

**RIADENIE PRÍSTUPU A PREVÁDZKY  
S PROTOKOLMI IPv4 A IPv6 SSH,  
PREKLAD ADRIES PROTOKOLOM DNS,  
SPRÁVA SIETE S ICMPv4/ICMPv6**

Bc. Lukáš Urbančok



# 1 RIADENIE PRÍSTUPU A PREVÁDZKY S IPV4 A IPV6 SECURE SHELL (SSH)

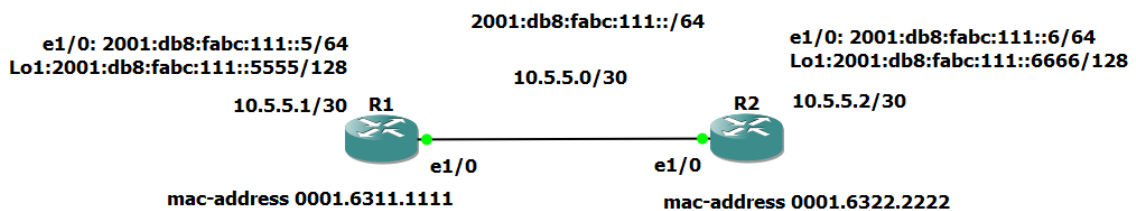
V tejto úlohe sa preskúmajú možnosti secure shellu (SSH) pre vzdialenú správu a administráciu smerovača z laptopu pripojeného do siete. Pomocou Wiresharku sa analyzuje vytvorenie **SSH relácie** s využitím *L4* protokola *TCP* a známeho **portu 22 štvrtej vrstvy** na SSH serveri, ktorý načúva a čaká na prichádzajúce TCP spojenie. K tomuto účelu je použitá jednoduchá topológia v *GNS3* z predchádzajúcej laboratórnej úlohy Ethernet. V úlohe je **aplikovaná aj IPv6** pre úplnosť popisu *SSH IPv6*. [1][2]

## 1.1 Zadanie:

Vytvor jednoduchú topológiu 2 smerovačov a over funkčnosť SSH.

## 1.2 Topológia:

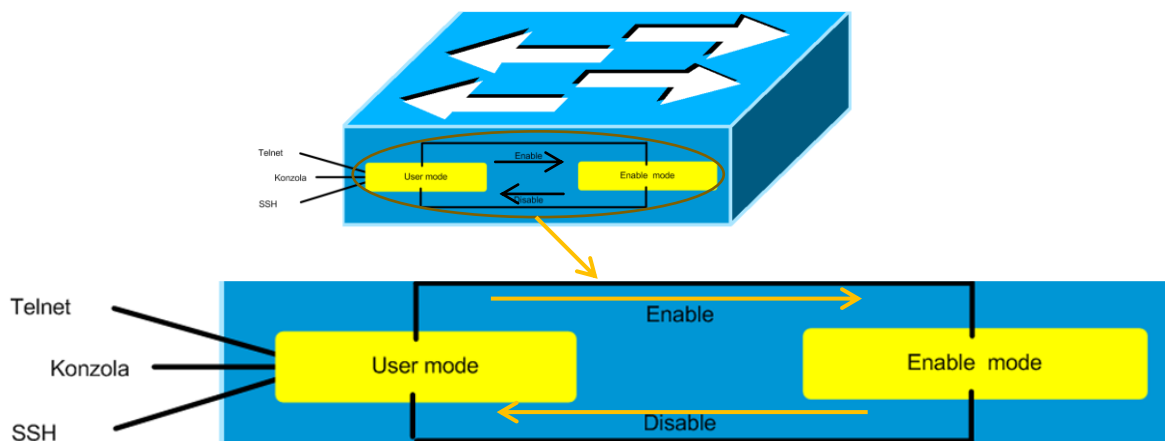
Konfigurácia IPv6 je rovnaká ako u protokolu IPv4 musia mať heslo, doménu a kľúče.



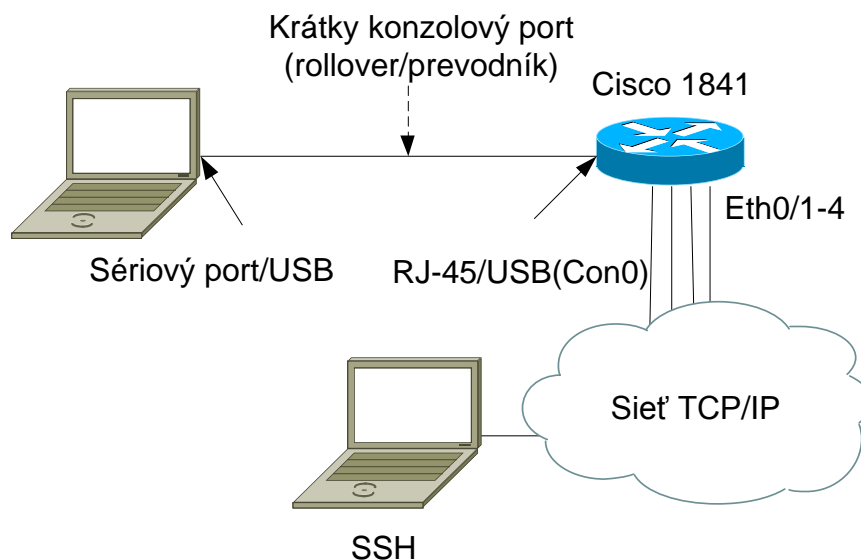
Obr. 1: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie SSH[3] [autor]

## 1.3 Teória:

SSH aplikácia povoľuje emulovať komunikáciu so vzdialeným zariadením. Prístup je podobný ako s využitím telnetu, avšak samotné dáta (payload) sú **zabezpečené** a šifrované. Protokoly **SSH aplikácie** sa volajú **SSH klient** (terminálové emulátory) a zariadenie, ktoré **načúva** na známom **porte 22** a **odpovedá** na príkazy sa nazýva **SSH server**. [4]



Obr. 2: Možnosti prechodu medzi Uživatelským a Privilegovaným módom [2]



Obr. 3: CLI prístup pomocou SSH do EXEC módu [autor]

Pre zvýšenie bezpečnosti vždy by malo byť nastavená užívateľská **autentifikácia** na všetkých **virtuálny linkách zariadenia**. Navyše by mal byť vytvorený prístupový zoznam (ACL) pre obmedzenie zdrojových adries, ktoré majú oprávnenie na prístup. **SSH** v poslednej verzii 2 používa silné šifrovanie a **vylepšuje debug (ladenie, hľadanie chýb) SSHv2** a kompatibilitu Virtual Router Forwarding, čo je nad rámec tejto témy. Novú verziu 2 SSH je možné zapnúť s príkazom `ip SSH version 2` v konfiguračnom režime. [3]

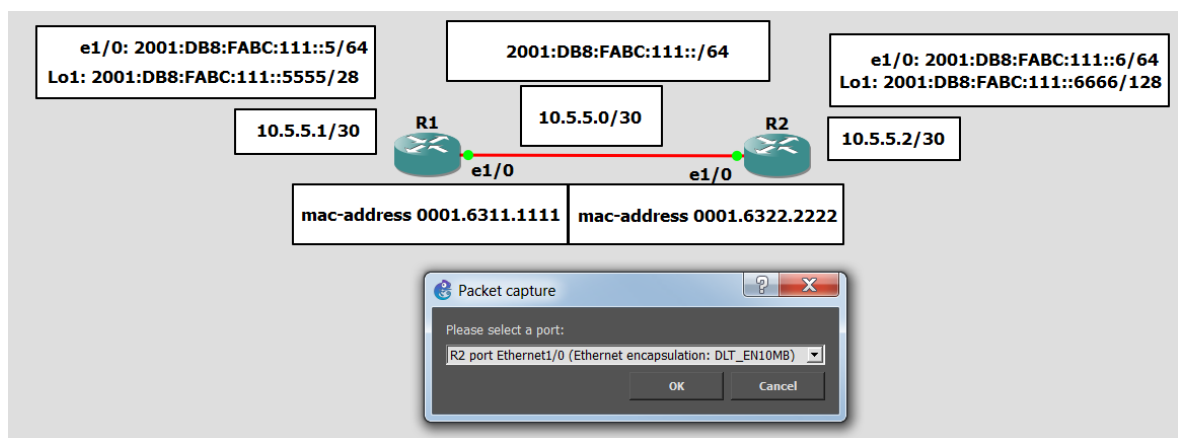
#### 1.4 Požadované zdroje:

GNS3 a Wireshark

IOS smerovače – šablóna smerovača s ethernet rozhraním

## 1.5 Postup:

Topológia obsahuje 2 smerovače **c7200**, ktoré sú navzájom prepojené pomocou rozhrania *Ethernet 1/0*. Sú priradené adresy z A podsiete 10.5.50/30 a aktivované porty príkazom *no shutdown*. Pre konfigurovanie sa používa konzola putty, ktorú sa môže zmeniť na obľúbený terminál (*RemoteNG*, *SecureCRT* a pod.). Pri vysielaní sa špecifikuje MAC adresa pre *R1* a *R2*. Nasledujúce príkazy budú **doplňovať konfiguráciu** z *Ethernet CDP*, kde bol použitý rovnaký sieťový rozsah. Vytvorí sa **užívateľ admin** so špecifickou privilegovanou úrovňou. **Pod** nastavením **logických virtuálnych liniek**, sa špecifikuje, že sa chce **overovať prihlasovanie z lokálnej databázi**. V základnom stave sú oba protokoly Telnet aj SSH povolené. Pokiaľ sa chce povoliť len jeden, bude k tomu potrebovať *transport input SSH*, čím sa eliminuje telnet a po vygenerovaní verejného, súkromného kľúča a nastavení domény, SSH je pripravené na použitie. Z **generovaných kľúčov** je zrejmé, že SSH používa **asymetrické šifrovanie RSA**. Bezpečnosť protokola sa zvyšuje s dĺžkou kľúčov. Pred tým ako sa pripojíme, opäť sa nastaví odchyťvanie paketov: [4]



Obr. 4: Spustenie zachytávania paketov pomocou Wiresharku možnosťou výberu portu[3]

Pre priradenie adres a aktivovanie portov používame nasledujúce príkazy:

Tab. 1: Syntax aplikovaných príkazov a vysvetlenie významu [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu: <b>Krok 1:</b>	<b>line vty 0 4</b> R2(config)#line vty 0 4	Vstup do konfiguračného nastavenia 5 virtuálnych
Syntax príkazu: <b>Krok 2:</b>	<b>login local</b> R2(config-line)#login local	Overovanie lokálnych užívateľských hesiel
Syntax príkazu: <b>Krok 3:</b>	<b>privilege level</b> R2(config)#username admin priv 15 secret FAIUTB16	Nastavenie špecifickej privilegovanej úrovne.

