UNIVERZITA PARDUBICE

FAKULTA FILOZOFICKÁ

ZÁVĚREČNÁ PRÁCE

2023 Zdeněk Drvota

Univerzita Pardubice

Fakulta filozofická

Návrh učebního textu pro předmět Počítačové sítě na střední odborné škole

Závěrečná práce

2023 Zdeněk Drvota

Univerzita Pardubice
Fakulta filozofická

ZADÁNÍ
tématu závěrečné písemné práce doplňujícího pedagogického studia

Jméno a příjmení studenta: …… Zdeněk Drvota ……
titul: …Ing…… název absolvované VŠ: VŠCHT Pardubice……
rok ukončení VŠ…1988….. rok zahájení DPS: ……2021……

Práce je svým obsahem zaměřena převážně do oblasti: **psychologie, pedagogika, obecná didaktika, oborová didaktika, metodologie, sociologie**. (podtrhni)

Téma práce:
Návrh učebního textu pro předmět Počítačové sítě na střední odborné škole

Obsah práce:
Cílem práce je připravit vybranou kapitolu učebního textu pro výuku předmětu Počítačové sítě na střední odborné škole se zaměřením na informatiku. Výsledný text bude použitelný jako doplňující materiál v českém jazyce k originálním textům kurzu Cisco Netacad, které jsou obvykle používány ve výuce v anglické verzi.

Základní literatura dle ISO 690:

1) SKALKOVÁ, Jarmila. *Obecná didaktika-2., rozšířené a aktualizované vydání.* Grada Publishing as, 2007.
2) FOJTÍK, Rostislav. Didaktika informatiky II. *Ostrava: Ostravská univerzita*, 2005.
3) *CCNA: Introduction to Networks* [online]. San Jose, Kalifornie, USA: Cisco Networking Academy, 2021 [cit. 2022-05-15]. Dostupné z: https://www.netacad.com/courses/networking/ccna-introduction-networks

Termín odevzdání práce: ……15.4.2023……

Vedoucí práce: PhDr. Mgr. Ilona Ďatko, Ph.D. Podpis vedoucího ……

Prohlašuji, že jsem se seznámil(a) se zásadami pro vypracování závěrečné písemné práce v rámci DPS.

v Pardubicích dne:..4.7.2022 .. **Podpis studující(ho):**.

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 8.6.2023

Zdeněk Drvota

PODĚKOVÁNÍ

Autor děkuje akademickým pracovníkům Katedry věd o výchově za všechny poskytnuté informace, potřebné k vytvoření této práce, a svým zaměstnavatelům za umožnění účasti na výuce DPS a poskytnutí prostoru pro provedení výzkumu mezi žáky a studenty.

ANOTACE

Práce je věnována přípravě učebního textu v českém jazyce pro výuku počítačových sítí s podporou kurzů Cisco NetAcad, které jsou používány běžně v českých středních a vysokých školách s originálními texty a materiály v anglickém jazyce. Práce obsahuje připravený český učební text a také výsledky kvantitativního výzkumu dotazníku k používání učebních textů.

KLÍČOVÁ SLOVA

učební text, cisco, netacad, počítačové sítě, výuka

TITLE

Design of a teaching text for the Computer Networks subject at a secondary vocational school

ANNOTATION

The work is dedicated to the preparation of a teaching text in the Czech language for teaching computer networks with the support of Cisco NetAcad courses, which are commonly used in Czech high schools and universities with original texts and materials in the English language. The thesis contains a prepared Czech textbook as well as the results of a quantitative research, questionnaire on the use of textbooks.

KEYWORDS

textbook, cisco, netacad, computer networks, teaching

OBSAH

SEZNAM ZKRATEK A ZNAČEK

AJ – anglický jazyk

CCNA1 – Cisco Certified Network Associate 1 Introduction to Networks, první z kurzů počítačových sítí

Cisco – Cisco Systems, Inc. San Francisco, California, United States

ČJ – český jazyk

DELTA – DELTA – Střední škola informatiky a ekonomie, s.r.o.

