EDUROAM, GÄSTNÄT OCH IDENTITETER

TL;DR

Många lärosäten tvingas driva komplexa lösningar för trådlösa nät för att hantera olika typer av identiteter som ska ha tillgång till resurser på campus. Ett nytt projekt inom GEANT som heter geteduroam kan bli en del av en ny och enklare hantering av identiteter för trådlösa nät som också kan innefatta en bättre hantering av gästanvändare på campus.

CAMPUS VS WIFI

När de trådlösa näten började dyka upp på campus för många år sedan var wifi en lyx som var förbehållen de som hade råd att ha en laptop. Driften av wifi-nätet var inte kritiskt och kunde skötas ”med vänsterhanden”. I och med att laptops blev vanliga och tom vanligare än ”fast dator” blev wifi-nätet i vissa avseenden viktigare än det fasta nätet. Nästa steg i utvecklingen var och är naturligtvis mobilens framsteg som den viktigaste metoden för Internet-access. Detta har paradoxalt gjort att betydelsen av wifi-nätet minskat på campus – ffa bland studenter som lika gärna kan använda sin mobil-data för ”surf”, speciellt om det upplevs som det minsta krångligt att ansluta till det trådlösa nätet på campus.

GÄSTER PÅ CAMPUS-NÄTET

Det finns fler användare av campus-nätet än lärare, forskare och studenter. Det finns många olika typer av användare som behöver access till campus-nätet: gästforskare, gästföreläsare, folk som jobbar på kaféer och kiosker på campus etc etc. Många lärosäten har idag processer, lösningar och rutiner för att hantera gästaccess till campus-wifi – mer eller mindre smidiga sådana. Behovet av identifiering av en gäst är ofta mycket låg. Det räcker ofta med att ha någon kontaktväg till användaren – epost, telefon eller liknande.

En inloggning via facebook eller google skulle säkert upplevas som tillräcklig för enklare nätaccess på campus. Det finns gott om lösningar på marknaden för att åstadkomma just detta. Emellertid finns det kanske inget egenvärde av att alla lärosäten bedriver sin egen process för att hantera gästanvändare!

EDUROAM

Under 2005 började eduroam dyka upp på Svenska universitet och tillväxten har gått med raketfart. Undersökningar har visat att eduroam idag är världens 5e största trådlösa nät. Jag tänker inte beskriva eduroam här – det finns gott om texter på nätet som beskriver hur eduroam funkar. Det jag vill fokusera på är varför eduroam har ett värde. De två viktigaste skälen till att eduroam har ett stort värde:

- eduroam ger en säker förbindelse till det trådlösa nätet
- eduroam ger en fantastisk användarupplevelse: när det finns eduroam så funkar det bara

Låt oss bena upp detta lite...

VARFÖR SPELAR WIFI-KAPACITET ROLL NÄR DET FINNS 4G?

Därför att plötsligt tar data-potten slut. Ofta tar potten slut när inlämningsuppgiften ska in. Studenter och andra använder wifi som offload-mekanism. Man ansluter till wifi när det behövs och då är det ofta viktigt att det funkar och att det är enkelt. Användarupplevelsen är eduroams styrka: genom att göra anslutningen till nätet så enkel att användaren inte ens är medveten om att det händer, kommer användaren att få tillgång till bästa möjliga kapacitet. Användarupplevelsen för att sätta upp eduroam på en ny telefon/platta/dator är dock inte alls lika enkel...

ÄR INTE SÄKERHETEN I SIM-KORTET BÄTTRE ÄN EDUROAM?

Jo ofta är detta tyvärr sant. Säkerheten i eduroam är *potentiellt* väldigt hög men om man använder samma lösenord i eduroam som man använder till sitt AD eller SWAMID-inloggningen så är det tyvärr ganska enkelt att samla in lösenord för alla anställda på

universitetet genom att lägga ut en falsk accesspunkt som annonserar nätet ”eduroam”, plockar ut lösenordet och kopplar ner användaren. Vi vet att denna typ av attacker förekommer.

