Autentizace, autorizace a accounting v prostředí IEEE 802.1X / RADIUS

2007 **Bc. Martin Stankuš**

Obsah

Abstrakt

Cílem této práce je zmapovat možnosti AAA (authentication, authorization, accounting) v síti při použití protokolu IEEE 802.1x a serveru RADIUS. Práce je zaměřena na použití switche Cisco Catalyst 2960 a RADIUS serveru FreeRADIUS, avšak obecné závěry jsou aplikovatelné i na jiný síťový hardware a software.

Abstract

This work describes possibilities of AAA (authentication, authorization, accounting) using IEEE 802.1x protocol and RADIUS server. Although effort was directed to Cisco catalyst 2960 Ethernet switch and RADIUS server FreeRADIUS, general conclusions are aplicable to wide range of network hardware and software.

1.) Úvod

Při výstavbě počítačových sítí je třeba brát zřetel na bezpečnost. Základem bezpečnosti je znemožnění přístupu k síti nežádoucím uživatelům a kontrola legitimních uživatelů. K dosažení těchto cílů lze použít prostředky AAA (authentication, authorization, accounting), které jsou poskytovány protokolem IEEE 802.1x a serverem RADIUS.

2.) AAA

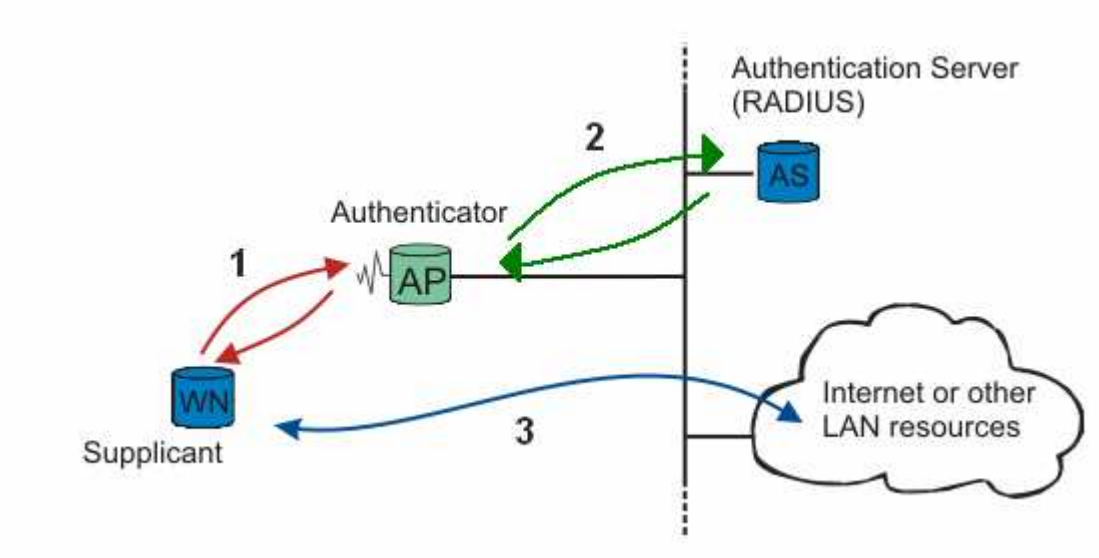
AAA je zkratka označující autentizaci, autorizaci a accounting. Autentizace je ověření identity uživatele autentizační autoritou, v tomto případě serverem RADIUS s použitím protokolu EAP. Autorizací se rozumí přidělení přístupových práv uživateli, který úspěšně absolvoval proces autentizace, respektive nepřidělení těchto práv uživateli, který autentizačním požadavkům nevyhověl. Accounting je sběr provozních informací o autorizovaném uživateli, typicky se jedná o údaje o přeneseném množství dat, trvání připojení k síti a identifikaci přístupového bodu, ze kterého bylo k síti přistupováno.

3.) EAP

EAP (Extensible Authentication Protocol) je rodina autentizačních protokolů. V této práci je použit protokol EAP-TLS, založený na asymetrické kryptografii a umožňující vzájemnou autentizaci nejen klienta autentizačnímu serveru, ale i autentizačního serveru klientovi, čímž lze předcházet útokům typu „evil twin“. Detailní popis standardu EAP přesahuje rámec této práce, je k dispozici např. ve zdroji [1].

4.) IEEE 802.1X

IEEE 802.1X (dále jen 802.1X) je protokol pro autentizaci klienta v lokální síti. Protokol pracuje na druhé vrstvě modelu OSI (Data Link Layer), jedná se proto o řízení přístupu na úrovni portu switche, nebo virtuálního portu přístupového bodu WLAN („port based network access control“). Podstatou protokolu 802.1X je enkapsulace zpráv protokolu EAP v rámcích sítě, na které je systém 802.1X provozován. Nejedná se tedy o nic jiného, než o pouhé „zabalení“ zpráv EAP tak, aby tyto zprávy bylo možné předávat bez účasti třetí vrstvy modelu OSI (Network Layer). Podle terminologie 802.1X je klient žádající o přístup do sítě nazýván „supplicant“, switch / access point zpracovávající požadavek je nazýván „authenticator“ (viz. obr. 1).

