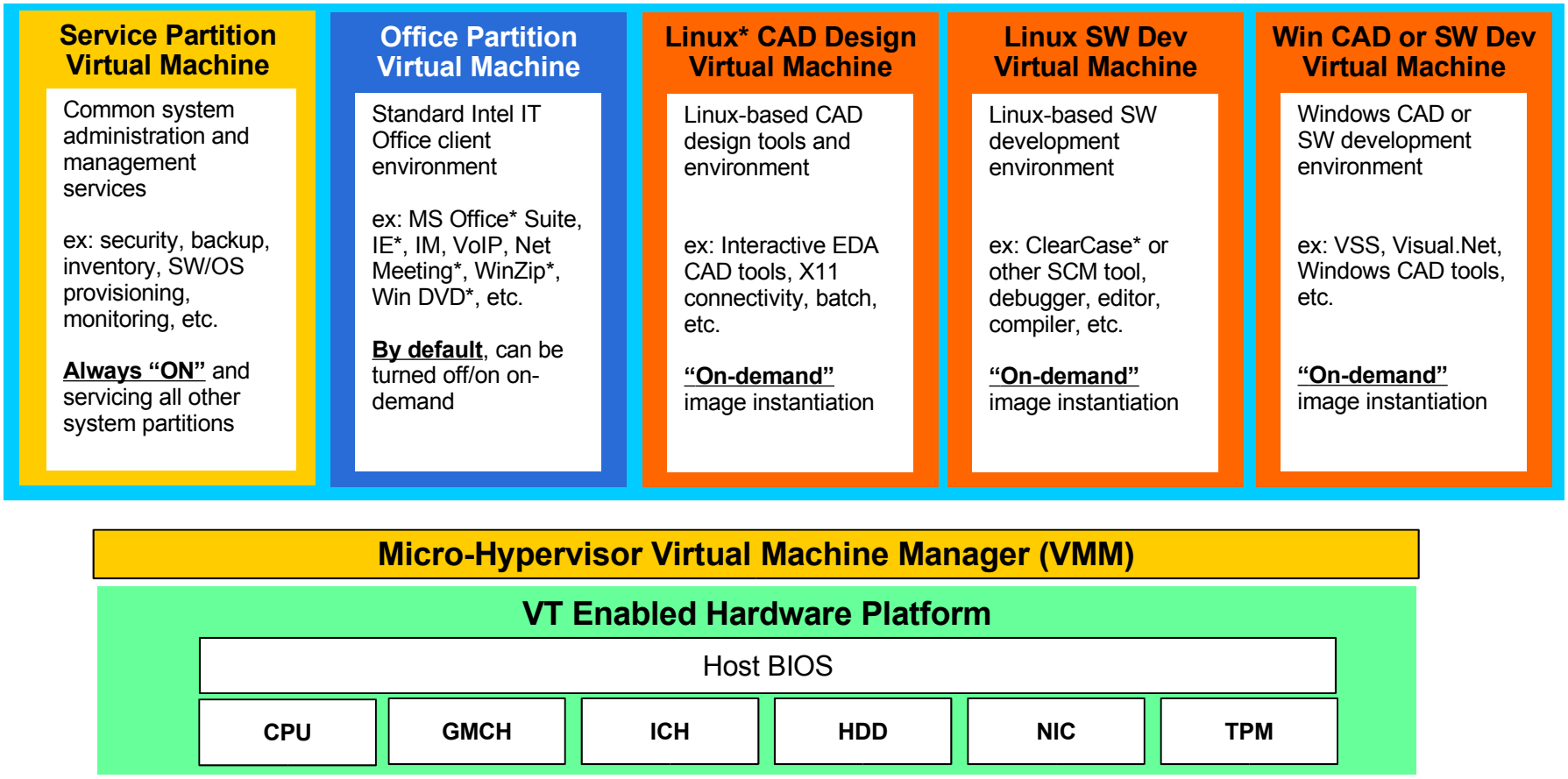
Typical Intel Design Center Environment



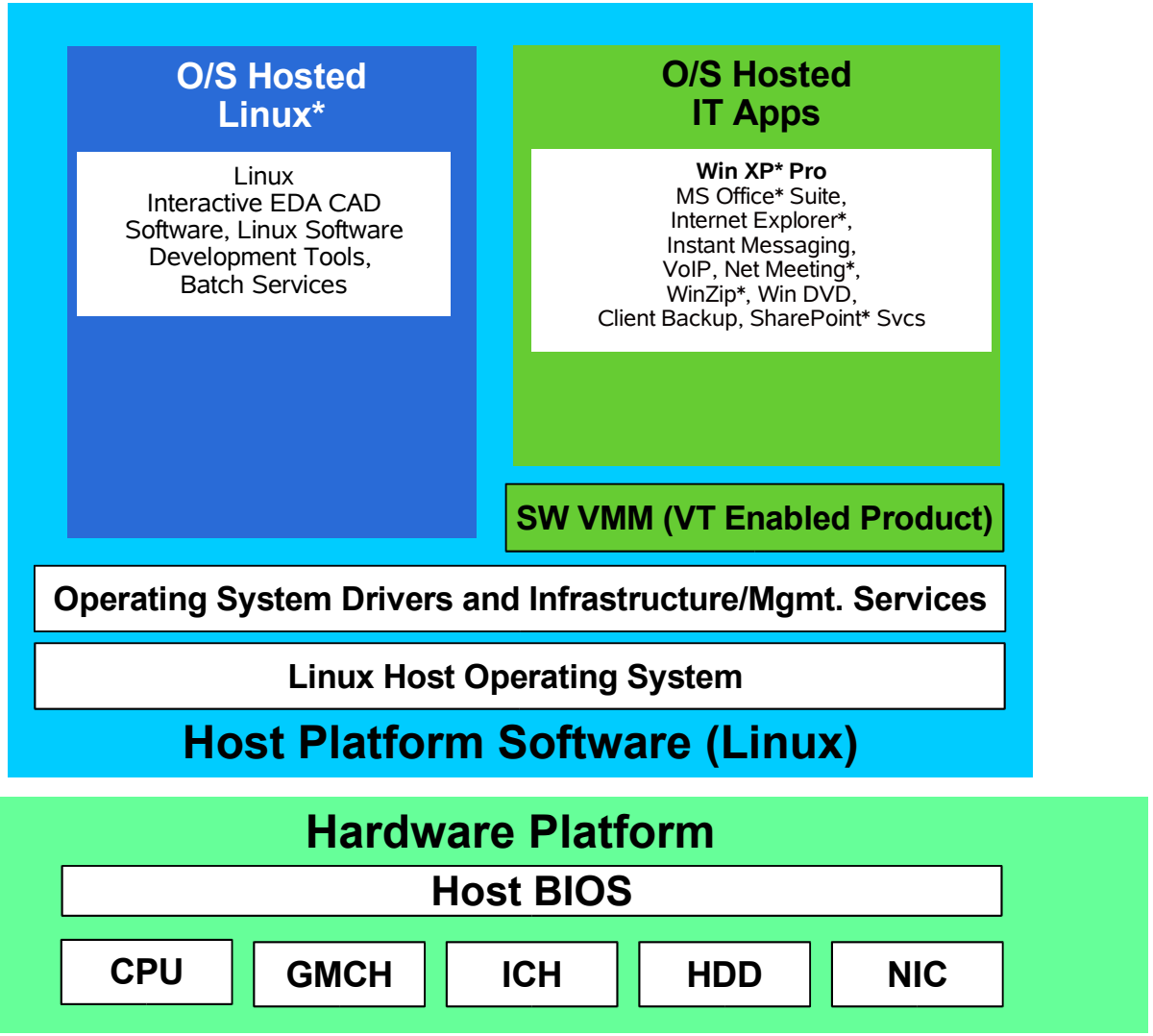
Typical Intel Design Center Environment: Future



2007 Unified Client Environment



2005 Unified Client Environment



Challenge: Secure NFS Access from Roaming Linux* Client

- Different types of connectivity:
  - Office LAN
  - Conference room WLAN
  - Home/public Internet via VPN
  - Remote site over WAN
  - Future: multiple Linux virtual machines from the same host with different security levels
- Can't rely on the existing NFSv3 security (IP-based netgroups)

Examined Options

Solution	Pros	Cons
NFSv4	· Kerberos support · Access Control Lists (ACLs) · Delegation and other WAN goodies	· Might not be mature enough · Lack of vendor support · Some features are not supported yet
NFSv3 + Kerberos	· Re-use existing infrastructure	· No support by all vendors · No support for ACLs, WAN
NFSv3 + netgroups	· Use existing exports restriction model -add “mobile-client” netgroup	· DNS and netgroups caching on file servers

