Autentizace uživatele připojeného přes 802.1X k přepínači Cisco Catalyst 2900/3550 pomocí služby RADIUS

Semestrální projekt z předmětu “Směrované a přepínané sítě”

2004/2005

David Mikula

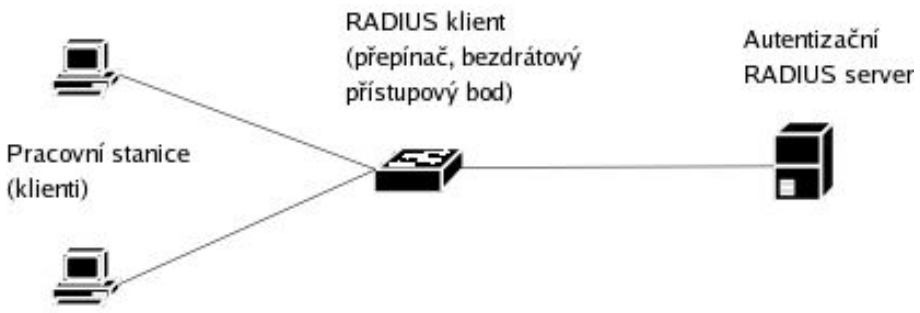
Marek Bielko

Standard IEEE 802.1X

Standtard IEEE 802.1X definuje protokol typu klient-server pro řízení přístupu, který zabraňuje přístupu neautorizovaných klientů do sítě přes veřejně přístupné porty. Autentizační server ověří každého klienta připojujícího se k portu přepínače dříve, než zpřístupní jakékoliv služby nabízené přepínačem nebo bezdrátovým přístupovým bodem. Dokud není klient autorizován, 802.1X dovolí přístup pouze pomocí protokolu Extensible Authentication Protocol over LAN (EAPOL) přes port ke kterému je klient připojen. Až po úspěšném ověření prochází přes port normální provoz.

Role zařízení

Protokol 802.1X rozlišuje tři důležité typy zařízení, viz. obrázek:



Klient

Klient je zařízení (pracovní stanice), které žádá o přístup do sítě LAN a ke službám přepínače. Na pracovní stanici musí běžet 802.1X klientský software – **supplicant**, který umožňuje klientovi žádat o autentizaci. Microsoft Windows XP nabízí vlastní klientský software, v prostředí Linuxu se využívá například software *Xsupplicant*.

Autentizační RADIUS server

RADIUS server slouží k ověřování připojeného klienta. Autentizační server ověří identitu klienta a oznámí RADIUS klientu (přepinači nebo bezdrátovému přístupovému bodu) zda je nebo není klient oprávněn přistupovat ke službám sítě. Každý klient připojený k RADIUS klientovi je jedinečně identifikován svou MAC adresou. Bezpečnostní systém Remote Authentication Dial-In User Service (RADIUS) s protokolem Extensible Authentication Protocol (EAP) pouze rozšiřuje skupinu podporovaných autentizačních serverů. RADIUS pracuje v režimu klient/server, ve kterém jsou autentizační informace posílány mezi RADIUS

serverem a jedním nebo více RADIUS klienty.

RADIUS klient (přepínač nebo bezdrátový přístupový bod)

RADIUS klient provádí kontrolu fyzického přístupu k síti, založeném na ověřování autentizačního stavu klienta. RADIUS klient funguje jako prostředník mezi klientem a autentizačním serverem.Autentizační server žádá identifikační informace od klienta, a odesílá zpět odpovědi klientovi. RADIUS klient je odpovědný za zapoudření/rozbalení Extensible Authentication Protocol (EAP) rámce a za komunikaci s autentizačním serverem.