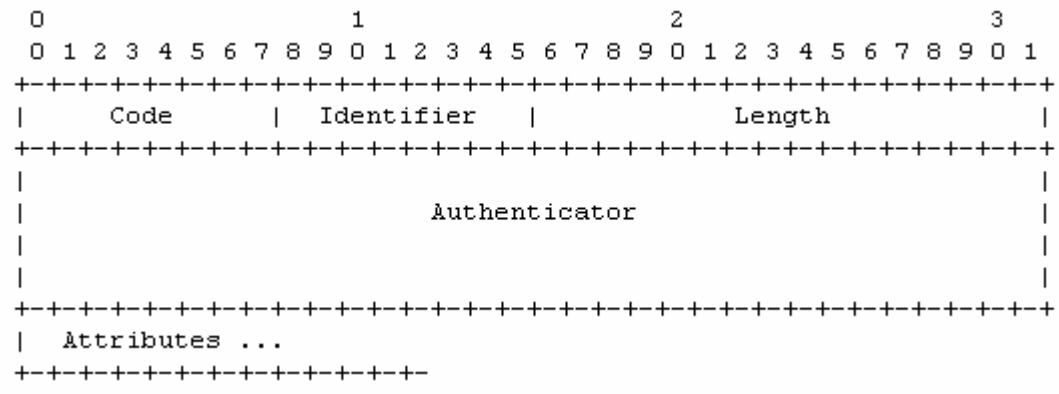


Obr. 1: IEEE 802.1X autentizace

Jak je patrné z obr. 1, přístup do sítě (označen 3) je povolen na základě 802.1X autentizace (označena 1). Je nezbytné upozornit na skutečnost, že nedochází k přímé komunikaci klienta s autentizačním serverem (obvykle se jedná o server RADIUS, jak je uvedeno na obrázku) a autentizační protokol 802.1X tedy nemá přímou souvislost s vlastní autentizací u serveru RADIUS. Komunikace s autentizačním serverem je vedena prostřednictvím switche / access pointu, který vystupuje v roli rozhraní mezi EAP zprávami enkapsulovanými v rámcích 802.1x podle standardu EAPOL (označeny 1) a EAP zprávami enkapsulovanými v atributech protokolu RADIUS (označeny 2).

5.) RADIUS

RADIUS (Remote Authentication Dial In User Service) je AAA systém umožňující zabezpečení sítě a sběr informací o uživatelích sítě prostřednictvím přístupových bodů sítě, například AP nebo switche. Server RADIUS poskytuje autheticatorovi služby autentizace a autorizace na UDP portu 1812, accounting je provozován na UDP portu 1813. Formát hlavičky paketu RADIUS je vždy stejný (viz. obr. 2).



Obr. 2: Hlavička paketu RADIUS

Pole Code obsahuje identifikátor požadované operace. Možné hodnoty jsou uvedeny v tabulce 1.

Hodnota pole Code	Operace	Význam
1	Access-Request	Authenticator -> RADIUS, žádost o autentizaci
2	Access-Accept	RADIUS -> Authenticator, autentizace úspěšná, autorizace
3	Access-Reject	RADIUS -> Authenticator, autentizace neúspěšná
4	Accounting-Request	Authenticator -> RADIUS, žádost o accounting
5	Accounting-Response	RADIUS -> Authenticator, potvrzení accountingu
11	Access-Challenge	RADIUS -> Authenticator, žádost o další informace od klienta (pokračování EAP toku)

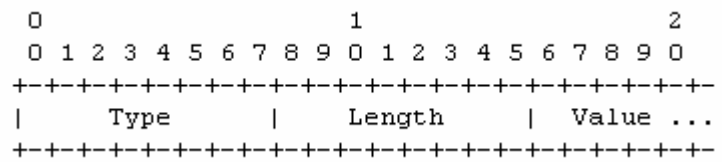
Tab. 1: Pole Code paketu RADIUS

Pole Identifier obsahuje pomocnou náhodnou hodnotu umožňující identifikovat duplicitní pakety. Toto pole je nezbytné, protože systém RADIUS využívá jako transportní protokol bezstavový protokol UDP.

Pole Length udává celkovou velikost paketu v oktetech, minimální velikost činí 20 B, maximální velikost činí 4096 B.

Pole Authenticator je použito k zabezpečení komunikace mezi authenticatorem a serverem RADIUS. Obsahem pole v paketu pocházejícím v authenticatorovi je náhodné číslo. Pokud paket pochází ze serveru RADIUS, je jeho hodnotou MD5 hash vypočítaný z přijaté zprávy Access-Request / Accounting-Request a sdíleného hesla, které je známé jak authenticatorovi, tak serveru RADIUS. Z toho vyplývá, že autentizován je jen server RADIUS authenticatorovi, naopak ne. Autentizace authenticatora serveru RADIUS je možná při použití RADIUS atributu „User-Password“, tento atribut ale není v prostředí 802.1X používán. Velikost pole Authenticator je 16 oktetů.

Za hlavičkou paketu RADIUS následují specifické atributy, tzv. hodnoty AVP (Attribute Value Pair). Formát AVP se může podle typu atributu poněkud lišit, obecné schéma je patrné z obrázku 3.

