

Autentizace portů pomocí 802.1X

802.1X port authentication

Peter Ušiak

Bakalářská práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Peter UŠIAK**
Osobní číslo: **A09751**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Autentizace portů pomocí 802.1X**

Zásady pro vypracování:

1. Popište princip činnosti autentizace portů pomocí 802.1X.
2. Popište konfiguraci všech nutných součástí systému.
3. Zrealizujte a ověřte činnost systému s využitím zařízení učebny.
4. Zhodnoťte výhody a nevýhody tohoto řešení při použití na reálné síti.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2009, 333 s. Cisco Press networking technology series. ISBN 15-870-5610-0.
2. Catalyst 2960 Switch Software Configuration Guide: Configuring IEEE 802.1x Port-Based Authentication. CISCO SYSTEMS, Inc. [online]. Icit. 2012-01-05]. Dostupné z: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/c
3. ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-802-5125-205.
4. BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.
5. LUDVÍK, Miroslav a Bohumír ŠTĚDRŮŇ. Teorie bezpečnosti počítačových sítí. Vyd. 1. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-808-6686-356.

Vedoucí bakalářské práce:

Ing. Jiří Korbel, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

24. února 2012


Termín odevzdání bakalářské práce:

8. června 2012

Ve Zlíně dne 24. února 2012


prof. Ing. Vladimír Vašek, CSc.
děkan




prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Bakalárska práca sa zaoberá pripojením a autentizáciou užívateľov do počítačovej siete klasickou káblovou formou štandardom IEEE 802.1x. Prvá teoretická časť popisuje funkčnosti a princípy jednotlivých protokolov v rámci štandardu, úlohy zariadení vystupujúcich v zapojení, postupný priebeh po pripojení a autentizácie klienta do siete. V druhej praktickej časti práce ide o konkrétne zapojenie, praktickú realizáciu a overenie funkčnosti autentizácie klienta. Toto spočíva v konfigurácií jednotlivých zariadení a nastavenia programového vybavenia nutného pre správne fungovanie autentizácie portov pomocou 802.1x. Prebrané sú aj výhody a nevýhody tohto riešenia predovšetkým s ohľadom na bezpečnosť počítačových sietí.

Kľúčová slova: počítačová sieť, 802.1x, EAP, EAPOL, switch, autentizácia, overenie, klient, RADIUS, server, LAN, VLAN, port, IEEE

ABSTRACT

The Bachelor work deals with the connection and clients authentication into the computer network with traditional cable form IEEE 802.1x. The first theoretical part describes functionality and principles of the standard protocols, devices rules included in the network and the authentication process after connection client to the network. The second practical part is about concrete connectivity, practical realization verifying the client authentication. This is the configuration of device settings and software necessary for the proper functioning of the ports with 802.1x authentication. The advantages and disadvantages of this solution particularly with regard to network security are notices as well.

Keywords: computer network, 802.1x, EAP, EAPOL, switch, authentication, verification, client, RADIUS, server, LAN, VLAN, port, IEEE

Týmto by som chcel poďakovať vedúcemu bakalárskej práce Ing. Jřímu Korbelovi, Ph.D., za jeho cenné pripomienky a čas ktorý mi venoval pri písaní tejto práce. Taktiež za poskytnutie prístupu k zariadeniam nutným k tejto práci.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	9
I TEORETICKÁ ČASŤ	10
1 PROBLEMATIKA AUTENTIZÁCIE PORTOV POMOCOU 802.1X	11
1.1 ŠTANDARD IEEE 802.1X	11
1.2 PROTOKOLY VYUŽÍVANÉ V 802.1X	11
1.2.1 EAP	11
1.2.2 EAPOL.....	12
1.2.3 CDP.....	13
1.2.4 802.1d STP	13
1.3 ÚLOHY JEDNOTLIVÝCH ZARIADENÍ V PROCESSE AUTENTIZÁCIE	14
1.4 PRIEBEH AUTENTIZÁCIE.....	15
1.5 SPUSTENIE AUTENTIZÁCIE A VÝMENA SPRÁV	17
1.6 STAVY PORTOV SWITCHU.....	19
1.7 802.1X ACCOUNTING	20
1.8 AUTENTIZÁCIA S PRIRADENÍM DO VLAN	20
1.8.1 Ako funguje VLAN prirad'ovanie.....	20
2 VŠEOBECNÉ ZÁSADY SPREVÁDZKOVANIA IEEE 802.1X	22
2.1 RADIUS SERVER	22
2.2 KONFIGURÁCIA CISCO SWITCH CATALYST.....	22
2.3 NASTAVENIE KLIENTA	23
II PRAKTICKÁ ČASŤ	24
3 SCHÉMA A ZAPOJENIE	25
4 KONFIGURÁCIA AUTENTIZÁCIE 802.1X	27
4.1 KONFIGURÁCIA RADIUS SERVERA	27
4.1.1 TekRADIUS.....	27
4.1.2 Konfigurácia TekRADIUS	27
4.1.3 Microsoft Windows Server 2008 R2	33
4.1.4 Konfigurácia MS Windows Server 2008 R2	33
4.2 KONFIGURÁCIA CISCO SWITCH CATALYST 2960	38
4.3 KONFIGURÁCIA KLIENTA	40
4.4 PRIEBEH AUTENTIZÁCIE.....	41
5 VÝHODY A NEVÝHODY RIEŠENIA	46
5.1 VÝHODY	46
5.2 NEVÝHODY	48
ZÁVER	49

CONCLUSION.....	50
ZOZNAM POUŽITEJ LITERATÚRY	50
ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....	52
ZOZNAM OBRÁZKOV	53
ZOZNAM TABULIEK	54
ZOZNAM PRÍLOH	55

ÚVOD

Práca na počítači dnes patrí k úplne základným schopnostiam každého z nás, nutných pri jeho využívaní či už v osobnom alebo pracovnom živote pre potreby získavania on-line informácií alebo komunikácie medzi ľuďmi. Z toho vyplýva, že počítač nepripojený či už k lokálnej alebo k celosvetovej sieti Internet by stratil široké možnosti z hľadiska svojho využitia.

Dnes je samozrejmosťou takmer v každom väčšom alebo menšom podniku, škole či rôznych úradoch a iných inštitúciách využívanie siete a Internetu. Z tohto dôvodu sa kladie veľký dôraz na bezpečnosť a ochranu dát v počítačových sieťach pred prístupmi nechcených užívateľov chcujúcich získať, zneužiť alebo poškodiť informácie, ktoré im nepatria.

Preto boli a sú vytvárané mechanizmy, ktoré sa zdokonaľujú aby zabránili takýmto útokom, prípadne zamedzili prístupu nechceným užívateľom. Z istého hľadiska to prináša vždy určité výhody nutné predovšetkým z hľadiska bezpečnosti, no bohužiaľ na druhú stranu sú s tým spojené aj nevýhody a určité obmedzenia. Avšak bezpečnosť by mala byť vždy na prvom mieste v akejkoľvek oblasti. Preto je veľmi dôležité sústrediť sa aj na túto bezpečnostnú otázku v rámci počítačových sietí a venovať jej dostatok pozornosti.

Cieľ tejto bakalárskej práce je realizácia a overenie funkčnosti jedného z veľa možných spôsobov zabezpečenia siete. Konkrétne ide o autentizáciu portov pomocou štandardu 802.1x a teda užívateľov k nim pripájaných, aby mohli využívať služby siete a mali prístup len užívatelia, ktorí sú na to oprávnení. To práve zreteľne zabezpečuje spomínaný protokol, ktorý zaručuje zvýšenie úrovne zabezpečenia a znižuje možnosti pripojenia neoprávnených užívateľov.

I. TEORETICKÁ ČASŤ

1 PROBLEMATIKA AUTENTIZÁCIE PORTOV POMOCOU 802.1X

1.1 Štandard IEEE 802.1X

Štandard IEEE 802.1X definuje protokol typu klient – server ktorý slúži pre riadenie prístupu. Jeho úlohou je zabraňovať prístupu neautorizovaných klientov do počítačovej siete cez verejné prístupové porty. Pri pripojení autentizačný server overuje každého klienta pripájajúceho sa na porty switchu a to skôr ako mu sprístupní akékoľvek sieťové služby ktoré switch prípadne bezdrôtový prístupový bod poskytuje.

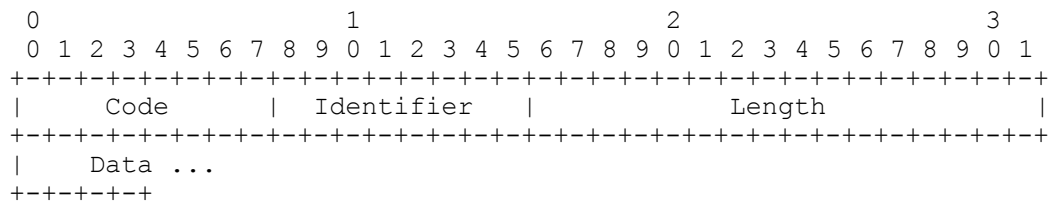
Počas doby, kým nie je klient autorizovaný 802.1x povoľuje prístup danému portu ku ktorému je klient pripojený iba pomocou protokolov Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP) a Spanning Tree Protocol (STP). Následne sa klient dostáva k bežnému prístupu cez port až po úspešnom overení autorizačným serverom.[2]

1.2 Protokoly využívané v 802.1x

1.2.1 EAP

EAP je rodina autentizačných protokolov často používaná vo wireless sieťach a Point-to-Point pripojeniach. Je definovaná v RFC 3740. Úlohou EAP je poskytovanie prenosu, používanie kľúčových dát a parametrov generovaných pomocou jednotlivých EAP metód. Existuje viacero metód, ktoré sú definované štandardami RFC a špecifickými metódami výrobcov ako napríklad EAP-TLS, EAP-MD5, EAP-PSK, EAP-TTLS a iné. EAP nie je klasický *wire* protokol (napr. v rámci transportnej vrstvy ako TCP alebo UDP), ale definuje len formát správy. Tzn. že každý z protokolov, ktorý používa EAP definuje spôsob ako zapuzdrovať EAP do vnútra rámca posiadaného daným protokolom.

EAP má široké využitie. Napríklad v IEEE 802.11 (WiFi) štandardy WPA a WPA2 využívajú ako oficiálny autentizačný mechanizmus 802.1x s piatimi typmi EAP. [6]



Obr. 1 Formát EAP packetu [7]

Code – identifikuje typ EAP packetu, môže obsahovať hodnoty:

- Request – požiadavka
- Response – odpoveď
- Success – úspešné
- Failure - zlyhanie

Identifier – párovacie pole pre Response a Request

Length – indikuje dĺžku pola celého EAP packetu vrátane Code, Identifier, Length a Data

Data – formát dátového pola je určený v závislosti od pola Code

Detailný popis protokolu a jeho celá dokumentácia je k dispozícii napr. na [7].

1.2.2 EAPOL

V sieťach LAN je pre 802.1x nutné, aby existoval nejaký spôsob komunikácie medzi **supplicant** (klient) a **authenticator** (switch/prístupový bod). Celá táto komunikácia medzi nimi sa odohráva priamo v druhej vrstve OSI modelu (spojová vrstva), čo si vyžaduje informácie identifikujúce klienta v podobe MAC adresy. Práve preto je pre túto komunikáciu používaný EAPOL ktorý prakticky znamená zapuzdrovanie EAP rámcov v LAN do rámcov EAPOL formátu. EAP je pritom samozrejme stále samostatný protokol (rodina protokolov) používaný pre autentizáciu.

Destination	Source	EtherType	Protocol	Packet	Body	Packet
MAC	MAC	Code	Version	Type	Length	Body
6 Bytes	6 Bytes	2 Bytes	1 Byte	1 Byte	2 Bytes	

Tabuľka 1 Formát EAPOL

kde typ packetu je nasledovný:

0	EAP Packet
1	EAPOL Start
2	EAPOL Logoff
3	EAPOL key
4	EAPOL Encapsulated ASF Alert

Tabuľka 2 Typ packetu

1.2.3 CDP

Cisco Discovery Protocol je nástroj ktorý slúži k sledovaniu siete a riešenia problémov s ňou. Úlohou CDP je získavať informácie ohľadom priamo pripojených Cisco zariadení a teda umožňuje administrátorovi získať súhrn informácií ako je napríklad IP adresa alebo protokol. Cisco zariadenia ktoré sú k sebe priamo pripojené do siete pravidelne vysielajú správy, ktoré sú nazývané ako CDP advertisementts (oznámenia). Tieto oznámenia obsahujú informácie typu zariadenia (router, switch, ...) rozhrania routeru, ku ktorému sú pripojené, alebo tiež číslo modelu zariadenia.

K zobrazeniu informácií o susedným zariadeniach sa dostaneme pomocou príkazu *show cdp neighbors* alebo *show cdp neighbors detail*.

1.2.4 802.1d STP

Switche, prípadne bridge môžu byť popísané štandardom IEEE 802.1d Spanning-Tree Protocol a používajú spanning-tree algoritmus pre vytvorenie logickej topológie bez smyčiek s čo najkratšou cestou. Najkratšia cesta je založená na vzrastajúcej cene linky (**link cost**) a cena linky je závislá na rýchlosti spoja.