Když RADIUS klient přijme EAPOL rámec, Ethernetová hlavička je odstraněna a zbývající EAP rámec je znovu zabalen do RADIUS formátu a odeslán autentizačnímu serveru. EAP rámec není během zabalení upravován ani nijak zkoumán a autentizační server musí podporovat EAP jako přirozený formát rámce. Když RADIUS klient přijme rámec z autentizačního serveru, odstraní hlavičku rámce, zůstane EAP rámec, který je pak zabalen pro Ethernet a poslán klientovi.
Mezi zařízení, které mohou působit jako RADIUS klient, patří například přepínače Cisco Catalyst 2900, 2950 a 3550. Na těchto zařízení musí běžet podpůrný software pro podporu RADIUS klienta a 802.1X.

Spuštění autentizace a výměna zpráv

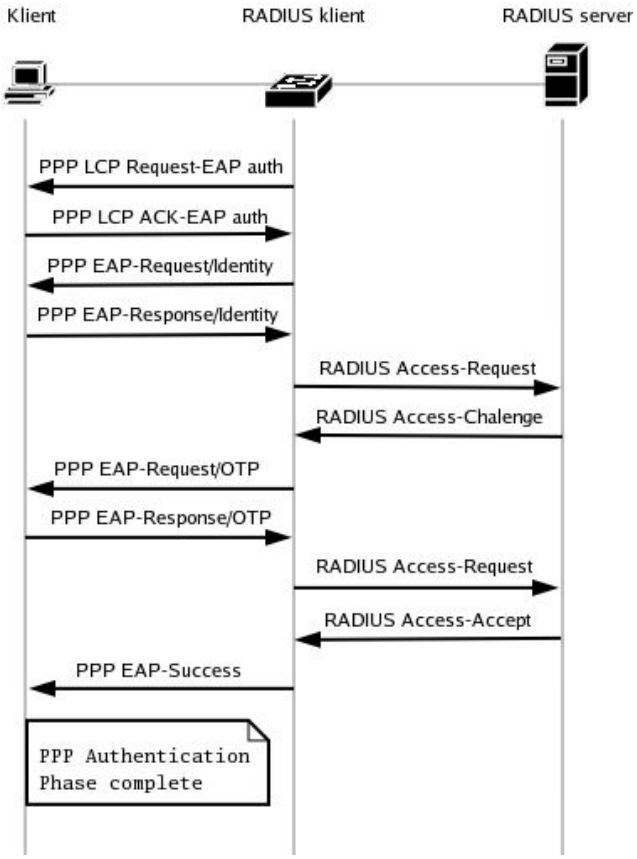
Následující text (zejména konfigurační příkazy) přepokládá na místě RADIUS klienta použití přepínače Cisco Catalyst 2900, 2950 nebo 3550.

Autentizaci může spustit přepínač nebo klient. Jestliže je zapnuta autentizace na portu přepínače pomocí konfiguračního příkazu **dot1x port-control auto**, přepínač musí spustit autentizaci, když port přejde do aktivního stavu. Přepínač pošle EAP požadavek klientovi pro ověření jeho identity (typicky přepínač posílá počáteční požadavek ověření identity následovaný jedním nebo více požadavkem o autentizační informace). Po přijetí rámce klientem tento odpoví EAP identifikačním rámcem.