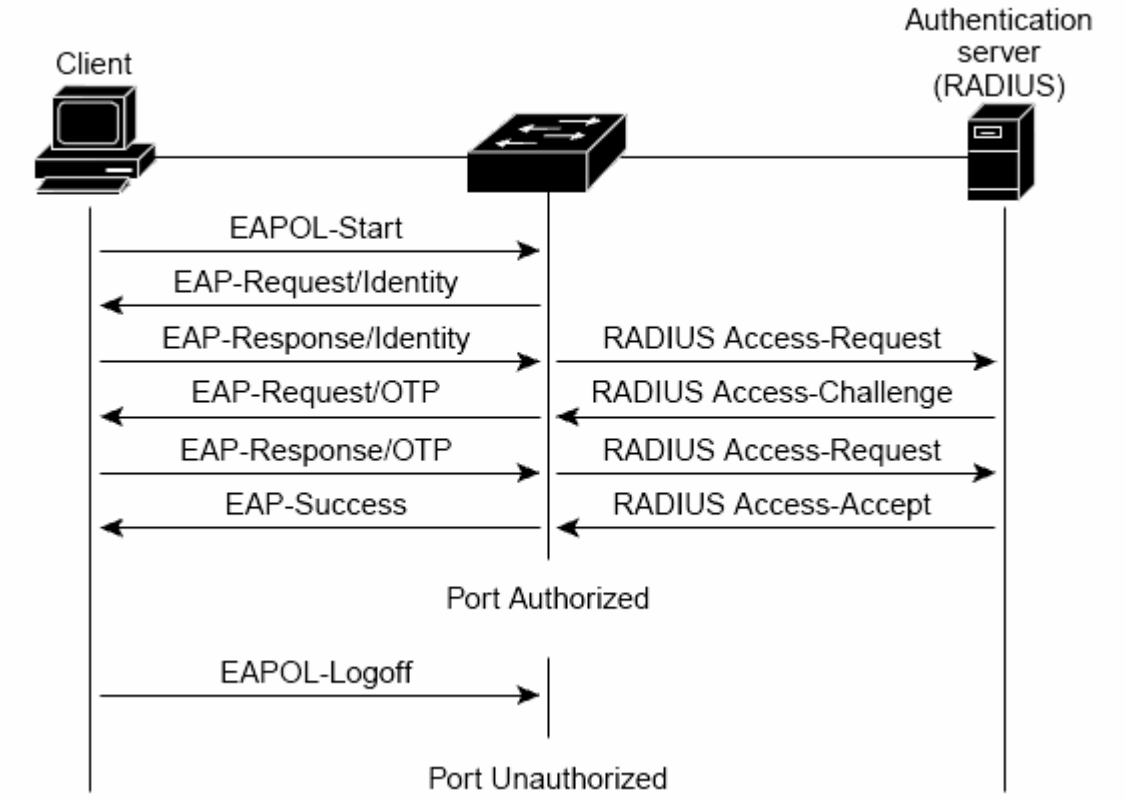


Obr. 3: Formát AVP protokolu RADIUS

Pole Type v AVP hodnotě specifikuje typ atributu. Pole Length udává velikost AVP hodnoty v oktetech. Položka Value je vlastní obsah atributu. Formát dat v položce Value může být řetězec binárních dat, textový řetězec kódovaný ve standardu UTF-8, znaménkové / bezznaménkové 32-bitové celé číslo ve formátu big-endian nebo čas v sekundách od 1. ledna 1970.

Možných atributů protokolu RADIUS existuje více než 100, v prostředí 802.1X se však smí vyskytovat jen několik desítek z nich (viz. zdroj [3]). Atributů umožňujících konfigurovat autorizaci na přepínači Cisco Catalyst 2960 je ještě podstatně méně (viz. kapitola 8).

Autentizace je v případě protokolu 802.1X založena výhradně na protokolu EAP. Switch / access point hraje úlohu rozhraní, které překládá EAP zprávy z formátu EAPOL do formátu atributu RADIUS „EAP-Message“ a naopak. Žádost o autentizaci má formu zprávy RADIUS typu „Access-Request“. Pokud server RADIUS potřebuje k autentizaci další údaje (jedná se například o pokračování toku EAP-TLS), vyžádá si je zprávou typu „Access-Challenge“. Odpověď je serveru RADIUS zaslána opět jako zpráva typu „Access-Request“. Autentizace končí zasláním zprávy typu „Access-Accept“ v případě úspěšné autentizace a zprávy typu „Access-Reject“ v případě neúspěšné autentizace. Zpráva „Access-Accept“ je authentiatorem vyhodnocena jako příkaz k odeslání 802.1X zpávy „EAP-Success“ a povolení provozu na příslušném portu. Průběh autentizace je patrný z obr. 4.

