

Počítačová síť a Internet

seznam možných otázek k zápočtu

Poslední aktualizace: 23. května 2024

Co lze používat při písemce: počítač se softwarovými prostředky, které jsou standardní součástí běžné instalace operačního systému (příkazový řádek/terminál, nápověda, dialogová okna nástrojů operačního systému), dále Wireshark a Packet Tracer (můžete si vybrat mezi použitím Packet Traceru a reálných zařízení).

Je zakázáno používat jakékoliv dokumenty vlastní či cizí výroby, které nejsou součástí standardní nápovědy systému či některého ze zmiňovaných nástrojů, zákaz se vztahuje i na skripta. Můžete používat své vlastní poznámky (ručně napsané na papíru či v sešitě).

V části o aplikačních protokolech je povoleno na chvíli spustit webový prohlížeč s konkrétní adresou pro účely vygenerování provozu, hned po vygenerování webový prohlížeč ukončete.

Pokud je cílem otázky napsání příkazu v textovém režimu nebo vypsání určitého postupu v grafickém rozhraní, pak si můžete zvolit, ve kterém operačním systému budete postupovat – Windows nebo Linux. Na papír s písemkou *napište dotyčný příkaz, ne jeho výstup*.

Po dokončení písemky bude výsledek konfigurace zkontrolován vyučujícím, AŽ POTOM vyčistíte zařízení/uzavřete soubor apod.

Jestliže je v následujícím seznamu k otázce dopsána poznámka, berte na vědomí, že na písemce se tato poznámka nacházet nebude.

1 Počítačová síť na hostitelském zařízení

1. Napište příkazy, které nejdříve deaktivují síťovou kartu a následně ji aktivují.
2. Kterým příkazem v textovém režimu zjistíte název zařízení, na kterém právě pracujete?
3. Jak zjistíte svou MAC adresu (příkazem v textovém režimu)?
4. Zjistěte, zda je následující MAC adresa lokální či globální a zda je individuální či skupinová.

Pozn.: Znamená to, že potřebujete zjistit, jestli jsou nastaveny bity L/G a I/G.

5. Kterým příkazem zjistíte své IP adresy?
6. Následující IPv6 adresu převedte do kanonického tvaru (tj. proveďte krácení):

...

7. Napište postup, jak se v grafickém režimu dostanete k oknu, ve kterém lze nastavit IP adresu a další související údaje.

2 Standardy

1. Najděte na internetu standard RFC ... a v dokumentu zjistěte tyto informace:

...

(Pozn.: typicky půjde o název dokumentu, zda není nahrazen jiným dokumentem, tedy obsolete, kdy byl publikován, na které straně je probíráno určité téma – v tom případě použijte obsah, atd.)

2. Jaké číslo má RFC standardizující ...?

(Pozn.: můžete použít webový prohlížeč včetně vyhledávače)

3 Lokální síť - Ethernet

1. Když propojujete dva switche, má se správně použít přímý nebo křížený kabel?
2. Když propojujete PC a switch, má se správně použít přímý nebo křížený kabel?
3. Když propojujete router a switch, má se správně použít přímý nebo křížený kabel?
4. Když propojujete dva routery, má se správně použít přímý nebo křížený kabel?

4+7 Packet Tracer a konfigurace, Pokračujeme v konfiguraci

1. Součástí písemky bude vytvoření zadné sítě v Packet Traceru a její základní konfigurace:

- název zařízení, nasazení hesel na konzoli, linkách, do enabled módu, vytvoření uživatele, autentizace buď heslem nebo k lokální databázi (uživatel), hashování hesel, banner, synchronizace logování
- IP adresy (router: na rozhraních, switch: na virtuálním rozhraní), na switchi brána, na routeru taky IPv6 adresy
- směrovací tabulka, statické směrování
- konfigurace VLAN včetně směrování mezi VLAN sítěmi
- zprovoznění SSH, nastavení minimální délky hesla, automatické odhlášení po určité době nečinnosti (toto vše je ke konci kapitoly 7)
- show příkazy

5 Číselné soustavy

1. Převed'te číslo v binární soustavě ... do desítkové soustavy.
2. Převed'te číslo v desítkové soustavě ... do binární soustavy.
3. Převed'te číslo v šestnáctkové soustavě ... do binární soustavy.
4. Převed'te číslo v binární soustavě ... do šestnáctkové soustavy.
5. Převed'te číslo v šestnáctkové soustavě ... do desítkové soustavy (přes binární).

