

SKA 2007-11-05

torbjorn.eklov@interlan.se

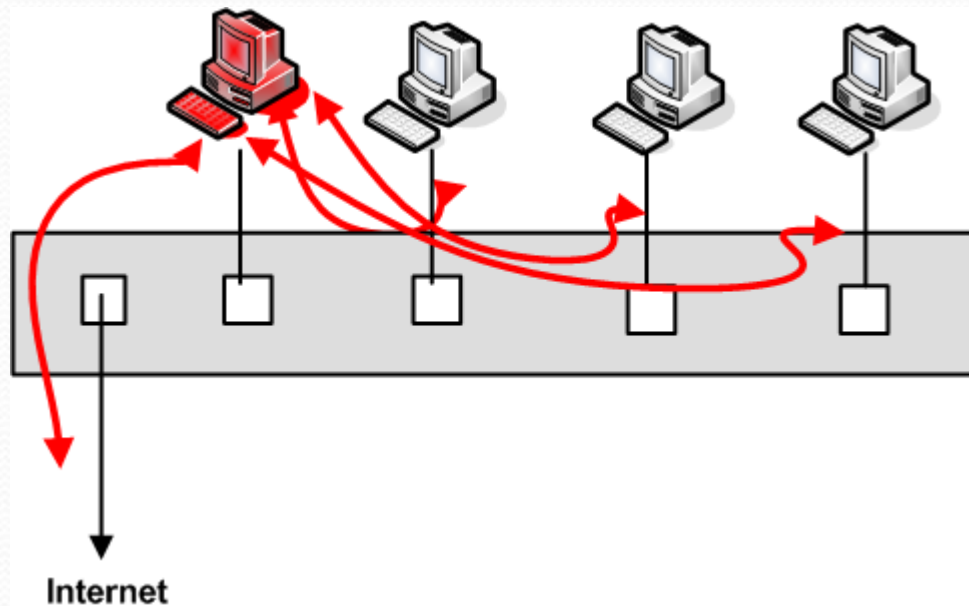
Svenska stadsnätföreningen

- Robusta nät
- Robusta noder
- SKA

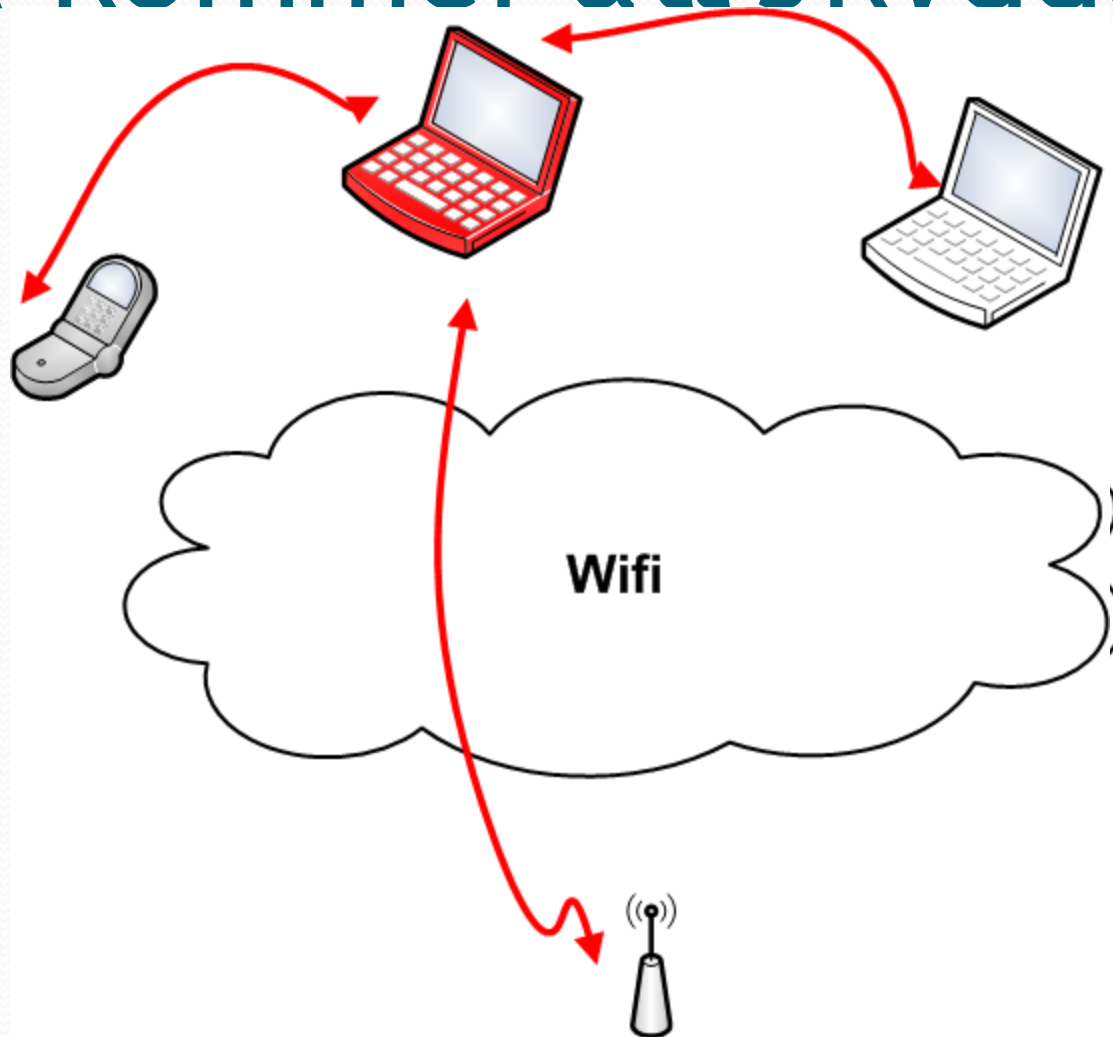
SKA - Säker KundAnslutning

- Varför startade SKA?
- Säkerställa att en bredbandsanslutning uppfyller vissa säkerhetskrav
- Det tänks för mycket på
QOS, Triple Play
Hög bandbredd
Låg kostnad

S KA skall skydda mot



S KA kommer att skvdda mot



Kan ni skydda er?

- Ni duktig och har/kör:
- Bredbandsrouter
- Mjukvarubrandvägg
- Antivirus
- Antispion och antiphishingprogram
- Kör Windows update
- Krypterar allt kommunikation
- NEJ!!!

ain

File View Configure Tools Help

NTLM AUTH CHALL SP00F RESET CHALL SP00F NTLM

Decoders Network Sniffer Cracker Traceroute CCDU Wireless

Passwords

- FTP (7)
- HTTP (63)
- IMAP (0)
- LDAP (0)
- POP3 (6)
- SMB (0)
- Telnet (0)
- VNC (0)
- TDS (0)
- SMTP (0)
- NNTP (0)
- DCE/RPC (0)
- MSKerb5-PreAuth (0)
- Radius-Keys (0)
- Radius-Users (0)
- ICQ (0)
- IKE-PSK (0)
- MySQL (0)
- SNMP (0)
- SIP (3)

Timestamp	POP3 server	Client	Username	Password	AuthType	Hash	challenge
16/09/2007 - 21:57:44	213.226.123.12	213.226.01.72	bill...	adadad	ClearText		
16/09/2007 - 21:59:00	213.				ClearText		
16/09/2007 - 21:59:00	81.2				ClearText		
16/09/2007 - 21:59:00	212.				ClearText		
16/09/2007 - 21:59:00	195.				ClearText		
16/09/2007 - 21:59:00	213.				ClearText		

