

KCSIRT- the CERT for Kennisnet

Don Stikvoort, *on behalf of* nl.tree
23 January 2003

Kennisnet

Kennisnet =

- **the Dutch national network for all schools except ...**
 - ... for the academic, research and higher education community, which is served by SURFnet (and CERT-NL)**
- **conservative constituency size estimates:**
 - > **10,000+ schools**
 - > **100,000+ workstations**
 - > **1,000,000+ users**
- **central funding until end of 2003, but *no subsidizing* of nl.tree**

Kennisnet – the history

- ***August 1997***: ministry of education issues CfP
- ***August 1998***: consortium of Dutch CTV companies and Enertel selected
- ***October 1998***: start pilot connecting 400 schools
- ***November 1999***: nl.tree main contractor, CTVs & Enertel subcontractors
- ***November 1999***: ministry of education signs contract for 12,000 connections plus services
- ***Mid 2002***: 12,000 schools connected !!
- ***December 2003***: contract ends, but Kennisnet will continue (new elements: decentral funding and competition)

Kennisnet – the network

Internet connection

- > AMSIX (national peerings) :: 155M
- > Level3 (international) :: 155M

Firewall & Serverpark

- > SUN & IPlanet
- > 1M mail users ...

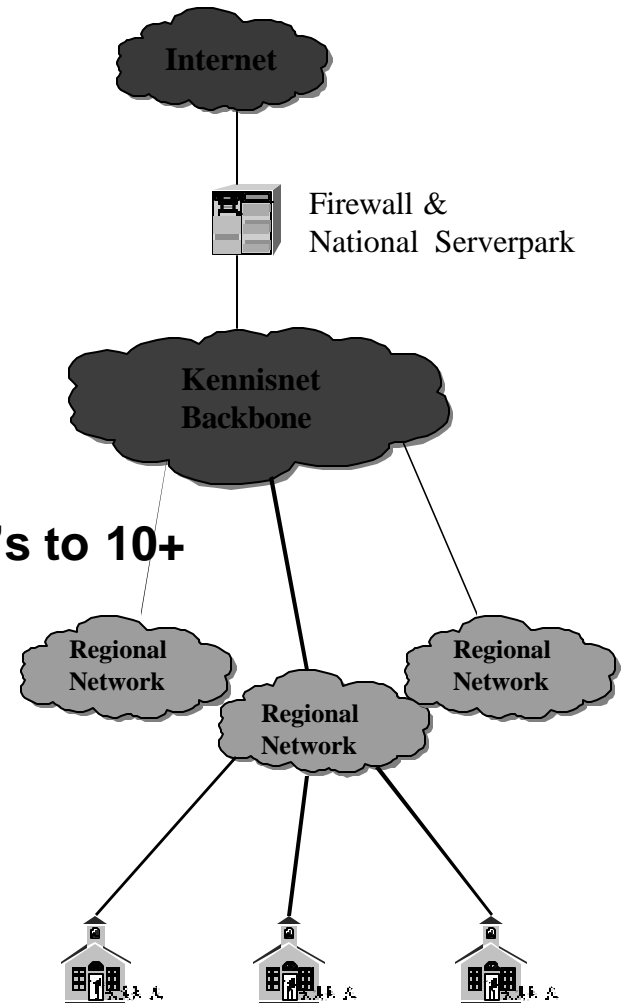
Kennisnet Backbone

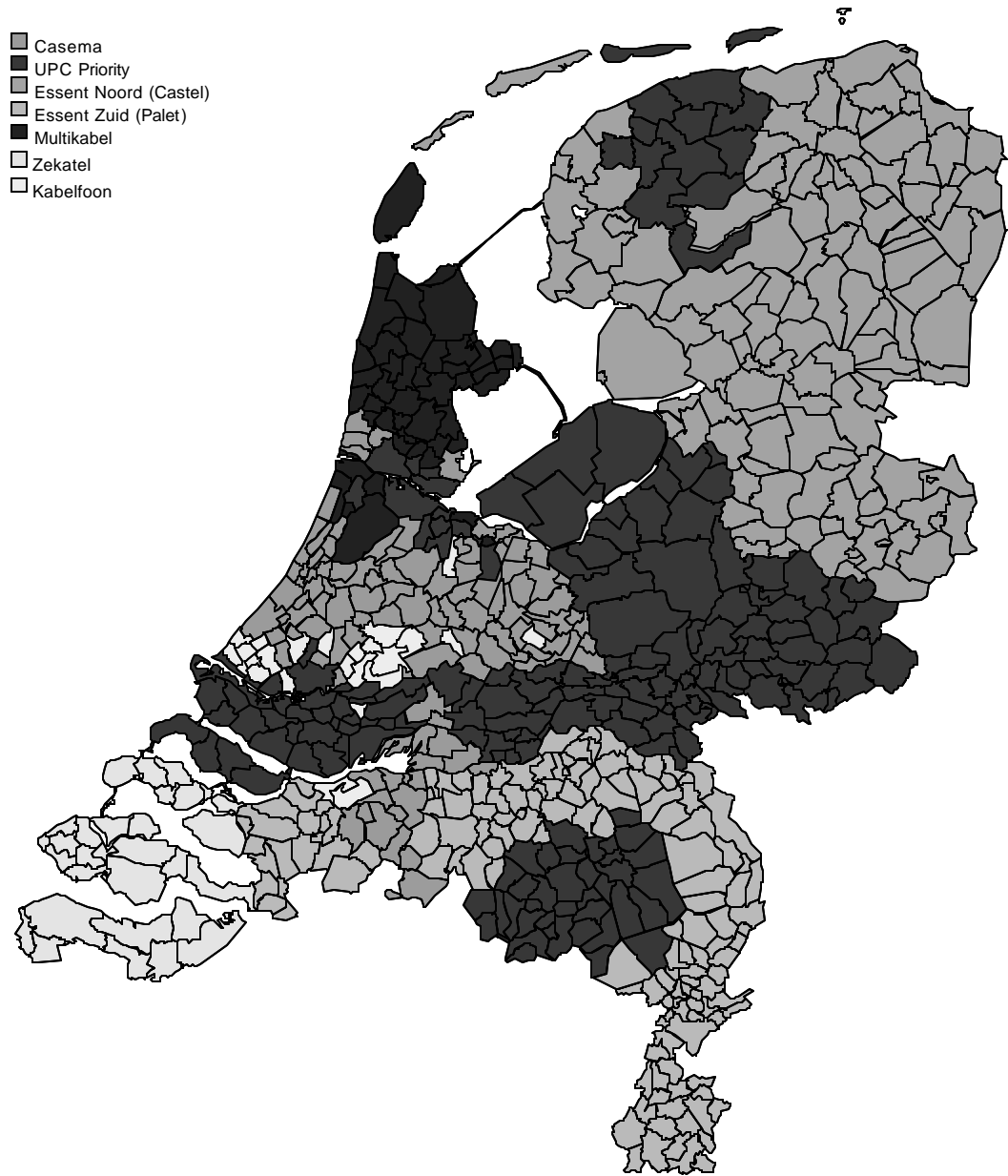
- > 4-hub redundant ATM network with PVC's to 10+ regional networks :: 1G total (sep 2002)
- > Operated by Enertel

Regional Networks

- > CTV networks (Essent, Casema, UPC ..)
- > Most schools coax connected
:: 256k-4M asymmetric
- > Big schools by I.I. or fiber :: 2-155M sym
- > Remote locations by ISDN*N or satellite

Traffic: 0.5G doubling each year





Kennisnet – the services

- open interschool connectivity
 - secured Internet connectivity
 - > Now: per-school filterrules
 - > Future: open firewall and *local* security
 - webhosting & co-location service
 - e-mail & webmail
 - VPNs for schools or schoolclusters
 - remote access from anywhere (new)