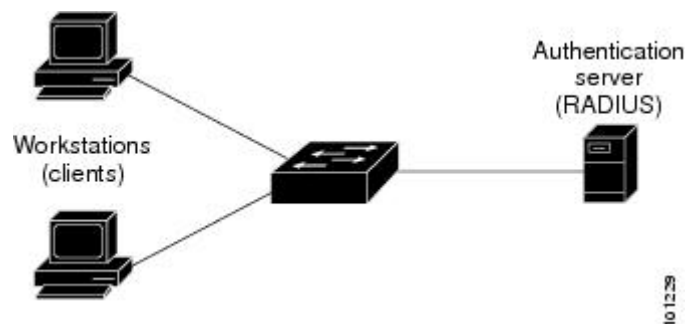
Logická topológia bez smyčiek sa nazýva strom (tree). Logická topológia je hviezda alebo rozšírená (extended) hviezda. Táto topológia je **vetviaci sa strom** (spanning-tree).

STP je teda využívaný v sieťach s redundantnou sieťovou topológiou (siete s väčším počtom fyzických uzlov) kde je nutné aby bola zaistená funkčnosť celej siete aj v prípade, ak by zlyhal jeden bod siete.

Ak by v takýchto typoch sietí nebol práve využitý STP, nastal by problém plytvania šírkou pásma. Je to z dôvodu, že v hlavičke druhej vrstvy nie je hodnota TTL a pokiaľ je rámec druhej vrstvy poslaný do switchu v sieti so smyčkami, bude preposielaný do nekonečna. Z toho vyplýva, že prepínaná sieť pre správnu funkčnosť nemôže mať fyzické smyčky ale pre zvýšenie dostupnosti siete sú kľúčové. Riešením je teda mať síce fyzické smyčky, ale vytvoriť pomocou STP logickú topológiu bez smyčiek.

1.3 Úlohy jednotlivých zariadení v procese autentizácie

Protokol 802.1X rozoznáva tri dôležité druhy zariadení, z ktorých každé z nich plní svoju úlohu pri procese overovania.



Obr. 2 802.1x Úlohy zariadení [2]

Klient (pracovná stanica) – je zariadenie, ktoré žiada o prístup do siete LAN a k službám poskytovaných switchom. Na danej pracovnej stanici musí bežať klientský software (v 802.1x nazývaný **supplicant**), ktorý ponúkajú napríklad operačné systémy Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7. V prípade prostredia Linuxu sa využíva napríklad software Xsupplicant.

Autentizačný server (RADIUS server) – vykonáva overenie pripojeného klienta. RADIUS server overí identitu klienta a oznámi RADIUS klientovi (switch, prípadne bezdrôtový prístupový bod) či daný klient má oprávnenie pristupovať k službám siete. Každý jeden klient pripojený k RADIUS klientovi je jednoznačne identifikovaný pomocou jeho jedinečnej MAC adresy. Bezpečnostný systém RADIUS s protokolom EAP rozširuje

skupinu podporovaných autentizačných serverov. RADIUS funguje v režime typu klient – server, kde sú informácie o autentizácii klientov posielané medzi RADIUS serverom a jedným prípadne viacerými RADIUS klientami.

Switch/bezdrôtový prístupový bod (RADIUS klient) – RADIUS klient vykonáva kontrolovanie fyzického prístupu k sieti založeného na overovaní autentizačného stavu klienta. Switch sa správa ako prostredné zariadenie medzi klientom a autentizačným serverom, žiadajúce identifikačné údaje od klienta, potvrdenie overenia klienta od autentizačného servera, kde nakoniec odosiela informáciu späť klientovi o jeho úspešnom či neúspešnom pripojení do siete.

Switch resp. RADIUS klient zodpovedá za zapúzdrovanie a rozbalovanie EAP rámcov a za komunikáciu s autentizačným serverom.

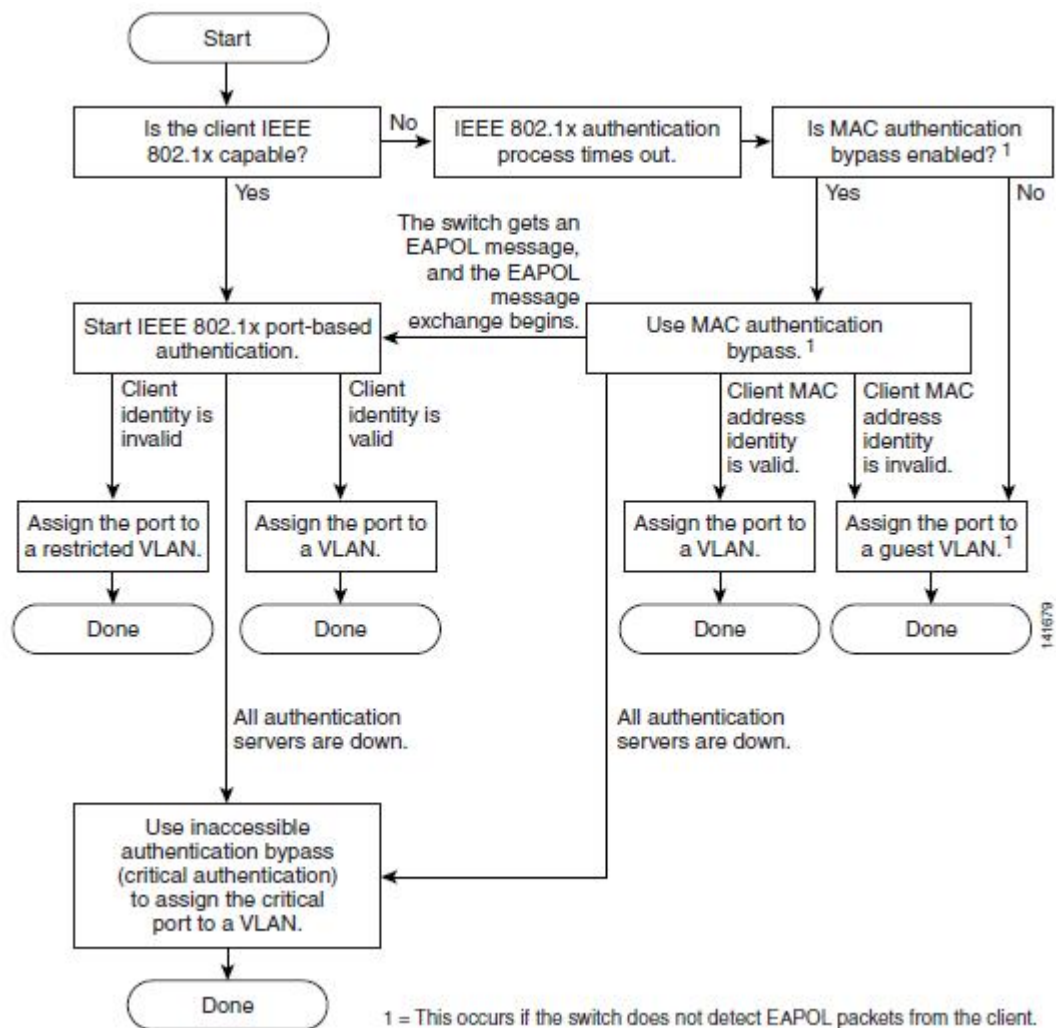
Keď switch prijme EAPOL rámec pred odoslaním na autentizačný server odstráni Ethernetovú hlavičku. Zostávajúci EAP rámec opäť zabalí do rámca RADIUS formátu a odošle ho autentizačnému serveru. Počas zapúzdrenia nie je EAP rámec nijako upravovaný a taktiež je nutné aby autentizačný server podporoval EAP ako natívny formát rámca. Keď switch prijme rámec z autentizačného servera znovu ho odbalí a odstráni hlavičku. Zostávajúci odbalený EAP rámec znovu zapúzdri pre Ethernet a odošle ho klientovi.[2]

1.4 Priebeh autentizácie

Ak je autentizácia pomocou 802.1x aktívna a klienti podporujú 802.1x - klientský software, dochádza k týmto udalostiam:

- ak je identita klienta úspešne overená, switch poskytne klientovi pripojenie do siete
- ak vyprší čas autentizácie počas čakania na EAPOL správu a *MAC authentication bypass* je zapnutá, switch môže použiť klientovu MAC adresu pre autentizáciu. Ak je klientova MAC adresa správna a autorizácia prebehne úspešne, switch poskytne klientovi pripojenie do siete. Ak klientova MAC adresa nie je správna a autorizácia zlyhá, switch pridelí klienta do hosťovskej VLAN, ktorá poskytuje obmedzené služby v prípade že je daná hosťovská VLAN vopred nakonfigurovaná.

- ak switch dostane nesprávne identifikačné údaje od klienta a je nakonfigurovaná VLAN pre obmedzených klientov, switch pridelí klienta do obmedzenej VLAN, ktorá poskytuje len obmedzené služby.
- ak je RADIUS server nedostupný a je zapnuté *inaccessible authentication bypass* (tiež nazývané *AAA fail policy*), switch poskytne klientovi prístup do siete tým že port prepne do stavu *critical – authentication* a pridelí ho VLAN špeciálne nakonfigurovanej pre tento prípad.



Obr. 3 Vývojový diagram možnosti procesu autentizácie [2]

Switch vykonáva re-autentizáciu klienta v nastávajúcich prípadoch:

- re-autentizácia je aktivovaná periodicky a vyprší jej nastavený časový interval
- re-autentizácia je vykonaná ručne

1.5 Spustenie autentizácie a výmena správ

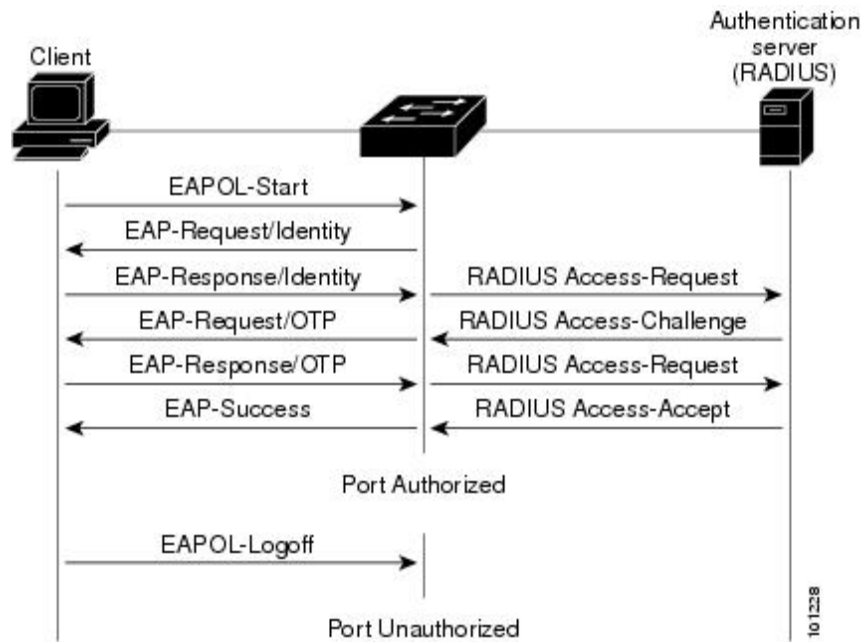
Samotné spustenie autentizácie môže byť vyvolané klientom alebo switchom. V prípade že je na danom porte nakonfigurovaná aktívna autentizácia, switch spúšťa autentizačný proces keď port prechádza z vypnutého stavu do zapnutého alebo periodicky tak dlho ako zostáva v neautentizovanom stave. Switch pošle EAP požiadavku, klient túto požiadavku prijme a odpovie identifikačným rámcom.

V situácií, kedy klient túto EAP požiadavku od switchu neobdrží, môže klient spustiť autentizačný proces sám poslaním EAPOL-start rámca, ktorý naštartuje switch k tomu aby okamžite poslal požiadavku pre EAP identifikačný rámec.

Keď klient odošle svoju identitu, zo switchu sa v danom momente stáva prostredné zariadenie. Preposiela EAP rámce medzi klientom a autentizačným serverom dovtedy, pokiaľ prebehne overenie úspešne alebo zlyhá. Ak prebehne autentizácia správne port sa stáva autorizovaným a poskytuje bežný prístup do siete a k sieťovým službám. V opačnom prípade môže byť znovu žiadaná autentizácia, port môže byť priradený do VLAN ktorá poskytuje obmedzený služby alebo prístup do siete port nepovolí.