POP3

Hosts APR Routing Passwords VoIP

<http://www.oxid.it>

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless

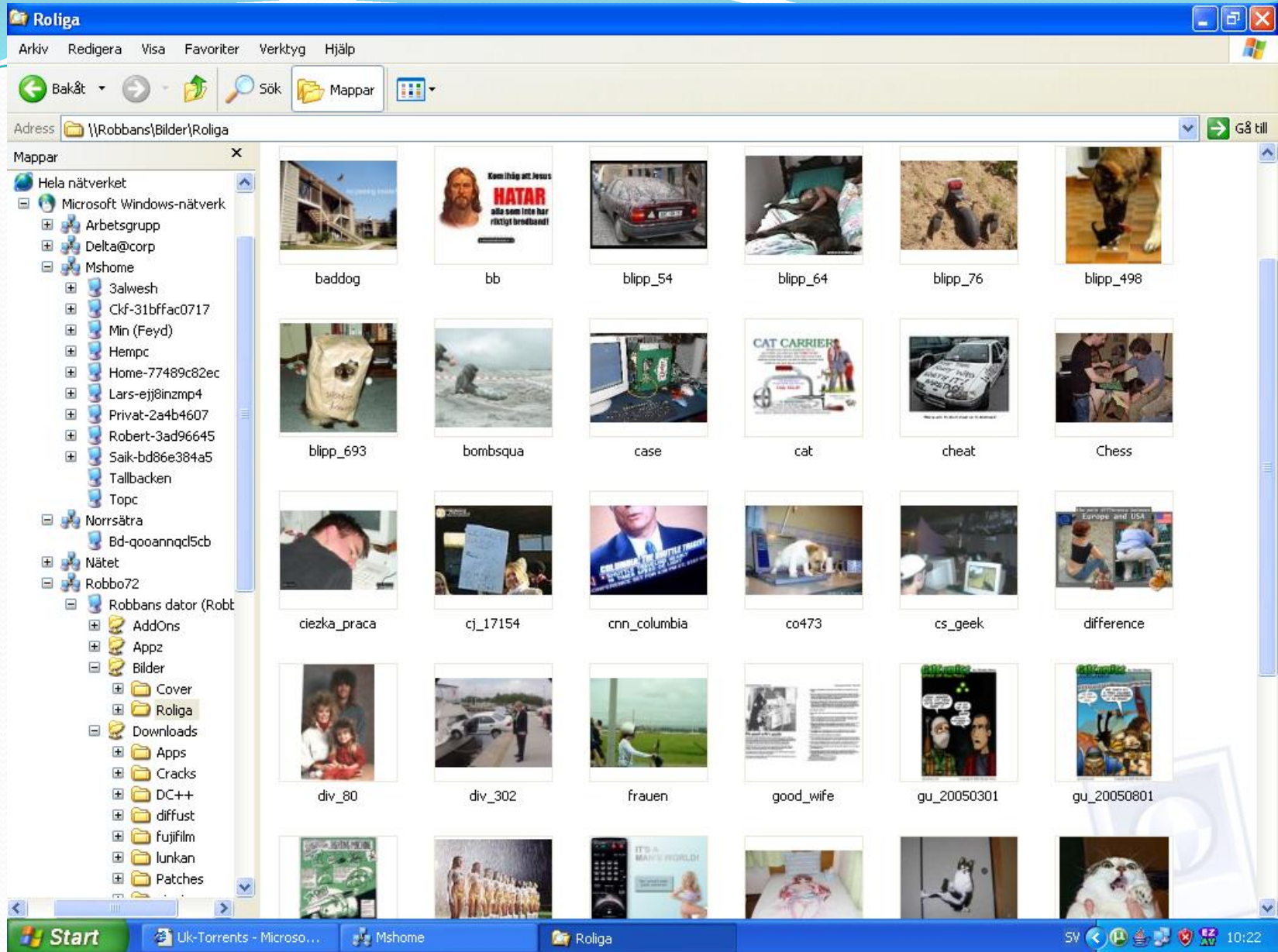
Passwords

Timestamp	HTTP server	Client	Username	Password	URL	AuthType	Domain
16/09/2007 - 21:58:02	85..					Cookie (GET)	
16/09/2007 - 21:58:02	85..					Cookie (GET)	
16/09/2007 - 21:58:04	81..					Basic (FORM-POST)	
16/09/2007 - 21:58:08	85..					Cookie (GET)	
16/09/2007 - 21:58:10	85..					Cookie (GET)	
16/09/2007 - 21:58:10	85..					Cookie (POST)	
16/09/2007 - 21:58:10	85..					Basic (FORM-POST)	
16/09/2007 - 21:58:10	85..					Cookie (GET)	
16/09/2007 - 21:58:11	195					it=&namn=DELT...	
16/09/2007 - 21:58:11	195					Basic (GET)	
16/09/2007 - 21:58:11	195					it=&namn=DELT...	
16/09/2007 - 21:58:15	83..					Basic (FORM-POST)	
16/09/2007 - 21:58:27	195					Basic (GET)	
16/09/2007 - 21:58:39	195					it=&namn=DELT...	
16/09/2007 - 21:58:39	195					Basic (GET)	
16/09/2007 - 21:58:40	85..					it=&namn=DELT...	
16/09/2007 - 21:59:01	195					Cookie (GET)	
16/09/2007 - 21:59:10	85..					itaco&ftgfilter=0&...	
16/09/2007 - 21:59:10	85..					Basic (GET)	
16/09/2007 - 21:59:30	195					Cookie (GET)	
16/09/2007 - 21:59:30	195					it=&namn=DELT...	
16/09/2007 - 21:59:30	195					Basic (GET)	
16/09/2007 - 21:59:40	85..					Cookie (GET)	
16/09/2007 - 21:59:55	195					itaco&ftgfilter=0&...	
16/09/2007 - 22:00:06	195					it=&namn=DELT...	
16/09/2007 - 22:00:07	195					Basic (GET)	