6. Převed'te číslo v desítkové soustavě ... do šestnáctkové soustavy (přes binární).

6 Co se děje na síťové a transportní vrstvě

1. Napište příkaz, kterým zjistíte svou IP adresu, masku podsítě a adresu brány.
2. Ve Wiresharku chvilku chyťte provoz na síti (v případě potřeby vygenerujte provoz zadáním příkazu `ping www.google.com` do příkazového řádku/terminálu). Najděte některý IP paket a vypište verzi protokolu IP a dále typy polí v jeho záhlaví. Vypište obsah pole určujícího typ zapouzdřeného obsahu (číselně i slovně).
3. Spusťte ve Wiresharku zachytávání paketů a hned poté pošlete ping na `www.google.com`. Najděte některý ICMP paket a vypište typy polí v jeho záhlaví i jejich hodnoty.
4. Napište příkaz, kterým zjistíte, zda je server `www.slu.cz` dosažitelný.
5. Napište příkaz, kterým otestujete funkčnost loopbacku na své síťové kartě.
6. Napište příkaz, kterým zjistíte cestu (routery na cestě) k serveru `www.slu.cz`.
7. Jaký řetězec napíšete do display filtru (filtru zobrazení) ve Wiresharku, pokud chcete zobrazit pouze ... (např. provoz týkající se zařízení s IP adresou `xxxx`, čísla portu `xxxx`, TCP segmenty s nastaveným příznakem SYN)?
8. Jak ve Wiresharku dostanete okno, ve kterém je souhrnně celá komunikace – obsah TCP paketů v konverzaci?
(Pozn.: tím je míněn *TCP flow*, tedy *Analyze-Follow-TCP stream*)
9. Jak ve Wiresharku vytáhnete z provozu přenášené soubory?
(Pozn.: tam se dostanete přes *File – Export objects...*, je to i na screenshotu)

8 Aplikační protokoly

1. Napište příkaz, kterým zjistíte IP adresy serveru `www.slu.cz`.
2. Napište příkaz, kterým zjistíte jmennou adresu (kanonické jméno) serveru s IP adresou `193.84.206.76`.
Pozn.: Nezapomeňte, jaký formát má příkaz `nslookup` – na prvním řádku výstupu („Server“ je jmenná adresa DNS serveru, který provádí překlad, až dále zjistíme kanonické jméno).
3. Spusťte ve Wiresharku zachytávání paketů a hned poté ve webovém prohlížeči (spuštěném na krátkou dobu pouze pro tento účel) zadejte adresu `www.google.com`, po zobrazení stránky webový prohlížeč ukončete. Najděte DNS paket s *dotazem* a vypište:
 - typy polí v jeho záhlaví,
 - který příznak je nastaven na 1,
 - u dotazované adresy typ a třídu adresy,
 - do čeho je tento DNS paket zapouzdřen (protokol).

4. Spusťte ve Wiresharku zachytávání paketů a hned poté ve webovém prohlížeči (spuštěném na krátkou dobu pouze pro tento účel) zadejte adresu `www.google.com`, po zobrazení stránky webový prohlížeč ukončete. Najděte tři TCP segmenty navazující spojení a vypište pro každý z nich:

- které příznaky jsou nastaveny,
- čísla portů pro zdroj a cíl,
- šířku okna pro potvrzování.

Pozn.: Je možné, že se vám tam bude „motat“ i jiný provoz a že TCP segmenty pro three-way handshake se budou hledat těžko. Doporučuji použít filtr.

5. Spusťte ve Wiresharku zachytávání paketů a hned poté ve webovém prohlížeči (spuštěném na krátkou dobu pouze pro tento účel) zadejte adresu `http://packetlife.net/`, po zobrazení stránky webový prohlížeč ukončete. Najděte některou HTTP zprávu *pro dotaz na server* a vypište:

- typ HTTP zprávy,
- do čeho je HTTP zpráva zapouzdřena (protokol na vrstvě L4) a čísla portů.

6. Napište příkaz, který vypíše plnou statistiku pro všechny protokoly a přidá i sloupeček s označením komunikujících procesů.

Pozn.: případně jiná varianta příkazu `nslookup`, a pozor na to, ve kterém jste zrovna operačním systému. Můžete použít nápovědu.

9 Internetworking a průzkum paketů

1. Napište příkaz, který vypíše tabulku sousedů platnou pro IPv4/IPv6.
2. Součástí písemky bude příklad na subnetting (dostanete zadanou adresu a údaje pro podsítě).
3. Napište příkaz, který vypíše směrovací tabulku pro vaše zařízení.

Co určitě bude na písemce:

- konfigurace viz výše,
- subnetting,
- něco dalšího (Wireshark, příkazy...).