DFJP – Dopravní fakulta Jana Pernera

ISBN –International Standard Book Number

IT – informační technologie

KH – kritická hodnota

NetAcad – Cisco Networking Academy

QR – „Quick Response" prostředek pro automatizovaný sběr dat

TK – testovací kritérium

UPCE – Univerzita Pardubice

0 Úvod

Svět digitálních, počítačových sítí hraje klíčovou roli v dnešní době. S rozšiřováním a neustálým vývojem sítí se zvyšuje poptávka po kvalifikovaných síťových inženýrech.

0.1 Cisco Networking Academy

Společnost Cisco Systems, při vědomí těchto potřeb, představila Cisco Networking Academy (NetAcad) komplexní vzdělávací program s cílem vybavit jednotlivce znalostmi a dovednostmi potřebnými pro úspěch v oblasti sítí. Program, který byl zahájen v říjnu 1997, začal v 64 vzdělávacích institucích v sedmi amerických státech Arizona, Kalifornie, Florida, Minnesota, Missouri, New York a Severní Karolína.[1]

Cisco Networking Academy nabízí strukturovaný vzdělávací program zahrnující různé kurzy, které pokrývají širokou škálu síťových témat. Program využívá kombinaci online modulů s vlastním tempem studia a praktických laboratorních cvičení, aby studentům poskytl komplexní učební zkušenost. Obsah kurzu je pravidelně aktualizován tak, aby odpovídal aktuálním trendům a technologickým pokrokům, což zajišťuje, že studenti získají relevantní a moderní znalosti.

Cisco Networking Academy využívá učební přístup zaměřený na studenta, který klade důraz na aktivní zapojení a praktické aplikace konceptů. Studenti mají přístup k virtuálním prostředím, kde mohou simulovat reálné síťové scénáře a uplatnit své teoretické znalosti v bezpečném prostředí. Tato praxe posiluje jejich schopnosti řešit problémy a kriticky myslet, připravuje je na skutečné výzvy, které je čekají v reálném světě.

Cisco Networking Academy měl významný dopad na studenty a společnost jako celek. Díky poskytování přístupného a kvalitního vzdělání v oblasti sítí program překonává digitální propast a umožňuje jednotlivcům z různých sociálních a ekonomických prostředí získat cenné dovednosti. Navíc program aktivně podporuje inkluzivitu tím, že vytváří prostředí, které vítá různorodost a přijímá studenty ze všech sfér života.

Jedním významným aspektem Cisco Networking Academy je podpora genderové rozmanitosti v oblasti sítí. Program podporuje a vede ženy k tomu, aby se věnovaly kariéře v síťových technologiích. Skrze iniciativy, jako jsou mentorské programy, soutěže a stipendia, akademie se snaží vytvořit vyváženější a inkluzivnější pracovní sílu.

Vzhledem k neustálému vývoji sítí zůstává důležitou rolí programu Cisco Networking Academy vytvářet talentovanou a rozmanitou pracovní sílu, která pohání technologické inovace a splňuje potřeby průmyslu.

Cisco Networking Academy (NetAcad) má v České republice významnou přítomnost a aktivně působí v oblasti vzdělávání v síťových technologiích. NetAcad spolupracuje s řadou vzdělávacích institucí, jako jsou vysoké školy, střední školy a odborná učiliště, aby poskytovala kvalitní vzdělání a certifikace v oblasti sítí.

Jako součást programu NetAcad jsou v České republice nabízeny různé kurzy a certifikace, které pokrývají širokou škálu síťových technologií a dovedností. Tyto kurzy se zaměřují na různé úrovně, od základních až po pokročilé, a umožňují studentům získat praktické znalosti a dovednosti, které jsou nezbytné pro úspěšnou kariéru v oblasti sítí.

