INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato inovace předmětu Analýza dat je spolufinancována Evropským sociálním fondem a Státním rozpočtem ČR, projekt č. CZ.1.07/2.2.00/28.0014, "Interdisciplinární vzdělávání v ICT s jazykovou kompetencí".

Digitální analýza Cisco směrovačů a přepínačů 2

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Co nového se naučíme a na jaké otázky odpovíme?

- Jak a včem si napsat vlastní skripty pro sběr dat (vytvoření, spuštění, kam směrovat výstup).
- Kde ve směrovači (přepínači) hledat a jaká data sbírat (paměti a jejich obsah).
- Která data jsou stálá a která nestálá? Jak je můžeme svým chováním znehodnotit?
- Jak postupovat a čemu se vyvarovat při vzniklém incidentu? Aneb myslíme „forenzně“.
- Jaké lze použít metody pro sběr dat?
- Možnosti simulace (tréninku) mimo reálné zařízení.

Pro testování příkladů v průběhu výklady si všichni zapojte a nastavte přímé spojení s libovolným směrovačem v racku.

Tool Commnad Language

Základní charakteristika

- Tool Command Language (zkráceně TCL), vyslovuj „tykl“.
- Multiplatformní skriptovací jazyk odvozený z Lispu.
- Široká možnost použití při programovávní aplikací i při administraci a testování počítačových sítí.
- Podrobnější informace na: http://www.tcl.tk/.

Integrace TCL do Cisco IOS

- Nás bude zajímat integrace TCL do prostředí Cisco IOS.
- Implementován do IOS od verze 12.2 (v dalších verzích IOS rozšíření).

Integrace TCL do Cisco IOS

- V praxi vhodný k nasazení v situacích, když potřebujeme filtrovat rozsáhlé výpisy (např. routovací tabulka páteřního směrovače) nebo provést sekvenčně mnoho stejných příkazů s různou proměnou (např. otestovat konektivitu zařízení v celé podsíti). Pomocí skriptu lze řešit i konfiguraci.
- Skripty se spouští v konfiguračním režimu TCL do kterého se dostanete z priviledge-exec režimu.
- Cisco IOS příkazy se píší v TCL skriptech v uvozovkách.
- Pozor: špatně napsané skripty vedou k zamrznutí. Nikdy poprvé netestujte v reálném prostředí ale např. v simulátoru GNS3 (viz.dále).

Přechod do konfiguračního režimu TCL

Integrace TCL do Cisco IOS

- Použití vyžaduje znalost jazyka TCL i Cisco IOS příkazů.
- Skripty mohou být i velmi rozsáhle, proto je vhodné použít TCL skripty v kombinaci s TFTP serverem.
- Skripty můžeme upravovat v sobouru .tcl a pohodlně je zpouštět z TFTP serveru.
- Podrobný návod na použití TCL v Cisco IOS:

  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_tcl.html.

TCL skripty a forenzní analýza

- Prostřednictvím jediného TCL skriptu můžeme posbírat všechna nestálá i stálá data ze směrovače.
- Předem napsané skripty pomáhájí vyvarovat se překlepů při psaní řady #**show** příkazů při zkoumání směrovače.

TCL skripty a forenzní analýza

- Tato „automatizace“ při sběru především nestálých dat celý proces urychlý. Což je u dat měnících rychle svůj stav jistě přínosem.
- Př. otevřená vzdálená spojení, přihlášení uživatelé, stav rozhraní, obsah routovací tabulky, ...
- Veškeré výpisy #**show** příkazů mohou být přesměrovány a uloženy na TFTP server k pozdější analýze.

Systax příkazu pro spuštění TCL skriptu z TFTP serveru

```
Router#tclsh tftp://<IP_tftp_Server
>/<Directory>/<File_name.tcl>
```

Ukázka triviálního TCL skriptu pro sběr dat

Příkaz který spustí skript na směrovači

```
Router#tclsh tftp://192.168.0.2/aa.tcl
```

Obsah samotného skriptu

```
puts "\nexecuting show ip interface brief"

show ip interface brief | redirect tftp://192.168.0.2/ShowIpIntBr.txt

puts "\nexecuting show startup-config"

show startup-config | redirect tftp://192.168.0.2/startup.txt
```

- Skript spustíme na směrovači příkazem úplně nahoře. Skript provede dva #**show** příkazy, přičemž výsput z každého pošle do zvláštního souboru .txt na TFTP server zadaný IP adresou.