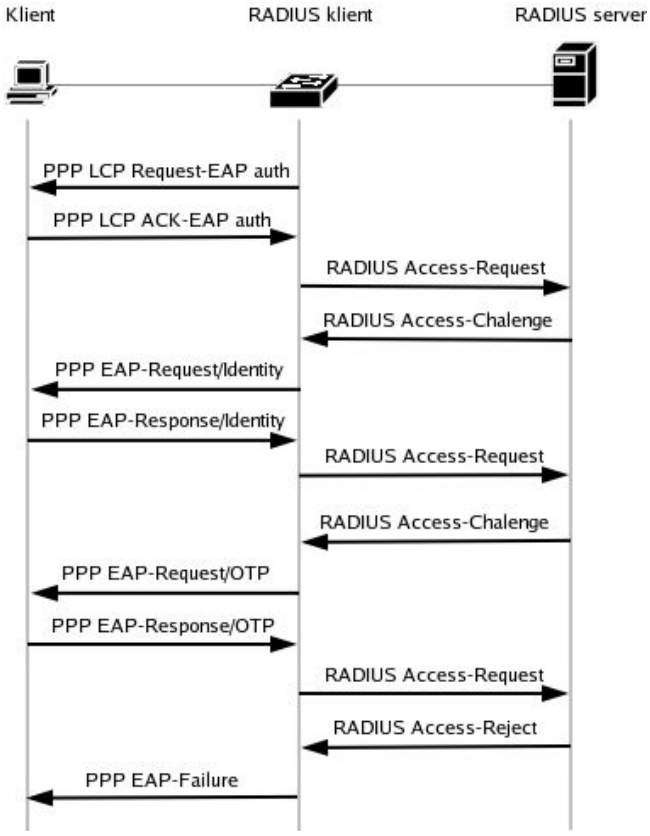
Jestliže klient nepřijme EAP rámce z přepínače, může sám spustit autentizaci zasláním EAPOL-start rámce, který vyzve přepínač k ověření klientovy identity.

Když klient předá svou identitu, přepínač se stává prostředníkem a posílá EAP rámce mezi klientem a autentizačním serverem do té doby, než ověření uspěje nebo selže. Jestliže autentizace uspěje, port na přepínači se stává autorizovaný a umožňuje běžný síťový provoz.

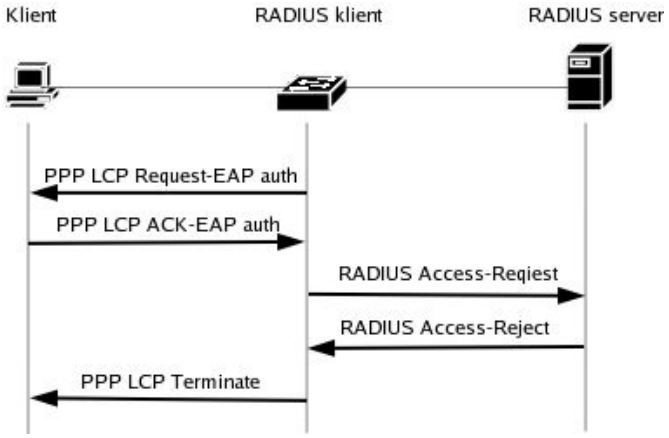
Následující obrázek ukazuje počáteční výměnu zpráv při úspěšné autentizaci mezi klientem, používající One-Time-Password (OTP) autentizaci, a RADIUS serverem.



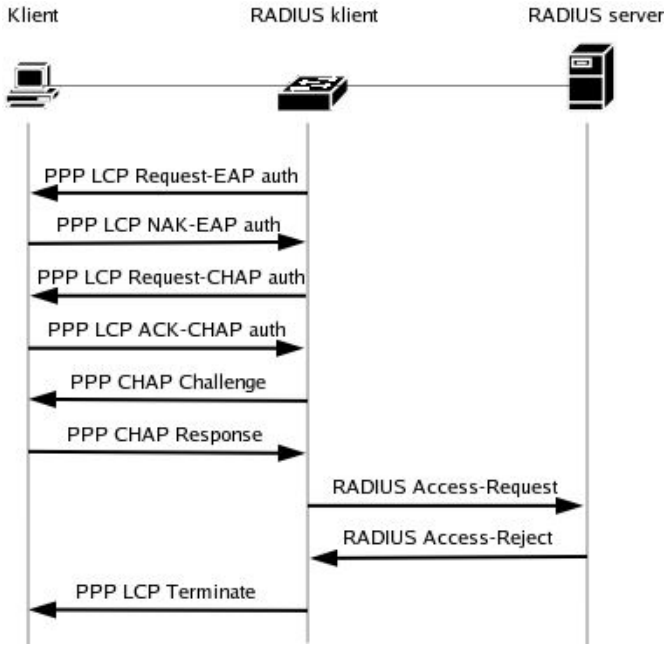
Další obrázek ukazuje stejný případ jako předchozí, avšak při neúspěšné autentizaci klienta:



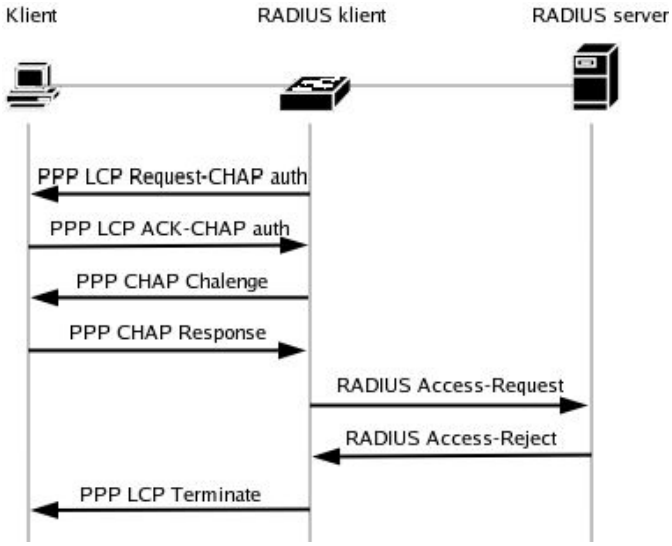
V případě, že RADIUS server nepodporuje EAP zprávy, vypadá komunikace následovně:



Klient nepodporuje EAP, který je vyžadován:



RADIUS klient nepodporuje EAP, který je vyžadován:



Formát RADIUS paketů

Standardtně jsou RADIUS pakety zapozdřeny v UDP, cílový port je nastaven na hodnotu 1812.

Struktura RADIUS paketů vypadá následovně:

Položka **Code** má velikost 8 bitů. Identifikuje RADIUS paket. Když je přijat paket s neplatnou položkou Code, je zahozen. Význam jednotlivých kódů je následující:

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimentální)
13	Status-Client (experimentální)
255	Rezervováno

Položka **Identifier** má velikost 8 bitů. Pomáhá zpárovat odpovídající požadavky a odpovědi. Také umožňuje detekovat duplicitní požadavky (pomocí IP adresy, zdrojového UDP portu a položky Identifier).

Položka **Length** má délku 16 bitů. Určuje délku paketu včetně položek Code, Identifier, Length, Authenticator a atributů. Data přesahující tuto velikost jsou ignorovány. Pokud je paket kratší než specifikovaná délka, je zahozen. Minimální délka je 20 a maximální 4096.

Položka **Authenticator** má délku 128 bitů. Její hodnota je použita pro samotný autentizační proces.

Stavy portu přepínače

Stav portu přepínače určuje, zda má klient přístup do sítě nebo nikoliv. Počáteční stav portu je neautorizovaný. V tomto stavu port blokuje veškerý provoz kromě paketů protokolu 802.1X. Jestliže je klient úspěšně autentizován, port přechází do autorizovaného stavu a povoluje veškerý síťový provoz.

Jestliže klient, který nepodporuje protokol 802.1X, je připojen k neautorizovanému portu, tak neodpovídá na požadavky přepínače na autentizaci klienta. Port tak zůstává v neautorizovaném stavu a klient nemá přístup k síti.

Naopak, klient podporující 802.1X připojený k portu, na kterém neběží 802.1X protkol, se snaží nastartovat autentizační proces vysláním EAPOL-start rámce. Když nedostává odpověď, několikrát svůj požadavek opakuje. Poté se klient snaží využívat port jako by byl v autorizovaném stavu.