NetAcad díky kombinaci několika složek, které jako celek tvoří systém podpory studia, efektivně nahrazují nebo alespoň doplňují klasickou formu vzdělávání:

- online studium a přístup k multimediálnímu studijnímu materiálu (kurikulu) přes portál na internetu (24x7)
- systém průběžného testování znalostí pro podporu procesu vyhodnocení úspěšnosti osvojování obsahu, režim zpřístupnění testů je řízen lektorem a studentům je umožněn přístup v daném čase prostřednictvím internetu
- praktické cvičení v laboratoři na reálných zařízeních simulujících provoz v sítích s cílem získat praktické zkušenosti s konfigurací, instalací, údržbou síťových prvků a také návrhem designu pro síťová řešení
- individuální nebo skupinové konzultace v průběhu studia s cílem vytvořit prostor pro vyhodnocování úspěšnosti studia
- závěrečný test, který představuje souhrnné ověření znalostí problematiky, úspěšně ukončené studium je možné rozšířit o celosvětově akceptované certifikační zkoušky společnosti Cisco Systems

NetAcad vytváří partnerství s institucemi vzdělávání, vládními organizacemi a průmyslovými partnery v České republice s cílem podporovat technické vzdělávání a rozvoj síťových profesionálů. Díky těmto partnerstvím mohou studenti mít přístup ke špičkovým zařízením, laboratořím a dalším prostředkům potřebným pro praktickou výuku.[1]

Autor této závěrečné práce je certifikovaným lektorem NetAcad již patnáct let.

Ministerstvo školství, mládeže a tělovýchovy České republiky se obecně snaží podporovat inovativní a kvalitní vzdělávací programy, které přispívají k rozvoji dovedností studentů a odpovídají potřebám trhu práce. NetAcad je ministerstvem dlouhodobě uznávanou a respektovanou vzdělávací platformou v oblasti sítí, která přispívá k rozvoji technického vzdělávání a přípravě síťových profesionálů, což je podloženo i smluvně.[2]

Ačkoliv se většina kurzů NetAcad poskytuje ve více jazykových mutacích, český jazyk mezi ně bohužel nepatří. Používá se při výuce počítačových sítí na středních odborných školách, i na školách vysokých, v bakalářských i magisterských oborech, zaměřených na informatiku. Na školách, kde jako lektor NetAcad autor práce aktivně působí (DELTA, UPCE), ale i v dalších českých školách, ze kterých má informace, se používají zpravidla anglické verze. Pro žáky a studenty jazykově méně schopné to může být jistou bariérou ve studiu kurzů.

0.2 Didaktika učebních textů z oboru informatiky

Účinné vzdělávání nejen v oblasti informatiky vyžaduje správně strukturované a didakticky připravené učební texty.

Didaktika je disciplína, která se zabývá výzkumem a aplikací principů a metod, které usnadňují proces výuky a učení. V oblasti informatiky, a zejména počítačových sítí, má didaktika klíčový význam při tvorbě učebních materiálů, které mají za cíl předat studentům složité koncepty a dovednosti.[4][5]

Didaktika v informatice je nezbytná pro efektivní přenos znalostí a porozumění konceptům počítačových sítí. Dobře strukturované a didakticky připravené učební texty mohou studentům usnadnit pochopení složitých principů a procesů v oblasti počítačových sítí.[6]

Efektivní učební texty v oblasti počítačových sítí by měly mít jasnou a logickou strukturu. Kapitoly by měly být rozděleny podle tematických okruhů, které postupně představují klíčové koncepty a postupy. Důležitou součástí struktury je také vhodné zařazení příkladů, ilustrací a případových studií, které studentům pomáhají aplikovat teoretické znalosti na reálné situace.

Skládání učebních materiálů by mělo respektovat principy konstruktivistického přístupu k vzdělávání Studenti by měli být aktivně zapojeni do procesu učení a měli by mít možnost aplikovat své znalosti prostřednictvím interaktivních úkolů a praktických příkladů.[7]

Učební texty by měly být napsány srozumitelným jazykem, který minimalizuje používání složitých technických termínů a odborných výrazů, které by mohly způsobit nedorozumění. Používání jednoduchého a přístupného jazyka umožňuje studentům snadno porozumět

a pojmout obsah textu. Je také důležité dbát na strukturovanost vět a odstavců, aby se zajišťovala čitelnost a snadná orientace v textu.