16/09/2007 - 22:00:10	85..					Cookie (GET)	
16/09/2007 - 22:00:20	195					itaco&ftgfilter=0&...	
16/09/2007 - 22:00:21	195					Basic (GET)	
16/09/2007 - 22:00:22	195					itaco&ftgfilter=0&...	
16/09/2007 - 22:00:40	85..					Basic (GET)	
16/09/2007 - 22:00:42	195					Cookie (GET)	
16/09/2007 - 22:00:42	195					it=&namn=DELT...	
16/09/2007 - 22:00:42	195					Basic (GET)	
16/09/2007 - 22:00:49	195					itaco&ftgfilter=0&...	
16/09/2007 - 22:00:58	195					Basic (GET)	
16/09/2007 - 22:00:58	195					it=&namn=DELT...	
16/09/2007 - 22:01:10	85..					Basic (GET)	
16/09/2007 - 22:01:22	195					Cookie (GET)	
16/09/2007 - 22:01:30	195					itaco&ftgfilter=0&...	
16/09/2007 - 22:01:34	195					Basic (GET)	
16/09/2007 - 22:01:38	195					itaco&ftgfilter=0&...	
16/09/2007 - 22:01:40	85..					Basic (GET)	
16/09/2007 - 22:02:02	217					Cookie (GET)	
16/09/2007 - 22:02:02	195					Basic (FORM-POST)	
16/09/2007 - 22:02:06	195					Basic (GET)	
16/09/2007 - 22:02:10	85..					itaco&ftgfilter=0&...	
16/09/2007 - 22:02:11	89..					Cookie (GET)	
16/09/2007 - 22:02:12	89..					Cookie (GET)	
16/09/2007 - 22:02:12	89..					Cookie (GET)	
16/09/2007 - 22:02:13	89..					Cookie (GET)	
16/09/2007 - 22:02:13	89..					Cookie (GET)	
16/09/2007 - 22:02:14	89..					Cookie (GET)	
16/09/2007 - 22:02:14	89..					Cookie (GET)	
16/09/2007 - 22:02:15	89..					Cookie (GET)	
16/09/2007 - 22:02:15	89..					Cookie (GET)	
16/09/2007 - 22:02:15	89..					Cookie (GET)	
16/09/2007 - 22:02:16	85..					Cookie (GET)	

