SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Sustavi za praćenje i vođenje procesa

SEMINARSKI RAD

RADIUS 802.1x

Maja Vlah

Zagreb, 06.2004.

Uvod

Bežične lokalne mreže se danas sve više koriste zbog slobode koju bežična komunikacija pruža i zbog sve manje cijene takve tehnologije. Međutim, jedan od najvećih problema takvih mreža su dakako siguronosni problemi. Premda IEEE 802.11 standard za bežične mreže definira protokole za autentifikaciju i šifriranje, pokazalo se da ovi protokoli imaju dosta mana, ostavljajući bežičnu komunikaciju otvorenu za više vrsta napada. Novi standardi, poput IEEE 802.1x, pokušavaju dati rješenja za ove slabosti.

Pregled 802.1x

IEEE 802.1x standard, kontrola pristupu mrežama temeljena na portovima, definira mehanizam za kontrolu pristupa mrežama temeljena na portovima koji koristi fizikalne karakteristike pristupa IEEE 802 LAN strukture. Pruža način autentifikacije i autorizacije korisnika priključenih na LAN port koji ima karakteristike od-točke-do-točke (point-to-point) veze. On omogućuje automatsku identifikaciju korisnika, centraliziranu autentifikaciju, upravljanje ključem i praćenje povezanosti na LAN. Također sprječava pristup portu u slučaju da autentifikacija i autorizacija ne uspiju.

802.1x specifikacija uključuje brojna obilježja posebno ciljana za podršku upotrebe kontrole pristupa portovima u IEEE 802.11 WLAN. Ovo uključuje mogućnost WLAN točka pristupa (AP) da distribuira ili pridobije informacije o globalnom ključu od/do priključenih stanica, putem EAPOL-Ključ poruke, nakon uspješne autentifikacije. 802.1x specifikacija djeluje na fizičkom portu OSI sloja 2.

IEEE 802.11 radna grupa je donijela 802.1x 2001. godine, kako bi povećala sigurnost originalnog 802.11 standarda (IEEE, 2001). 802.1x je namijenjen da pruži jaku autentifikaciju, kontrolu pristupa i upravljanje ključevima, i da omogući WLAN da se skalira, omogućujući autentifikaciju bežičnih korisnika.

802.1x je osnovan na postojećem autentifikacijskom protokolu poznatom kao EAP (Extensible Authentication Protocol) koji je opet nastavak PPP–a. EAP provodi autentifikacijski proces. On veže PPP protokol na fizički sloj, OSI Layer 1. EAP over LAN (EAPOL) je obuhvaćen 802 frame-om. 802.1x nije ograničen na neku spcifičnu mrežnu strukturu, već služi kao podloga za definiranje načina autentifikacije korisnika na fizičku mrežu, neovisno o podređenim mrežnim protokolima. Thus, 802.1x map EAP to the physical medium, bez obzira da li je u pitanju Ethernet, Token Ring ili WLAN. Također podržava višestruke autentifikacijske metode, uključujući token kartice, Kerberos, jednokratne zaporke, certifikate, i autentifikacija javnim ključem.

Potreba za kontrolom mreže «po-portu» (per-port)

Kako je port korisnička pristupna točka, to će biti logično mjesto da se kontrolira pristup korisnika. To je također logično mjesto da se primijeni pakiranje i filtriranje protokola. Stoga, kontroliranjem korisničke mrežne pristupne točke, korisnička mrežna okolina može niti prilagođena korisničkim potrebama.

Potreba za AAA

Mnoge organizacije su uložile u autentifikaciju, autorizaciju, i accounting (AAA) tehnologiju kako bi kontrolirali svojim korisnicima pristup mreži, tipično dial-in daljinski pristup ili pristup via firewall-a. 802.1x može iskoristiti postojeće AAA servere, tipično RADIUS server, kako bi pružili ove funkcije novim 802.1x klijentima.

802.1x mehanika

802.1x autentifikacija ima tri glavne komponente: klijenta, autentifikatora (ovdje AP) i autentifikacijskog server. Autentifikacijski server je obično RADIUS server, iako nije neophodno.