Syntax příkazu: <b>Krok 4:</b>	<b>password cisco</b> R1/R2(config-line)# password cisco	Nastavenie hesla virtuálnej linky v prípade login
Syntax příkazu: <b>Krok 5:</b>	<b>ipv6 unicast-routing</b> R1/R2(config)#ipv6 unicast-routing	Zasielanie IPv6 prenos z CEF na smerovači
Syntax příkazu: <b>Krok 6:</b>	<b>ipv6 address IP Address</b> R1(config-if)# ipv6 address 2001:DB8:FABC:111::5/64	Nastavenie IPv6 adresy pre dané rozhranie s prefixom
Syntax příkazu: <b>Krok 7:</b>	<b>ipv6 address IPv6 Address</b> R2(config-if)# ipv6 address 2001:DB8:FABC:111::6/64	Nastavenie IPv6 adresy pre dané rozhranie s prefixom
Syntax příkazu: <b>Krok 8:</b>	<b>ip address IP Address</b> R1/R2(config-if)# ip address 10.2.2.1 255.255.255.252	Nastavenie IP dresy pre dané rozhranie
Syntax příkazu: <b>Krok 9:</b>	<b>ipv6 enable</b> R1/R2(config-if)# ipv6 enable	Povolenie spracovávanía IPv6 na danom rozhraní
Syntax příkazu: <b>Krok 10:</b>	<b>transport input SSH</b> R2(config-line)#transport input SSH	Povolenie len SSH pripojenia, možnosť povolenia Adminovi
Syntax příkazu: <b>Krok 11:</b>	<b>ip domain-name DNS-server-domain-name</b> R2(config)#ip domain name fai.utb.cz	Nastavenie domény niekedy je to <i>domain name</i> závisí na IOS
Syntax příkazu: <b>Krok 11:</b>	<b>crypto key generate rsa modulus [ modulus-size ]</b> R2(config)#crypto key generate rsa modulus 2048	Generovanie verejného, súkromného kľúča špecifickej
Syntax příkazu: <b>Krok 12:</b>	<b>SSH -l username IP address</b> R1# SSH -l admin 10.2.2.2	Vytvorenie SSH relácie zadaním mena a hosťovskej adresy.
Syntax příkazu: <b>Krok 13:</b>	<b>SSH -l username IP address</b> R1# SSH -l admin 2001:DB8:FABC:111::6	Vytvorenie SSH relácie zadaním mena a hosťovskej adresy.
Syntax příkazu: <b>Krok 14:</b>	<b>mac-address [mac address xxx.xxx.xxx]</b> R2 (config-if)# mac-address 0000.0222.2222	Konfigurácia MAC adresy pre špecifického výrobcu XEROX
Syntax příkazu: <b>Krok 15:</b>	<b>copy running-config startup-config /write memory</b> R2 (config-if) # # copy running-config startup-config	Uloženie aktuálneho nastavenia do NVRAM.

Pred samotným SSH pripojením sa na server, je spustené zachytávanie paketov na R2 porte. Po prihlásení na R2 sa môže overiť otvorené TCP relácie a overiť použitie známeho portu 22. [5]

Tab. 2: Príkazy pre overenie implementovaných konfiguračných zmien a ladenie [autor]

	Syntax + Príkaz	Význam/Účel
Syntax příkazu: <b>Krok 1:</b>	<b>show tcp brief</b> R2# show tcp brief	Zobrazenie lokálnych a vzdialených TCP relácií.
Syntax příkazu: <b>Krok 2:</b>	<b>show users</b> R2#show users	Zobrazenie IP parametrov pre dané rozhranie eth1/0

Pri úspešnom TCP spojení, sa pokračuje otázkou na heslo. Po autentifikácii je preložený do virtuálnej linky terminála, čo sa môže skontrolovať pomocou príkazu *show users*, kde sa nachádzajú IP adresy.

```
R2#show users
  Line      User      Host(s)      Idle      Location
  0 con 0
* 2 vty 0    admin      idle        00:00:00 10.5.5.1
```

```
R2#show ssh
Connection Version Mode Encryption Hmac      State      Username
0          2.0    IN   aes128-cbc hmac-sha1 Session started admin
0          2.0    OUT  aes128-cbc hmac-sha1 Session started admin
%No SSHv1 server connections running.
```

Obr. 5: Zobrazenie prihlásených užívateľov a záznamu o SSH reláciách [autor]

V každom momente sme teda schopný **kontrolovať užívateľov**. GNS3 používa Con0 pre prístup a ostatné 2 spojenia sú naše testy z *R1* a *R2* samotného. Ďalšou skvelou pomôckou pri trasovaní, na prihláseného užívateľa je príkaz *show tcp brief*. **Podľa IP adresy lokácie vzdialeného host'a** a portu pomocou **Wiresharku**, by sme mali byť **schopný dohľadať host'a**. [3] [8]

```
R2#show tcp brief
TCB          Local Address      Foreign Address      (state)
68DA8218    10.5.5.2.22       10.5.5.1.17358      ESTAB
```

Obr. 6: Zobrazenie prihlásených užívateľov [autor]

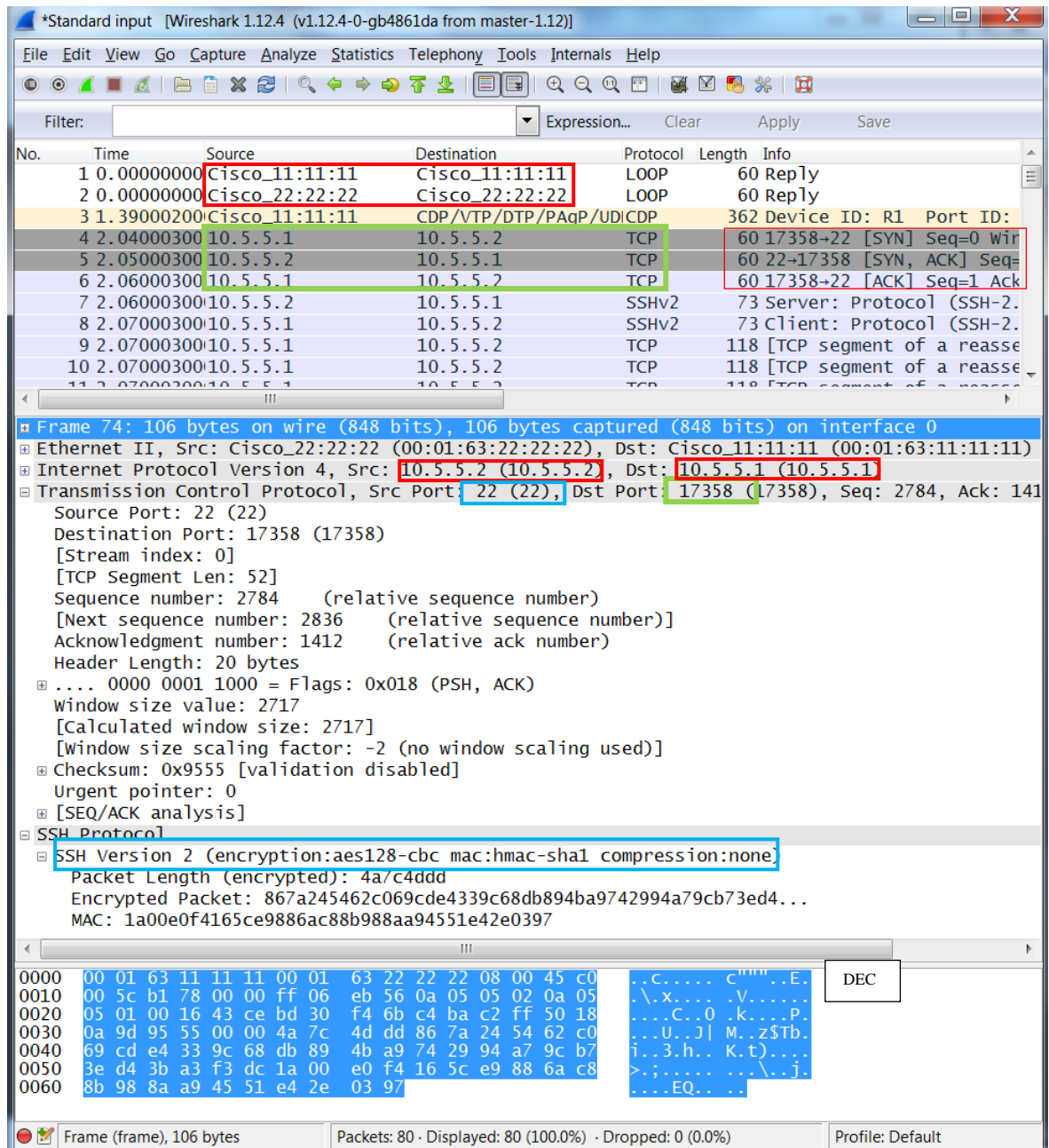
Pri **analýze prvých paketov** je vidieť TCP spojenie (*žiadost' SYN, potvrdenie SYN,ACK a pôvodný SYN*). Nasleduje **vyjednávanie o SSH relácií** medzi *R1* a *R2*. Keď prejde ďalej do paketu 74 ako príklad. Je zrejmé, že paket je už šifrovaný, môže si overiť ethernet hlavičku, zdrojovú a cieľovú *L2 a L3 adresu*. V *L3 informáciách* sa odkazuje na protokol 6, čo je TCP a vo vnútri je vidieť informácie o zdrojovom a cieľovom porte odpovedajúce výpisu na *R2 show tcp brief*. Podstatné je, **že všetky dáta sú šifrované** a bez správneho kľúča nie sme schopný nič dešifrovať. Toto je primárny benefit Secure Shellu. V tejto úlohe sa postavili laboratórnu úlohu s *R1* v roli SSH klienta a po vytvorení *SSH relácie* je vo Wiresharku analyzovaný obsah paketov na sieti. [2]

Nastavenie *IPv6 SSH* na smerovači sa v zásade od *IPv4* nelíši. Výhodou u *IPv6* je **možnosť používania obecného prefixu** pre adresy. Riadenie prístupu je rovnaké ako pre telnet. Pre *SSH* je dôležitá konfigurácia lokálneho užívateľa alebo AAA, nutné je nastaviť názov domény a **generovať kľúče pre RSA**. Konfigurácia protokolu *SSH* pre *IPv6* v operačnom systéme IOS:

Tab. 3: Konfigurácia IPv4 a IPv6 adres a riadenie prístupu len pomocou SSH [autor]

```
ipv6 unicast-routing
aaa new-model
user admin password faiutb
inter Lo1
    ipv6 enable
    ipv6 address 2001:DB8:FABC:111:5555/128
    no shut
ipv6 access-list riad-vstup-v6
    permit tcp 2001:DB8:FABC::/48 host 2001:DB8:FABC:111::5555
    deny ipv6 any any log-input
ip domain name fai.utb.cz
crypto key generate
inter e1/0
    ipv6 enable
    ipv6 address 2001:db8:fab8:111::0005/64
    no shu
line vty 0 4
    session-timeout 3
    password 7 011F09125E0709192440411F1C
    ipv6 access-class riad-vstup-v6 in
    logging synchronous
    login local
    exec prompt timestamp
    transport input SSH
```

Na systémy NX OS sa musia povoliť protokoly pomocou *feature*. Rovnako je tomu aj na SSH a kľúče, ktoré generujú pomocou *SSH key rsa*. [1]



Obr. 7: Zachytené SSH dáta medzi SSH klientom a serverom R1 a R2 [autor]

Pretože na R1 nie je vygenerovaná správna dvojica kľúčov pri pokuse o prihlásenie, prístup je odmietnutý vzdialeným host'om alebo sieťovým zariadením.

```
R2#ssh -l admin 10.5.5.1
% Connection refused by remote host
```

Obr. 8: Ping medzi R1 a multicast groupou 224.66.255.10 [autor]

Pre zobrazenie vygenerovaného RSA verejného kľúča je potrebné zadať príkaz `show crypto key mypubkey rsa:`

```
R2# show crypto key mypubkey rsa
% Key pair was generated at: 15:46:14 UTC Feb 14 2016
Key name: R2.fai.utb.cz
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00B8054D 97E4A07A D029C010 FB8E18A7 971F8D64 60868395 B4E4E586 FD49D316
C54CEA11 38C1E4FE 0AE31FB9 90C69172 4E60615C D7562AA9 6B0F54DF 26C0F9C6
64EA020B 7C6D477F 1764E537 1713FE2F 824A1A42 F88E4D33 D3744EB8 DE07BAF4
1400E7E6 1DC5173E 4BB45BBC FC715407 BB00F3B3 E716EABC 2930463A 1766BA42
BD7E9AE4 F93B8D3C AB1DD6EB BF82C88C 3C49B9E1 61EE6E72 7D9A5744 EC6B8911
AFFAEC70 8180961B 0E4472F4 37F96ADA DAFA8BAB 3AB5FA46 12CAEE74 FD771B27
74A2AFDF 409936A4 F633DC94 22F05987 53A2CAFD 5C875A96 8A660AE9 BE03D604
B84C8F20 9EE4C30E 2E1B113B 2C20A0D0 7C65C7CA 0AC4EAF5 CF1384FC 63A48A26
43020301 0001
% Key pair was generated at: 15:46:15 UTC Feb 14 2016
Key name: R2.fai.utb.cz.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable. Redundancy enabled.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C96650 6F6945BF
A7A44AB0 D554EED1 8C4DCAE3 FB707B22 F3D740C4 4947D026 CF64121C 441464FA
F7FEFB5C 70A9CC7F 07AAAF57 6A5D07D2 2EF3DBFA 0EBC0607 3076EA16 3E43E6C6
A30049D4 F7D0F7D3 FEBB02D7 1C6412F4 0918A9FE 9429CB1D CB020301 0001
```

Obr. 9: Show príkazy overujúce implementované konfigurácie [autor]

```
R2# show crypto key pubkey-chain rsa
Codes: M - Manually configured, C - Extracted from certificate




Code Usage      IP-Address/VRF      Keyring      Name
C      Signing
C      Signing
C      Signing
C      Signing
,o=VeriSign, Inc.,c=US
cn=Cisco Root CA M1,o=Cisco
cn=Cisco Root CA 2048,o=Cisco Systems
cn=Cisco Manufacturing CA,o=Cisco Systems
ou=Class 3 Public Primary Certification Authority
```

Obr. 10: Vygenerovaný RSA verejný kľúč [autor]

RSA asymetrické šifrovanie využíva **faktorizáciu súčinu dvoch veľkých prvočísel**.  
 Pokiaľ chcete vymazať starý RSA kľúč použite *crypto key zeroize rsa*. [2]

Výsledné nastavenie smerovačov pre overenie funkčnosti SSH:

Tab. 4: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

R1	R2	Wireshark
 R1 ssh.txt	 R2 ssh.txt	 ssh.pcapng

## 1.1 Otázky na zamyslenie o SSH:

1. Môže sa kontrolovať SSH alebo telnet, kto sa prihlási ? Ako ? Na základe analógie z laboratórnej úlohy vytvor príklad kontrolovania SSH.

**Áno**, pomocou prístupového zoznamu (ACL).

Tab. 5: Konfigurácia IPv4 prístupového zoznamu pre virtuálne linky [autor]

```
line vty 0 15
 login
 password cisco
 access-class 6 in
```

Nasledujúci príkaz sa zadáva v konfiguračnom režime a má za cieľ povoliť zdrojové adresy začínajúce s 10.10.10

Tab. 6: Konfigurácia povolenia zdrojovej adresy začínajúcej s 10.10.10.x [autor]

```
access-list 6 permit 10.10.10.0 0.0.0.255
```

2. Správca vložil do smerovača nasledujúce príkazy. Avšak pri pokuse sa prihlásiť vzdialene cez SSH vyskočila správa “password required, but not set.” Čo je príčinou problému ? [1]

Tab. 7: Správna konfigurácia SSH a riadenie prístupu na virtuálnej linke [autor]

```
R1(config)#ip domain-name lukatest.cz
R1(config)#crypto key generate rsa
R1(config)#ip SSH version 2
R1(config)#line vty 0 4
R1(config-line)#transport input SSH
```

**R1 nemá nakonfigurované heslo pod virtuálnou linkou.**

3. Mal by byť protokol SSH vypnutý, aby zamedzil odchyťávaniu komunikácie o zariadeniach?

**Nie, SSH poskytuje šifrovanú vzdialenú správu zariadení.**

4. Čo znamená pokiaľ pod VTY line 0 15 je zadané login authentication default?

**V prípade, že sa administrátor pokúsi pripojiť cez SSH a bude nastavené heslo virtuálne linky, lokálne meno a RADIUS, tak poradie v akom bude kontrolovať (credentials) je RADIUS server -> lokálne meno-> heslo virtuálnej linky [6]**

## 2 SPRÁVA SIETE IPV4 S ICMP A IPV6 S ICMPV6

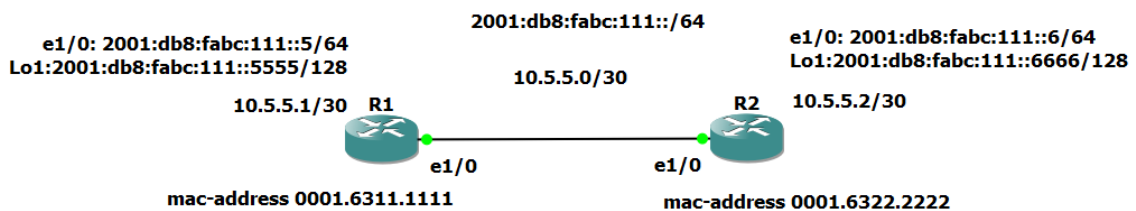
V tejto tejto úlohe sa preskúma **použitie protokola ICMP** (Internet Control Message Protocol) jeho spoluprácu s *IPv4* a *IPv6* pre správu siete. Pomocou **Wiresharku** sa **analyzuje** vytvorenie *SSH relácie* s využitím 4. protokolu TCP a známeho portu 22 štvrtej vrstvy na *SSH server*, ktorý načúva a čaká na prichádzajúce TCP spojenie. K tomuto účelu je použitá jednoduchá topológia v *GNS3* z predchádzajúcej laboratórnej úlohy Ethernet. V úlohe je aplikovaná aj *IPv6* pre úplnosť popisu riadenia prístupu a SSH IPv6 bude mať svoju laboratórnu úlohu.[1]

### 2.1 Zadanie:

Vytvor jednoduchú topológiu 2 smerovačov a over funkčnosť SSH.

### 2.2 Topológia:

Konfigurácia IPv6 je rovnaká ako u protokolu IPv4, t.j. musí mať heslo, doménu a kľúče.



Obr. 11: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie SSH [autor]

### 2.3 Teória:

Protokol **ICMP** generuje **informačné** a **chybové správy**. Je označený číslom 1, rovnako ako *TCP 6* a *UDP 17* v dekadickom čísle. ICMP v **IPv4** sieti sa stará o **ping žiadosti a odpovede**, rovnako tak sa stará o **informovanie nedostupnosti**, vypršanie TTL, presmerovanie paketu lepšou cestou, nastavenie fragmentácie paketov, keď príjemca nestíha zaťaženie, vďaka ICMP odosielateľ spomalí. Pre IPv6 sa používa pri **zistovaní susedov** (správy *NS, NA, RS, RA*. NA správy ak sú žiadne, RA správy sú periodicky posielané.), zistovaní MTU a protokola Multicast Listener Discovery. V **IPv6** je definovaný v **rozširujúcej hlavičke** s číslom 58. Obsahuje typ, kód, kontrolný súčet a samotné dáta. *ICMP* je vhodné použiť i pri **ladení problémov** pomocou chybových správ *debug ip/ipv6 icmp* je schopný určiť **koreňovú príčinu**. Hneď sa to otestuje v GNS3, nie je to skvelé? [1] [2]

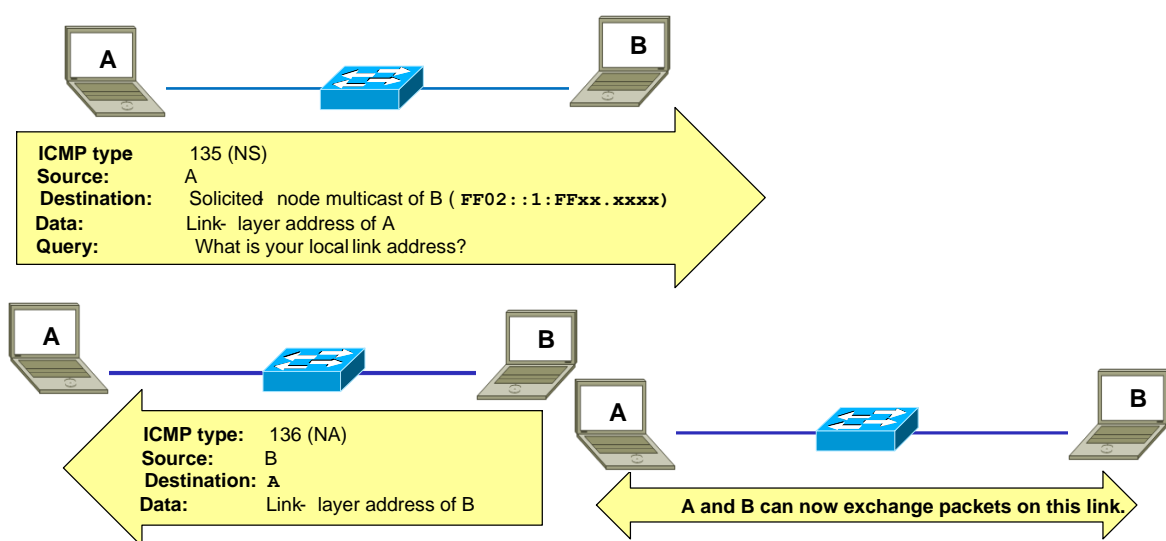
```
R1#ping 2001:DB8:FABC:111::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FABC:111::6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/28 ms
```