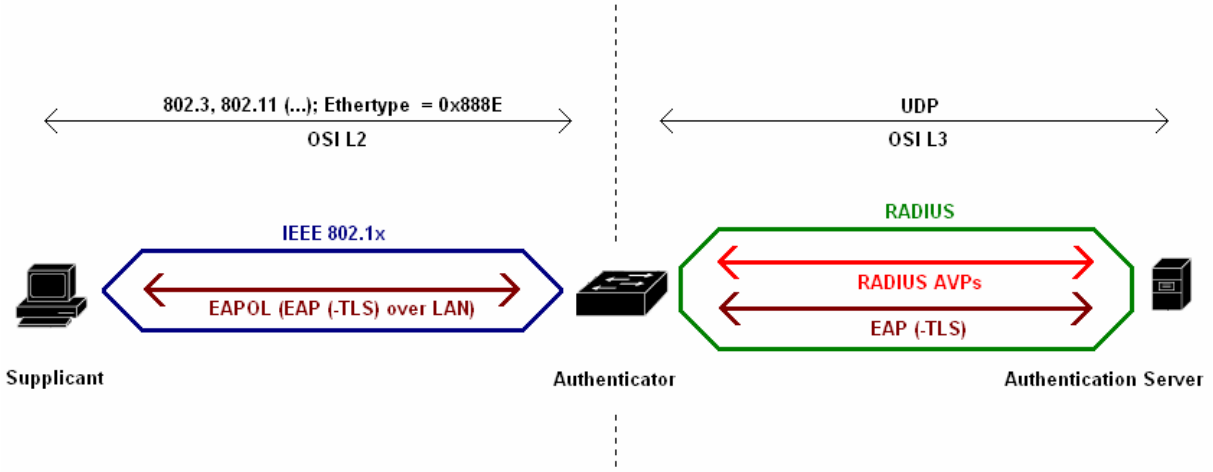


Obr. 4: Průběh 802.1X / RADIUS autentizace

V případě úspěšné autentizace je možné založit autorizaci buď jen na samotném faktu, že autentizace byla úspěšná, nebo je možné přihlédnout k dalším AVP hodnotám zaslaným authenticatorem, např. k MAC adrese klienta, číslu portu authenticatora apod. Je také možné ovlivnit průběh autorizace na základě hodnot accountingu téhož klienta shromážděných při jeho předchozích přístupech k síti. Nastavení autorizace je realizováno zasláním sady AVP hodnot authenticatorovi v RADIUS paketu typu „Access-Accept“.

Accounting je založen na zasílání paketů RADIUS typu „Accounting-Request“ authenticatorem serveru RADIUS. Typicky se tak děje po autorizaci klienta a po přerušení spojení s klientem. V příslušných AVP hodnotách jsou zaslány údaje o činnosti klienta v síti. Z praktického hlediska jsou zajímavé především údaje o době trvání spojení a o množství přenesených dat.

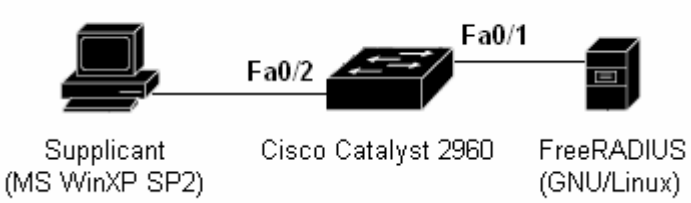
Podrobnější informace k autorizaci a accountingu jsou uvedeny v kapitolách 7 a 8. Na obrázku 5 lze vidět celkový pohled na data předávaná mezi aktéry AAA v prostředí 802.1X / RADIUS včetně příslušné enkapsulace.



Obr. 5: Komunikace v prostředí 802.1X / RADIUS

6.) Parametry pokusné sítě

K průzkumu možností AAA (se zvláštním zřetelem na proces autorizace) v lokální síti s použitím platformy 802.1X / RADIUS jsem sestavil pokusnou síť. Síť se skládá z PC s operačním systémem Microsoft Windows XP SP2 v roli supplicanta, switche Cisco Catalyst 2960 s operačním systémem IOS 12.2 v roli authenticatora a PC s operačním systémem GNU/Linux Fedora Core (kernel 2.6.20) a RADIUS serverem FreeRADIUS 1.1.6 v roli authentication serveru (viz. obr. 6).