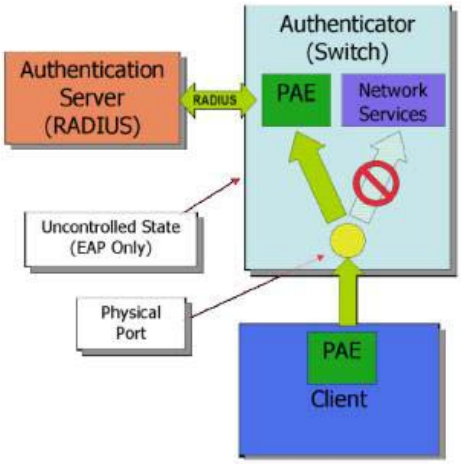


Figure 1 - Before Authentication

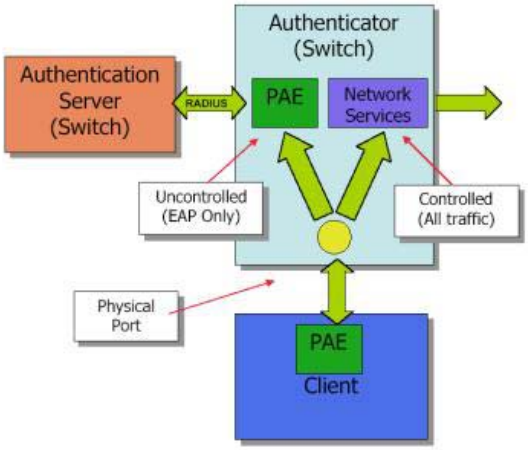


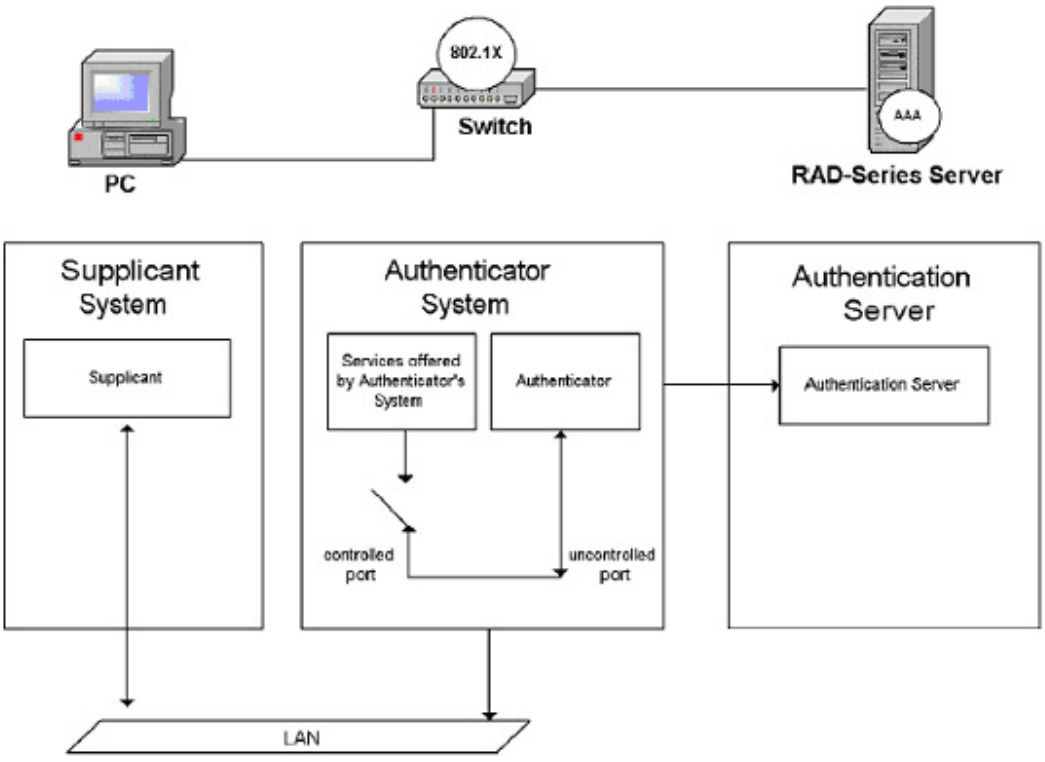
Figure 2 - After successful authentication

802.1x autentifikacija:

1. Klijent (suplicant) pošalje zahtjev za autentifikaciju AP – u. Autentifikacija se provodi EAP-om na link sloju (layer), što je neophodno zbog siguronosnih razloga. Ovaj sloj omogućuje tek toliko komunikacijskog protokola kako bi se autentificiralo ne dopuštajući klijentu nadozvoljeni pristup mreži.
2. AP odgovara zahtjevom da se klijent identificira, i blokira sav drugi promet, kao što su HTTP, DHCP i POP3 paketi, sve dok AP ne provjeri klijentov identitet koristeći autentifikacijski server.
3. Kiljent šalje odgovor, koji sadržava identitet, autentifikacijskom serveru. (Tip identifikacije nije definiran u protokolu, već je ostavljen proizvođačima tako da autentifikacija može biti u bilo kojem obliku).
4. authentication server dobija zahtjev i, uz upotrebu odgovarajućih autentifikacijskih algoritama, provjerava klijentov identitet. Ako je klijenta moguće identificirati, šalje se potvrdna poruka AP-u, inače se šalje negirajuća poruka.