Obr. 12: Testovanie pingom susednej IP pred aplikáciou prístupového zoznamu [autor]

```
R2#debug ipv6 icmp
ICMP Packet debugging is on
R2#
*Feb 14 23:19:48.875: ICMPv6: Received echo request, Src=2001:DB8:FABC:111::5, Dst=2001:DB8:FABC:111::6
*Feb 14 23:19:48.879: ICMPv6: Sent echo reply, Src=2001:DB8:FABC:111::6, Dst=2001:DB8:FABC:111::5
*Feb 14 23:19:48.907: ICMPv6: Received echo request, Src=2001:DB8:FABC:111::5, Dst=2001:DB8:FABC:111::6
*Feb 14 23:19:48.911: ICMPv6: Sent echo reply, Src=2001:DB8:FABC:111::6, Dst=2001:DB8:FABC:111::5
*Feb 14 23:19:48.931: ICMPv6: Received echo request, Src=2001:DB8:FABC:111::5, Dst=2001:DB8:FABC:111::6
*Feb 14 23:19:48.931: ICMPv6: Sent echo reply, Src=2001:DB8:FABC:111::6, Dst=2001:DB8:FABC:111::5
```

Obr. 13: Ladenie problémov pomocou informačných správ ICMP, echo žiadosť a odpoveď [autor]

Objavovanie susedov používa **špeciálne ICMP správy NS (Neighbor Solicitation)** a **NA (Neighbor Advertisement)**. **NS** sa správa ako **ARP žiadosť**, kedy sa pýta hosťa so špecifickou IPv6 adresou, aby mu odpovedal. **NA** je verná kópia **ARP** odpovede a načúva hosťovej MAC adrese. Ďalšou novinkou sú správy **RS (Router Solicitation)** a **RA (Router Advertisement)**, čo je **rovnaké**, akurát **špecifikujú len smerovače**, čo už vyplýva z názvu. [5][7]



Obr. 14: Všeobecný proces zisťovania susedov, ktorý používa ICMP pakety v IPv6 [2]

NS používa špeciálnu **multicast adresu** pre všetky sieťové zariadenia (**FF02::1**). NS žiada host'a so špecifickou **IPv6 adresou**, aby mu poslal **NA s vlastnou MAC adresou**; používa ako cieľovú adresu solicited-mode **multicast**, na ktorú **odpovedia hostia**, ktorých posledných 6 hex čísel sa zhoduje.[1][2]

## 2.4 Požadované zdroje:

GNS3 a Wireshark

IOS smerovače – šablóna smerovača s ethernet rozhraním

## 2.5 Postup:

V tejto úlohe sa bude diskutovať, **testovať a konfigurovať protokol ICMP**. Opäť využije základnú **topológiu dvoch smerovačov** a vytvorí jednoduchý prístupový zoznam, ktorý bude zahadzovať prevádzku medzi smerovačmi *R1* a *R2*. Nadefinuje sa veľmi prísne pravidlo, že **celá prevádzka bude zahadzovaná medzi smerovačmi**. Ako pre *IPv4*, tak pre *IPv6*. Ladenie problémov naďalej sa nechávajú zapnuté a porovnávajú sa s Wiresharkom. [8]

```
R1#ping 2001:DB8:FABC:111::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FABC:111::6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/28/68 ms
R1#ping 2001:DB8:FABC:111::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:FABC:111::6, timeout is 2 seconds:
AAAAA
Success rate is 0 percent (0/5)
```

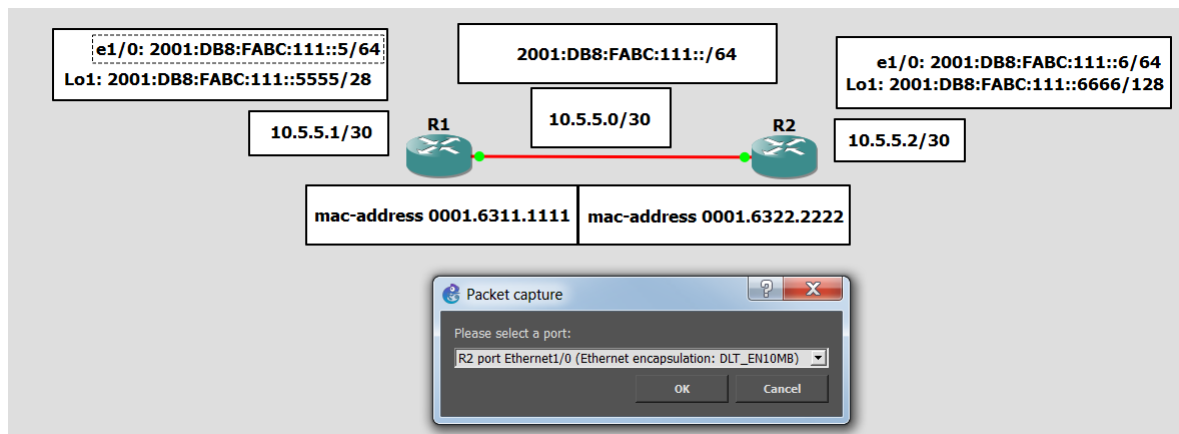
*Obr. 15: Ping pred a po aplikovaní prístupového zoznamu REKTORAT-ACL-6 [autor]*

Nakoľko v prvých úlohách s ethernetom sa testovalo hlavne *IPv4* teraz **sa zameria predovšetkým na IPv6**. Pri testovaní pingu z *R1* som na **strane susedného smerovača** aplikoval prístupový zoznam pod rozhraním e1/0 a následne ho odobral pre testovanie. [2]

```
*Feb 14 23:47:03.031: ICMPv6: Sent echo reply, Src=2001:DB8:FABC:111::6, Dst=2001:DB8:FABC:111::5
*Feb 14 23:47:03.043: ICMPv6: Received echo request, Src=2001:DB8:FABC:111::5, Dst=2001:DB8:FABC:111::6
*Feb 14 23:47:03.043: ICMPv6: Sent echo reply, Src=2001:DB8:FABC:111::6, Dst=R2(config-if)#=2001:DB8:FABC:111::5
R2(config-if)# ipv6 traffic-filter REKTORAT-ACL-6 in
R2(config-if)#
*Feb 14 23:47:04.195: ICMPv6: Sent N-Solicit, Src=FE80::C802:1AFF:FE34:1C, Dst=FE80::C801:19FF:FE24:1C
*Feb 14 23:47:04.255: ICMPv6: Received N-Advert, Src=FE80::C801:19FF:FE24:1C, Dst=FE80::C802:1AFF:FE34:1C
R2(config-if)#
*Feb 14 23:47:07.743: ICMPv6: Sent Unreachable code 1, Src=2001:DB8:FABC:111::6, Dst=2001:DB8:FABC:111::5
*Feb 14 23:47:07.795: ICMPv6: Sent Unreachable code 1, Src=2001:DB8:FABC:111::6, Dst=2001:DB8:FABC:111::5
```

Obr. 16: Ladenie ICMPv6 paketov pred a po aplikovaní ACL REKTORAT-ACL-6 [autor]

Nastavenia vytvárania užívateľov, hesiel a základnom nastavení mena a adresácie sa už vynecháva a úloha sa venuje ICMP protokolu IPv4 a IPv6. [5]



Obr. 17: Spustenie zachytávania paketov, nezáleží na porte, ktorý sa vyberie [autor]

Pre priradenie adries a aktivovanie prístupových zoznamov sa používajú príkazy:

Tab. 8: Syntax aplikovaných príkazov a vysvetlenie významu [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu: <b>Krok 1:</b>	<b>username [username] secret [password]</b> R1/R2 (config)# username admin secret cisco	Nastavenie lokálneho užívateľského mena a hesla
Syntax príkazu: <b>Krok 2:</b>	<b>line vty 0 4</b> R1/R2 (config)#line vty 0 4	Vstup do konfiguračného nastavenia 5 virtuálnych
Syntax príkazu: <b>Krok 3:</b>	<b>password cisco</b> R1/R2(config-line)# password cisco	Nastavenie hesla virtuálnej linky v prípade login
Syntax príkazu: <b>Krok 4:</b>	<b>logging synchronous</b> R1/R2 (config-line)# logging synchronous	Nastavenie synchronizácie časovania konzoly - prerušenie.
Syntax príkazu: <b>Krok 5:</b>	<b>login local</b> R1/R2 (config-line)#login local	Overovanie lokálnych užívateľských hesiel

Syntax príkazu: <b>Krok 6:</b>	<b>ipv6 unicast-routing</b> R1/R2(config)#ipv6 unicast-routing	Aktivovanie IPv6 a zasielanie IPv6 prenos u z CEF na smerovanie
Syntax príkazu: <b>Krok 7:</b>	<b>ipv6 address IP Address</b> R1(config-if)# ipv6 address 2001:DB8:FABC:111::5/64	Nastavenie IPv6 adresy pre dané rozhranie s prefixom
Syntax príkazu: <b>Krok 8:</b>	<b>ipv6 address IPv6 Address</b> R2(config-if)# ipv6 address 2001:DB8:FABC:111::6/64	Nastavenie IPv6 adresy pre dané rozhranie s prefixom
Syntax príkazu: <b>Krok 9:</b>	<b>ip address IP Address</b> R1/R2(config-if)# ip address 10.5.5.1/2 255.255.255.252	Nastavenie IP dresy pre dané rozhranie
Syntax príkazu: <b>Krok 10:</b>	<b>no shutdown</b> R1/R2(config-if)# no shutdown	Aktivovanie portu
Syntax príkazu: <b>Krok 11:</b>	<b>ip access-list extended [name]</b> R2(config-ext-nacl)#ip access-list exte REKTORAT-ACL	Nastavenie rozšíreného ACL s menom pre IPv4
Syntax príkazu: <b>Krok 12:</b>	<b>deny icmp any any</b> R2(config-if)# deny icmp any any	Nastavenie ACL pre zahadzovanie všetkých ICMP IPv4 paketov
Syntax príkazu: <b>Krok 11:</b>	<b>ipv6 access-list extended [name]</b> R2(config-ext-nacl)#ipv6 access-list extended REKTORAT-	Nastavenie rozšíreného ACL s menom pre IPv6
Syntax príkazu: <b>Krok 12:</b>	<b>deny icmp any any</b> R2(config-if)# deny icmp any any	Nastavenie ACL pre zahadzovanie všetkých ICMP IPv6 paketov
Syntax príkazu: <b>Krok 13:</b>	<b>interface Ethernet1/0</b> R2(config)# interface Ethernet1/0	Vstup do konfigurácie rozhrania Ethernet1/0
Syntax príkazu: <b>Krok 14:</b>	<b>ip access-group REKTORAT-ACL in</b> R2(config-if)# ip access-group REKTORAT-ACL in	Aplikovanie ACL pre všetky IPv4 pakety, ktoré idú smerom do R2 .
Syntax príkazu: <b>Krok 15:</b>	<b>copy running-config startup-config /write memory</b> R2 (config-if)# # copy running-config startup-config	Uloženie aktuálneho nastavenia do NVRAM.