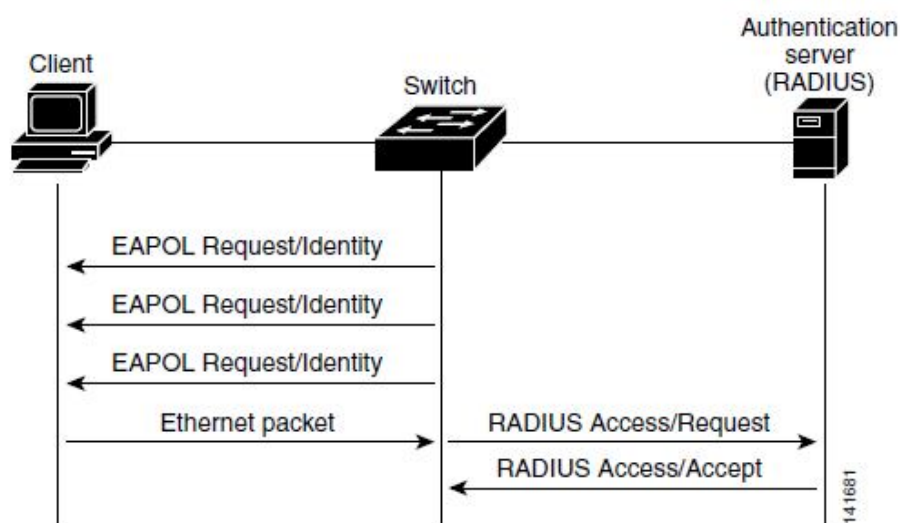
V prípade že na porte nie je nastavená 802.1x autentizácia alebo nie je podporovaná zariadením, všetky EAPOL rámce odoslané klientom sú automaticky zahodené.

Spôsob výmeny EAP rámcov závisí od autentizačnej metódy ktorá je použitá pri výmene. Obrázok 4 znázorňuje počiatočnú výmenu správy spustenú klientom, kde klient používa OTP autentizačnú metódu s RADIUS serverom.



Obr. 4 Výmena správ [2]

Ak vyprší čas autentizácie počas čakania na EAPOL správu a *MAC authentication bypass* je zapnutá, switch môže autorizovať klienta prijatím Ethernet packetu od klienta. Switch použije klientovu MAC adresu ako identifikáciu, zabalí ju do RADIUS-access/request rámca, ktorý pošle RADIUS serveru. Potom ako RADIUS server odpovie switchu (autORIZÁCIA bola úspešná), port sa dostáva do autorizovaného stavu a switch poskytne klientovi pripojenie do siete. Ak autorizácia zlyhá, switch pridelí klienta do hosťovskej VLAN, ktorá poskytuje obmedzené služby v prípade že je daná hosťovská VLAN vopred nakonfigurovaná.



Obr. 5 Výmena správ počas MAC Authentication Bypass [2]

1.6 Stavy portov switchu

V priebehu autentizácie v závislosti na stave portu switchu môže byť poskytnutý prístup do siete, tzn. že stav portu switchu určuje či má alebo nemá klient prístup do siete. Implicitne je port nastavený v stave *neautorizovaný*, avšak i keď v tomto stave port blokuje prístup do siete a k jej službám, prebieha výmena packetov v rámci protokolu 802.1x, CDP a STP. V prípade že je port korektné autentizovaný, prepne sa do stavu *autorizovaný* a je poskytnutý prístup do siete.

Ak nastane situácia, keď klient nepodporuje autentizáciu protokolom 802.1x a switch žiada o identifikačné údaje a klient na túto požiadavku neodpovedá, port automaticky ostáva v stave *neautorizovaný* a nemá povolený prístup do siete.

V opačnom prípade, keď je klient podporujúci autentizáciu 802.1x, je pripojený k portu kde nebeží tento protokol a snaží sa naštartovať autentizáciu pomocou EAPOL-start rámca na ktorú nedostane odpoveď, opakuje túto požiadavku niekoľkokrát. Následne pretože port neodošle žiadnu odpoveď sa pokúša port využívať ako keby bol v stave *autorizovaný*.

Porty switchu môžu byť nakonfigurované v stavoch:

- **force-authorized** – autentizácia 802.1x je deaktivovaná a stav portu je natrvalo nastavený ako *autorizovaný* bez akejkoľvek nutnosti autentizačného procesu klienta
- **force-unauthorized** – stav portu je natrvalo *neautorizovaný*, nie sú akceptované žiadne požiadavky klienta na autentizáciu
- **auto** – autentizácia 802.1x je aktivovaná, port je implicitne nastavený v stave *neautorizovaný*, povoľujúci iba prenos EAPOL rámcov. Po úspešnej autentizácii klienta port prechádza do stavu *autorizovaný*. Každý klient žiadajúci o prístup do siete je jednoznačne identifikovaný switchom, kde je používaná klientova jedinečná MAC adresa.

Po odhlásení zo siete odošle klient EAPOL-logoff rámec, ktorý zapríčini okamžitú zmenu stavu portu na *neautorizovaný* a tým opäť zabezpečí sieť pred prípadným pripojením nepovoleného prístupu do siete. [2]

1.7 802.1x Accounting

Ako je už v úplnom úvode spomínané štandard 802.1x definuje ako sú užívatelia (klienti) pre prístup do siete autorizovaní a autentizovaní, ale nestarajú sa o zaznamenávanie jej využívania, čo je z pohľadu bezpečnosti tiež veľmi dôležité.

Implicitne je táto funkcia neaktívna, avšak tento monitoring môže byť na jednotlivých portoch aktivovaný, pričom zaznamenáva aktivity:

- úspešná autentizácia užívateľa
- odhlásenie užívateľa
- ak je prerušená komunikácia na danom porte
- úspešná re-autentizácia užívateľa
- neúspešná re-autentizácia užívateľa

Samotný switch tento monitoring u seba neukladá, ale všetky informácie sú posielané RADIUS serveru, ktorý v tomto prípade musí byť nakonfigurovaný na zaznamenávanie správ.

1.8 Autentizácia s priradením do VLAN

Protokol 802.1x v spolupráci so switchom a RADIUS serverom ponúka možnosť dynamicky priradovať porty do jednotlivých VLAN podľa autentizačných údajov poskytnutých klientom. Je to určitá výhoda a to z pohľadu že nie je nutné jednotlivo konfigurovať každý fyzický port switchu do ktorej (klient alebo užívateľ) VLAN má byť priradený a pritom nie je viazaný na fyzický port (prípadne rozsah portov), kde sa musí pripojiť. Naopak sa užívateľ môže pripojiť na ktoromkoľvek mieste či počítači (klientovi) a bude patriť do správnej VLAN. Avšak je nutné dodať, že obecné táto možnosť funguje iba v prípade autentizácie užívateľa a nie počítača(klienta) a preto je potrebné zvoliť vhodnú autentizačnú metódu EAP.

1.8.1 Ako funguje VLAN priradenie

V momente keď je klient pripojený do portu switchu sa ako prvé naštartuje komunikácia medzi supplicant (pripojeným klientom) a portom pomocou EAPOL, čím sa vyžadujú identifikačné údaje. Supplicant odpovie na požiadavku autentizačného klienta

užívateľským menom a heslom a následne sú tieto autentizačné údaje odoslané vopred nastavenému RADIUS serveru. Na tomto serveri beží užívateľská databáza podporujúca EAP, ktorá povoľuje členstvo v jednotlivých VLAN každému užívateľovi individuálne. Po úspešnej autorizácii sa autentizovaný port stáva členom definovanej VLAN.

2 VŠEOBECNÉ ZÁSADY SPREVÁDZKOVANIA IEEE 802.1X

2.1 RADIUS server

Pri návrhu siete s využitím 802.1x je potrebné zvoliť si vhodný software, ktorý bude vykonávať úlohu RADIUS servera. Voľba je dôležitá z rôznych hľadísk a kritérií, ktoré vyžaduje konkrétna realizácia riešenia. Taktiež je potrebné zvoliť si v ktorom operačnom systéme bude pracovať a s akou databázou bude spolupracovať. Taktiež nie je zanedbateľné, či bude daný SW neplatenou alebo naopak platenou verziou, od čoho sa odvíjajú aj jeho funkcie.

Preto je každá realizácia siete špecifická, napriek tomu existujú všeobecné zásady, ktoré je nutné dodržať pre správne fungovanie RADIUS servera:

- 1) Sprevádzkovanie databázy
- 2) Sprevádzkovanie RADIUS servera (software) a komunikácie s databázou
- 3) Konfigurácia RADIUS servera:
 - a. Vytvorenie klientov
 - b. Vytvorenie politiky siete a prístupových práv
 - c. Nastavenie špecifických prístupov do siete

2.2 Konfigurácia CISCO SWITCH CATALYST

Konfigurácia 802.1x switchu v Cisco IOS prebieha v jednotlivých nevyhnutných krokoch, ktoré sú potrebné pre fungovanie samotnej autentizácie [3]:

- 1) Zapnutie mechanizmu AAA globálnym príkazom **aaa new-model**
- 2) Pri komunikácii so serverom RADIUS musí byť nadefinovaná IP adresa alebo adresy serverov a príslušné šifrovacie kľúče pomocou príkazov **radius-server host** a **radius-server key**
- 3) Nadefinovanie autentizačnej metódy 802.1x (RADIUS) príkazom **aaa authentication dot1x default**, v prípade viacej skupín pomocou príkazov **aaa authentication dot1x group názov**

- 4) Zapnutie globálneho mechanizmu príkazom **dot1x system auth-control**
- 5) Nakoniec pri každom rozhraní pomocou príslušného príkazu rozhrania **dot1x port-control { auto | force-authorized | force-unauthorized }** zapnutie jedného z troch možných prevádzkových nastavení

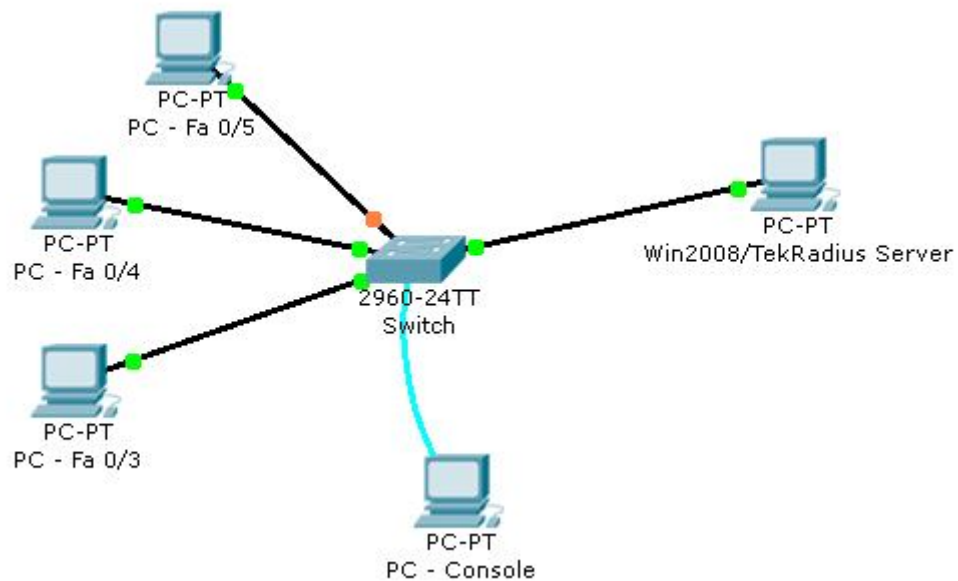
2.3 Nastavenie klienta

V súčasnosti najčastejšie používané operačné systémy ako sú Microsoft Windows, rôzne edície Linuxu či Mac OS obsahujú podporu pre protokol IEEE 802.1x. Podobne ako pri konfigurácii RADIUS servera v závislosti od softwaru (v prípade nastavenia klienta od OS) je nastavenie v každom rozdielnom spôsobe, avšak je dôležité aby nastavenia **odpovedali práve tým, aké sú nastavené na RADIUS serveri**. Všeobecné zásady potrebné k nastaveniu klienta:

- 1) Dostupné a správne nastavené sieťové pripojenie.
- 2) Povolené využitie protokolu 802.1x.
- 3) Zvolená autentizačná metóda EAP.

II. PRAKTICKÁ ČASŤ

3 SCHÉMA A ZAPOJENIE



Obr. 6 Schéma zapojenia

Na Obr. 6 je znázornená schéma zrealizovaného testovaného zapojenia počas autentizácie a na Obr. 7 je toto zapojenie aplikované na reálne zariadenia. V zapojení je použitá jedna pracovná stanica PC-Console pripojená cez sériový port k Cisco Switch Catalyst 2690, ako konzola cez ktorú sa nakonfigurovalo toto zariadenie. Ďalej boli použité tri pracovné stanice PC 01 až PC 03 ako ukážka pri zapojení do jednotlivých vopred nakonfigurovaných portov switchu (Fa 0/1, Fa 0/3 a Fa 0/5), kde každý z nich bol uvedený v inom stave a síce force-authorized, auto a force-unauthorized. Pochopiteľne nakoniec najviac dôležitý server, ktorý mal za úlohu autentizovať pracovné stanice.



Obr. 7 Zapojenie v Rack-u

4 KONFIGURÁCIA AUTENTIZÁCIE 802.1X

Pre správne fungovanie autentizácie protokolom 802.1x je potrebné nastaviť ako aj RADIUS server, tak aj switch a klienta. V tejto časti sú uvedené konkrétne nastavenia a overenie funkčnosti na reálnych zariadeniach. Ako RADIUS server bol pre túto realizáciu použitý TekRADIUS a MS Windows Server 2008 R2, ako RADIUS klient Cisco Catalyst 2690 Switch a ako klient pracovná stanica s operačným systémom Microsoft Windows XP Professional.