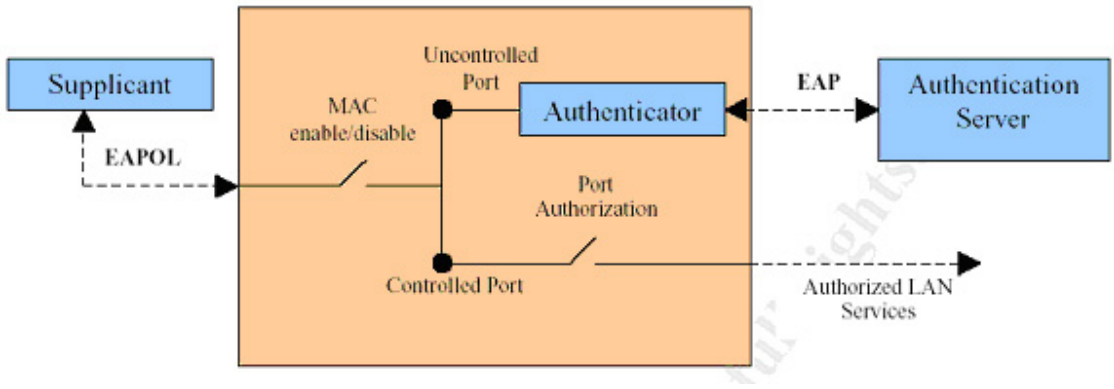
5. Ako autentifikacijski server prihvati klijenta, tada AP prebacuje klijentov port u autorizirano stanje i prosljeđuje dodatni promet.

Autentifikacijski proces se može ostvariti neovisno o IP adresama i imenu rezolucije, što ublažava moguće siguronosne rupe i minimizira vrijeme procesiranja. Brzo je, jednostavno, jeftino, i autentifikacija na link sloju je već podržana u PPP, IEEE 802 i većini drugih popularnih primjenjivih protokola. Izbjegavajući mrežni sloj (network layer) izbjegavaju se neke komplikacije. Autentifikator pakira EAP poruke u RADIUS pakete za RADIUS server.



EAP

The Extensible Authentication protokol (EAP) je metoda sprovođenja autentifikacijske konverzacije između korisnika i autentifikacijskog servera, poput EAP-TTLS. Specificirana je kao IETF RFC 2284. EAP je kompatibilan sa Ethernet-om, Token Ring-om, 802.11, i ostalim popularnim mrežnim protokolima. Intermediate devices poput AP-a i proxy servera ne učestvuju u razgovoru. Njihova uloga je da usmjerava EAP poruke između stranaka koje izvode autentifikaciju. 802.1x zapošljava EAP kao autentifikacijski framework.