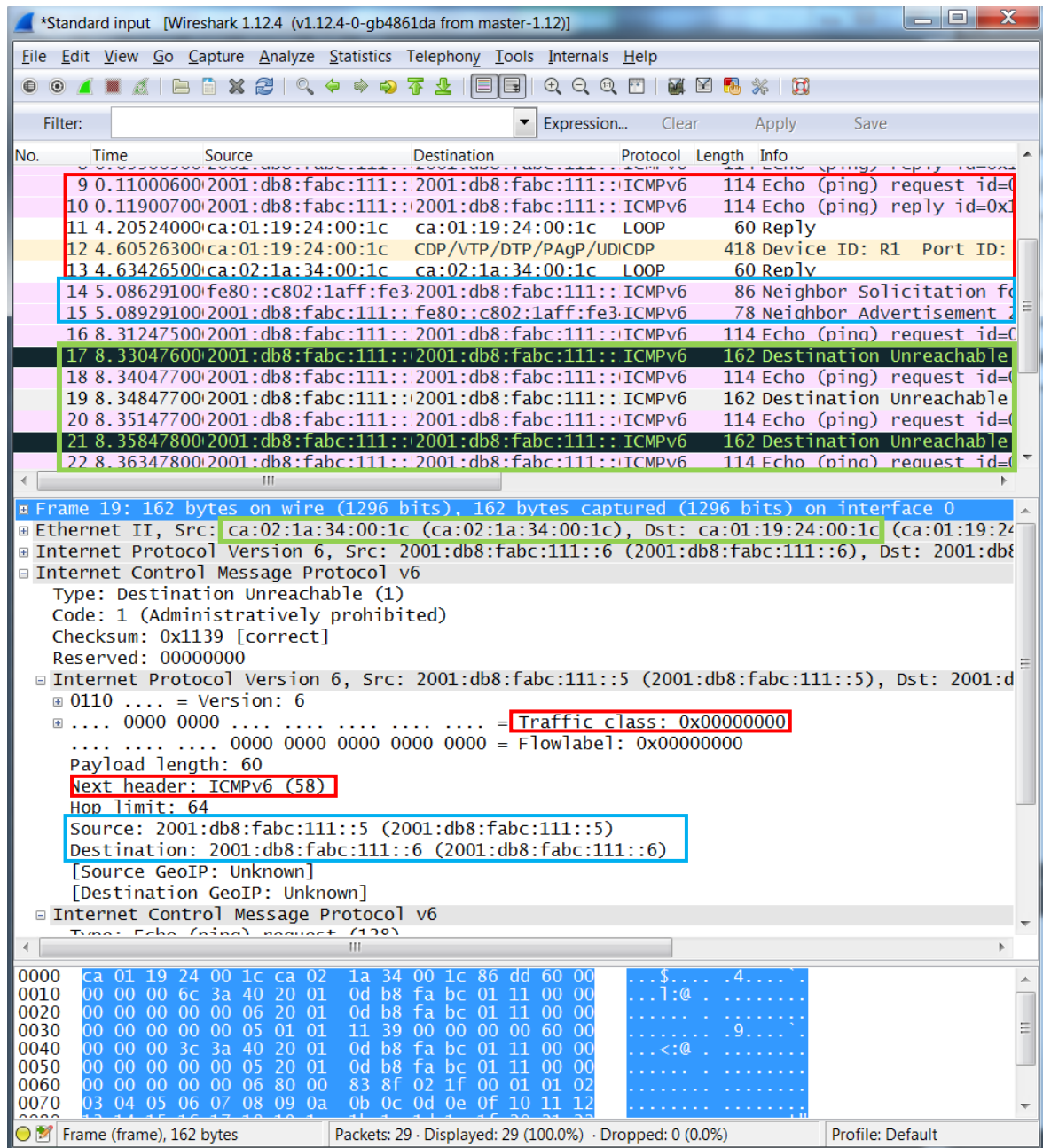
Pred samotným aplikovaním ACL a pingom je zahájené spustenie paketov na R2 porte. Po nalogovaní do R2 si môžu **overiť otvorené TCP relácie** i po odstavení premávky. [5]

Tab. 9: Príkazy pre overenie implementovaných konfiguračných zmien a ladenie [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu: <b>Krok 1:</b>	<b>show ip inter et1/0   in list</b> R2# show ip inter et1/0   in list	Zobrazenie vstup/výstupných kontrolných zoznamov-rozhr e1/0
Syntax príkazu: <b>Krok 2:</b>	<b>R2#show ipv6 inter et1/0   in list</b> R2#show ipv6 inter et1/0   in list	Zobrazenie vstup/výstupných kontrolných zoznamov-rozhr e1/0
Syntax príkazu: <b>Krok 3:</b>	<b>show ip access-lists REKTORAT-ACL</b> R2# show ip access-lists REKTORAT-ACL	Zobrazenie chytania na kontrolných zoznamoch IPv4
Syntax príkazu: <b>Krok 4:</b>	<b>show ipv6 access-list REKTORAT-ACL-6</b> R2# show ipv6 access-list REKTORAT-ACL-6	Zobrazenie chytania na kontrolných zoznamoch IPv6
Syntax príkazu: <b>Krok 5:</b>	<b>show run   in list</b> R2# show run   in list	Zobrazenie konfigurácie pre kontrolné zoznamy IPv6
Syntax príkazu: <b>Krok 6:</b>	<b>debug ipv6 icmp</b> R2#debug ip/ipv6 icmp	Aktivovanie ladenia a zobrazovanie paketov na term pre

Pri **analýze** paketov prvé *pakety 9 a 10* sú ICMPv6 protokoly, konkrétne **echo žiadosť a odpoveď pingu**, ktoré sú označené červenou na *Obr. 18*. Následne bol aplikovaný

kontrolný zoznam *REKTORAT-ACL-6* na vstupnú prevádzku do smerovača *R2* na porte *Eth1/0*. Ladenie a **Wireshark** presne odpovedajú. *Paket* číslo *17* je už zahodený a *ICMPv6* posielala správu o nedostupnosti host'a , ktoré sú označené zelenou na *Obr. 18*. Pri detailnej **analýze paketu ICMPv6** si môžu rozrolovať pôvodnú žiadosť. V *ICMPv6* sa vidí, že ide o rozširujúcu novú hlavičku *58* , zdrojovú a cieľovú adresu *3.* vrstvy a že na daný paket sa vzťahuje *traffic class* (kontrolný zoznam pre *IPv6*), čo je i dôvodom jeho zahodenia. V neposlednej rade sú na *Obr. 18* vyznačené modrou *NS* a *NA* pakety pri zisťovaní host'a *R2*, k tomu je použitá *multicast* adresa *fe80::c802:1aff:fe34:1c*, čo odpovedá *L2 MAC* adrese *ca:02:1a:34:00:1c*. Pri *IPv4* paket má v **ICMP správe** v *IPv4* "*Communication admin. Filtered*" a vracia sa *ICMP* správa o **nedostupnosti** host'a. [1][6][7]



Obr. 18: Zachytené ICMPv6 pakety o nedostupnosti R2 medzi R1 a R2 [autor]




Nasledujúca tabuľka **porovnáva nastavenie kontrolných zoznamov** pre obmedzenie ICMPv6 paketov. Ide o najjednoduchšie kontrolné zoznamy. Detailnejší rozbor a použitie bude urobený v nasledujúcich laboratórnych úlohách. Je to **úvod do použitia** aplikácie Wiresharku. Každý kontrolný zoznam je definovaný v konfiguračnom móde a pod rozhraním môže byť aplikovaný. **Výpisom** `show ip/ipv6 access-lists` si môže **skontrolovať**, koľko zachytil paketov a vo **Wiresharku** dohľadať konkrétne adresy prípadne **aktivovať** ladenie. [3] [8]

Tab. 10: Show príkazy overujúce implementované konfigurácie ACL pre IPv4/IPv6 [5]