4.1 Konfigurácia RADIUS servera

4.1.1 TekRADIUS

Pre fungovanie a využívanie TekRADIUS servera je nutné mať databázu, s ktorou samotný software spolupracuje a zapisuje všetky údaje o užívateľoch, skupinách, sessions atď. Ja som preto zvolil MS SQL Server 2008 R2, ktorý ponúka širokú škálu možností pre prácu s databázou. Taktiež je bezproblémovo kompatibilný s TekRADIUS a spĺňa jeho systémové požiadavky. Obidva SW som implementoval pod operačným systémom MS Windows XP Professional.

4.1.2 Konfigurácia TekRADIUS

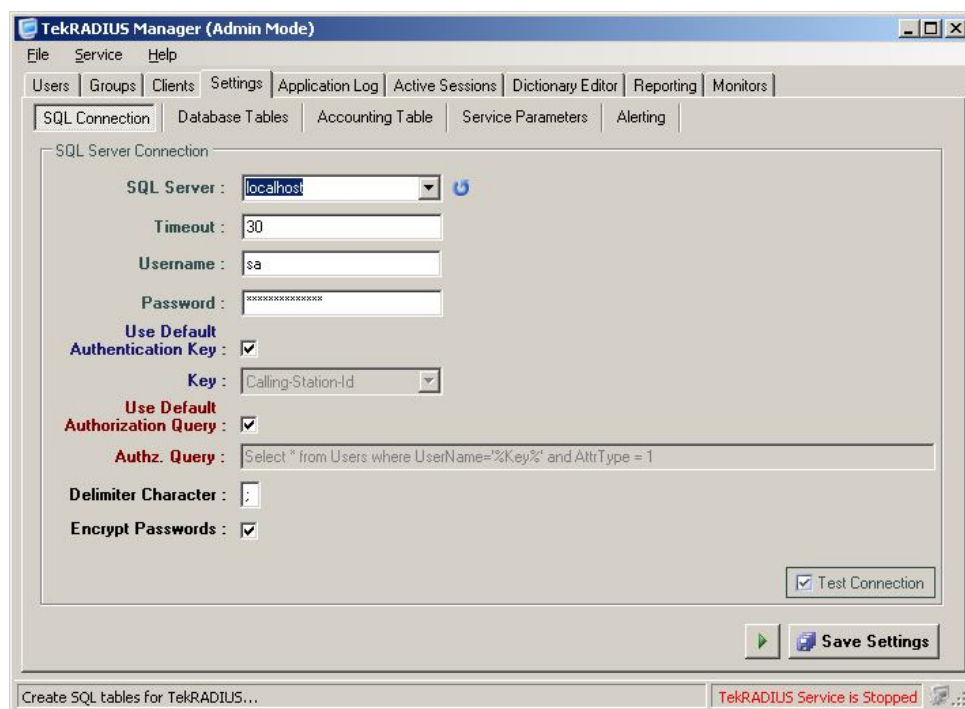
Keďže TekRADIUS ponúka pomerne dosť možností a nastavení nie je možné v rámci práce uvádzať všetky detailné významy každého (checkbox) poľa, avšak všetky údaje sú popísané v dokumentácii a preto uvádzam len môj postup. Celý manuál k TekRADIUS je voľne stiahnuteľný na [8].

Po inštalácii TekRADIUS, nastavenie a správa servera prebieha pomocou *TekRADIUS Manager*. Tu je dôležité pre možnú prácu s administračným módom (plnými právami) manažera, aby mal užívateľ prihlásený v OS práva administrátora. V opačnom prípade sa manager automaticky spustí v operačnom móde, ktorý je obmedzený o správu niektorých kľúčových častí programu napr. užívateľa, monitoring aktívnych sessions a ďalšie. Prístup do databázy je nutné samozrejme mať tiež pod užívateľom, ktorý má plný prístup. V tomto prípade sa jedná o užívateľa OS **Administrátor** a SQL **sa**, ktorí majú plné práva.

Úplne prvé nastavenia smerujú do záložky SETTINGS, kde sú všetky nutné stavenia pre spojazdnenie servera.

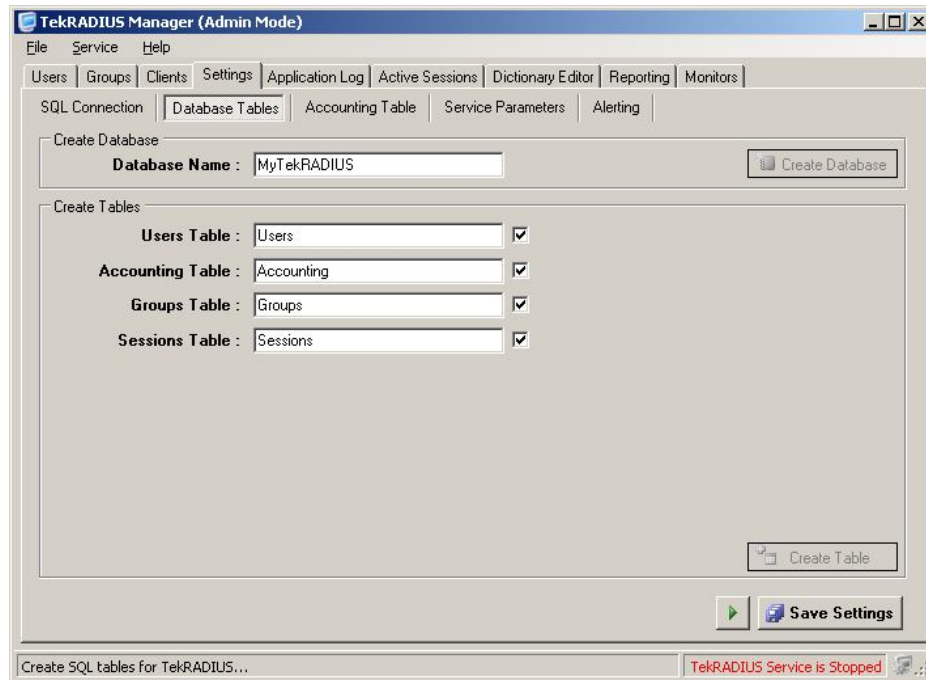
Nastavenie SQL spojenia s DB:

Nastavenie pripojenia k DB je vidieť na Obr. 5, kde SQL Server predstavuje localhost, keďže DB je na rovnakej pracovnej stanici ako je TekRADIUS. Prihlasovacie údaje do databázy a ďalšie voliteľné polia.



Obr. 8 Nastavenie SQL spojenia s DB

Po správnom nastavení prebehol “Test Connection” správne a ako ďalší krok je vytvorenie samotnej databázy a tabuliek v nej pomocou “Create Database” a “Create Table”:

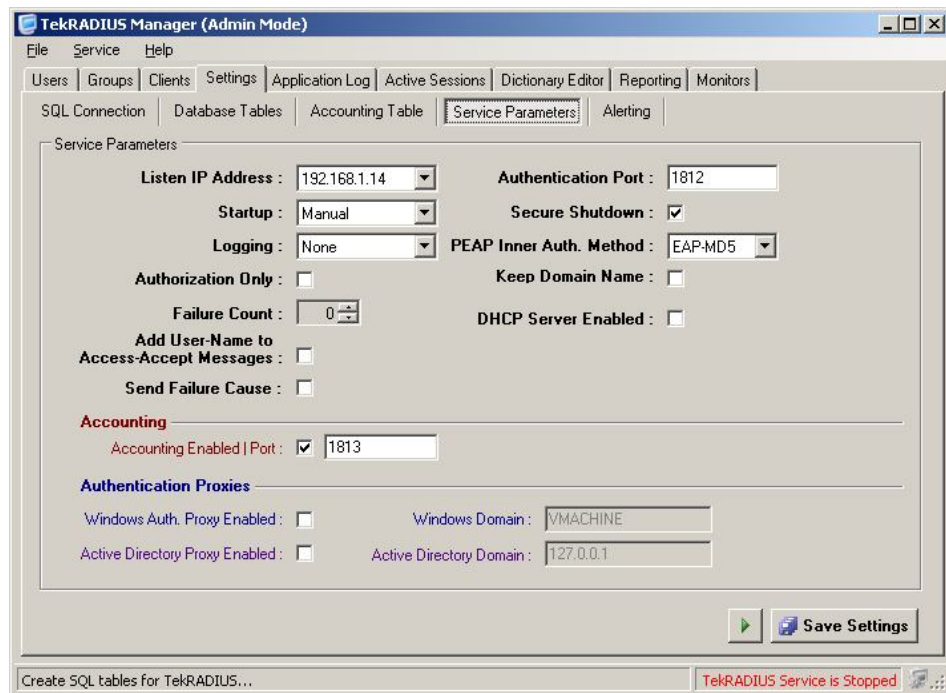


Obr. 9 Vytvorenie tabuliek v DB SQL

Vytvorenie tabuliek je taktiež možné aj priamo pomocou dotazov v SQL. Tieto dotazy sú uvedené v prílohe P I.

Nastavenie parametrov služby TekRADIUS server:

Za zmienku stoja jedny z nie málo dôležitých nastavení na Obr. 7 “Listen IP Address” – IP adresa servera, na ktorej bude počúvaná služba (prístup zo siete), “Authentication Port” na ktorom beží služba, “PEAP Inner Auth. Method” nastavenie autentizačnej metódy a taktiež nepovinné ale veľmi užitočný a často používaný “Accounting Enabled Port” zaznamenávanie prístupov užívateľov v 802.1x.

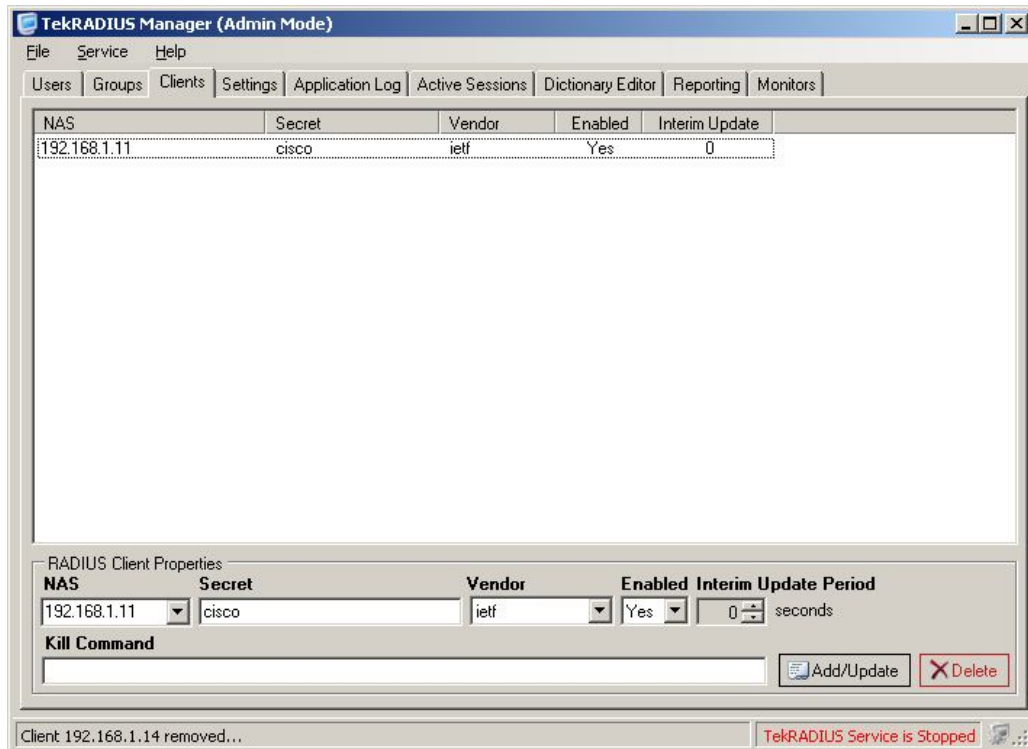


Obr. 10 Nastavenie service parametrov

Posledná záložka ALERTING (slúžiaca na varovné správy administrátorovi cez SMTP) nie je povinná a v tomto prípade pre potreby testovania 802.1x nebola nastavená.