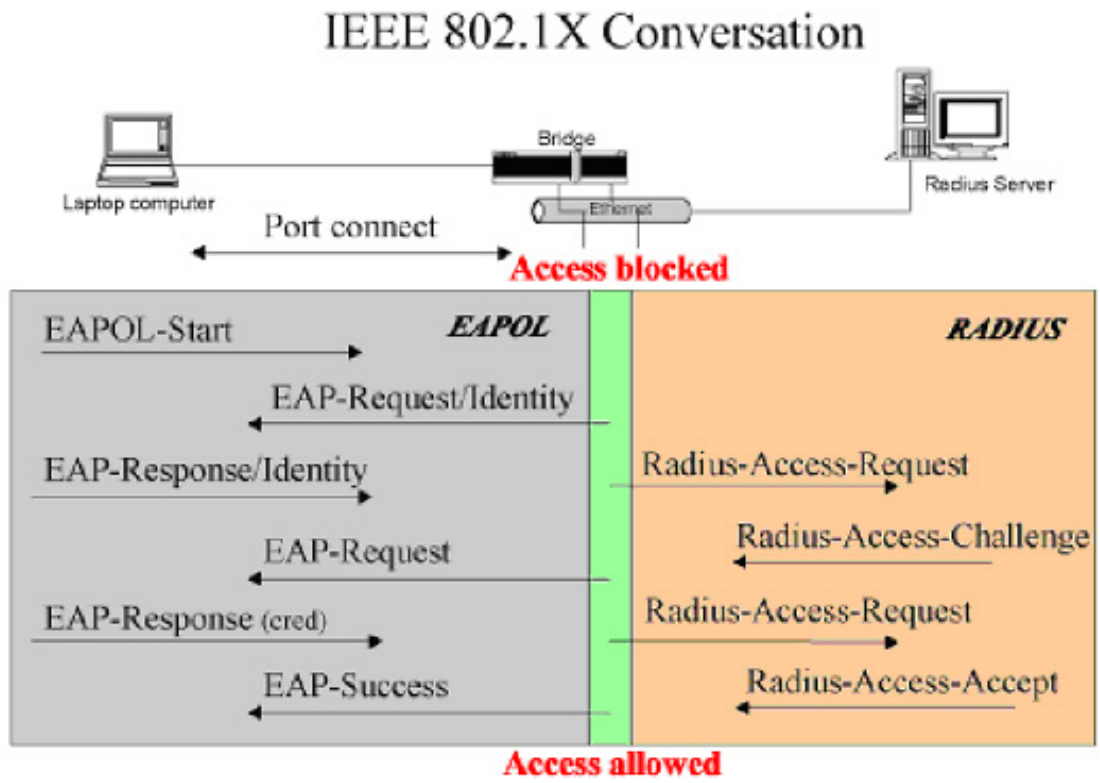


Extensible Authentication Protocol Over LAN (EAPOL)

802.1x definira standard za pakiranje EAP poruka tako da se njima može direktno služiti LAN MAC service. Ovaj zapakirani oblik EAP frame-a je poznat kao EAPOL. Pomoću ovog komuniciraju autentifikator i klijent za vrijeme trajanja autentifikacijskog procesa. Na početku autentifikacije 802.1x generira jedinstveni ključ za tu sesiju. Nakon toga, 802.1x definira EAP-podržanu metodu koja podržava sigurno, dinamičko izvođenje ključa.Kao dodatak nošenju EAP paketa, EAPOL također omogućuje kontrolne funkcije poput start, logoff i distribucije ključa.

EAPOL definira set paketa koji nose dijelove informacija :

- EAP-Packet : najčešći paket u 802.1x, nosi EAP konverzaciju
- EAPOL-Start :naređuje autentifikatoru da započne autentifikaciju
- EAPOL-Logoff : Javlja autentifikatoru da je korisnik isključen (log off)
- EAPOL-Key : nosi informaciju o bežičnom ključu za šifriranje
- EAPOL-ASF-Alert.



RADIUS

RADIUS je Remote Access Dial In User Service. To je standardni način pružanja usluga autentifikacije (utvrđivanje identita), autorizacije (određivanje što korisnik smije raditi) i accounting-a (prikupljanje podataka o korištenju mreže). RADIUS koristi UDP kao protokol za prijenos podataka. Prvobitno je razvijen da bude dial-in pristup mrežama, danas se koristi za kontrolu pristupa. Iako podrška RADIUS protokola je optional unutar 802.1x, za očekivati je da mnogi 802.1x autentifikatori funkiconiraju kao RADIUS klijenti. U stvari, Annex D of 802.1x

standarda daje upute za korištenje 802.1x RADIUS a i većina access points, koji podržavaju 802.1x, koriste RADIUS.

Baza podataka RADIUS-a stvara dobru početnu točku za kompletnu autentifikaciju i autorizaciju sustava jer, uz osnovne podatke poput korisničkog imena (user-ID) i zaporke, također može sadržavati detaljnije informacije o korisničkim privilegijama pristupa. Specifične mrežne privilegije, kao na koji port, uslugu i VLAN smije korisnik pristupiti, također se mogu priključiti. Tip informacije koji se može pohraniti u bazu RADIUS-a je fleksibilan. IEEE 802.1x može korisno upotrijebiti RADIUS i dovesti sigurnost na višu razinu.

RADIUS sadrži Mrežni Pristupni Server (Network Access Server - NAS), koji djeluje kao klijent RADIUS-a tijekom procesa autentifikacije korisnika. Klijent je odgovoran za prenošenje informacija do željenih RADIUS servera, i djelujući na odgovor koji im je poslan. RADIUS server može poslužiti kao proxy klijent drugim RADIUS serverima. Transakcije između klijenta i RADIUS servera su autentificirane upotrebom zajedničkih ključeva, koji se nikad ne šalju preko mreže.