Srozumitelnost jazyka je klíčová pro efektivní učení. Učební texty by měly být napsány tak, aby studenti s různými úrovněmi znalostí a dovedností mohli snadno porozumět obsahu. Důležité je také vysvětlovat nové termíny a koncepty a poskytovat dostatek příkladů a ilustrací k jejich ilustraci.[8]

Interaktivita je klíčovým prvkem v didaktice počítačových sítí. Učební texty by měly obsahovat interaktivní prvky, které motivují studenty k aktivnímu zapojení a aplikaci naučených poznatků. Toho lze dosáhnout prostřednictvím různých metod, jako jsou otázky a odpovědi, cvičení, simulace a laboratorní experimenty.

Klíčovým faktorem je rovněž interaktivita při učení počítačových sítí. Interaktivní prvky umožňují studentům praktickou aplikaci teoretických znalostí a jejich ověření v praxi. Mohou zahrnovat simulace konfigurace sítě, řešení praktických scénářů nebo laboratorních úkolů, které studentům umožňují experimentovat s reálnými situacemi a provádět konkrétní kroky.

Vizuální prvky jsou důležitou součástí didaktiky učebních textů z oboru počítačových sítí. Schémata, diagramy, grafy, animace a videa pomáhají studentům vizualizovat a lépe porozumět složitým konceptům a strukturám sítí. Vizuální prvky mohou být doplněny vysvětlujícím textem a komentáři, aby studenti měli kompletní a srozumitelný obraz dané problematiky.

Využití vizuálních prvků je důležité pro efektivní přenos informací a porozumění. Vizuální prvky mohou zahrnovat topologie sítě, síťové diagramy, tok dat, příklady konfigurace zařízení a další. Správné použití vizuálních prvků může zlepšit vizuální reprezentaci a zapamatování si složitých konceptů počítačových sítí.

Učební texty by měly obsahovat také praktické příklady, které umožňují studentům aplikovat naučené poznatky na konkrétní situace. Tyto příklady by měly být relevantní a relevantní pro současné trendy v oblasti počítačových sítí. Studenti by měli mít příležitost řešit problémy, řešit scénáře a provádět praktické úkoly, které je připraví na reálné výzvy, se kterými se mohou setkat ve svém profesním životě.

Při tvorbě učebních textů je důležité sledovat aktuální vývoj v oblasti počítačových sítí. Technologie a protokoly se neustále vyvíjejí, a proto je důležité, aby učební materiály reflektovaly tyto nové trendy. Toto je zvláště důležité v oblasti počítačových sítí, která je dynamická a rychle se vyvíjející.

0.3 Dostupnost učebních textů v českém jazyce

Jako další zdroj informací vedle NetAcad v cizích jazycích je k dispozici v českém jazyce např. doporučovaná tištěná kniha ODOM, Wendell. Počítačové sítě bez předchozích znalostí [9], nebo PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z [10] v různých vydáních, bohužel jich však není vždy dostatek pro všechny zájemce.

Dále lze využívat doporučované volně přístupné online materiály, soubor přednášek a článků EArchiv.cz: Archiv článků a přednášek Jiřího Peterky, postupně aktualizovaný.

0.4 Důvody pro sestavení učebních textů v českém jazyce

Kromě výše uvedené horší dostupnosti tištěných knih platí i pro uvedené online zdroje vážnější námitka, že struktura těchto textů neodpovídá materiálům a rozložení kapitol v NetAcad, často obsahuje informace v danou chvíli nadbytečné, zbytečně detailní, nebo více technicky zaměřené, nebo naopak příliš populárně podané, než by bylo vhodné. Pro žáky a studenty může být obtížnější se ve velkém objemu informací orientovat a vybrat si v danou chvíli to relevantní.