Příklady na TCL skripty

Příklady na TCL skripty využitelné nejen k forenzní analýze

- Napište si vlastní skripty v TCL pro sběr dat ze zařízení.
- Napište TCL skript, který ověří konektivitu směrovačů v multi-access oblasti.
- Zamyslete se, k čemu ve Vaší praxi by jste mohli využít skriptů TCL a skript napište.

Cisco Router Evidence Extraction Disk

- Tvůrce softwaru je Thomas Akin
- Jedná se o bootovací floopy disk, který od uživatele vyžaduje pouze nastavit připojení na zařízení. Automaticky vykoná 24 #**show** příkazů, jejichž obsah uloží.
- Vnáší jistou „automatizaci“ do sběru dat z Cisco směrovače.
- Byl vytvořen k obsluze netrénovaným personálem ve zkoumání digitálních důkázů a provádění forenzní analýzy na směrovači.
- Bohužel, ke stažení se nachází pouze v jediném archivu a image je zřejmě poškozená. I po několika stažení nikdy neodpovídá kontrolní součet a software nefuguje.
- Tento projekt mě velmi zaujal a nebylo by špatné takový nástroj napsat!!!
- Odkaz na archiv, kde jsou bližší informace:

  http://web.archive.org/web/20040214172413/http://cybercrime.kennesaw.edu/creed/.

Pamětí a jejich obsah ve směrovačích a přepínačích

Co si v této části povíme?

Cílem této části je připomenout jaký typ pamětí lze nalézt ve směrovačích a přepínačích. Také nás bude zajímat, jaká data tyto pamětí obsahují a samozřejmě jejich „trvanlivost“ vzhledem k závyslosti na napájení.

Jste schopni nyní odpovědět na následující otázky?

- Jaké typy pamětí lze nalézt v přepínačích a směrovačích?
- Dokážete je při otevření boxu identifikovat?
- Jaká data a soubory v pamětech můžete nalézt?
- Jaké příkazy můžete použít na zjištění HW konfigurace zařízení?
- Popište, co se děje při zapnutí směrovače.

Typy pamětí

- Existuje mnoha řad Cisco směrovačů a přepínačů, ale všechny mají prakticky stejné typy pamětí.
- Flash, NVRAM, RAM, ROM
- Chceme-li vykonávat forenzní analýzu síťových prvků, patří precizní vědomosti o pamětech (obecně komponentách) zařízení, souborech mezi klíčové.

Flash paměť

- Energeticky nezávislá paměť. Velikost této paměti je různá od typu řady (základní řady mají omezení v rozšíření paměti).
- Primární účel je uložení operačního systému (IOS).IOSu může být na Flash paměti uloženo více. Do paměti lze i zapisovat.
- Během bootování se IOS kopíruje do paměti RAM.
- Dále obsahuje inforamce o VLANs v souboru vlan.dat.
- Výpis paměti pomocí #**show flash:/** nebo #**dir flash:/**.

Typy pamětí

Non-volative random access memory

- Energeticky nezávyslá paměť - neztrácí obsah po odpojení od zdroje energie.
- Slouží k uložení konfiguračního souboru (startup-config).
- Výpis paměti pomocí #**dir nvram:/**.

Random Access Memory

- Energeticky závyslá, rychlá paměť - po odpojení od zdroje energie ztrácí svůj obsah.
- Obshuje konfigurační soubor (running-config).
- Po startu zařízení se do RAM načte IOS.
- Mezi další obsah paměti patří: ARP Cache, routovací tabulky, Buffer zpracovávaných paketů.
- Výpis paměti pomocí #**show memory:/**.

Typy pamětí

Read Only Memory (ROM)

- Energeticky nezávislá paměť.
- Z ROM paměťi jsou spouštěny procesy jako POST, Bootstrap, ROM monitor (pro případ, že není načten IOS).

Externí síťová uložiště

- Pozor, nezapomeňte na fakt, že např. TFTP server nepoužíváme jen k zálohování a jako uložiště pro naše potencionální důkazy. TFTP server může být také použit k natažení IOS při startu směrovače. Tím lze mimochodem obejít situaci, kdy nemáte dostatečnou kapacitu Flash paměti.
- Pokud je IOS načítán z TFTP serveru, je nutné toto uložiště identifiovat a IOS zkopírovat při sběru stálých dat.