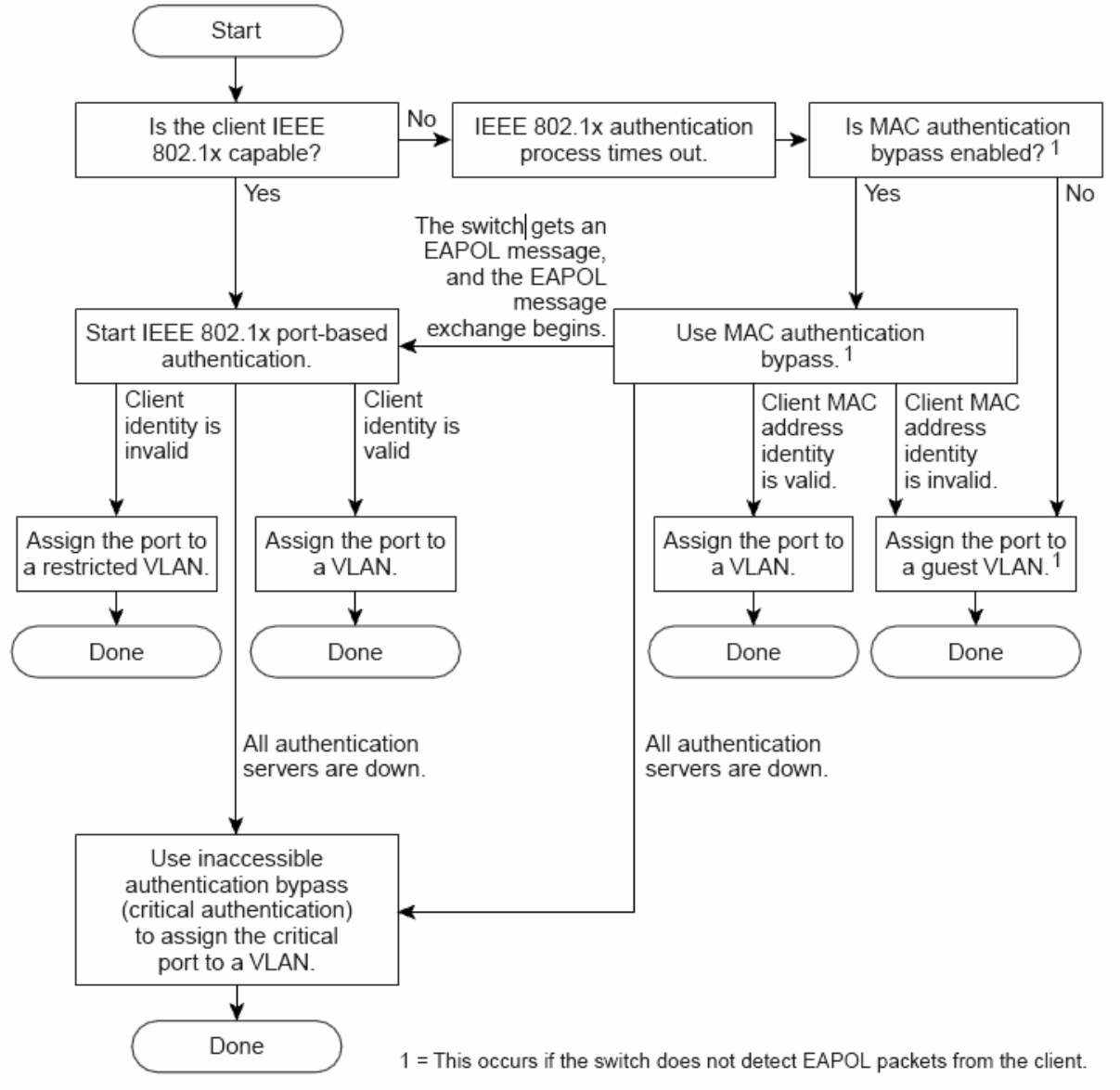


Obr. 6: Topologie testovací sítě

K autentizaci jsem vybral protokol EAP-TLS. Certifikační autoritu a certifikáty standardu X.509 v3, které jsou k provozu EAP-TLS nezbytné, jsem vygeneroval pomocí utility OpenSSL. K snadnější obsluze utility OpenSSL jsem vyvinul kolekci skriptů (viz. příloha [1]).

7.) Konfigurace switche Cisco Catalyst 2960

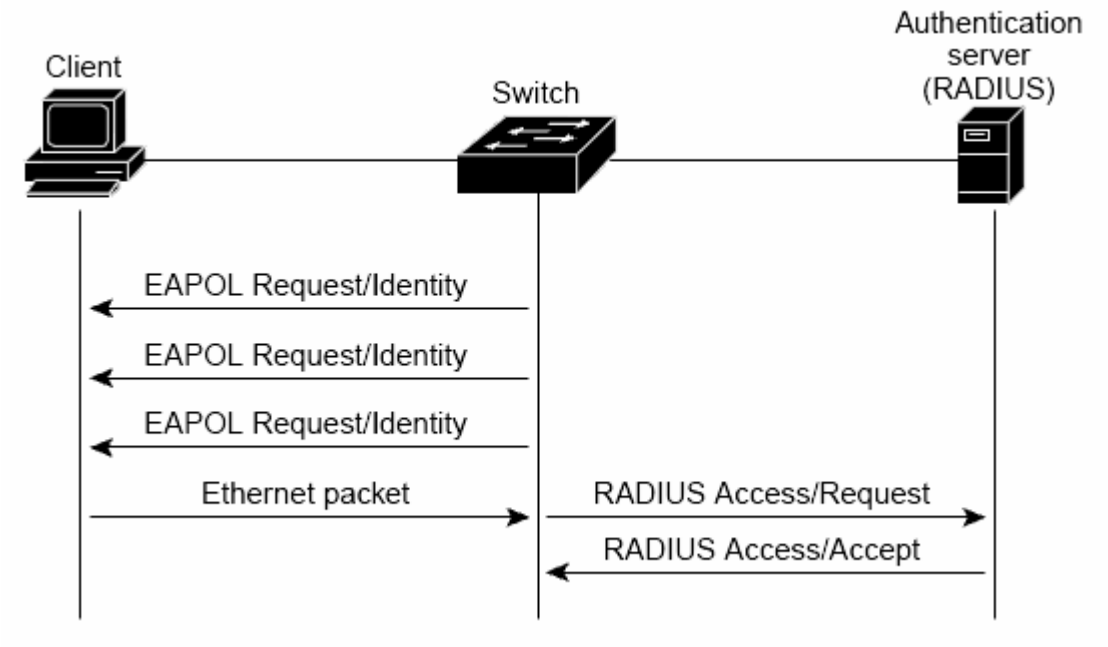
Pro roli authenticatora jsem zvolil switch Cisco Catalyst 2960 vybavený 24 porty 100Base-TX a 2 porty 1000Base-T. Nastavení jiných switchů rodiny Catalyst se může poněkud lišit, nemělo by se ale jednat o zásadní rozdíly. Konfiguraci jsem prováděl pomocí PC s emulátorem terminálu připojeného rozhraním RS232 ke konzolovému portu switche. Port switche Cisto Catalyst 2960, na němž je zapnutá podpora 802.1X, se vždy nachází v jednom ze stavů popsaných na obr. 7.