Texty v anglickém jazyce zvládá mladší generace žáků, studentů již obvykle snadněji, nemusí se ale stejně dobře orientovat v odborných termínech, u starších studentů, zejména kombinovaného studia je obvykle průměrná úroveň znalosti angličtiny nižší, a problémy s porozuměním odborného anglického textu tedy větší. Může to znamenat pomalejší postup při studiu materiálů kurzu. Zapnutí online překladu na stránkách kurzu NetAcad nemusí přinášet kýžený efekt, často překlad nefunguje správně, protože se nepoužívá vždy čistý text, ale i texty, popisky ve schématech nebo obrázcích. Problematický je zpravidla i automatický překlad kvízů a testů, stává se často, že smysl otázek a odpovědí se posune významově k nepoužitelnosti. A nakonec automatickým překladem se občas znefunkční některé části kurzu, ovládání uživatelského rozhraní nepracuje správně.

To vše tedy vede k potřebě mít k dispozici české učební texty, které by strukturou v ideálním případě odpovídali rozvržení kapitol a částí studijním textům anglickým v NetAcad. Zároveň aby i v tištěné verzi byla k dispozici alespoň částečná interaktivita, jako je v originální online verzi.

1 Provedení průzkumu – dotazníkové šetření

V rámci přípravy ne tvorbu učebních textů bylo provedeno dotazníkové šetření, kvantitativní výzkum, s cílem zjistit míru používání e-learningových nástrojů Cisco Netacad a jiných studijních materiálů při výuce počítačových sítí v anglickém (AJ) nebo českém jazyce (ČJ) v závislosti na schopnosti komunikace v AJ, a na odborných znalostech (studijním oboru).

1.1 Formulace hypotéz

1.1.1 Hypotéza 1:

Studenti IT oboru/zaměření považují Netacad kurz za snadnější než studenti jiných oborů

H01: Hodnocení obtížnosti kurzu je stejné v různých studijních oborech

HA1: Hodnocení obtížnosti kurzu se liší v různých studijních oborech

1.1.2 Hypotéza 2:

Studenti s menšími předchozími odbornými znalostmi počítačových sítí (IT) používají e-learningové materiály více

H01: Používání e-learningových materiálů je stejné bez ohledu na předchozí odborné znalosti

HA1: Používání e-learningových materiálů se liší podle předchozích odborných znalostí

1.1.3 Hypotéza 3:

Studenti s menšími jazykovými znalostmi AJ používají doplňkové materiály v českém jazyce více

H01: Používání doplňkových materiálů v českém jazyce je stejné bez ohledu na předchozí jazykové znalosti

HA1: Používání doplňkových materiálů v českém jazyce se liší vzhledem k předchozím jazykovým znalostem

1.2 Popis metodologie výzkumu

Výzkumný soubor tvořili žáci druhého, třetího a čtvrtého ročníku střední odborné školy (DELTA - Střední škola informatiky a ekonomie, s.r.o.), a studenti volitelného předmětu Počítačové sítě denního a kombinovaného studia DFJP Univerzity Pardubice, ve kterých jsou používány kurzy Cisco Netacad. Dotazník předán formou odkazu na elektronickou formu. Z oslovených bylo získáno 90 vyplněných dotazníků od respondentů.

Ve výzkumu byla použita metoda kvantitativního dotazníkového šetření. Bylo využito otázek uzavřených, otevřených, a metody škálování.

Dotazník vlastní byl rozeslán v online formě, a to odkazem do skupin žáků a studentů v emailu, nebo prostřednictvím Cisco Netacad. Dotazník byl vytvořen na platformě Google Forms. Účast byla dobrovolná a dotazník byl zaslán pouze účastníkům kurzů Cisco Netacad.

Zde jsou uvedeny jen základní shrnuté informace a výsledky, kompletní zpráva s daty, výpočty, tabulkami a grafy je uvedena jako Příloha B.