R1	R2
<pre>R1#show run inter eth 1/0 Building configuration...  Current configuration : 130 bytes ! interface Ethernet1/0 ip address 10.5.5.1 255.255.255.252 duplex full ipv6 address 2001:DB8:FABC:111::5/64 ipv6 enable end  R1#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is not set R1#show ipv6 inter et1/0   in list R1#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is not set R1#show ipv6 inter et1/0   in list R1#show ip access-lists REKTORAT-ACL R1#show ipv6 access-list REKTORAT-ACL-6</pre>	<pre>R2#show run inter eth 1/0 Building configuration...  Current configuration : 202 bytes ! interface Ethernet1/0 ip address 10.5.5.2 255.255.255.252 ip access-group REKTORAT-ACL in duplex full ipv6 address 2001:DB8:FABC:111::6/64 ipv6 enable ipv6 traffic-filter REKTORAT-ACL-6 in end  R2#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is REKTORAT-ACL R2#show ipv6 inter et1/0   in list Inbound access list REKTORAT-ACL-6 R2#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is REKTORAT-ACL R2#show ipv6 inter et1/0   in list Inbound access list REKTORAT-ACL-6 R2#show ip access-lists REKTORAT-ACL Extended IP access list REKTORAT-ACL 10 deny icmp any any (4 matches) R2#show ipv6 access-list REKTORAT-ACL-6 IPv6 access list REKTORAT-ACL-6 deny icmp any any (109 matches) sequence 10</pre>
<pre>R1#show run inter eth 1/0 Interface Ethernet1/0 ip address 10.5.5.1 255.255.255.252 duplex full ipv6 address 2001:DB8:FABC:111::5/64 ipv6 enable</pre>	<pre>R2#show run inter eth 1/0 interface Ethernet1/0 ip address 10.5.5.2 255.255.255.252 ip access-group REKTORAT-ACL in duplex full ipv6 address 2001:DB8:FABC:111::6/64 ipv6 enable ipv6 traffic-filter REKTORAT-ACL-6 in</pre>
<pre>R1#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is not set</pre>	<pre>R2#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is REKTORAT-ACL</pre>
<pre>R1#show ipv6 inter et1/0   in list</pre>	<pre>R2#show ipv6 inter et1/0   in list Inbound access list REKTORAT-ACL-6</pre>
<pre>R1#show ip inter et1/0   in list Outgoing access list is not set Inbound access list is not set</pre>	<pre>R2#show run   in list ip access-list extended REKTORAT-ACL ipv6 access-list REKTORAT-ACL-6</pre>
<pre>R1#show ipv6 inter et1/0   in list</pre>	<pre>R2#show ipv6 inter et1/0   in list Inbound access list REKTORAT-ACL-6</pre>
<pre>R1#show ip access-lists REKTORAT-ACL</pre>	<pre>R2#show ip access-lists REKTORAT-ACL Extended IP access list REKTORAT-ACL 10 deny icmp any any (4 matches)</pre>
<pre>R1#show ipv6 access-list REKTORAT-ACL-6</pre>	<pre>R2#show ipv6 access-list REKTORAT-ACL-6 IPv6 access list REKTORAT-ACL-6 deny icmp any any (106 matches) sequence 10</pre>

Výsledné nastavenie smerovačov pre overenie funkčnosti SSH:

Tab. 11: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

R1	R2	Wireshark
 <p>R1 ICMP.txt</p>	 <p>R2 ICMP.txt</p>	 <p>icmp pcapng.pcapng</p>

## 2.6 Otázky na zamyslenie o ICMP:

1. Na ktorej vrstve modelu OSI je ICMP (Overte odpovede pomocou Wiresharku) ? [8]

**Obe ICMP i ICMPv6 sú 3. sieťovej vrstve**

2. Aká je základná hodnota odozvy ICMP pri pingu ?

**2 sekundy**

3. Aký príkaz slúži pre aktivovanie ladenia ICMP paketov?

**debug ip ICMP**

4. Aký príkaz sa používa pre zobrazenie správ o nedostupnosti host'ov. [1]

**show ip ICMP rate-limit**

### 3 PREKLAD ADRIES DNS

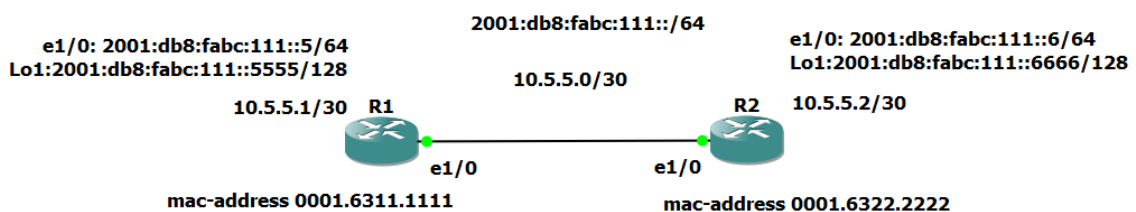
V tejto úlohe preskúmame **použitie protokola DNS** (Domain Name System) jeho **spoluprácu s IPv4** pre preklad *URL* na *IP* adresu. Pomocou **Wiresharku** sa **analyzuje preklad domén** s využitím aplikačného protokola *DNS* a známeho **portu 53**. K tomu účelu je použitá jednoduchá topológia v **GNS3** z predchádzajúcej úlohy o *ICMP*. [8]

#### 3.1 Zadanie:

Vytvor jednoduchú topológiu 2 smerovačov DNS a over funkčnosť vo Wiresharku.

#### 3.2 Topológia:

Konfigurácia IPv6 je rovnaká ako u protokolu IPv4.



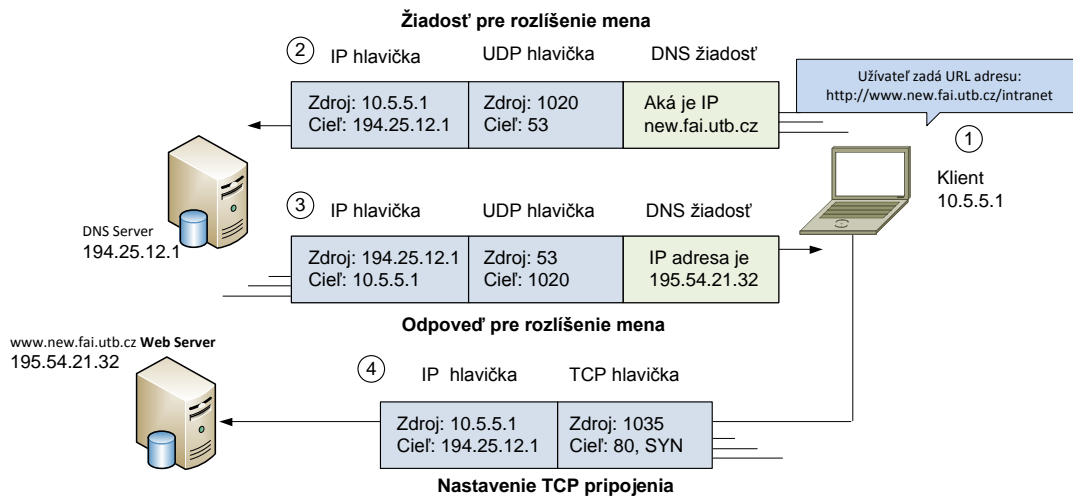
Obr. 19: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie SSH [autor]

#### 3.3 Teória:

Vďaka protokolu **DNS** užívateľ pri zadaní *WWW* adresy zistí *IP* adresu, ktorá **odpovedá** zadanému **webovému portálu**. Zjednodušene sa **DNS** môže predstaviť ako **zoznam záznamov** *IP* adries (*A*=*IPv4*, *AAAA*=*IPv6*), domén (*CNAME* - Canonical name), mail server (*MX* - Mail Exchange) prípadne ukazovateľ (*PTR* - Pointer) pri **reverznom hľadaní** **DNS** servera. V laboratórnej úlohe sa ukáže ako nastaviť, aby sa smerovač choval ako **DNS** server. [1] [4]

Pred samotným **spracovaním** prehliadač môže poslať **paket do webového servera**, potrebuje **zistiť meno**, ktoré odpovedá *URL* adrese. Ako je zobrazené na *Obr. 27* užívateľ zadá do prehliadača adresu (<http://www.new.fai.utb.cz/intranet>) výsledné meno pre **DNS** je [www.new.fai.utb.cz](http://www.new.fai.utb.cz), k čomu **hľadá IP**, aby začal **posielat' pakety** pre web server. Základné **DNS požiadavky** používajú *UDP*, cieľový *UDP* port 53. [1]

Tento preklad je zhrnutý do 4 krokov:



Obr. 20: DNS rozlíšenie mena a žiadosť webovej stránky [4]

1. Užívateľ **zadá URL**, `http://www.new.fai.utb.cz/intranet` do internetového prehliadača
2. Klientský laptop **posiela DNS žiadosť** pre DNS server. Obvykle, klient sa učí DNS IP pomocou DHCP. DNS žiadosť používa **UDP** hlavičku s cieľovým známym portom 53.
3. DNS server posiela odpoveď, že web `www.new.fai.utb.cz` **načúva na IP** adrese `15.54.21.32`. Odpoveď má cieľovú adresu klientovu IP. Vo Wiresharku si môže overiť aj UDP port 53 a pre klienta použitý **voľný verejný port**.
4. Klient začne proces **nadväzovania TCP spojenia** s web serverom klasickým TCP **spojením**. Paket obsahuje **TCP hlavičku**, pretože **HTTP** používa TCP. Cieľový TCP port je 80, ktorý odpovedá HTTP. Nakoniec sa **zobrazí SYN bit** ako dôkaz, že začal proces nadväzovania. Následne bude prebiehať HTTP proces **výmeny dát** pomocou **HTTP GET**. [1] [2]

### 3.4 Požadované zdroje:

GNS3 a Wireshark

IOS smerovače– s ethernet rozhraním `c3640-ik9o3s-mz124-13` a `c7200-advipservicesk9-mz`

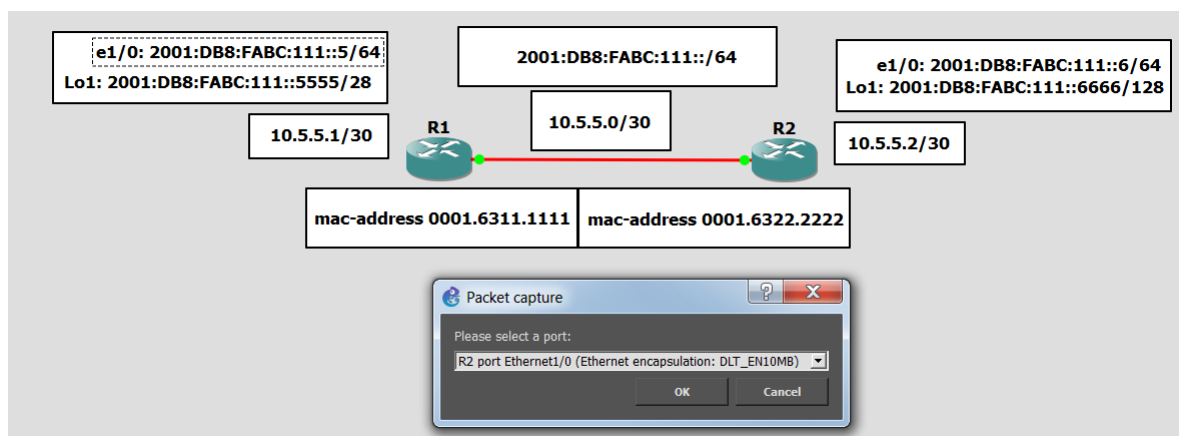
### 3.5 Postup:

V tejto úlohe sa bude diskutovať, **testovať** a **konfigurovať** protokol DNS. Z konfigurácie laboratórnej úlohy sa odoberú nepotrebné kontrolné zoznamy pod rozhraním e1/0. Opäť sa **využije základná topológia** dvoch smerovačov. Je potrebné povedať, že nie každý IOS môže byť DNS serverom. Pomocou príkazu `ip DNS server` v konfiguračnom móde na R1 nastaví DNS. R1 používa `c3640-ik9o3s-mz124-13` a R2 `c7200-advipservicesk9-mz`. Na smerovači R1 sa nastaví funkcionálna DNS servera, ktorý bude R2 používať pre **riešenie prekladu domén**. Následne si inicializuje prevádzku, ktorá spustí **DNS zisťovanie adries** z domény. Pred tým sa môže zapnúť ladenie UDP prevádzky `debug ip udp`. [1]

```
R1#debug ip udp
UDP packet debugging is on
R1#
*Mar  1 00:20:49.863: UDP: rcvd src=10.5.5.2(50811), dst=10.5.5.1(53), length=48
*Mar  1 00:20:49.867: UDP: sent src=10.5.5.1(53), dst=10.5.5.2(50811), length=48
*Mar  1 00:20:49.935: UDP: rcvd src=10.5.5.2(49879), dst=10.5.5.1(53), length=48
*Mar  1 00:20:49.939: UDP: sent src=10.5.5.1(53), dst=10.5.5.2(49879), length=64
```

Obr. 21: Ping s ladením UDP prevádzky pri preklade domén [autor]

Nastavenia **vytvárania užívateľov, hesiel a základnom nastavení mena a adresácie** sa už preskočí a úloha sa venuje ICMP protokolu IPv4.