HTTP

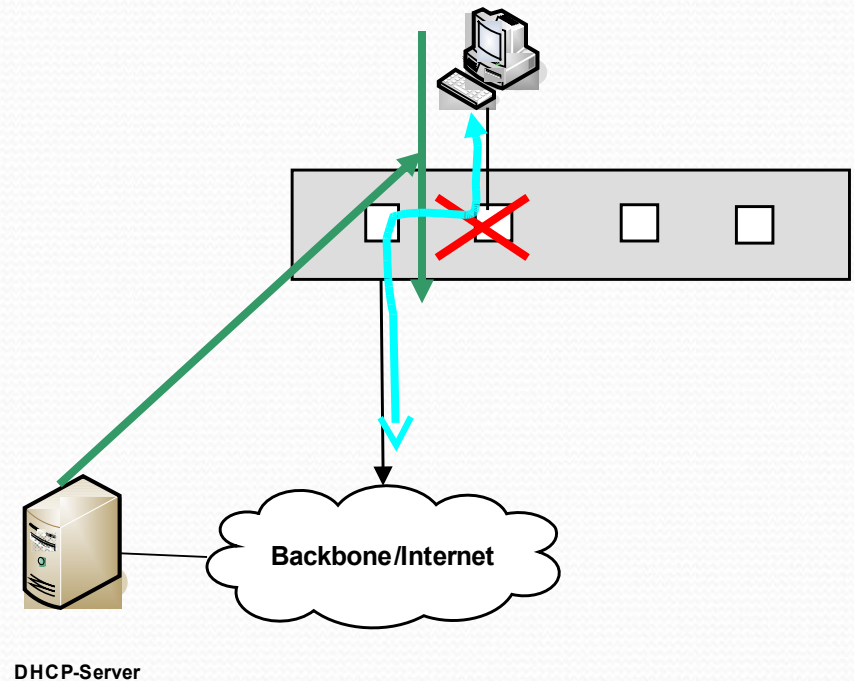
Hosts APR Routing Passwords VoIP

http://www.oxid.it



Vilka krav ställer vi?

- Kundport default stängd
- En DHCP-förfrågan går igenom
- DHCP-servern tilldelar en IP-adress
- Porten öppnas för tilldelad MAC och IP-adress för IP och ARP-protokollet
- DHCP/syslog-servern loggar MAC, IP-adress, switch och port



Filtrering

- Bör filtrera bort all M icrosoft-trafik mellan kunder
 - ~ D e tror att de delar ut bilderna till farsan men hela världen kan se dem...
- UPnP ska filtreras
 - ~ U tskrifter som hamnar hos grannen
- Falska IPv6-routrar
 - M er och mer V ista med IPv6 igång default

S tarten 2005-11

- PTS och SSNf finansierar
- Testar och godkänner hårdvara
- Lite utbildningar

Status för ett år sedan

- Kurser, föredrag och testar utrustning
- Större och större kännedom om projektet
- Många organisationer/företag använder SKA som krav i upphandlingar

Status idag

- Fem stycken godkända tillverkare, 4 st till ska testas inom kort.
- Nästan alla känner till SK A
- Vilka ställer SK A -kraven vid upphandling?



S KA - fas två

- Fas ett, vi testar och godkänner utrustning
- Fas två, vi ska testa och godkänna hela nät
- .SE går in och delfinansierar fas två
- Stora och små är intresserade, även utomlands