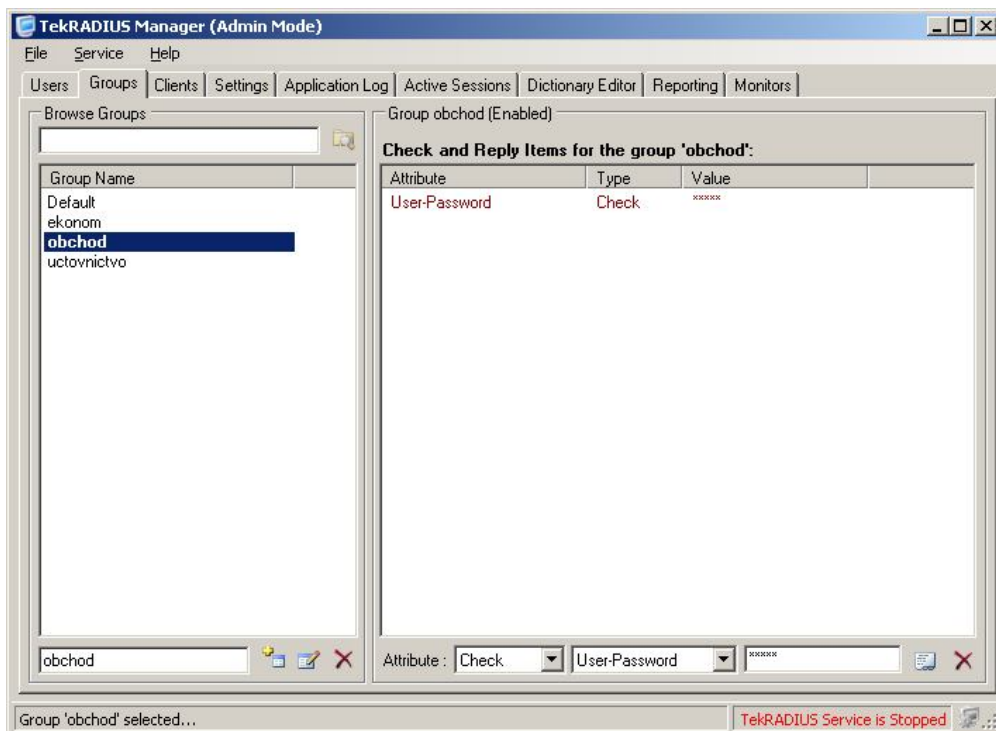
Nastavenie RADIUS klientov:

V tomto prípade je nastavený jeden RADIUS klient so zdieľaným kľúčom(secret), ktorý predstavuje daný CISCO SWITCH CATALYST 2960.



Obr. 11 Nastavenie RADIUS klienta

Vytvorenie skupín užívateľov:

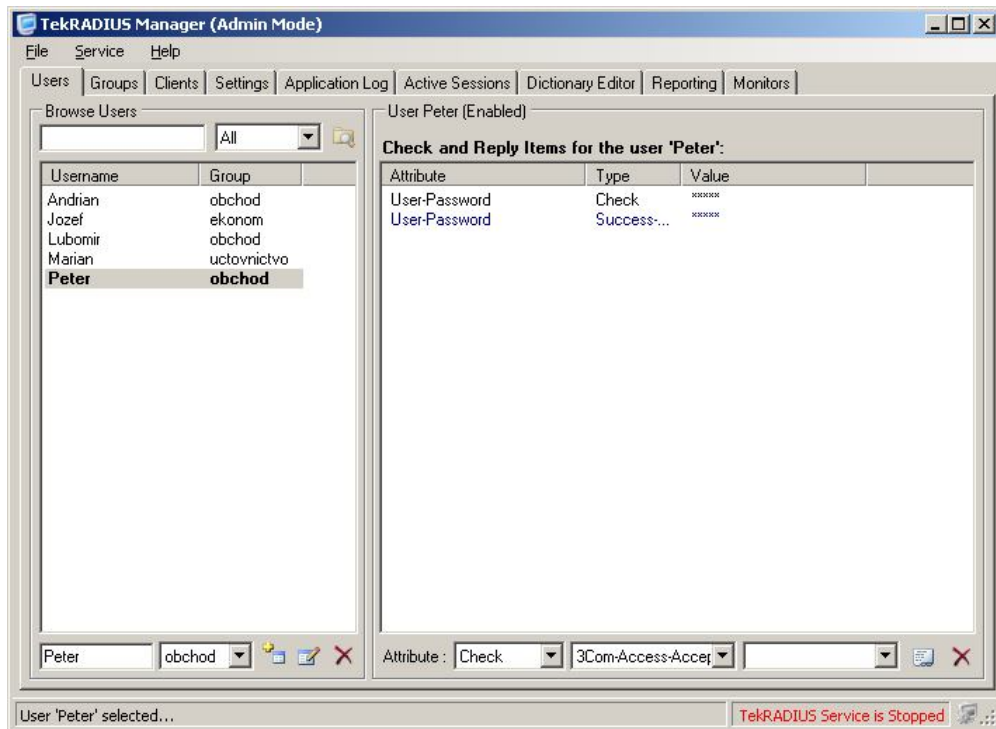


Obr. 12 Vytvorenie skupín užívateľov

Vytvorenie skupín je výhodné pre globálne nastavenie atribútov pre užívateľov, ktorý budú danej skupine prislúchať. Avšak je potrebné vedieť že atribúty skupiny sú sekundárne pred

užívateľskými atribútmi (tzn. užívateľské atribúty majú prednosť) v prípade, ak ich má užívateľ tiež nastavené. Skupina "Default" je automaticky vytvorená pri vytváraní databázových tabuliek a nie je možné ju zmazať, ale je možné ju upravovať.

Vytvorenie užívateľov:

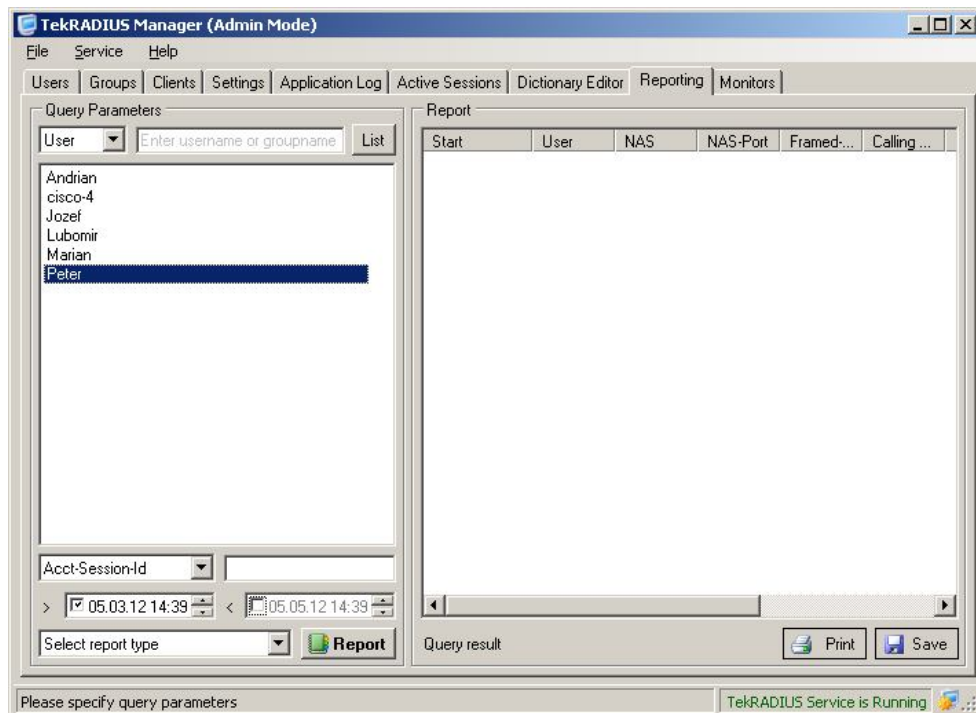


Obr. 13 Vytvorenie užívateľov

Užívateľov je nutné zaradiť do príslušajúcej skupiny a je možné im priradiť rôzne atribúty, ktoré pri autentizácii musí splniť. Atribúty užívateľa majú prednosť pred atribútmi skupiny.

Reporting - Accounting Records:

Táto časť slúži ako jednoduchý interface záznamov (prístupov) ktoré sú zaznamenávané počas autentizácie v accounting tabuľkách. Zobrazovať report je možné za jednotlivých užívateľov, v prípade nutnosti aj za skupiny.



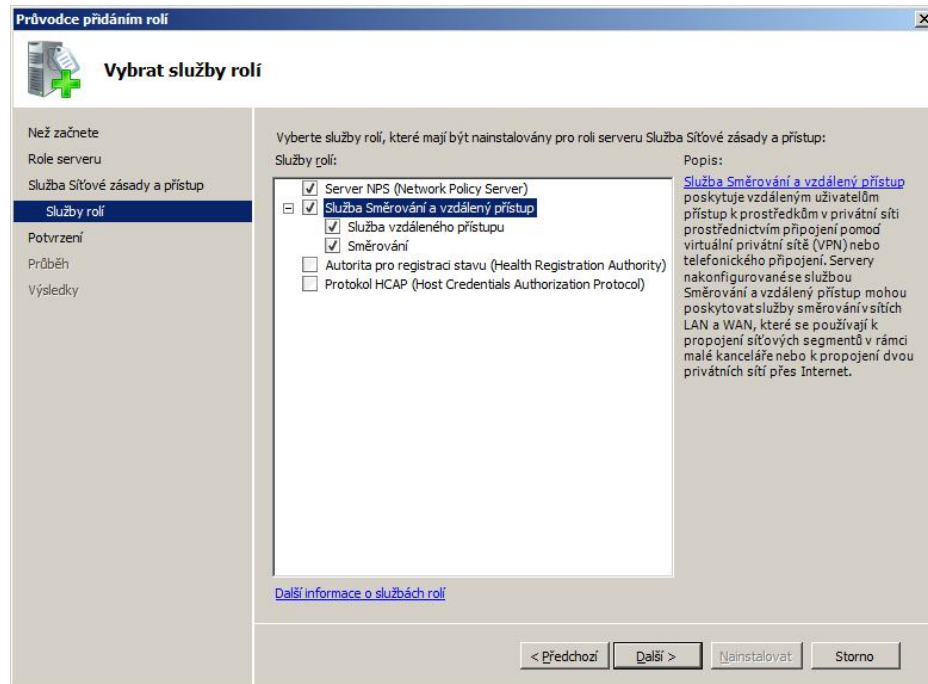
Obr. 14 Reporting

4.1.3 Microsoft Windows Server 2008 R2

Pre malé porovnanie RADIUS serverov som sa rozhodol pre testovanie nasadiť aj Windows Server 2008 R2. Nie je to síce vyslovene aplikácia určená len pre autentizáciu klientov ako TekRADIUS, no naopak je to komplexný serverový operačný systém ponúkajúci veľmi veľa ďalších možností v rámci práce so sieťou a službami počítačovej siete. Považujem to za pomerne veľkú výhodu práve aj v súvislosti s RADIUS serverom, keďže pomocou týchto funkcií môže zaujímavo rozšíriť možnosti nastavenia a využitia samotného servera.

4.1.4 Konfigurácia MS Windows Server 2008 R2

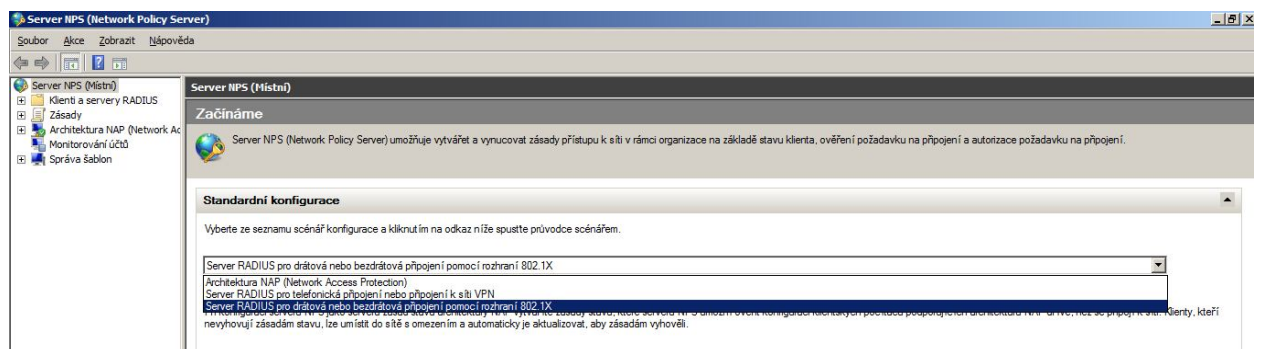
Ako prvý krok pre možnosť využívania služby autentizácie je nutné nainštalovať doplnujúcu rolu NPS (v starších verziach Windows Server IAS) v samotnom operačnom systéme (Obr. 15). NPS predstavuje vo Windows Server 2008 vlastne akúsi funkciu RADIUS vykonávajúcu AAA, poskytuje teda autentizačné a autentifikačné služby remote access klientov.



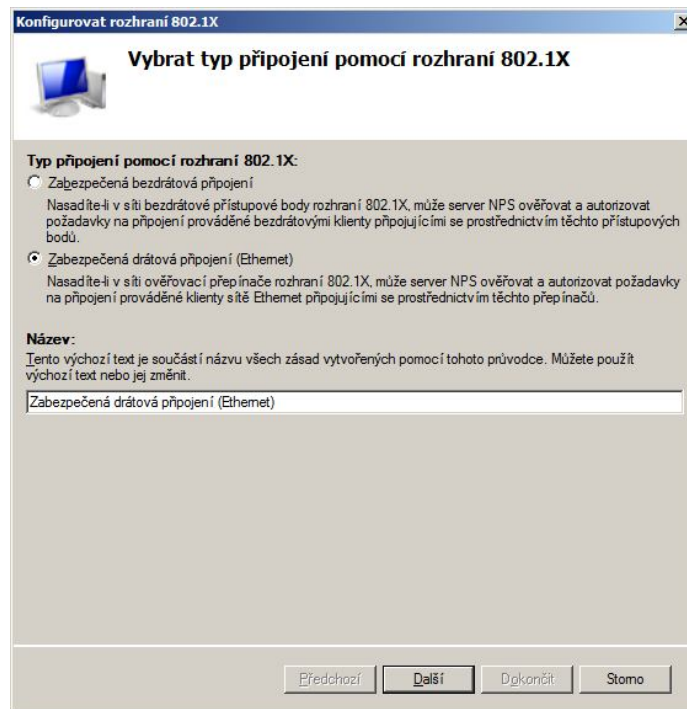
Obr. 15 Inštalácia NPS

Vytvorenie autentizačného klienta.