Genom att använda bättre och säkrare teknologi (tex EAP-TLS) är det enkelt att omöjliggöra denna attack men dessa teknologier är tyvärr komplexa och dyra att sköta.

EDU#FAIL?

Är eduroam en framgång? Om man ser till nätets täckning så är det onekligen en framgång. I Sverige finns eduroam på högskolor, flygplatser, busstationer, vissa pubar & hotellkedjor samt på bibliotek och öppenvård i Stockholm och på många andra platser. Var man än reser i världen så är det god chans att man hitta fungerande eduroam.

Å andra sidan är det inte enormt många användare som kör eduroam dagligen – högst ovetenskapliga diskussioner med kollegor i de andra Nordiska länderna pekar på mellan 10% och 20% av antalet möjliga användare som faktiskt nyttjar tjänsten eduroam.

Hur kommer det sig att så få använder eduroam?

Det finns säkert flera förklaringar men en av de viktigaste torde vara att det ofta är ganska svårt att sätta upp eduroam för en vanlig användare. I mobila platformar (iOS, Android) har användarna kommit att förvänta sig enklare onboarding-mekanismer än vad konfiguration av eduroam ofta innebär. Denna komplexitet beror i sig på en kombination av de tekniska val som många lärosäten har gjort (ibland som en konsekvens av att man velat skydda sig mot fejk-eduroam-attacken ovan) tillsammans med en viss ”grundnivå” av komplexitet som är inbyggt i eduroam.

Personer som reser mycket är villiga att acceptera ”smärtan” av att konfigurera eduroam eftersom tjänsten är så värdefull för en forskare/student på resande fot.

Om vi vill att eduroam ska vara användbar för många fler användare så behöver vi ta oss från 10-20% till 80-90% av anslutna användare. Detta kräver ett nytänkande kring hur vi provisionerar användare och mobila enheter i eduroam så att vi gör det mycket enklare för användare att ansluta sig än idag.

PUTTING IT ALL TOGETHER: GETEDUROAM

På initiativ från SUNET diskuterar de Nordiska länderna och GEANT att genomföra ett utvecklingsprojekt med syfte att göra det mycket enklare för vanliga användare att ansluta sig till eduroam. Projektet har arbetsnamnet geteduroam och är tänkt att leverera en PoC (Proof of Concept) under 2017. Under 2018 är det tänkt att SUNET, NORDUnet och/eller GEANT skulle kunna etablera en tjänst baserat på projektet.

Tanken med geteduroam är att bygga en infrastruktur för EAP-TLS där användare identifieras med ”vanlig” webinloggning via eduGAIN – dvs den gemensamma internationella federationen av federationer där SWAMID ingår. Denna lösning skulle tom göra det möjligt för ett lärosäte att helt sluta göra egen hantering av identiteter och konfiguration för eduroam bara man har en fungerande IdP i SWAMID.

En av sidoeffekterna av geteduroam är att det skulle bli möjligt att även bygga ett gemensamt system för gästanvändare baserat på samma teknologi – istället för inloggning via eduGAIN/SWAMID gör man inloggning via google eller facebook. Ett sådant system skulle inte nödvändigtvis släppa in gästanvändare till *nätet* eduroam utan man kan tänka sig att koppla gästanvändare till ett lokalt gästnät på campus men i övrigt behöver det inte skilja speciellt mycket mellan att provisionera en eduroam-användare och att provisionera en gästanvändare (annat än hur länge man ger access).

För närvarande pågår arbetet med att definiera geteduroam som subtask till JRA3-T4 i GEANT-projektet där det finns gott om finansiering för att genomföra hela projektet samt erfarenhet av att bygga och etablera nya tjänster. Arbetet i GEANT-projektet är baserat på tillgång till resurser från högskolesektorn i EU och geteduroam kommer att behöva bemannas. Som vanligt utgår finansiering för tid och resor men dessutom innebär engagemang i GEANT-projekt intressanta utmaningar och ovärderliga kontakter för de som deltar.

Om någon är intresserad av att vara med & bidra till geteduroam så vore det väldigt kul att höra av er!

Skriven av

LEIF JOHANSSON

Blogs about past, present and future technology initiatives in the CTO-blog.