Obr. 22: Spustenie zachytávania paketov, nezáleží na porte, ktorý sa vyberie

Nakoľko väčšina **konfigurácie** sa preberá z laboratórnej úlohy ICMP, odoberú sa ACL, aktivujú sa porty `E1/0` a **pridajú sa DNS**. Výsledná konfigurácia sa **porovnáva s pôvodnou**: [2]

Tab. 12: Možnosť porovnania zmien pred a po uložení zmien do NVRAM [autor]

```
show archive config differences nvram:startup-config system:running-config
```

Tab. 13: Syntax aplikovaných príkazov a vysvetlenie významu [autor]

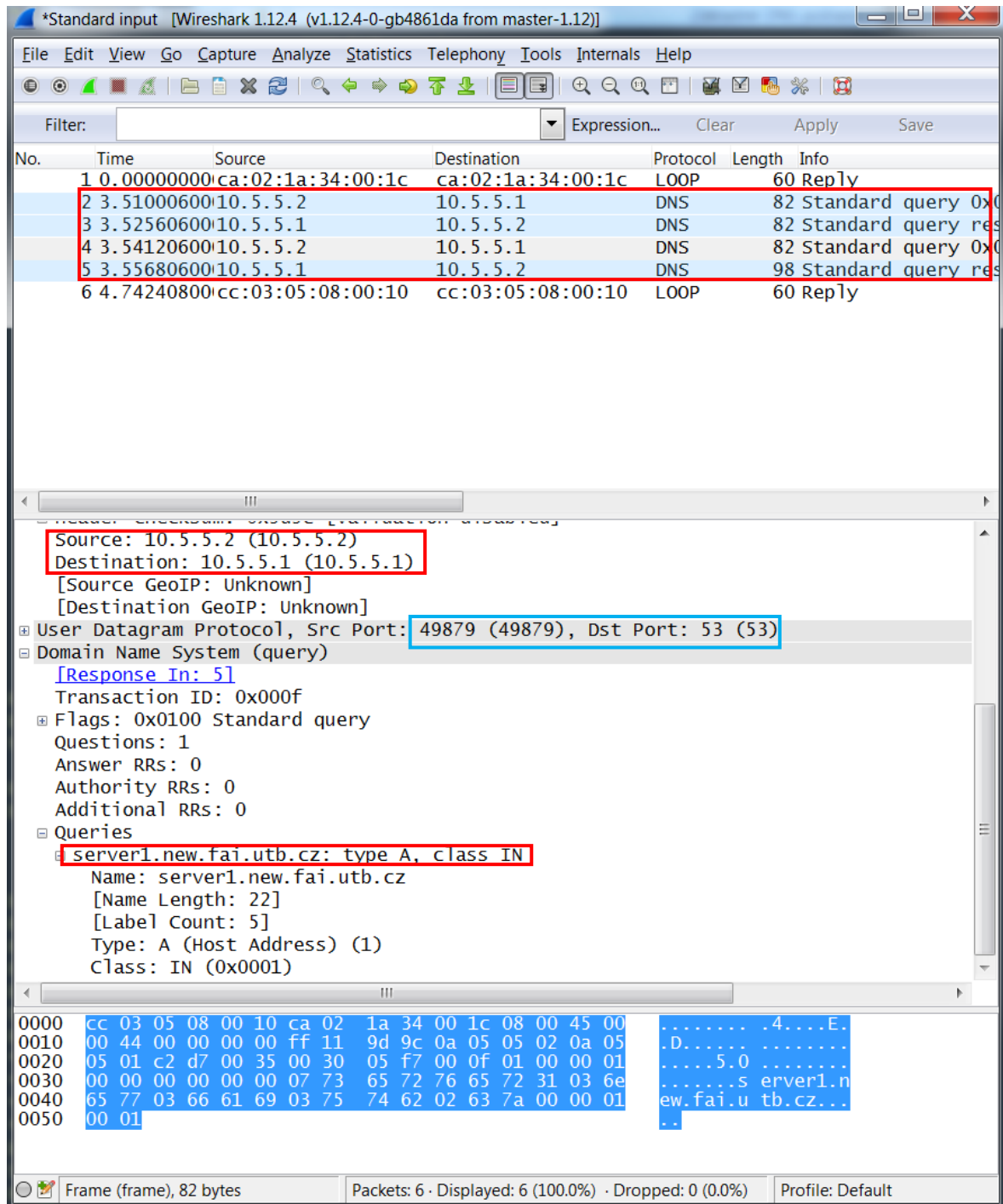
	Syntax + Príkaz	Význam/Účel
Syntax príkazu: <b>Krok 1:</b>	<b>no ip access-group name [in/out]</b> R2 (config-if)# no ip access-group REKTORAT-ACL in	Odobratie kontrolných zoznamov pre prevádzku IPv4 z rozhrania
Syntax príkazu: <b>Krok 2:</b>	<b>no ipv6 traffic-filter name [in/out]</b> R1/R2 (config-if)# no ipv6 traffic-filter REKTORAT-ACL-6	Odobratie kontrolných zoznamov pre prevádzku IPv6 z rozhrania
Syntax príkazu: <b>Krok 3:</b>	<b>ip DNS server</b> R1(config-line)# ip DNS server	Nastavenie role smerovača do role DNS servera
Syntax príkazu: <b>Krok 4:</b>	<b>ip host [Name of host] [IP address]</b> R1 (config)# ip host server1.new.fai.utb.cz 10.5.5.2	Nastavenie DNS záznamu časovania konzoly - prerušenie.
Syntax príkazu: <b>Krok 5:</b>	<b>ip domain lookup</b> R2 (config-line)# ip domain lookup	Nastavenie dohľadovania domén obvykle sa vypína, keď nie je DNS
Syntax príkazu: <b>Krok 6:</b>	<b>ip name-server 10.5.5.1</b> R2(config)# ip name-server 10.5.5.1	Nastavenie IP adresy doménového serveru
Syntax príkazu: <b>Krok 7:</b>	<b>ipv6 address IPv6 Address</b> R1# ipv6 address 2001:DB8:FABC:111::6/64	Nastavenie ladenia UDP prevádzky na DNS serveri
Syntax príkazu: <b>Krok 8:</b>	<b>copy running-config startup-config /write memory</b> R2 (config-if)# # copy running-config startup-config	Uloženie aktuálneho nastavenia do NVRAM.

Pred samotným pingom novej domény *server1.new.fai.utb.cz* a pingom odpovedajúcej IP adrese nastaví zachytávanie paketov na R2 porte.

Tab. 14: Príkazy pre overenie implementovaných konfiguračných zmien a ladenie [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu: <b>Krok 1:</b>	<b>show ip DNS statistics</b> R1#show ip DNS statistics	Zobrazenie štatistiky žiadostí a odpovedí na otázky záznamov.
Syntax príkazu: <b>Krok 2:</b>	<b>debug ip udp</b> R1(config-if)# debug ip udp	Aktivovanie s ladenia UDP prevádzky pri preklade domén
Syntax príkazu: <b>Krok 3:</b>	<b>ping new.fai.utb.cz repeat 1</b> R2# ping new.fai.utb.cz repeat 1	Testovanie prekladu domény <b>new.fai.utb.cz IP</b>

Pri analýze prvých paketov 2-5 sú DNS protokoly konkrétne **otázky na DNS server** a odpovede z 10.5.5.1, ktoré sú označené červenou na Obr. 23. Paket číslo 4 je **otázka na doménu server1.new.fai.utb.cz**. Je k tomu využitý **voľný UDP port**, ktorý odpovedá ladeniu v termináli, označeného modrou. Ďalšou zaujímavosťou je označenie **typu a otázky** vždy na IPv4 – A záznam a IPv6 – AAAA záznam, čo dokazuje vzájomnú kompatibilitu. V GNS3 sa ako posledný krok môže pozrieť na **štatistiky žiadostí a odpovedí na otázky záznamov domén a adries**. [5]



Obr. 23: Zachytené DNS dotazy a UPD o doméne er1.new.fai.utb.cz [autor]

Následující tabuľka




Tab. 15 porovná nastavenie DNS na R1 a R2. Výpisom `show run inter E1/0` sa vidí nastavenie rozhrania a `show run | in server` vyfiltrujeme všetky konfiguráciu pre DNS. [1][4]

Tab. 15: Show príkazy overujúce implementované DNS [autor]

R1	R2
<pre>R1#show run inter e1/0 interface Ethernet1/0 ip address 10.5.5.1 255.255.255.252 full-duplex ipv6 address 2001:DB8:FABC:111::5/64 ipv6 enable</pre>	<pre>R2#show run inter e1/0 interface Ethernet1/0 ip address 10.5.5.2 255.255.255.252 duplex full ipv6 address 2001:DB8:FABC:111::6/64 ipv6 enable</pre>
<pre>R1#show run   in server ip host server1.new.fai.utb.cz 10.5.5.2 no ip http server no ip http secure-server ip DNS server</pre>	<pre>R2#show run   in server ip name-server 10.5.5.1 no ip http server no ip http secure-server</pre>
<pre>R1#R1show archive config differences nvram:startup-config system:running- config Contextual Config Diffs: +hostname R1 +no ip domain lookup +ip host server1.new.fai.utb.cz 10.5.5.2 +ipv6 unicast-routing +ipv6 cef +username admin secret 5 \$1\$MrMK\$pWkt6rqDWQqWV.1BxYCsg 0 +ip tcp synwait-time 5 interface Ethernet1/0 +ip address 10.5.5.1 255.255.255.252 +full-duplex +ipv6 address 2001:DB8:FABC:111::5/64 +ipv6 enable ...</pre>	<pre>R2# R2 show archive config differences nvram:startup-config system:running-config R2#\$e config differences nvram:startup-config system:running-config !Contextual Config Diffs: +ip name-server 10.5.5.1 line con 0 +length 0 interface Ethernet1/0 -ip access-group REKTORAT-ACL in -ipv6 traffic-filter REKTORAT-ACL-6 in</pre>