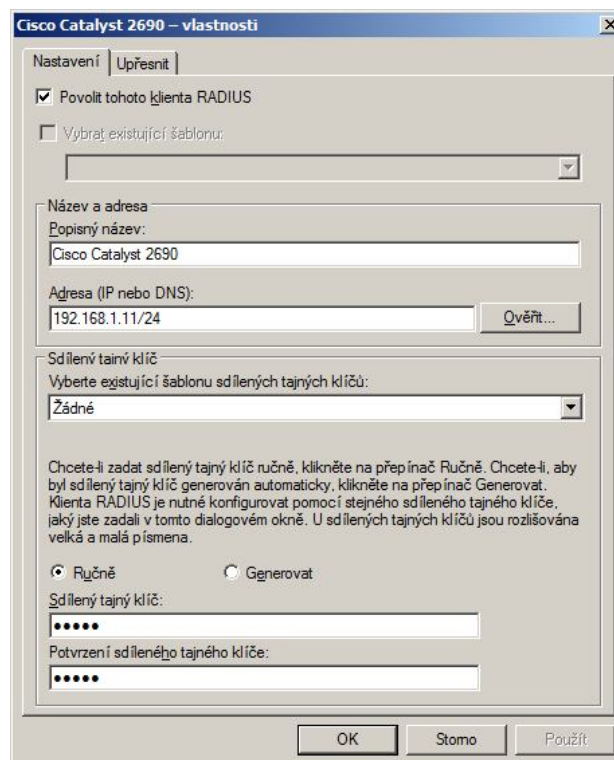
Po inštalácii NPS ďalej pokračujeme vytvorením profilu autentizačného klienta, nastavením jeho IP adresy a zdieľaného kľúča cez rozhranie NPS.



Obr. 16 Server NPS

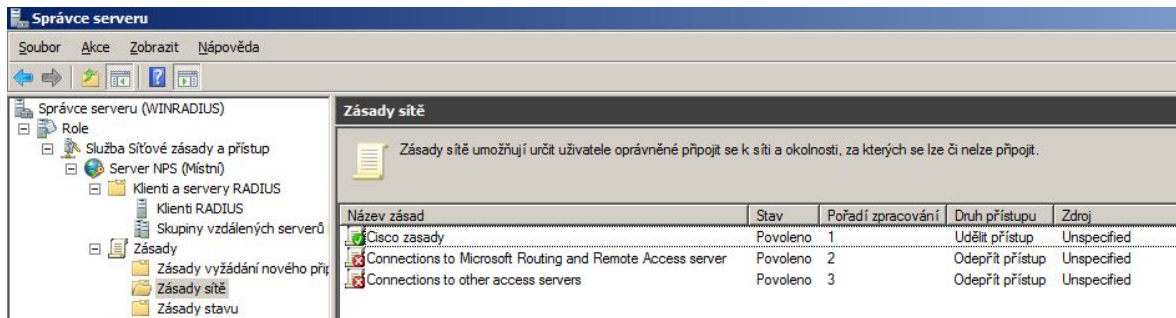


Obr. 17 Výber pripojenia

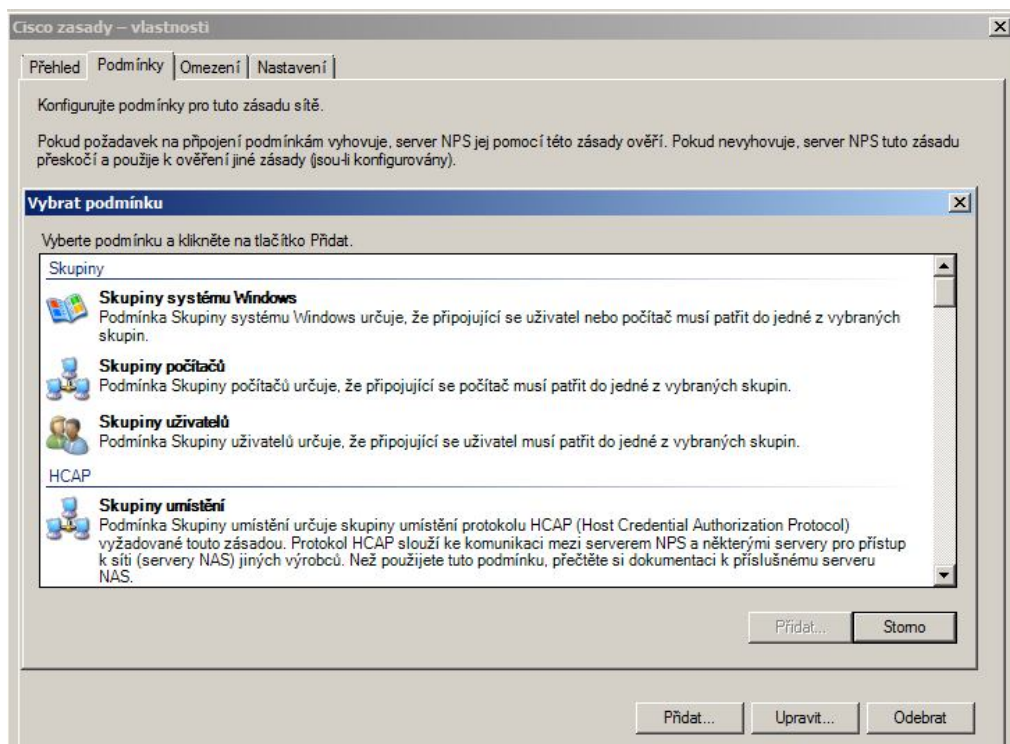


Obr. 18 Nastavenie RADIUS klienta

Následně pokračujeme vytvořením zásady sítě, kde se definují všechny podmínky, za kterých bude mít klient povolený přístup do sítě cez daný port. Podmínek, které se dají nadefinovat je skutečně velá a preto je možné vytvořit širokú kombinovanú škálu zásad.



Obr. 19 Vytvorenie zásady siete



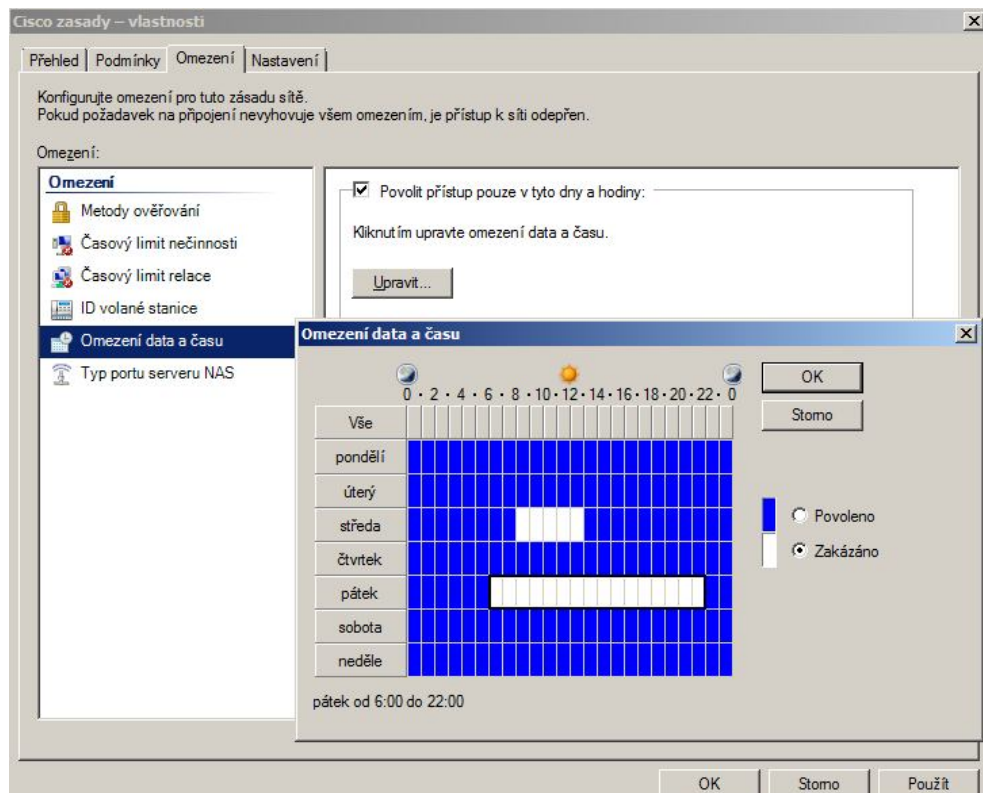
Obr. 20 Výber podmienky prístupu do siete

Taktiež je tu možné definovať rôzne obmedzenia napr. doby a dĺžky prístupu, definovanie typu metódy overovania a pod.

Pri testovaní v danom zapojení boli pre povolenie prístupu užívateľ'a do siete zvolené tieto podmienky:

- Skupiny užívateľ'ov: Administrators, Users
- IPv4 adresa klienta s prístupom: 192.168.1.21
- Povolené typy protokolov EAP:
 - Microsoft: Protokol PEAP (Protected EAP)

- Microsoft: Zabezpečené heslo (EAP-MSCHAP v2)



Obr. 21 Nastavenie obmedzení

Ďalšou z výhod Windows Serveru je, že v zásade nie je nutné využiť niektorý z iných databázových serverov (ale nie je to podmienka) ako tomu je pri TekRADIUS ktorý v tomto prípade využíva SQL databázu.

Užívateľ, ktorý prístupuje do siete pomocou 802.1x sa na pracovnej stanici prihlasuje pomocou užívateľského účtu, ktorý má vytvorený v samotnom Windows serveri a samozrejme musí spĺňať vopred vytvorené podmienky prístupu do siete. Obdobne to potom funguje aj skupinami, takže rôzne prístupové podmienky môžu byť aplikované aj na celé skupiny.



Obr. 22 Správa uživatel'ov a skupin

4.2 Konfigurácia CISCO SWITCH CATALYST 2960

Po zapnutí konzoly je aktivovaný globálny konfiguračný mód. Následne ďalšie riadky postupne zapínajú AAA, definujú že 802.1x má používať skupinu RADIUS zloženú zo všetkých definovaných RADIUS serverov a globálne zapínajú 802.1x.

```
Switch>enable
Switch>configure terminal
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system auth-control
```

Konfigurácia adresy RADIUS servera, portov pre autentizáciu a accounting a zdieľaného hesla(secret):

```
Switch(config)#radius-server host 192.168.1.14 auth-port 1812 acct-port 1813
Switch(config)#radius-server key cisco
```

Pre ukážku porty fa0/1 a fa0/2 nie je autentizácia vyžadovaná, čiže prístup do siete bude vždy povolený.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control force-authorized
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control force-authorized
Switch(config-if)#exit
```

Pre porty fa0/3 a fa0/4 je autentizácia vyžadovaná na základe toho ako je nastavený RADIUS server.

```
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
```

```
Switch(config-if)#exit
```

Všetky ostatné porty switchu ktoré sú nevyužívané z hľadiska bezpečnosti uvádzam do stavu neautorizovaného (*force-unauthorized*), tzn. že pokiaľ nebude zadaný `dot1x port control` budú tieto porty povoľovať len priechod rámcov CDP, STP a EAPoL.

```
Switch(config)#int range fa0/5 - 23
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#dot1x port-control force-unauthorized
Switch(config-if-range)#exit
```

Aby komunikácia medzi autentizačným RADIUS serverom a switchom správne fungovala je nutné ešte nastaviť VLAN s IP adresou a do tejto VLAN musí byť tiež pripojený samotný RADIUS server, ktorý je zapojený na porte fa 0/24.

```
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.1.11 255.255.255.0
Switch(config-if)#exit
Switch(config)#int fa0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#end
```

Nasledujúcim príkazom už len pre kontrolu zobrazím nastavenia jednotlivých nastavených portov.