Struktura RADIUS protokola		
Kod	Identifikator	Duljina
8 bits	16 bits	32 bits
autentifikator (16 byte-ova)		

Pod kodom može biti jedna od poruka:

- Kod – tip poruke može biti:

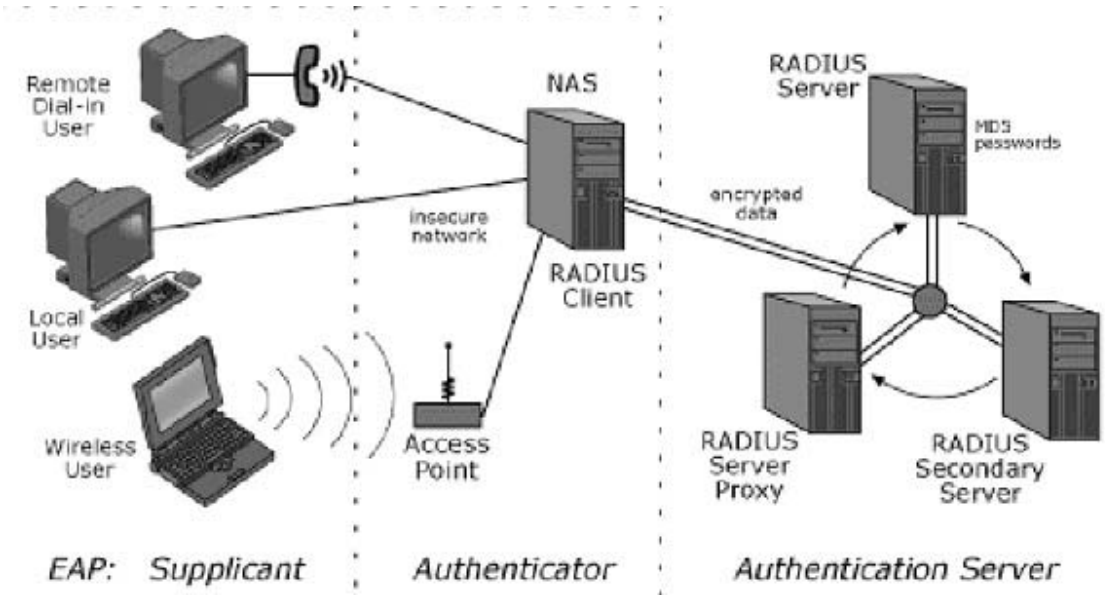
    1 Access-Request
    2 Access-Accept
    3 Access-Reject
    4 Accounting-Request
    5 Accounting-Response
    11 Access-Challenge
    12 Status-Server (experimental)

13 Status-Client (experimental)
255 Reserved

- Identifikator – odgovara zahtjevima i odgovorima.
- Duljina – duljina poruke zajedno sa zaglavljem.

Autentifikator – polje koje služi za autentifikaciju odgovora od RADIUS servera i u šifrirani skriveni algoritam.

Korisnik može biti lokalno spojen na NAS (preko login pristup) ili iz daljine na NAS preko AP-a (modem ili 802.11 bežična veza). Korisnik inicira zahtjev za pristup NAS-u, koji služi kao čuvar. NAS se sigurno spaja na RADIUS server koristeći zajednički tajni ključ (simetrično šifriranje). U slučaju da je primarni RADIUS server pao,naknadni zahtjev može biti poslan sekundarnom serveru. Ako sam server ne može identificirati korisnika, može djelovati kao proxy za drugi RADIUS server sa kojim dijeli tajnu šifru. I tako se to odvija sve dok autentifikacija ne bude zadovoljena. Dalje, RADIUS server prosleđuje privilegije pristupa NAS-u, koji će prema tome dopustiti ili zabraniti korisniku pristup mreži. Informacija na RADIUS serverima je šifrirana radi većih siguronosnih mjera.



RADIUS metoda autentifikacije služi kao odlična osnova. Veoma je fleksibilna i izgrađena je kao “umom otvorena”. Nažalost, postoji slaba karika u ovoj metodi; leži u komunikaciji između NAS-a i korisničkog stroja. Ova ranjivost je slična kao kod WEP (Wired Equivalent Privacy) protokola, koji je izrazito ranjiv dio IEEE 802.11 bežičnog standarda. Tada, RADIUS autentifikator se oslanja na AP ili NAS (koji je ponekad sam autentifikator) kako bi sigurno komunicirao sa korisničkim strojem. Neke implementacije su pokušale rješiti ovaj problem koristeći VPN tunel; ipak, ukradena mašina će moći pristupiti.