Rozdělení dat - Volative Data

„Nestálá data“ - Volative Data

- Nachází se v paměti typu RAM.
- Právě tento typ dat může významně dokreslit celý incident.
- Vzhledem k tomu, že tato data velmi rychle mění svou povahu (ARP cache, routovací tabulky, . . .), mělo by zkoumání začít právě sběrem těchto dat.
- Do této kategorie dat řadíme např. následující: running-config, routovací tabulky, ARP tabulka, informace o NAT překladech, statistiky rozhraní, ACLs matches, lokální logy, statistiky routovacích protokolů, stavy portů, informace o DHCP (binding), přihlášení uživatelé, tabulka MAC adres, historie zadaných příkazů, . . .
- Pozor, ve chvíli kdy odpojíte zařízení od energie, nebo provedete password recovery na směrovači či přepínači, nenávratně o tyto data příjdete.

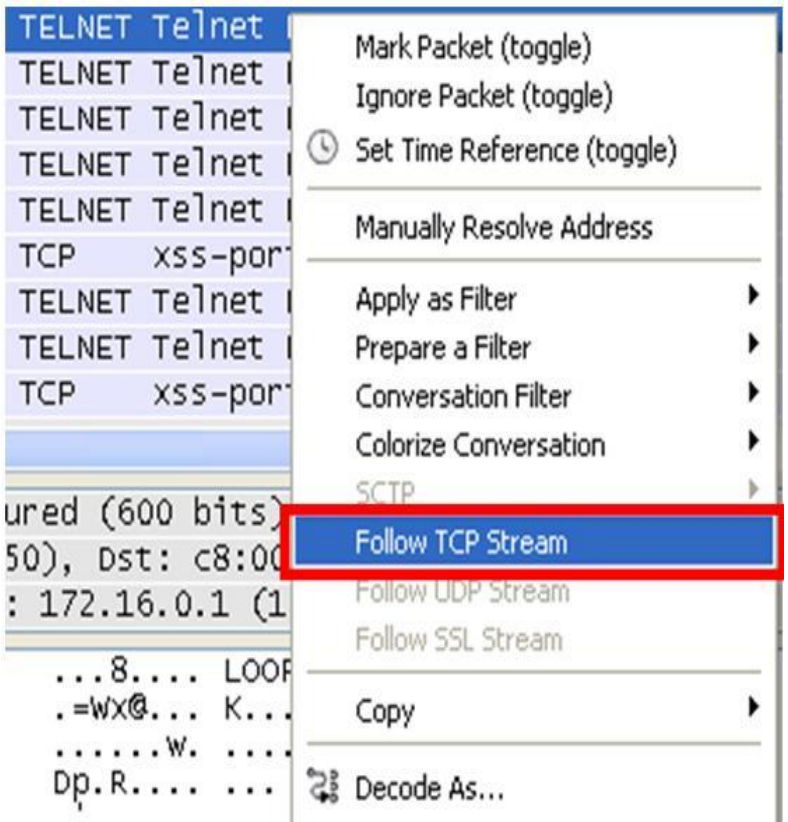
Rozdělení dat - Volative Data

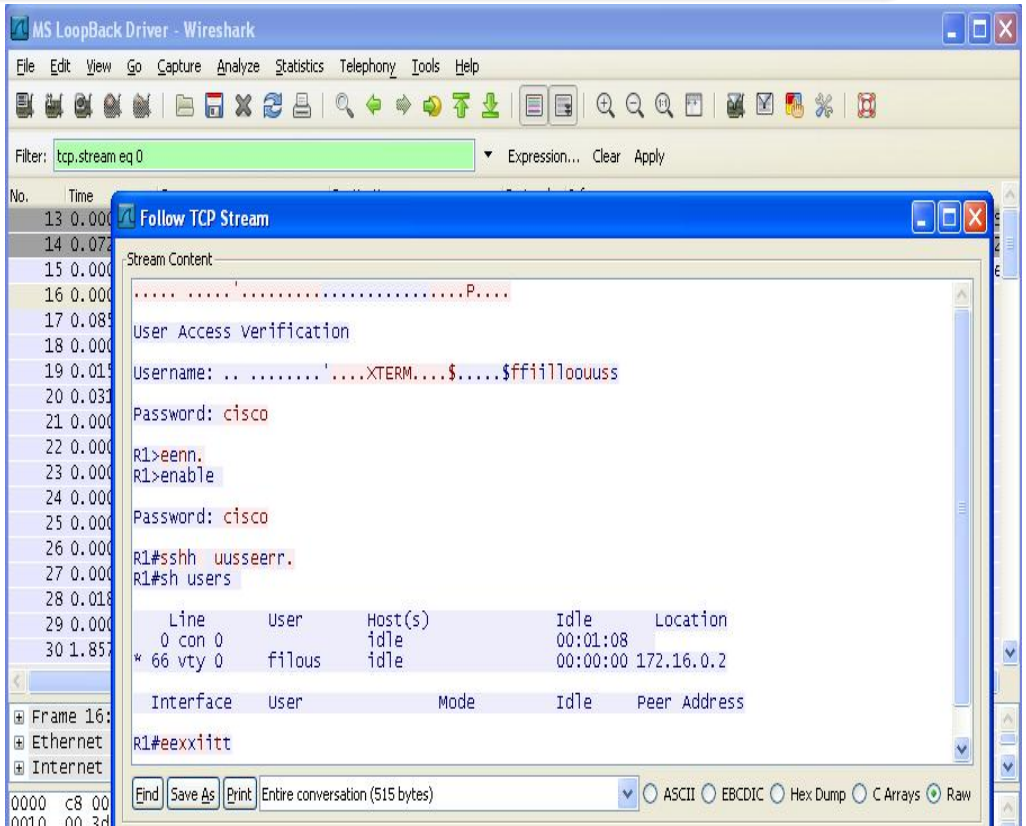
„Nestálá data“ hledejte i jinde

- Pokud incident stále probíhá, sběr nestálých dat se neomezuje pouze na směrovač nebo přepínač. Síťový traffic představuje také nestálá data.
- Aktivn prvek, jako směrovač mohl být pouze přestupním místem při útoku.
- Je-li zasaženo např. datové centrum a útok stále probíhá, potom nestálá data můžeme získat i ze sítě pomocí packet snifferu.
- Příklady packet snifferů: Wireshark, TcpDump, WinDump,. . .
- Seznámili jsme se s nimi již dříve v tomto kurzu.

Rozdělení dat - Volative Data

- Vezmeme-li v úvahu provozní režii packet snifferů, nabízí se použít TcpDump, jako textový packet sniffer k zachycení provozu a grafický sniffer Wireshark k pozdější analýze.
- Zachycený provoz můžeme uložit a použít jako důkazní materiál. Využijte při analýze vlastnost vidět celý stream.