 - user community services (SIGs, training)
 - KCSIRT – the CERT for Kennisnet
- middleware: LDAP directory, proxyserver, DHCP, DNS

KCSIRT – timeline

- > 1 June 2000 handling of abuse@ , security@ and phone (through Kennisnet servicedesk)
- 2001: ISO certification of network management & servicedesk, including KCSIRT – advantages mainly in terms of systematic procedural approach
- 2002: application of security management to Kennisnet organisation & product – KCSIRT embedded in security organisation
- November 2002: established relation with Dutch government CERT-RO
- 18 Dec 2002: accreditation by TI
- Jan/Feb 2003: working with CERT-NL (Jacques Schuurman) on FIRST membership

KCSIRT – outline

- **see www.ti.terena.nl (also restricted website) ...**
 - > **Servicedesk answers phone and relays to KCSIRT**
 - > **KCSIRT operates e-mail and request-tracker DB**
- **services:**
 - > **Incident coordination for network and schools**
 - > **Advisory service for network**
 - > **No structural advice for schools yet**
- **environment:**
 - > **Schools: “ICT coordinators” can call on KCSIRT**
 - > **Netherlands: peering with CERT-RO, CERT-NL, ...**
 - > **Dutch Police (following formal procedure)**
 - > **World: through TI and FIRST relationships**
- **organisation:**
 - > **Chair: Aad Hartevelde, head of networkmgmt**
 - > **Up to 2 FTE operational (embedded in NOC)**
 - > **On-call team of experts to deal with special issues**
 - > **Escalations via chair and nl.tree security officer**

KCSIRT – characteristics

- incidents mainly of abuse type (e.g. towards teachers),
- ##: less than one per day
- very little cracking *noticed* up to date
- Kennisnet still very closed from the Internet however (little port scanning activity...)
- cracking expertise of pupils increasing
- security expertise in K12 schools “variable”
- with growing awareness among pupils, lagging expertise within schools and increasing openness of Kennisnet, KCSIRT expects more work ...

Thank you for your attention !
Any questions ?