Mane WEP-a: korisnici se obično autentificiraju preko hardware-ske MAC adrese, koja se može lažirati ili ukrasti. Također, većina implementacija koristi globalne ključeve, koji se rijetko mijenjaju (ako ikad). Ovi se ključevi lako provale sa alatima poput AirSnort i WEPcrack. Međutim, 802.1x osigurava klijenta, tjerajući zajednički ključ da se regenerira za svaku autentifikacijsku sesiju, tako ublažavajući ovaj konkretan problem. WEP također koristi lošu implementaciju RC4 algoritma kao i kratak početni vektor (Initial Vector - IV) bez zaštite ponavljanja.

Prednosti: sigurnost (centralizirane korisničke informacije u proxy bazama), skaliranost (proxy-rani autentifikacijski serveri dopuštaju brojčani rast krajnjih korisnika, bez većih promjena konfiguracije), fleksibilnost (za svaku organizaciju da kontrolira ko pristupa mreži sa vlastitog servera).

802.1x ARHITEKTURA

802.1x Port-based kontrola pristupa ima efekt kreiranja dvije udaljene točke pristupa na autentifikatoski priključak na LAN. Jedna točka pristupa omogućuje razmjenu frame-ova između sustava i ostalih sustava na mreži. Često, ovaj nekontrolirani port omogućuje samo autentifikacijske poruke (EAP poruke) da se razmijene. Druga (kontrolirana) točka pristupa dopušta razmjenu frame-ova jedino ako je port autoriziran.

Kada se host spoji na LAN port na 802.1x sklopku autentičnost domaćina je određena preko sklopke prema protokolu određenim 802.1x, prije nego što se omogući pristup services na taj port. Dok autentifikacija nije kompletna, samo EAPOL frames se smiju razmijenjivati. Kad se postigne uspješna autentifikacija, the port switches prometuju kao regularan port.

802.1x je nastao radi adresiranja point-to point mreža. Drugim riječima, mora postojati jedan-na-jedan veza između klijenta i autentifikatora.

802.1x u WLAN

802.1x specifikacija uključuje dvije glavne postavke posebno ciljane da podrže upotrebu Port Access Control u IEEE 802.11 LAN:

1. *Logične portove*. Sposobnost da se iskoristi MAC adresa stanice i AP-a odredišne adrese u EAPOL protokol komunikaciji.
2. *Key Management*: Sposobnost pristupne točke da distribuira i dohvati informaciju o globalnom ključu od/do priključenih stanica putem EAPOL-Ključ poruke, nakon uspješne autentifikacije.

Logički portovi i MAC Adrese

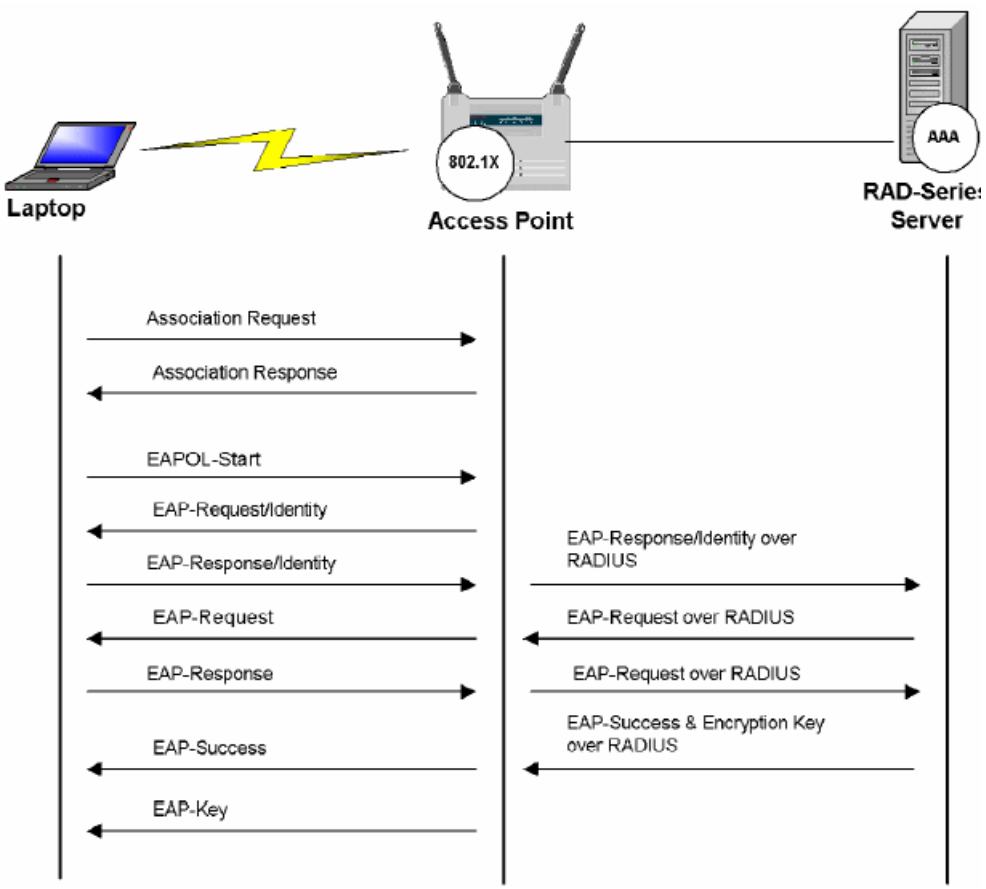
U 802.11 LAN okruženju, stanice nisu fizički povezane na mrežu. Uz to, više stanica dijeli medij za pristup mreži (RF zračni prostor). U IEEE 802.11 Wireless LANs postoji poseban dio koji govori o zajedničkom pristupu medija, prema kojemu stanica mora uspostaviti vezu sa pristupnom točkom kako bi se koristio LAN-om. Protokol koji uspostavlja ovu vezu omogućuje stanicama i pristupnoj točki da nauče jedno drugom MAC adresu. Ovo tvori «logički port» kojega stanica može upotrijebiti za komunikaciju sa AP. AP su konfigurirani da koriste Open Authentication. Ovo omogućuje klijentu da se poveže sa AP prije dinamički dostavljenih WEP ključeva (prije nego su dostupni). Kad se uspostavi veza, ta priključena stanica se može autentificirati koristeći EAP.