Rozdělení dat - Non-volative Data

„Stálá data“ - Non-volative Data

- Nachází se v paměti typu NVRAM nebo Flash.
- Oproti předcházejícím nemění rychle svou povahu.
- Tento typ pamětí je energeticky nezávyslí, tedy po odpojení zařízení od energie se data nesmažou.
- Do této kategorie dat řadíme následující: IOS (může jich být i více), startup-config, vlan.dat, ...
- Mnoho informací zjistíme dále z výpisů.
- Pozor, v této kategorii dat se nachází mnoho souborů, ze kterých budeme chtít vytvořit kopii a uložit tyto kopie na TFTP server. Nezapomeňte vytvořit pomocí hashovací funkce kontrolní součet jak z originálu v paměti zařízení tak z kopie po přenesení na TFTP server. Aby byla zaručena integrita dat.

Závěrečné shrunutí metod zkoumaní

Dokumentovat, dokumentovat, dokumentovat

- Dokumentace je klíčová ve všech metodách zkoumání.

Veškerý pohyb a vykonané kroky při zkoumání zařízení musí být výborně zdokumentované. To platí pro všechny oblasti forenzní analýzy. Na základě dokumentace (např. všech použitých příkazů) lze v případě nutnosti vyvrátit, že konfigurace byla změněna až v průběhu zkoumaní.

- Zaznačte všechny příkazy a jejich výstupy.

Co lze použít k dokumentaci

- Poznámky „načmárané“ v rychlosti na papír nevypadájí příliš důvěryhodně a mohly by být u soudu napadeny.
- Textový dokument je lepší varianta než předchozí má však stále nedostatky. Forensic CaseNotes vnáší do dokumentace systém a zajišťuje i integritu našich poznámek.

Zkoumání potřebuje plán

- Fotoaparát (pozor na správné nastavení datum/čas), print screen monitoru (ALT+PrtSc - aktivní okno).