1.2.1 Výsledky výzkumu

Pro výzkum bylo získáno 90 odpovědí, z toho od 7 od studentů vysoké školy a 83 od žáků střední školy, odpovědi slovní, číselné, škálované. Pro výzkumný problém a ověření tří hypotéz v této práci byly zpracovány slovní a škálované odpovědi, s absolutní četností. Pro statistické ověření byl zvolen chí-kvadrát test, který se používá ke zjištění, zdali mezi diskrétními kvantitativními veličinami existuje prokazatelně výrazný vztah. Odpovědi a grafy byly zpracovány pomocí programu Microsoft Excel.

1.2.1.1 Hypotéza 1 výsledky:

$\alpha = 0,05$ (hladina významnosti)

TK = 0,412828035 (testové kritérium)

KH = 5,991464547 (kritická hodnota

p-hodnota= 0,813496205

Testovací kritérium není větší než kritická hodnota, H_{01} se nezamítá

Závěr: Hodnocení obtížnosti kurzu je stejné v různých studijních oborech

1.2.1.2 Hypotéza 2 výsledky:

$\alpha = 0,05$ (hladina významnosti)

TK = 7,568041736 (testové kritérium)

KH = 9,487729037 (kritická hodnota

p-hodnota= 0,057199145

Testovací kritérium není větší než kritická hodnota, H01 se nezamítá

Závěr: Používání e-learningových materiálů v AJ je stejné bez ohledu na předchozí odborné znalosti

1.2.1.3 Hypotéza 3 výsledky:

$\alpha = 0,05$ (hladina významnosti)

TK = 29,04456399 (testové kritérium)

KH = 24,99579014 (kritická hodnota

p-hodnota= 0,057199145

Testovací kritérium je větší než kritická hodnota, H01 se zamítá

Závěr: Používání doplňkových materiálů v českém jazyce se liší vzhledem k předchozím jazykovým znalostem (Peterka)

Korelace mezi znalostmi AJ a používáním materiálů (Peterka) je však zanedbatelná, nelze vysledovat žádný trend. Podobně je to i u ostatních materiálů.

1.2.2 Interpretace dat z výzkumu

U hypotézy 1 se předpokládalo, že hodnocení obtížnosti kurzů bude rozdílné, a obtížnější bude pro účastníky s menšími odbornými znalostmi, pro obory jiného než IT zaměření.

Statisticky se však potvrdilo, že pro všechny obory nebo studijní zaměření se jeví obtížnost studia kurzů Cisco Netacad jako stejná.

U hypotézy 2 se předpokládalo, že účastníci kurzů s menšími předchozími odbornými znalostmi počítačových sítí (IT) používají základní e-learningové materiály v AJ více

Statisticky se však potvrdilo, že Cisco Netacad materiály používají bez ohledu na úroveň odborných znalostí stejnou mírou.

U hypotézy 3 se předpokládalo, že účastníci kurzů s menšími jazykovými znalostmi AJ používají doplňkové materiály v českém jazyce více.

Statisticky se však potvrdilo, že sice není na stanovené hladině významnosti míra používání materiálů v ČJ stejná pro různé znalosti AJ, nicméně korelace je prakticky zanedbatelné hodnoty.

1.3 Závěry z výzkumu

Dodatečnými rozhovory s účastníky výzkumu bylo zjištěno, že hlavními důvody nízkého používání učebních materiálů v českém jazyce, jsou, jak bylo uvedeno v předchozí kapitole, zejména:

- Nedostatečná dostupnost nebo „dostupnost“ materiálů (hlavně tištěných knih)
- Jiná struktura textů, jiné řazení informací
- Jiná úroveň odbornosti textu

Podporuje to tedy rozhodnutí vytvořit vlastní učební texty v českém jazyce, které by strukturou a obsahem odpovídaly kurzům NetAcad.

(Kompletní zpráva je uvedena v příloze.)