WEP Key Management

802.1x niti isključuje niti zahtijeva WEP ili bilo koji drugi algoritam šifriranja. On pruža mehanizam za distribuciju informaciju ključeva za šifriranje od AP do klijenta koristeći EAPOL-Ključ poruku. Ako uljez uspije otkriti WEP ključ, nakon završetka sesije neće biti upotrebljiv.

Udruživanje and EAP Autentifikacijska procedura

Kao što je prije spomenuto, stanica se mora prvo povezati sa datim AP. Tada može izmijeniti EAP poruke sa autentifikacijskim serverom kako bi autorizirao port. Prije nego što se logični port autorizira, on samo razmijenjuje EAP poruke.



Dakle EAP dijalog je se provodi EAPOL-om između stanice i AP-a. Dijalog is nošen EAP-om preko RADIUS-a između AP-a i autentifikacijskog servera. Ovo efektno stvara EAP konverzaciju između stanice i autentifikacijskog servera koji dopušta korisniku da se autentificira. Jednom kad se korisnik autentificira,EAP-Ključ poruka se pošalje da usmjerava informacije između stanica.

Prednosti korištenja 802.1x u WLAN-ovima

Postoje mnoge prednosti korištenja 802.1x u 802.11 LAN-ovima.

Kontrola na rubu mreže

802.1x omogućuje mreži da zabrani pristup na rubu, gdje se najlakše dade manipulirati. Kontrolirani portovi, bežični ili ne, zaustavljaju neautentificirane uljeze da pristupe ikad mreži.

Upravljanje dinamičkim ključevima za sesije

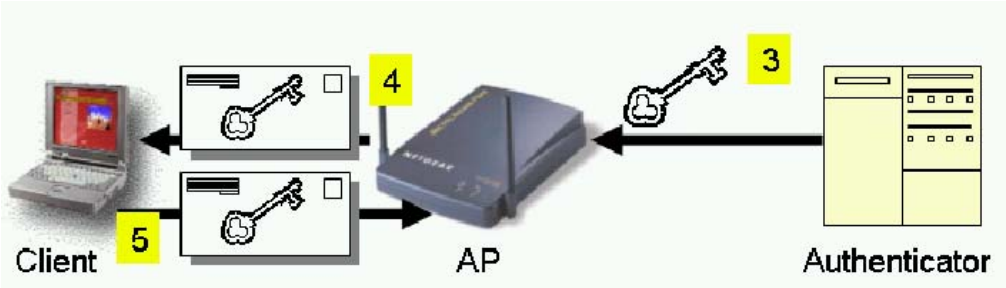
802.1x ima framework koji omogućuje sustavu upotrebu dinamičkih enkripcijskih ključeva; da se periočki re-key sesija; a i da se periodički re-autentificira korisnik. Ovo poboljšava sigurnost eliminacijom statičkih enkripcijskih ključeva, koji zahtjevaju velike količine podataka šifrirane sa jednim jedinim ključem.