```
Switch#show dot1x all
```

```

COM1 - PuTTY
Switch#sh dot1x all
Sysauthcontrol          Enabled
Dot1x Protocol Version  2

Dot1x Info for FastEthernet0/1
-----
PAE                      = AUTHENTICATOR
PortControl              = FORCE_AUTHORIZED
ControlDirection        = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout           = 0
SuppTimeout             = 30
ReAuthMax                = 2
MaxReq                  = 2
TxPeriod                = 30

Dot1x Info for FastEthernet0/2
-----
PAE                      = AUTHENTICATOR
PortControl              = FORCE_AUTHORIZED
ControlDirection        = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout           = 0
SuppTimeout             = 30
ReAuthMax                = 2
MaxReq                  = 2
TxPeriod                = 30

Dot1x Info for FastEthernet0/3
-----
PAE                      = AUTHENTICATOR
PortControl              = AUTO
ControlDirection        = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout           = 0
SuppTimeout             = 30
ReAuthMax                = 2
MaxReq                  = 2
TxPeriod                = 30

Dot1x Info for FastEthernet0/4
-----
PAE                      = AUTHENTICATOR
PortControl              = AUTO
ControlDirection        = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout           = 0
SuppTimeout             = 30
ReAuthMax                = 2
MaxReq                  = 2
TxPeriod                = 30

Dot1x Info for FastEthernet0/5
-----
PAE                      = AUTHENTICATOR
PortControl              = FORCE_UNAUTHORIZED

```

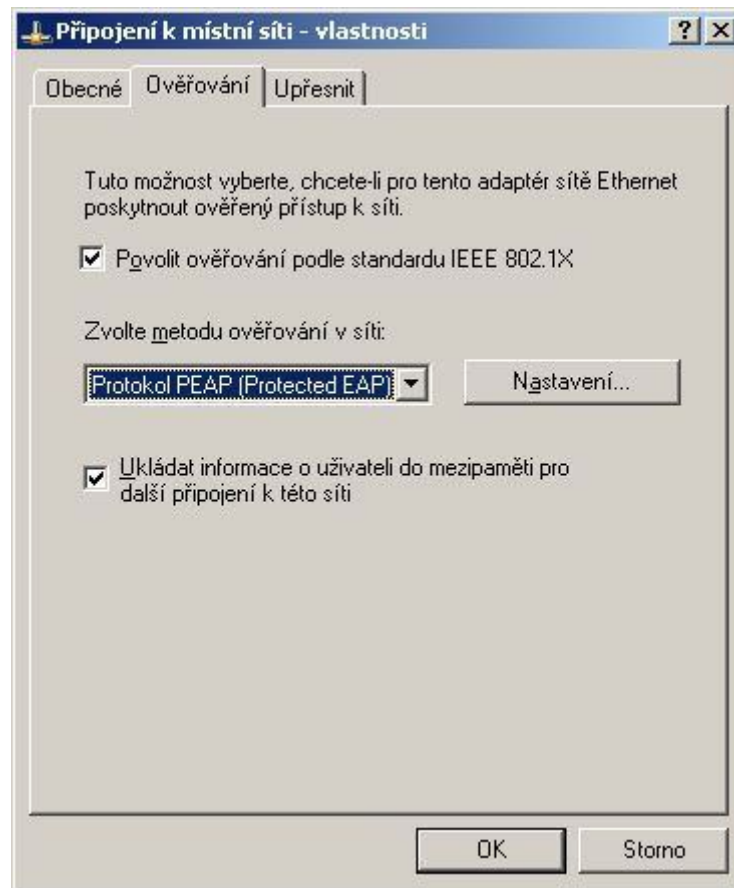
Obr. 23 Výpis nastavenia portov pomocou show

Na záver je potrebné uložiť nakonfigurované nastavenia.

```
Switch#copy running-config startup-config
```

4.3 Konfigurácia klienta

MS Windows XP ale taktiež Windows Vista, 7 či rôzne edície Linuxu alebo Mac OS obsahujú podporu pre protokol IEEE 802.1x. Zapnutie konfigurácie sa vykonáva pre jednotlivé sieťové pripojenia. V prípade že podpora pre 802.1x nie je vo Windows zapnutá, je nutné pre jej využitie naštartovať službu *Wired AutoConfig*.



Obr. 24 Nastavenie vo WIN XP

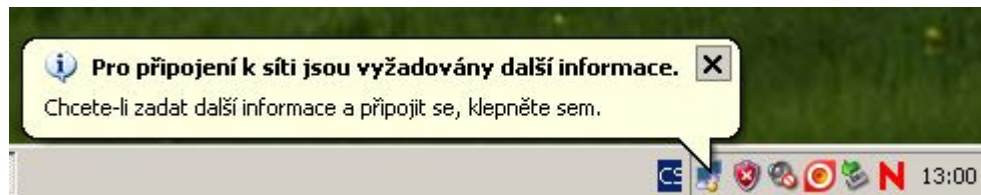
Nastavenie samozrejme odpovedá tomu, ako je nastavený RADIUS server.

- Prvá položka “Povolit ověřování podle standardu IEEE 802.1X” povoľuje alebo zakazuje prístup využitia protokolu 802.1x
- V “Zvolte metodu ověřování v síti” je vybratá autentizačná metóda ktorá bude používaná pri overovaní

4.4 Priebeh autentizácie

Za predpokladov, že celá konfigurácia ako RADIUS servera tak aj RADIUS klienta je správna, po pripojení klienta káblovou formou do siete (v tomto prípade do portu fa 0/3 kde je autentizácia vyžadovaná) je automaticky spustená komunikácia cez EAPOL protokol medzi klientom a RADIUS klientom. Vznikne teda požiadavka na overenie od samotného klienta. Následne v závislosti na nastavení RADIUS servera (podmienky pripojenia) sú

switchom vyžiadané od užívateľa ďalšie informácie na základe ktorých závisí, či bude mať užívateľ prístup do siete povolený, alebo odmietnutý.



Obr. 25 Pripojenie klienta do siete



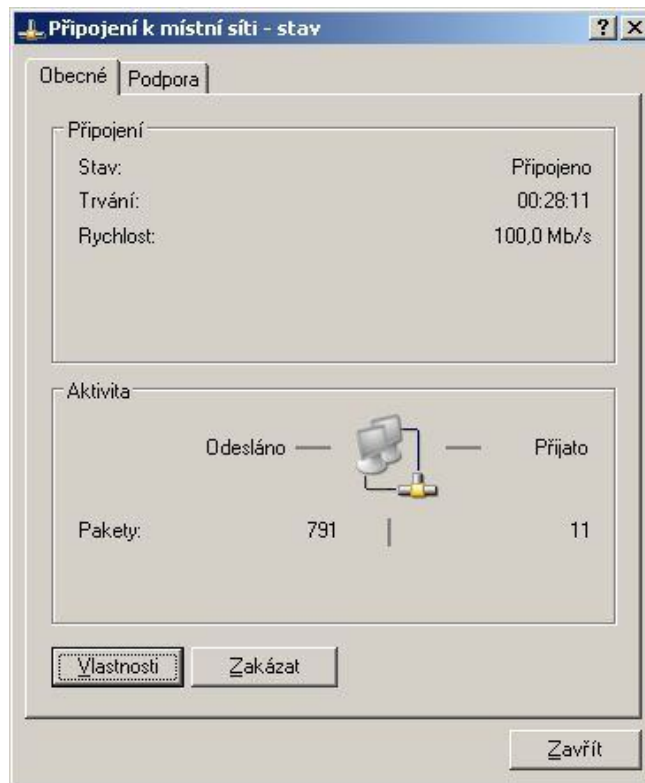
Obr. 26 Vyžiadanie prihl. mena a hesla

Pri splnení podmienok vopred nastavených na RADIUS serveri v prípade, že prebehne autentizácia užívateľa v poriadku má klient prístup do siete povolený. Priebieh takejto úspešnej autentizácie je zaznamenávaný aj priamo v konzole switchu, čoho je dôkazom aj samotný výpis CISCO SWITCH CATALYST:

```
*Mar 1 00:24:47.006: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
```

```
*Mar 1 00:25:04.060: %DOT1X-5-SUCCESS: Authentication successful for client (0019.990c.d36a) on Interface Fa0/1
```

```
*Mar 1 00:25:04.060: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (0019.990c.d36a) on Interface Fa0/3
```



Obr. 27 Povolený přístup

V opačnom prípade že klient nespĺňa podmienky je samozrejme jeho prístup do siete automaticky odmietnutý.

```
*Mar 1 00:17:55.838: %AUTHMGR-5-START: Starting 'dot1x' for client (0019.990c.d36a) on Interface Fa0/3
```

```
*Mar 1 00:18:35.231: %DOT1X-5-FAIL: Authentication failed for client (0019.990c.d36a) on Interface Fa0/3
```

```
*Mar 1 00:18:59.852: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```



Obr. 28 Prístup odmietnutý

Samozrejme obdobná situácia nastáva aj v prípadoch portov, ktoré sú nastavené v stavoch *force-authorized* (prístup vždy povolený bez autentizácie, fa 0/1 a fa 0/2) a *force-unauthorized* (prístup vždy odmietnutý, fa 0/5 až fa 0/23).

Čo sa deje v prípade odpojenia siete alebo nečinnosti pripojeného užívateľa v sieti?

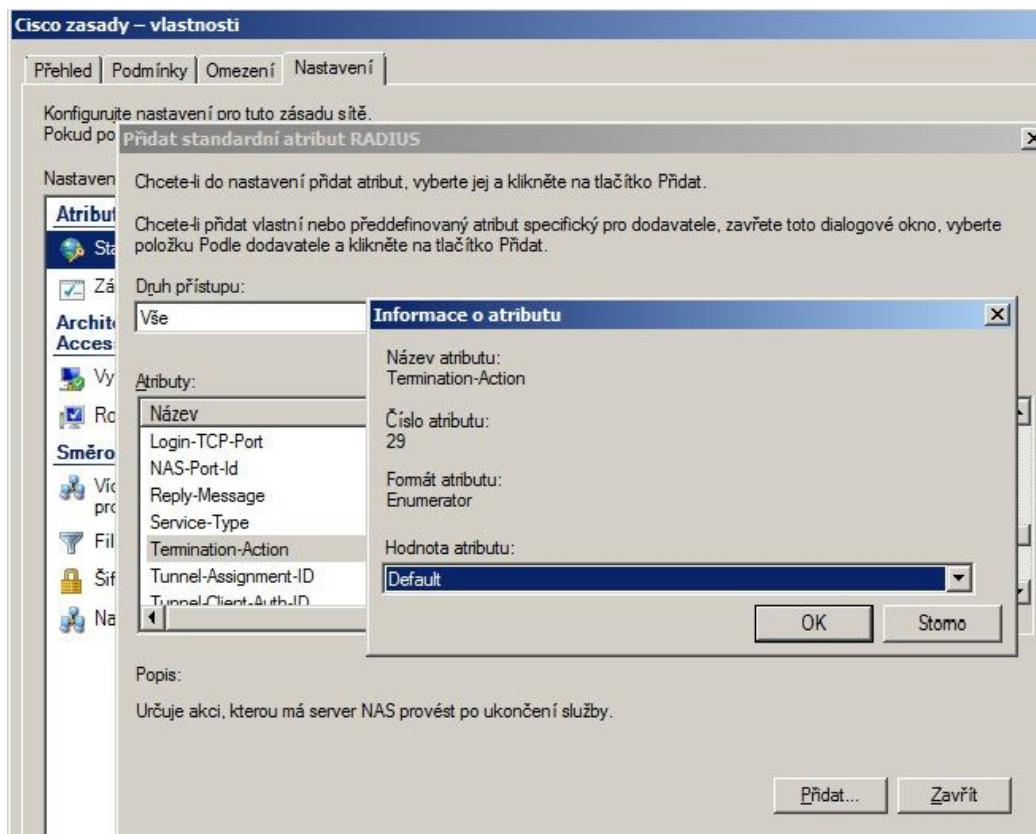
Ako už je spomínané v konfigurácií RADIUS servera či už sa jedná o TekRadius alebo MS Windows Server 2008, ponúka veľa možností nastavenia zásad bezpečnosti a ďalších pomocných nastavení, ktoré zvyšujú úroveň zabezpečenia, informácie o prehľade prístupov a stave siete.

S týmto sa spája aj základné zabezpečenie v prípade dlhšej nečinnosti, ale predovšetkým prípad kedy užívateľ ukončí prácu a vypne počítač. V takom prípade je jednoznačne nutné aby RADIUS server vykonával tzv. re-autentizáciu klienta, čo v prakticky znamená že znovu overí klientove identifikačné údaje a jeho prístup do siete bude znovu povolený alebo odmietnutý.

Switch vykonáva re-autentizáciu klienta v nastávajúcich prípadoch:

- re-autentizácia je aktivovaná periodicky a vyprší jej nastavený časový interval
- re-autentizácia je vykonaná ručne

V prípade **periodickej** re-autentizácie je potrebné nastaviť na serveri RADIUS atribúty *Session-Timeout* (Atribút [27]) a *Termination Action* (Atribút [29]). *Session-Timeout* definuje čas, po ktorom bude vykonávaná re-autentizácia (resp. periodičita). *Termination Action* definuje aké akcie budú vykonané po prebehnutí re-autentizácie, pričom sa jedná sa o akcie Inicializácia a re-autentizovanie užívateľa.



Obr. 29 Nastavenie atribútu Termination-Action

V prípade **manuálnej** reautentizácie je to možné urobiť cez konzolu vložením príkazu **dot1x re-authenticate interface**.

```
Switch#dot1x re-authenticate interface fa0/3
```

5 VÝHODY A NEVÝHODY RIEŠENIA

Keď zhrnieme výhody a nevýhody tohto riešenia, zistíme že v konečnom dôsledku je váha výhod prevažujúca druhú stranu nevýhod. Napokon je nutné dodať, že i keď si to bežný užívateľ pri použití počítača pripojeného k sieti neuvedomí, či už v menších lokálnych sieťach, veľkých korporáciách alebo v samotnej sieti Internet je práve toto zabezpečenie štandardom 802.1x úplnou samozrejmosťou. Tzn. že overovanie užívateľov prebieha takmer v každej sieti a osobne by som to ani nepriradil k výhodám ako takým, ale označil by som to priamo za nutnosť využívať v každej zabezpečenej sieti.