Stav portu se ovládá konfiguračním příkazem **dot1x port-control** následovaným jedním z těchto klíčových slov:

- **force-authorized** – zakazuje 802.1X, port je neustále v autorizovaném stavu bez nutnosti autorizace, přístup do sítě je otevřen.
- **force-unauthorized** – port je neustále v neautorizovaném stavu, ignoruje všechny pokusy klienta o autorizaci, nepovoluje síťový provoz.
- **auto** – zapíná nutnou autentizaci přes 802.1X.

Pro odhlášení ze sítě klient zašle zprávu EAPOL-logoff a port přepínače tak přejde do neautorizovaného stavu.

Konkrétní konfigurace přepínače Cisco Catalyst

Nastavení AAA a rozhraní FastEthernet 0/1 pro připojení klienta

Následující konfigurace slouží k nastavení 802.1X autorizace na portu FastEthernet 0/1 přepínače.

```
configure terminal
aaa new-model
aaa authentication dot1x default group radius
interface fastethernet 0/1
        switchport mode access
        dot1x portcontrol auto
dot1x system-auth-control
```

Nastavení komunikace mezi přepínačem a RADIUS serverem

Pro úspěšnou komunikaci mezi přepínačem a RADIUS serverem musí být na přepínači nastavena VLAN s IP adresou a do této VLAN musí být také připojen samotný RADIUS server. V našem případě používáme VLAN 2 s IP adresou 192.168.0.10, adresa RADIUS serveru je 192.168.0.2. Dále je nutno nastavit na přepínači a RADIUS serveru stejný komunikační klíč (v našem případě je klíčem slovo “testkey”). Náš RADIUS server provádí autentizaci klientů na standardním portu 1812 a je připojen k portu FastEthernet 0/2 přepínače.

```
configure terminal
radius-server host 192.168.0.2 auth-port 1812 key testkey
interface vlan 2
        ip address 192.168.0.10
interface fastethernet 0/2
        switchport mode access
        switchport access vlan 2
```

Konfigurace RADIUS serveru (freeradius)

Jako RADIUS server jsme použili open-source produkt **freeradius.** Freeradius podporuje několik způsobů ověřování klienta, my jsme použili ověřování pomocí uživatelského jména a hesla. Zde je uvedena základní – minimální konfigurace.

Základní konfigurační soubor – *radiusd.conf*

```
modules {
        pap {
                encryption_scheme = crypt
        }
        chap {
                authtype = CHAP
        }
        pam {
                pam_auth = radiusd
        }
        mschap {
```

```
                authtype = MS-CHAP
        }

authorize {
        preprocess
        chap
        mschap
        suffix
        eap
}

authenticate {
        Auth-Type PAP {
                pap
        }
        Auth-Type CHAP {
                chap
        }
        Auth-Type MS-CHAP {
                mschap
        }
        Auth-Type LDAP {
                ldap
        }
        eap
}
```

Konfigurace EAP– soubor *eap.conf*

```
eap {
        default_eap_type = md5
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no

        md5 {
        }
```

```
        leap {
        }
}
```

Nastavení informací o RADIUS klientu – soubor *clients.conf*

```
client 192.168.0.10 {
        secret          = test
        shortname       = radclient
        nastype         = cisco
}
```

Nastavení přihlašovacích údajů klientů – soubor *users*

Pro naše testovací účely jsme na RADIUS serveru zavedli jednoho uživatele s přihlašovacím jménem “testuser” a heslem “testpass”.

```
"testuser"      User-Password == "testpass"
```

Použité zdroje

[1] Catalyst 2950 Desktop Switch Software Configuration Guide, 12.1(11)YJ - Configuring 802.1X Port-Based Authentication

[2] Catalyst 2950 Desktop Switch Software Configuration Guide, 12.1(9)EA1 - Configuring VLANs

[3] RADIUS Extensions
RFC 2869 [http://www.faqs.org/rfcs/rfc2869.html]

[4] Remote Authentication Dial In User Service (RADIUS)
RFC 2865 [http://www.faqs.org/rfcs/rfc2865.html]