Kroky před zahájením zkoumání

- Nezapomeňte, před samotným zkoumáním je zapotřebí vše připravit a naplánovat.
- Spojit se s PoC a získat detailní informace o síti (konfigurace, topologie sítě, . . .),
- zjistit zdali existují zálohy běžících konfigurací, zjistit typ IOSu,
- přístupová hesla (VTY, Console, HTTPS, Enable) - zjistit, jaké přístupové metody jsou nakonfigurovány,
- porada s administračním týmem, zjistit včem je problém (jaká zařízení byla zasažena),
- určit postup a plán zkoumání, . . .

Lokální metoda

Lokální metoda

- Musíme mít fyzický přístup k zařízení.
- Propojení PC znalce přímo do console portu zařízení.
- Použijeme HyperTerminal k připojení. „Zachytávání textu“ spustíme ještě před přihlášením! Jako první příkaz vypíšeme čas/datum (tento příkaz několikrát v průběhů zkoumání zopakujeme).
- Upravíme TCL skript pro konkrétní situaci (např. IP addresa FTP serveru).
- Sběr dat pomocí skriptu.
- Výstupy spuštěných skriptů i kopie souborů posíláme na FTP (TFTP)server.
- Kontrolní součet (hash) vypočítame z originálů i z kopií.

Vzdálená metoda

Vzdálená metoda

- K zařízení, které je předmětem zkoumání není fyzický přístup.
- Ke vzdálenému přístupu vždy použít zabezpečených protokolů (SSH, HTTPS) (nikdy Telnet).
- K navázání spojení použijeme klienta Putty.
- Putty neumožňuje zachytávat text v průběhu zkoumání, proto je nutné tuto skutečnost řešit jiným způsobem.
- Upravíme TCL skript pro konkrétní situaci (např. změna IP addresy FTP serveru). Pokud tak neučiníte, zbytečně dojde po spuštění skriptu k výpisu mnoho chybových hlášení.
- Sběr dat pomocí skriptu.
- Výstupy spuštěných skriptů i kopie souborů posíláme na FTP (TFTP)server.
- Kontrolní součet vypočítame z originálů i z kopií.

Co dělat/nedělat při forenzní analýze

Okolnosti mohou určit mnohé. Nelze říci, že existuje jeden framework, který bude vždy, za všech situací bezvadně fungovat a my ho můžeme použít. Naopak, různé situace vyžadují individuální přístup, avšak nikdy nesmí dojít k poškození potencionálních důkazů.

Co dělat

- Pokud to lze, použit přímé připojení přes konzoly.
- K přihlášení použít HyperTerminal pro jeho funkci zachycení textu (aktivujte ještě před přihlášením).
- Použít raději FTP server než TFTP server.
- Vše dokumentovat (fotky, PrtSc, zápisky, časová osa zkoumání).
- Vždy ověřujte integritu dat při vytváření kopií (MD5, SHA-1, SHA-2).

Co dělat/nedělat při forenzní analýze

- Zaznamenat reálný čas a čas nastavený v zařízení.
- Na sběr dat z výpisů #**show** použít raději skripty.

Čemu se vyvarovat

- Nikdy se nepřihlašovat vzdáleně pomocí protokolu Telnet.
- Nikdy neměnit stávající konfiguraci.
- Nikdy nerestartujte zařízení. Příjdete o nestálá data.
- Nikdy neukládejte běžící konfiguraci do startup-config.
- Nezapomenout dokumentovat průběh zkoumaní.

Simulace a trénink

- Veškerá praktická řešení budou realizována na reálném řešení společnosti Cisco na cvičeních. Dále můžete využít konzultačních hodin nebo případně kdykoli po předchozí domluvě. Iniciativě se meze nekladou. :-)
- Pokud náhodou nemáte Cisco laboratoř doma :-) nabízí se v domácím prostředí využít služeb simulátoru GNS3 (pouze směrovače).