Obr. 7: Stavy portu switche Cisto Catalyst 2960 se zapnutou podporou 802.1X

Po připojení klienta na port je klientovi zaslána zpráva „EAP-Request/Identity“. Pokud klient odpoví zprávou „EAP-Response/Identity“, je tato zpráva předána serveru RADIUS jako paket „Access-Request“ a následuje proces autentizace s možným následným přiřazením portu switche do příslušného VLANu. Pokud však klient neodpovídá na výzvy k zahájení EAPOL

konverzace, je port switche buď ponechán v neautorizovaném stavu, nebo je provedena žádost o autentizaci u serveru RADIUS s použitím MAC adresy supplicanta místo uživatelského jména dodaného supplicantem (viz. obr. 8), pokud je switch Cisco catalyst 2960 k tomuto nakonfigurován.



Obr. 8: Náhrada chybějící podpory 802.1X MAC autentizací

Není nezbytné nakonfigurovat na switchi všechny stavy podle obr. 7. V případě, že není nakonfigurováno přiřazení VLANu v některém z „katastrofických“ stavů, je port po dosažení tohoto stavu ponechán v neautentizovaném stavu, tedy stavu, ve kterém není portem propouštěn žádný provoz.

K zapnutí podpory 802.1X / RADIUS je potřeba zadat příslušné příkazy jak v globálním konfiguračním režimu, tak v konfiguračních režimech příslušných portů.

Příkazy zadané v globálním konfiguračním režimu jsou následující:

Konfigurace VLANů - nepovinná:

```
!vlan propojující Cisco Catalyst 2960 a server RADIUS
vlan 1
     name default
!vlan pro úspěšně autorizované klienty
vlan 2
     name auth_ok
!vlan pro klienty s neúspěšnou EAP-TLS autentizací
vlan 3
     name tls_fail
!vlan pro klienty s neúspěšnou MAC autentizací
vlan 4
     name mac_fail
```

Konfigurace ACL (Access Control List) - nepovinná. Na základě výsledků autentizace může server RADIUS přiřadit danému supplicantovi IPv4 ACL ve vstupním směru. V takovém případě musí být všechny přiřazované ACL na switchi předkonfigurovány.

V testovací síti byl použit následující rozšířený ACL blokující ICMP zprávy Echo Reply:

```
access-list 101 deny icmp any any echo-reply
access-list 101 permit ip any any
```

Konfigurace adresy serveru RADIUS, portů pro autentizaci a accounting, sdíleného hesla („test“).

```
radius-server host 192.168.0.3 auth-port 1812 acct-port 1813
key test
```

Globální aktivace podpory 802.1X a AAA prostřednictvím serveru RADIUS. Z hlediska konfigurace autorizace prostřednictvím serveru RADIUS (například se jedná o dynamické přiřazení VLANu a ACL) je klíčová položka „aaa authorization network…“:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
```

Příkazy zadané v konfiguračních režimech jednotlivých rozhraní jsou následující:

Konfigurace IP adresy switche. Switch potřebuje vlastní IP adresu pro komunikaci se serverem RADIUS. Pro provoz v testovací síti byla zvolena adresa z privátního rozsahu:

```
interface vlan1
      ip address 192.168.0.2 255.255.255.0
```

Konfigurace rozhraní Fa0/1. Toto rohraní je v testovací síti použito ke spojení se serverem RADIUS:

```
interface FastEthernet0/1
      switchport mode access
      switchport access vlan 1
```

Konfigurace rozhraní Fa0/2. Tato konfigurace se zadává na všech rozhraních, na kterých je požadována podpora 802.1X:

```
interface FastEthernet0/2
```

Aktivace podpory 802.1X na portu:

```
dot1x port-control auto
```

Nastavení periodické reautentizace klienta, který již byl úspěšně autentizován. Perioda a typ reautentizace jsou poskytnuty serverem RADIUS v rámci nastavení autorizace (více viz. kapitola 9):

```
dot1x reauthentication
```

```
dot1x timeout reauth-period server
```

Nastavení periody (v sekundách) před reautentizací v případě selhání autentizace - nepovinné:

```
dot1x timeout quiet-period 30
```

Nastavení VLANu, který je přiřazen v případě neúspěšné autentizace. Nastavení počtu opakování autentizace, než je tento VLAN přiřazen. Toto nastavení je nepovinné, ale je závislé na předešlém vytvoření VLANu:

```
switchport mode access
dot1x auth-fail vlan 3
dot1x auth-fail max-attempts 2
```

Volitelné nastavení náhradní autentizace pomocí MAC adresy supplicanta, pokud supplicant neodpovídá na zprávy „EAP-Request/Identity“. Nastavení periody v sekundách mezi zprávami „EAP-Request/Identity“, počtu odeslání těchto zpráv před restartem autentizačního procesu a maximálního počtu restartů autentizačního procesu. Nastavení VLANu, který je přiřazen, pokud autentizace pomocí MAC adresy selže. Toto nastavení je nepovinné, ale je závislé na předešlém vytvoření VLANu:

```
switchport mode access
dot1x mac-auth-bypass eap
dot1x timeout tx-period 10
dot1x max-req 3
dot1x max-reauth-req 3
dot1x guest-vlan 4
```

8.) Konfigurace RADIUS serveru FreeRADIUS

Provoz serveru FreeRADIUS předpokládá kompletní nastavení všech náležitostí, včetně konfigurace certifikátů pro EAP-TLS autentizaci a konfigurace modulů serveru. Kompletní nastavení serveru přesahuje rámec této práce, pokyny k nastavení jsou dostupné např. ve zdroji [5]. Konfigurační soubory serveru FreeRADIUS, které jsem použil k provozu serveru v testovací síti, jsou dostupné v příloze [2].

Nejdůležitějším konfiguračním souborem z hlediska autentizace a autorizace je soubor „users“ (standardně umístěný v /etc/raddb). Soubor definuje jména supplicantů předávaná AVP hodnotou „User-Name“, doplňkové podmínky pro autentizaci a nastavení autorizace. Schéma položky v souboru „users“ je následující:

```
uživatelské_jméno Auth-Type := typ_autentizace, podmínka1,(…)
<tab>jméno_vracené_AVP_hodnota1 = hodnota1,
<tab>(…)
```

Uživatelským jménem se rozumí obsah AVP hodnoty „User-Name“ v paketu „Access-Request“. Typ autentizace je jedna z hodnot „EAP“, „Accept“ a „Reject“. Hodnota „EAP“ určuje, že příchozí požadavek bude předán modulu EAP k autentizaci. Hodnoty „Accept“ a „Reject“ určují, že příchozí požadavek na autentizaci bude automaticky přijat / odmítnut. Podmínky určují doplňková kritéria k autentizaci daného supplicanta. Soubor „users“ je

zpracováván podobně, jako jsou zpracovávány ACL: soubor je procházen od prvního uživatelského jména k poslednímu, dokud není nalezena shoda. V případě nalezení shody už nejsou další položky souboru zpracovávány. Tento proces lze ovlivnit vložením pseudoatributu „`Fall-Through = Yes`“ mezi vracené AVP hodnoty daného supplicanta.

K provozu serveru FreeRADIUS ve zkušební síti jsem použil následující obsah souboru „users“:

```
Administrator Auth-Type := EAP, Max-Daily-OutOct := 1000000, Max-
Daily-InOct := 1000000, Service-Type == Framed-User, Calling-Station-
Id == "00-16-76-69-01-BE"
      Session-Timeout = 900,
      Termination-Action = RADIUS-Request,
      Reply-Message = "Radius: Access granted!",
      Tunnel-Type = :1:VLAN,
      Tunnel-Medium-Type = :1:IEEE-802,
      Tunnel-Private-Group-ID = :1: auth_ok,
      Filter-Id = "101.in"

0016766901be Auth-Type := Accept, Service-Type == Call-Check, Called-
Station-Id == "00-1A-A1-63-4E-02", NAS-Port == 50002
      Session-Timeout = 1800,
      Termination-Action = Default,
      Reply-Message = "Radius: Access granted! (MAC)",
      Tunnel-Type = :1:VLAN,
      Tunnel-Medium-Type = :1:IEEE-802,
      Tunnel-Private-Group-ID = :1: auth_ok,
      Filter-Id = "101.in"

DEFAULT Auth-Type := Reject
        Reply-Message = "Radius: Access rejected!"
```

Z obsahu souboru „users“ je patrné, že jsou nakonfigurovány vstupy pro tři supplicanty: Administrator, 0016766901be a DEFAULT. Supplicant DEFAULT je aliasem pro všechny supplicanty, kteří nejsou v souboru „users“ explicitně uvedeni a je jim proto odepřena autentizace.

Supplicantovi Administrator je přiřazen autentizační modul EAP. Pokud se jedná o standardního supplicanta („`Service-Type == Framed-User`“) s předpokládanou MAC adresou („`Calling-Station-Id == "00-16-76-69-01-BE`“), jsou supplicantovi Administrator vráceny níže uvedené AVP hodnoty. Tyto hodnoty jsou mu vráceny nezávisle na tom, jestli EAP autentizace uspěje, nebo ne. Rozdíl je pouze v tom, jestli jsou mu vráceny v RADIUS paketu „Access-Accept“, nebo „Access-Reject“.

Supplicant 0016766901be je zaveden pro autentizaci supplicanta nepodporujícího 802.1X (viz. pravá část obr. 7). Může se jednat například o síťovou tiskárnu, nebo jiné jednoúčelové zařízení, které není možné doplnit o podporu 802.1X. Protože při autentizaci na základě MAC adresy nelze použít protokol EAP, je vhodné autentizaci omezit typem služby specifickým pro MAC autentizaci („`Service-Type == Call-Check`“), MAC adresou switche („`Called-Station-Id == "00-1A-A1-63-4E-02`“) a portem switche, na který je supplicant připojen („`NAS-Port == 50002`“).

Server RADIUS umožňuje konfigurovat autorizaci, pokud tuto možnost podporuje authenticator (v případě switche Cisco Catalyst 2960 lze podporu aktivovat příkazem „`aaa authorization network default group radius`“). V takovém případě je možné přiřadit portu IPv4 ACL ve vstupním směru (switch Cisco Catalyst nepodporuje ACL ve výstupním směru) AVP hodnotou „`Filter-Id = "101.in"`“, kde „101“ je číslo ACL. Podobně lze přiřadit VLAN AVP hodnotami „`Tunnel-Type = :1:VLAN`“, „`Tunnel-Medium-Type = :1:IEEE-802`“ a „`Tunnel-Private-Group-ID = :1: auth_ok`“, kde „auth_ok“ je jméno přiřazovaného VLANu. Ve všech třech AVP hodnotách pro přiřazení VLANu je přítomen tzv. tag („`:1:`“). Tag určuje, že tyto tři hodnoty spolu souvisí, teoreticky se může jednat o jakékoliv číslo z rozsahu 1 – 30. Podmínkou pro přiřazení ACL a VLANu prostřednictvím serveru RADIUS je předdefinování příslušného ACL a VLANu na switchi.

Za předpokladu, že je na switchi nakonfigurováno nejen obecné nastavení autorizace pomocí serveru RADIUS, ale také periodická reautentizace („`dot1x reauthentication`“ a „`dot1x timeout reauth-period server`“), lze prostřednictvím serveru RADIUS nastavit čas v sekundách mezi reautentizacemi („`Session-Timeout = 900`“) a průběh reautentizace („`Termination-Action = RADIUS-Request`“). Atribut „`Termination-Action`“ může mít dvě hodnoty, „`RADIUS-Request`“ a „`Default`“. Hodnota „`RADIUS-Request`“ určuje, že supplicant v průběhu reautentizace neztrácí konektivitu, hodnota „`Default`“ určuje, že supplicant v průběhu reautentizace konektivitu ztrácí.

V procesu autorizace lze využít i accounting. RADIUS server FreeRADIUS lze nakonfigurovat tak, aby kumuloval údaje určitého typu získané accountingem. Získanou hodnotu lze využít v autorizační podmínce daného supplicanta. Předpokladem pro kumulování hodnot atributu je zavedení modulu čítače v konfiguračním souboru „radiusd.conf“ (standardně umístěný v /etc/raddb) serveru FreeRADIUS. V serveru FreeRADIUS, provádějícím AAA v testovací síti, jsem zavedl následující čítače:

```
counter dailyin {
      filename = ${raddbdir}/db.daily
      key = User-Name
      count-attribute = Acct-Input-Octets
      reset = daily
      counter-name = Daily-Input-Octets
      check-name = Max-Daily-InOct
      cache-size = 5000
}

counter dailyout{
      filename = ${raddbdir}/db.daily
      key = User-Name
      count-attribute = Acct-Output-Octets
      reset = daily
      counter-name = Daily-Output-Octets
      check-name = Max-Daily-OutOct
      cache-size = 5000
}
```

Čítače určují, že pro každého supplicanta se budou akumulovat hodnoty accounting atributů „`Acct-Input-Octets`“ a „`Acct-Output-Octets`“ (počet přenesených oktetů ve vstupním a výstupním směru) v databázi „db.daily“, čítače budou denně nulovány a jejich hodnotu bude možné kontrolovat v průběhu autorizace pomocí pseudoatributů „`Max-Daily-InOct`“ a „`Max-Daily-OutOct`“. Tímto způsobem je pro každého supplicanta možné zvlášť nastavit

maximální množství přenesených dat, nebo maximální trvání připojení (např. omezení množství přenesených dat výrazem „`Max-Daily-OutOct := 1000000, Max-Daily-InOct := 1000000`“).

Soupis hodnot AVP předávaných switchem Cisco Catalyst 2960 v RADIUS paketech „Accounting-Request“ je uveden v tabulce 2.

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes	Sometimes
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Never	Always
Attribute[43]	Acct-Output-Octets	Never	Never	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Never	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

Tab. 2: Accounting AVP zasílané switchem Cisco Catalyst 2960

Z hlediska kumulace přicházejí v úvahu atributy „Acct-Input-Octets“ (počet přenesených oktetů ve vstupním směru), „Acct-Output-Octets“ (počet přenesených oktetů ve výstupním směru) a „Acct-Session-Time“ (čas strávený připojením v sekundách). Jak je naznačeno v tabulce 2, switch Cisco catalyst 2960 by měl zasílat atributy accountingu nejen po autorizaci a po přerušení spojení s klientem, ale i v průběhu spojení. Zasílání v průběhu spojení ale nebylo v testovací síti pozorováno.

9.) Provoz v prostředí 802.1X / RADIUS

Provoz v testovací síti jsem sledoval síťovým analyzérem Ethereal jak na straně supplicanta, tak na straně serveru RADIUS. Závěry uvedené v této práci jsou v nasbíraných datech patrné. Shromážděný síťový provoz je k dispozici jako příloha [3].

10.) Závěr

V této práci jsem demonstroval možnosti autentizace, autorizace a accountingu v prostředí 802.1X / RADIUS. Standardy 802.1X a RADIUS ve spojení s kvalitním síťovým hardwarem poskytují nástroje k dynamickému řízení přístupu k síťovým prostředkům a ke sledování činnosti uživatele v síti.

11.) Zdroje

[1] Extensible Authentication Protocol (EAP), RFC3748: http://tools.ietf.org/html/rfc3748
[2] Remote Authentication Dial In User Service (RADIUS),
RFC2865: http://tools.ietf.org/html/rfc2865
[3] IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines,
RFC3580: http://tools.ietf.org/html/rfc3580
[4] Dokumentace switche Cisco Catalyst 2960 (IEEE 802.1X):
http://linux456.vsb.cz/~sta048/AAA/sw8021x.pdf
[5] Dokumentace projektu FreeRADIUS: http://www.freeradius.org

12.) Přílohy

[1] Sada skriptů pro obsluhu utility OpenSSL:
http://linux456.vsb.cz/~sta048/AAA/openssl_utils.tar
[2] Vzorové konfigurační soubory serveru FreeRADIUS 1.1.6:
http://linux456.vsb.cz/~sta048/AAA/radius_conf.tar
[3] Provoz v testovací síti ve formátu Ethereal:
http://linux456.vsb.cz/~sta048/AAA/8021x_rad_traf.tar