Koristi Otvorene Standarde

802.1x se dobro integrira sa otvorenim standardima za autentifikaciju, autorizaciju i accounting (uključujući RADIUS) omogućujući implementiranje na postojeće infrastrukture za upravljanje dial-up mreže i VPN-ove.

802.1x i Dynamic Key Management

Važno je napomenuti da se 802.1x standard brine samo za autentifikaciju. Standard ne određuje konkretne tipove autentifikacije niti bilo kakav tip šifriranja. Štoviše, od lipnja 2002 nekoliko proizvođača nude odgovarajuće verzije upravljanja dinamičkih ključeva koristeći 802.1x kao dostavni mehanizam. Kroz dinamičku razmjenu ključeva autentifikacijski server može vratiti sesijske ključeve AP-u zajedno sa primljenom porukom.



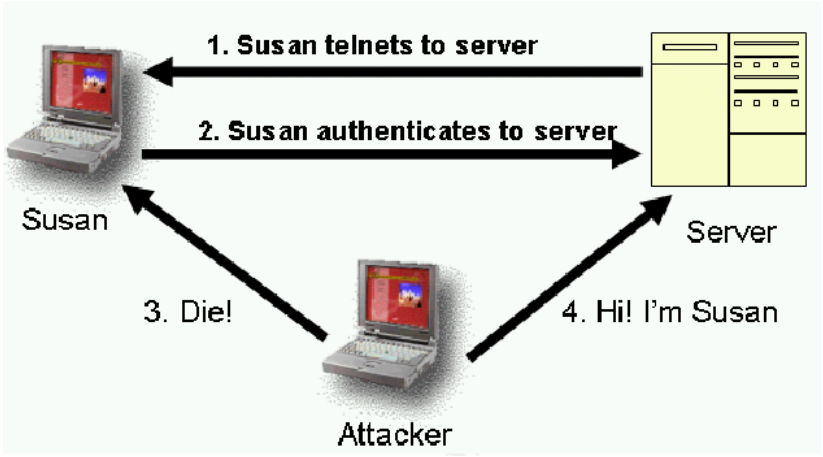
U trećem koraku, umjesto jednostavnog vraćanja potvrdne ili negirajuće poruke, autentifikator vraća rezultate autentifikacije i sesijski ključ. AP koristi sesijske ključeve od autentifikacijskog servera da potpiše i šifrira poruku koja je proslijeđena klijentu nakon slanja potvrdne poruke (korak 4). Klijent tada može iskoristiti sadržaj poruke s ključem da definira odgovarajuće korake šifriranja (korak 5 i nakon njega).

Mehanizam upravljanja dinamičkim ključevima pruža sigurniji mehanizam od ručnog održavanja ključa. 802.1x mehanizam dopušta klijentima – kroz uporabu upravljanja dinamičkim ključevima – da se automatski mijenjaju ključevi za šifriranje često koliko je potrebno da se minimizira mogućnost pasivnog napada.

Problemi sa 802.1x

Dakle, 802.1x protokol nije savršen. Istraživači na univerzitetu Maryland su otkrili da 802.1x je ranjiv na otimanje (hijacking) kao i na napade posrednika (Mishra & Arbaugh, 2001; Connolly, 2002; Schwartz, 2002).

Sesijsko otimanje je kad napadač preuzme postojeću sesiju, što znači da se napadač oslanja na postojeći autentificiranu vezu kako bi pristupio mrežnim izvorima.



Slika pokazuje da napadač čeka da se Susan (valjani korisnik) autentificira, tada ubije ili blokira Susanina vezu i pretvara se da je Susan.Ovo zahtijeva da napadač podvali autentifikacijsku korisničku IP adresu, kako bi održavao vezu.

Zaključak

IEEE 802.1x kontrola mrežnog pristupa temeljena na portovima pruža znatno poboljšana rješenja za autentifikaciju za WLAN i SLAN. To je način autentifikacije svakog korisnika koji pristupaLAN uslugama. Autentifikacija se mora izvesti prije bilo kakvog prometa između korisnika i mreže.

Prednosti 802.1x i EAP autentifikacije su:

- Pružaju interoperabilnost među proivođačima kod autentifikacije pristupa mreži.
- Pružaju proširivu autentifikacijsku podršku – EAP dozvoljava dodatne autentifikacijske metode kao što je autentifikacija putem zaporke.
- Poboljšana sigurnost u WLAN-u. Šifriranje i autentifikacija je poboljšana upotrebom dinamičkih WEP ključeva za šifriranje i međusobne autentifikacije.