Graphical Network Simulator

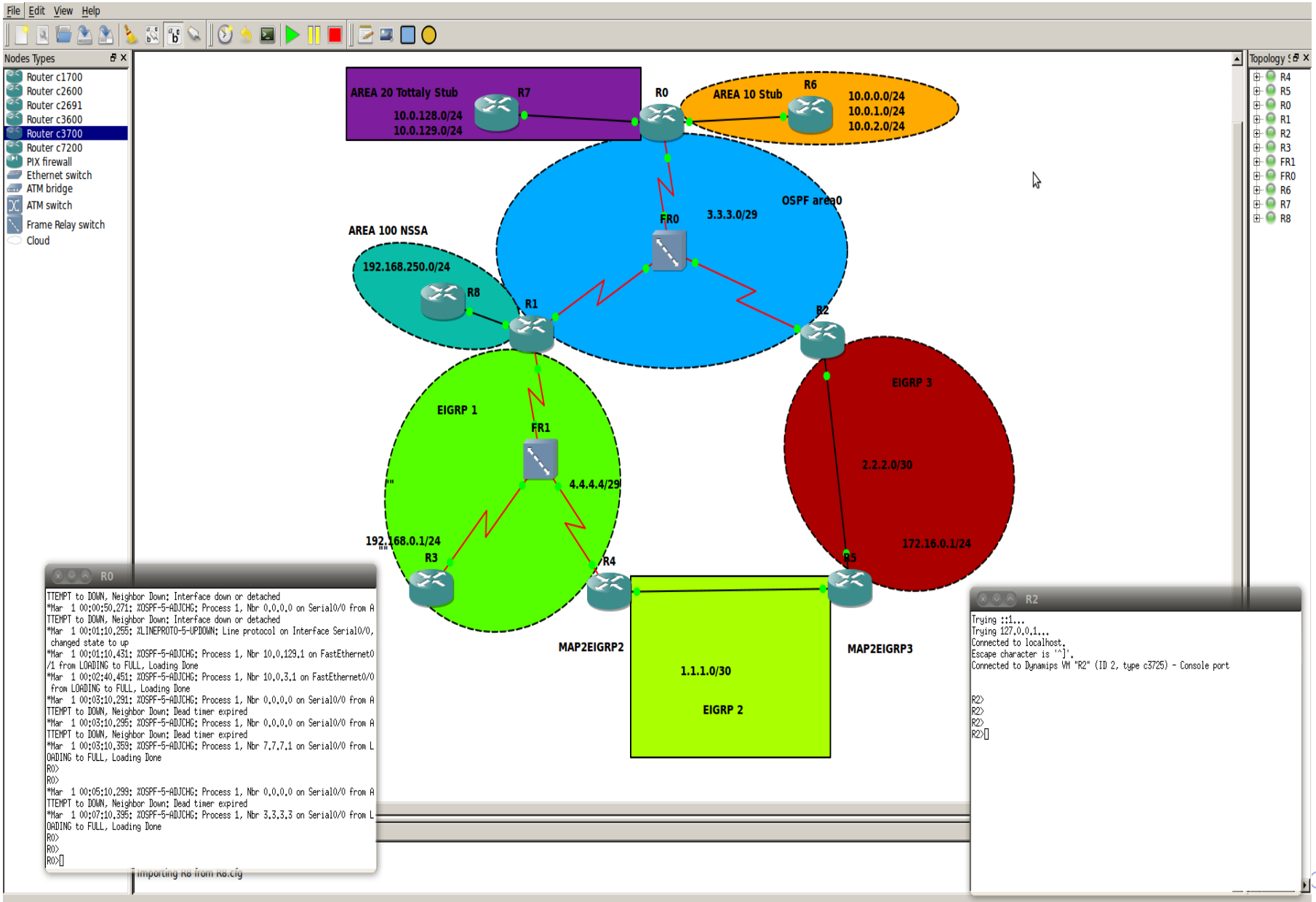
- Simuluje reálná zařízení Cisco (možnost i Juniper).
- Není omezen vlastnostmi - závysí pouze na IOSu, který nahrajete.
- Odkaz na oficiální stránky: http://www.gns3.net/.

Simulace a trénink

Graphical Network Simulator

- Umožňuje do simulátoru připojit i reálné zařízení, díky čemuž lze simulovat sítě kolosálních rozměrů (uvést příklad).
- Po vytvoření virtuálního rozhraní a propojení směrovače s Vašim PC můžete využívat všechny aplikace (Wireshark, Cain, Tftpd32 server, Putty, Vaše TCL skripty, . . .)
- Návod jak vytvořit a propojit virtální síťovku Vašeho PC se směrovačem najdete v mnou připraveném videu (v moodlu).
- Mnoho videí o nastavení a práci v GNS3 najdete najdete na oficiálních stránkách (viz. výše) nebo na youtube.com.
- Víte z jakých důvodů neexistují simulátory přepínačů na způsob GN3?

Ukázka příkladu ze simulátoru GNS3



Děkuji za pozornost!