Výsledné nastavenie smerovačov pre overenie funkčnosti SSH:

Tab. 16: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor]

R1	R2	Wireshark
 R1 DNS.txt	 R2 DNS.txt	 dns.pcapng

### 3.6 Otázky na zamyslenie o DNS:

5. Na ktorej vrstve modelu OSI je DNS (Overte odpovede pomocou Wiresharku) ? [8]

**Aplikačnej vrstve**

6. Aký well-known port je použitý ?

**53**

**ZOZNAM POUŽITÉJ LITERTÚRY**

- [1] LAMMLE, Todd. *CCNA: výukový průvodce*. 1. vydání. Překlad Jakub Goner. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [2] Cisco Networking Academy Course Catalog, [Online]. [cit. 2015-10-28].  
Dostupné z :  
[www.cisco.com/web/learning/netacad/course\\_catalog/CCNAexploration.html](http://www.cisco.com/web/learning/netacad/course_catalog/CCNAexploration.html).
- [3] *GNS3 / Graphical Network Simulator*. [Online]. [cit. 2015-10-28]. Dostupné z:  
[www.gns3.net](http://www.gns3.net).
- [4] ODOM, Wendell. *Cisco CCENT/CCNA ICND1 100-101 official cert guide, academic edition*. Academic edition. Indianapolis, IN: Cisco Press, 2013. ISBN 1587144859.
- [5] ODOM, Wendell. *Cisco CCNA routing and switching ICND2 200-101 official cert guide*. Indianapolis, Indiana: Cisco Press, 2013. ISBN 1587143739.
- [6] HUCABY, Dave. *CCNP routing and switching SWITCH 300-115 official cert guide*. Indianapolis, IN: Cisco press, 2015. ISBN 978-1-58720-560-6.
- [7] URBANČOK, Lukáš. *Technologie IPv6, její bezpečnost a simulace sítí s využitím GNS3*. Zlín, 2016. Diplomová práce. Fakulta aplikované informatiky - Univerzita Tomáše Bati ve Zlíně. Katedra počítačových a komunikačních systémů. Vedoucí kvalifikační práce Ing. Jiří Korbel, Ph.D.
- [8] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

**ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK**

AAA	Authentication, Authorization, and Accounting
ACK	Potvrdenie zdrojového portu a vytvorenia virtuálneho okruhu
ACL	Access-list = kontrolný zoznam = filter
BW	Šírka pásma (bandwidth)
CCNA	Cisco Certified Network Associate
CDP	Cisco Discovery Protocol- zhromažďovanie info o lokálne pripojen. zariadení
CLI	command-line interface = rohranie príkazového riadku
CNAME	Canonical name
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System – preklad názvov host'ov
E1/0	Ethernet 1/0
EXEC	Mód nad konfiguráciou, rozlišujúci práva užívateľov USER-, PRIVILEGED-
GES	Global Engineering Solutions
GNS3	Graphical Network Simulator 3
handshake	three-way handshake = trojcestné overovanie typu handshake
HTTP	Hypertext Transfer Protocol - riadi komunikáciu web prehliadač ↔ server
ICMP	Internet Control Message Protocol – poskytovateľ služieb zasielania správ IP
IF	Rozhranie (Interface)
IOS	Internetwork Operating System
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
Lo1	Zpätnovazbová Slučka (Loopback1)
Lx	Layer x – referencia na konkrétnu vrstvu modelu OSI
MAC	L2 adresa, ktorá jednoznačne identifikuje fyzické pripojenie hostiteľa
MX	Mail Exchange
NA	Neighbor advertisement
NS	Neighbor solication
NVRAM	Nonvolatile RAM – obsahuje platný startup-config používaný pri restarte
NX OS	Nexus Operating System- operačný systém Nexus, používaný Data Centrami
OS	Operating System - operačný systém
OSI	Open Systems Interconnection- Cisco model obsahuje 7 hierarchických vrstiev

plaintext	Čistý nešifrovaný text
PTR	Pointer
R/S	Routing and Switching
RA	Router advertisement
RADIUS	Remote Authentication Dial-in User Service – server pre AAA
RFC	Request For Comments
RS	Router solicitation
RSA	Rivest-Shamir-Adleman – šifrovací systém pre verejné kľúče
run-config	bežiacia konfigurácia
S2/1	Serial 2/1
session	relácia
SNMP	Simple Network Management Protocol – protokol pre správu siete
SSH	Secure Shell – zabezpečená relácia nad štandardným pripojením TCP/IP
SYN	Synchronizačná sekvencia s požiadavkom na virtuálnu reláciu
TACACS+	Terminal Access Controller Access-Control System + protokol pre AAA
TCP	Transmission Control Protocol– prijíma veľké bloky dát a delí ich na segment
TTL	Time to Live – zamedzenie neobmedzenej životnosti paketov
UDP	User Datagram Protocol
URL	Uniform Resource Locator, jednoznačne označuje webovú adresu
VTY	virtuálna linka pre správu/vzdialený prístup

**ZOZNAM OBRÁZKOV**

<i>Obr. 1: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie SSH[3] [autor] .....</i>	<i>2</i>
<i>Obr. 2: Možnosti prechodu medzi Užívateľským a Privilegovaným módom [2] .....</i>	<i>3</i>
<i>Obr. 3: CLI prístup pomocou SSH do EXEC módu [autor] .....</i>	<i>3</i>
<i>Obr. 4: Spustenie zachytávania paketov pomocou Wiresharku možnosťou výberu portu[3] .....</i>	<i>4</i>
<i>Obr. 5: Zobrazenie prihlásených užívateľov a záznamu o SSH reláciách [autor] .....</i>	<i>6</i>
<i>Obr. 6: Zobrazenie prihlásených užívateľov [autor] .....</i>	<i>6</i>
<i>Obr. 7: Zachytené SSH dáta medzi SSH klientom a serverom R1 a R2 [autor] .....</i>	<i>8</i>
<i>Obr. 8: Ping medzi R1 a multicast groupou 224.66.255.10 [autor] .....</i>	<i>8</i>
<i>Obr. 9: Show príkazy overujúce implementované konfigurácie [autor] .....</i>	<i>9</i>
<i>Obr. 10: Vygenerovaný RSA verejný kľúč [autor] .....</i>	<i>9</i>
<i>Obr. 11: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie SSH [autor] .....</i>	<i>11</i>
<i>Obr. 12: Testovanie pingom susednej IP pred aplikáciou prístupového zoznamu [autor] .....</i>	<i>12</i>
<i>Obr. 13: Ladenie problémov pomocou informačných správ ICMP, echo žiadosť a odpoveď [autor] .....</i>	<i>12</i>
<i>Obr. 14: Všeobecný proces zisťovania susedov, ktorý používa ICMP pakety v IPv6 [2] .....</i>	<i>12</i>
<i>Obr. 15: Ping pred a po aplikovaní prístupového zoznamu REKTORAT-ACL-6 [autor] .....</i>	<i>13</i>
<i>Obr. 16: Ladenie ICMPv6 paketov pred a po aplikovaní ACL REKTORAT-ACL-6 [autor] .....</i>	<i>14</i>
<i>Obr. 17: Spustenie zachytávania paketov, nezáleží na porte, ktorý sa vyberie [autor] .....</i>	<i>14</i>
<i>Obr. 18: Zachytené ICMPv6 pakety o nedostupnosti R2 medzi R1 a R2 [autor] .....</i>	<i>17</i>
<i>Obr. 19: GNS3 topológia z laboratórnej úlohy Ethernet pre overenie SSH [autor] .....</i>	<i>20</i>
<i>Obr. 20: DNS rozlíšenie mena a žiadosť webovej stránky [4] .....</i>	<i>21</i>
<i>Obr. 21: Ping s ladením UDP prevádzky pri preklade domén [autor] .....</i>	<i>22</i>
<i>Obr. 22: Spupstanie zachytávania paketov, nezáleží na porte, ktorý sa vyberie .....</i>	<i>22</i>
<i>Obr. 23: Zachytené DNS dotazy a UPD o doméne er1.new.fai.utb.cz [autor] .....</i>	<i>24</i>

**ZOZNAM TABULIEK**

<i>Tab. 1: Syntax aplikovaných příkazov a vysvetlenie významu [autor].....</i>	<i>4</i>
<i>Tab. 2: Příkazy pre overenie implementovaných konfiguračných zmien a ladenie [autor] .....</i>	<i>5</i>
<i>Tab. 3: Konfigurácia IPv4 a IPv6 adres a riadenie prístupu len pomocou SSH [autor] .....</i>	<i>7</i>
<i>Tab. 4: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor] .....</i>	<i>9</i>
<i>Tab. 5: Konfigurácia IPv4 prístupového zoznamu pre virtuálne linky [autor].....</i>	<i>10</i>
<i>Tab. 6: Konfigurácia povolenia zdrojovej adresy začínajúcej s 10.10.10.x [autor].....</i>	<i>10</i>
<i>Tab. 7: Správna konfigurácia SSH a riadenie prístupu na virtuálnej linke [autor] .....</i>	<i>10</i>
<i>Tab. 8: Syntax aplikovaných příkazov a vysvetlenie významu [autor].....</i>	<i>14</i>
<i>Tab. 9: Příkazy pre overenie implementovaných konfiguračných zmien a ladenie [autor] .....</i>	<i>15</i>
<i>Tab. 10: Show příkazy overujúce implementované konfigurácie ACL pre IPv4/IPv6 [5].....</i>	<i>18</i>
<i>Tab. 11: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor] .....</i>	<i>18</i>
<i>Tab. 12: Možnosť porovnania zmien pred a po uložení zmien do NVRAM [autor].....</i>	<i>22</i>
<i>Tab. 13: Syntax aplikovaných příkazov a vysvetlenie významu [autor].....</i>	<i>23</i>
<i>Tab. 14: Příkazy pre overenie implementovaných konfiguračných zmien a ladenie [autor] .....</i>	<i>23</i>
<i>Tab. 15: Show příkazy overujúce implementované DNS [autor] .....</i>	<i>25</i>
<i>Tab. 16: Konfigurácia smerovačov v Cisco IOS 15.2(4) S3 [autor] .....</i>	<i>25</i>