5.1 Výhody

Zvýšenie úrovne bezpečnosti siete

- blokovanie nežiaducich užívateľov – jedna z najzákladnejších úloh 802.1x je teda povoliť alebo odmietnuť užívateľovi prístup do počítačovej siete k všetkým informáciám a jej službám
- zadeľovanie užívateľov do vopred vytvorených užívateľských skupín – skupiny s vopred určenými zásadami, ktoré patria daným užívateľom zaradeným do špecifickej skupiny. Na základe toho nie je nutné definovať zásady pre každého užívateľa zvlášť, čo značne uľahčí prácu pri ich väčšom počte.
- Sledovanie činnosti užívateľov - súčasťou 802.1x je Accounting. Ide vlastne o možnosť sledovania každého jedného prístupu pripojeného k portu. Tzn. že je možné zbierať informácie (ktoré sú odosielané zo switchu na RADIUS server), ktorý počítač bol pripojený na daný port, dobu pripojenia, identifikácia užívateľa a rôzne iné informácie pomáhajúce identifikovať prípadné útoky alebo pokusy neoprávnených užívateľov od prístupu do siete.

Škálovateľná architektúra

RADIUS server vytvára akúsi centrálnu databázu užívateľov a dostupných služieb, pričom táto vlastnosť je oceňovaná predovšetkým v situáciách, kedy je počítačová sieť rozsiahla a obsahuje väčší počet vstupných zariadení ku ktorým sa je možné pripojiť v sieti. Každé jedno zariadenie, ktoré vie byť RADIUS klientom dokáže komunikovať s RADIUS

serverom. Práve toto zaručuje, že vzdialený užívateľ má umožnené pripojenie na ľubovoľné vstupné zariadenie (v tomto prípade switch) a vždy má poskytnutý rovnaký prístup.

Široké spektrum možnosti výberu programového ale i hardwarového vybavenia / otvorenosť voči budúcnosti

Spomedzi mnohých výrobcov ponúkajúcich (či už ide o HW alebo SW) dnes už veľké množstvo produktov, z ktorých je možno vybrať jeden vyhovujúci veľkosti a rôznym požiadavkám siete. Pri navrhovaní, prípadne pri rozširovaní siete je možné si zvoliť dodávateľa.

Mobilita užívateľa

Užívateľ sa môže pripojiť na akomkoľvek mieste, prípadne akomkoľvek počítači, ktorý má prístup do danej siete využívajúcej 802.1x. Môže sa teda prihlásiť pod danými prihlasovacími údajmi, sú mu pridelené vždy tie isté zásady a využíva tie isté služby siete.

Možnosti pridelovania užívateľov do tzv. VLAN sietí

Užívatelia sú na rovnakej fyzickej sieti, avšak na logickej úrovni môžu byť pridelení do jednotlivých virtuálnych sietí napr. na rôzne pracovné úseky podniku (účtovníci, administrátori, študenti, atď.). To má za dôsledok že daní užívatelia majú prístup výhradne k tej sieti a informáciám, ku ktorým patria a neohrozujú bezpečnosť ostatných sietí napr. vírusmi a pod.

Finančné náklady na sieť

V spojení s priradovaním do VLAN nie je nutné mať fyzicky rozsiahlu sieť s množstvom podsietí prepojených pomerne drahými zariadeniami ako sú routre, ale stačí práve pomocou technológie 802.1x pridelovať užívateľov do VLAN, čím je zabezpečená separácia užívateľov medzi sieťami. Je to jeden zo spôsobov ako ušetriť náklady a zjednodušiť fyzickú štruktúru siete.

5.2 Nevýhody

Vzdialená správa PC

V danom momente kedy je PC pripojené k portu ktorý je neautorizovaný, nemá prístup k sieti. Tu nastáva problém v prípade nutnosti správy daného PC formou vzdialeného prístupu, tzn. že v tomto prípade to nie je možné.

Nutnosť kombinácie zabezpečenia spolu s inými metódami

Všeobecne platí, že žiaden druh ochrany nie je tak dokonalý, aby zaručil sto percentnú bezpečnosť. Ak sa útočníkovi podarí prekonať druh zabezpečenia siete s využitím výhradne protokolu 802.1x, nie je zaručené žiadne ďalšie zabezpečenie. Pohyb a využitie služieb siete nie je nijak inak obmedzené. Z tohto vyplýva že je priam nutné využiť kombináciu ešte s iným druhom zabezpečenia.

ZÁVER

Cieľom tejto práce bolo popísať princípy činnosti autentizácie portov pomocou štandardu 802.1x, zrealizovať a overiť činnosť celého takéhoto systému s využitím konkrétnych zariadení a zhodnotiť výhody a nevýhody riešenia.

V prvej teoretickej časti práce sú v jednotlivých kapitolách vysvetlené dané protokoly, kde každý z nich zohráva svoju podstatnú úlohu pre komunikáciu a prenos informácií medzi jednotlivými zariadeniami v počítačovej sieti pri autentizácii. Ďalej sú popisované úlohy a princípy jednotlivých zariadení zúčastnených pri autentizácii, rôzne podrobnosti ohľadne možnosti nastavenia switchu, správania a stavov jeho portov po pripojení klienta. V ďalšej praktickej časti je už preberané konkrétne navrhnuté testovacie zapojenie siete, ktoré je možné vidieť na foto obrázku, konfigurácia týchto zariadení a ich programového vybavenia. Nakoniec sú zhrnuté výhody a nevýhody celého riešenia tohto systému.

Pri realizácii riešenia navrhnutého zapojenia sa konfigurovali tri zariadenia a síce RADIUS server, RADIUS klient a klient (pracovná stanica). Konkrétne RADIUS server, čo sa týka programového vybavenia volil ako prvý testovaný software pre RADIUS TekRadius pod operačným systémom MS Windows XP ako jednoduchšiu variantu z hľadiska konfigurácie. Tu sú v jednotlivých podkapitolách uvedené presné postupy konfigurácie. Pre porovnanie ako druhú variantu som zvolil za RADIUS server MS Windows Server 2008 RC2.

Z hľadiska možností využitia a prepojenia RADIUS servera z rôznymi službami ponúkajúcimi od MS Windows Server 2008 R2 vychádza lepšie. Je oveľa komplexnejší a ponúka väčšie spektrum možností. Z týchto troch zariadení sa pri testovaní autentizácie klienta na jednotlivých RADIUS serveroch v zásade u RADIUS klienta a klienta konfigurácia nemenila. Bohužiaľ pre pomerne veľké množstvo nastavení ponúkajúce oboma RADIUS servermi okrem overenia funkčnosti riešenia nebolo možné v rámci práce otestovať všetky možnosti nastavenia a ich kombinácie.

Čo sa týka tohto riešenia, RADIUS serverov je k dispozícii aktuálne veľké množstvo. Pochopiteľne v rámci tejto práce nebolo možné vyskúšať všetky. Avšak pokiaľ by som mal vybrať na základe tejto osobnej skúsenosti, zvolil by som MS Windows Server 2008 prípadne jeho novšiu verziu.

CONCLUSION

The aim of this study was to describe the operating principles of authentication ports by using 802.1x, realization and verifying the operation of such system using specific equipment and

assess the advantages and disadvantages of solutions.

In the first theoretical part each chapter explains the protocols, each of which plays a major role in the communication and transferring of the information between devices in a computer network on authentication. Also tasks are described, the principles of individual facilities participating in the authentication, options of switch settings, behavior and status of its ports for client connections. In another practical part has been discussed specifically designed test system involvement, which can be seen in the photo image, the configuration of these devices and their software. Finally, summarizing the advantages and disadvantages of the solution of this system.

In the realization of proposed solutions three devices are configured and although RADIUS server, RADIUS client and the client (workstation). Particular RADIUS server as the software elected as the first test software for RADIUS TekRadius the operating system MS Windows XP as an easier option in terms of configuration. Here are the various subsections the exact configuration procedures. For comparison, I chose the second option RADIUS server for MS Windows Server 2008 RC2.

In terms of the possibility of using a link from the RADIUS server offering various services from MS Windows Server 2008 R2 builds better. It is much more complex and offers a wider range of options. None of these three devices has changed in testing of client authentication to RADIUS servers in principle with the client and the RADIUS client configuration. Unfortunately, the relatively large number of settings that offer both RADIUS servers in addition to verifying the functionality of the solution was not possible in the work to test all settings and their combinations in the work.

In this solution, many RADIUS servers is currently available. Of course was not possible to test all of them, but if I can personally advise with this personal experience I would definitely recommend OS MS Windows Server 2008 or a later version.

ZOZNAM POUŽITÉJ LITERATURY

- [1] MCQUERRY, Steve, David JANSEN a Dave HUCABY. *Cisco LAN switching configuration handbook*. 2nd ed. Indianapolis, IN: Cisco Press, c2009, 333 s. Cisco Press networking technology series. ISBN 15-870-5610-0.
- [2] Catalyst 2960 Switch Software Configuration Guide: Configuring IEEE 802.1x Port-Based Authentication. CISCO SYSTEMS, Inc. [online]. [cit. 2012-01-05]. Dostupné z: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/sw8021x.html
- [3] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-802-5125-205.
- [4] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.
- [5] LUDVÍK, Miroslav a Bohumír ŠTĚDRŮŇ. *Teorie bezpečnosti počítačových sítí*. Vyd. 1. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-808-6686-356.
- [6] Extensible Authentication Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-12]. Dostupné z: http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
- [7] ABOBA, B., L. BLUNK, J. VOLLBRECHT, J. CARLSON a H. LEVKOWETZ. *The Internet Engineering Task Force* [online]. [June 2004] [cit. 2012-04-12]. Dostupné z: <http://tools.ietf.org/html/rfc3748>
- [8] TekRADIUS - Radius Server for Windows. KAPLAN, Yasin. *TekRADIUS - Radius Server for Windows: TekRADIUS Installation & Configuration Guide* [online]. 4.4. © 2007-2012 [cit. 2012-05-02]. Dostupné z: <http://www.tekradius.com/>

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AAA	Authentication Authorization Accounting
CDP	Cisco Discovery Protocol
EAP(OL)	Extensible Authentication Protocol (over LAN)
IAS	Internet Authentication Service
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetwork Operating System
IP	Internet Protocol (Address)
MAC	Media Access Control Address
NPS	Network Policy Server
OS	Operating System
OSI	Open Systems Interconnect
OTP	One – Time - Password
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
(V)LAN	(Virtual) Local Area Network

ZOZNAM OBRÁZKOV

OBR. 1	FORMÁT EAP PACKETU [7].....	12
OBR. 2	802.1X ÚLOHY ZARIADENÍ [2].....	14
OBR. 3	VÝVOJOVÝ DIAGRAM MOŽNOSTÍ PROCESU AUTENTIZÁCIE	16
OBR. 4	VÝMENA SPRÁV [2]	18
OBR. 5	VÝMENA SPRÁV POČAS MAC AUTHENTICATION BYPASS [2]	19
OBR. 6	SCHÉMA ZAPOJENIA.....	25
OBR. 7	ZAPOJENIE V RACK-U.....	26
OBR. 8	NASTAVENIE SQL SPOJENIA S DB.....	28
OBR. 9	VYTVORENIE TABULIEK V DB SQL.....	29
OBR. 10	NASTAVENIE SERVICE PARAMETROV	30
OBR. 11	NASTAVENIE RADIUS KLIENTA.....	31
OBR. 12	VYTVORENIE SKUPÍN UŽÍVATEĽOV	31
OBR. 13	VYTVORENIE UŽÍVATEĽOV	32
OBR. 14	REPORTING.....	33
OBR. 15	INŠTALÁCIA NPS.....	34
OBR. 16	SERVER NPS	34
OBR. 17	VÝBER PRIPOJENIA	35
OBR. 18	NASTAVENIE RADIUS KLIENTA.....	35
OBR. 19	VYTVORENIE ZÁSADY SIETE	36
OBR. 20	VÝBER PODMIENKY PRÍSTUPU DO SIETE	36
OBR. 21	NASTAVENIE OBMEDZENÍ.....	37
OBR. 22	SPRÁVA UŽÍVATEĽOV A SKUPÍN.....	37
OBR. 23	VÝPIS NASTAVENIA PORTOV POMOCOU SHOW	40
OBR. 24	NASTAVENIE VO WIN XP	41
OBR. 25	PRIPOJENIE KLIENTA DO SIETE	42
OBR. 26	VYŽIADANIE PRIHL. MENA A HESLA.....	42
OBR. 27	POVOLENÝ PRÍSTUP	43
OBR. 28	PRÍSTUP ODMIETNUTÝ.....	44
OBR. 29	NASTAVENIE ATRIBÚTU TERMINATION-ACTION.....	45

ZOZNAM TABULIEK

TABUĽKA 1	FORMÁT EAPOL.....	12
TABUĽKA 2	TYP PACKETU	13

ZOZNAM PRÍLOH

- P I Dotazy pre vytvorenie tabuliek v databáze SQL pre TekRadius server
 CD-ROM:\prilohy\dotazy_tekradius.sql
- P II Inštačný balík RADIUS serveru TekRadius
 CD-ROM:\prilohy\RadiusTestSetup.exe