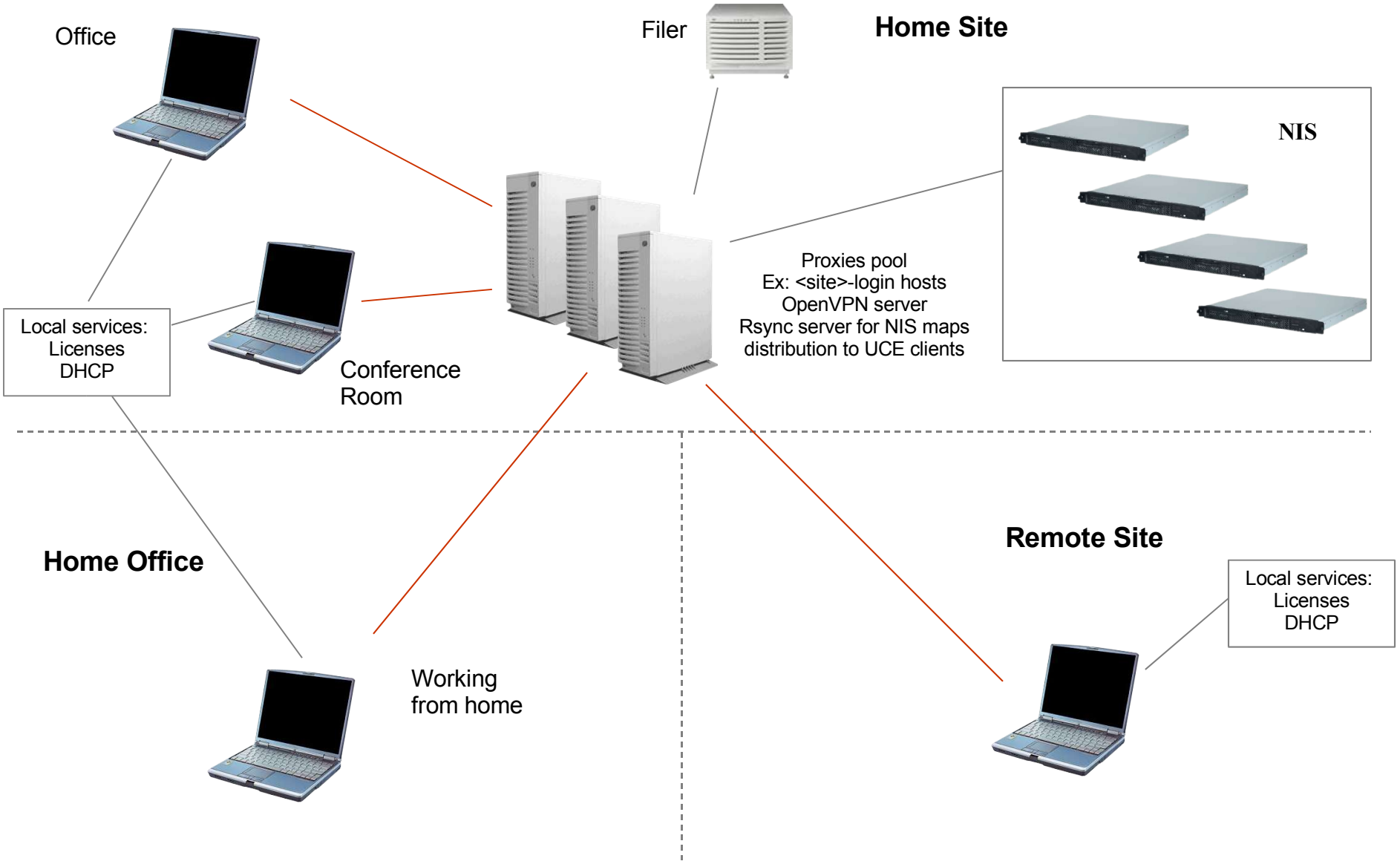
Examined Options (Continued)

Solution	Pros	Cons
NFSv3 over SSH tunnel		· Performance · Scalability · Support
NFSv3 over OpenVPN	· Transparent for roaming clients, tunnel survive client IP change · Certificates for authentication	· Performance · Extra IP addressees · VPN tunnel endpoint system
Smbmount through Samba		· Performance · Lack of full Unix semantics

Chosen Directions

- Short term
  - NFSv3 over OpenVPN tunnel
- Long term
  - NFSv4
    - Lots of integration will be required
    - OS vendors support is crucial

NFS over OpenVPN architecture



NFS over OpenVPN: Best Known Methods

- Automounter maps are cached on clients - updated hourly via rsync from the proxy
- Routing table on clients updated every time new NFS server appears on automounter map
- Several OpenVPN processes run on the proxy – for better performance
- Several OpenVPN servers share single DNS RR alias for load balancing and redundancy
- Certificates management/distribution mechanism should be defined

Next Steps

- Deploy certificates management solution for OpenSSL authentication
- Approach NFSv4 deployment towards multi-partitioned systems
  - Identification, Authentication integration
  - Automounter support
  - Backward compatibility – old NFS servers? Mixed security mode (v3/v4) for new servers
  - Vendors support
  - Performance
- Define secure file system sharing solution between different VMs within single client