2 Vlastní návrh učebního textu

2.1 Výběr tématu textu a zpracování

Pro návrh učebního textu byla vybrána kapitola (modul) 14 z CCNA1 na NetAcad, Texty byly připraveny tak, aby co nejvíce odpovídaly rozvržení kapitoly originální, je používána běžná česká odborná terminologie, spolu s anglickou, kde je to vhodné a možné.

2.2 Volba technologie pro interaktivitu

Pro interaktivitu bylo rozhodnuto kvízové otázky doplnit o správná řešení pomocí využití technologie QR kódů, bude tedy možno si zkontrolovat odpovědi i v případě tištěné verze v offline režimu, např. pomocí chytrého telefonu s příslušnou aplikací pro čtení QR kódů.

2.3 Typografie a grafické zpracování

Velká péče a hodně času bylo věnováno na úpravu vizuálních prvků, obrázků, diagramů a schémat, a také tabulek. Celkový vzhled byl inspirován originální úpravou kurzů NetAcad, ale pro verzi dokumentu ve formátu Word bylo nutno provést řadu změn. Oproti webové verzi originálu přibylo číslování stránek, záhlaví a zápatí, a obsah dokumentu (kapitoly), vynechány byly videonahrávky z technologických důvodů. Číslování kapitol bylo zachováno, aby bylo možno používat český text pro snadné doplnění originálního kurzu a jednotné odkazy.

Z těchto důvodů bude zde v tomto textu práce uvedena jen vybraná část 14.4 připraveného učebního textu, protože řadu z oněch prvků a formátování nelze sloučit a zachovat v nezměněné podobě v jednom dokumentu formátu Wordu. Kompletní učební text bude tedy uveden jako samostatná Příloha A, s maximálním zachováním věrnosti. Vybraná část zahrnuje většinu používaných prvků včetně kvízu s QR kódem, bohužel i zde je část formátování a typografie zkreslena.

2.4 Ukázka vybrané části učebního textu

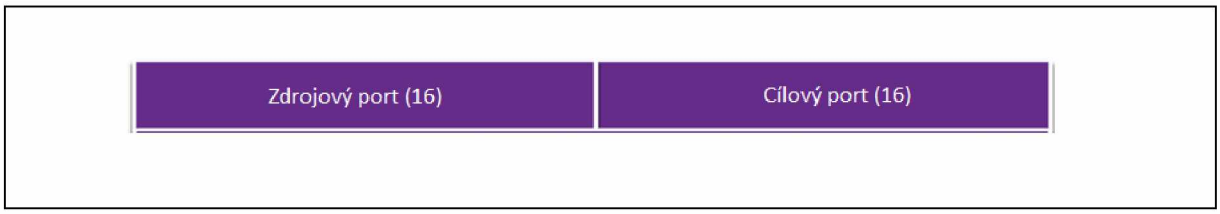
— začátek ukázky —

---

1. 14.4.1 Vícenásobná samostatná komunikace

Jak jste se dozvěděli, existují některé situace, ve kterých je TCP správným protokolem pro danou úlohu, a jiné situace, ve kterých by měl být použit protokol UDP. Bez ohledu na to, jaký typ dat se přenáší, TCP i UDP používají čísla portů.

Protokoly transportní vrstvy TCP a UDP používají čísla portů ke správě více současných konverzací. Jak je znázorněno na obrázku, pole záhlaví TCP a UDP identifikují číslo portu zdrojové a cílové aplikace.



Číslo zdrojového portu je přidruženo ke zdrojové aplikaci na místním hostiteli, zatímco číslo cílového portu je přidruženo k cílové aplikaci na vzdáleném hostiteli.

Předpokládejme například, že hostitel iniciuje požadavek na webovou stránku z webového serveru. Když hostitel zahájí požadavek webové stránky, hostitel dynamicky generuje číslo zdrojového portu, aby jednoznačně identifikoval konverzaci. Každý požadavek vygenerovaný hostitelem bude používat jiné dynamicky vytvořené zdrojové číslo portu. Tento proces umožňuje více konverzací současně.

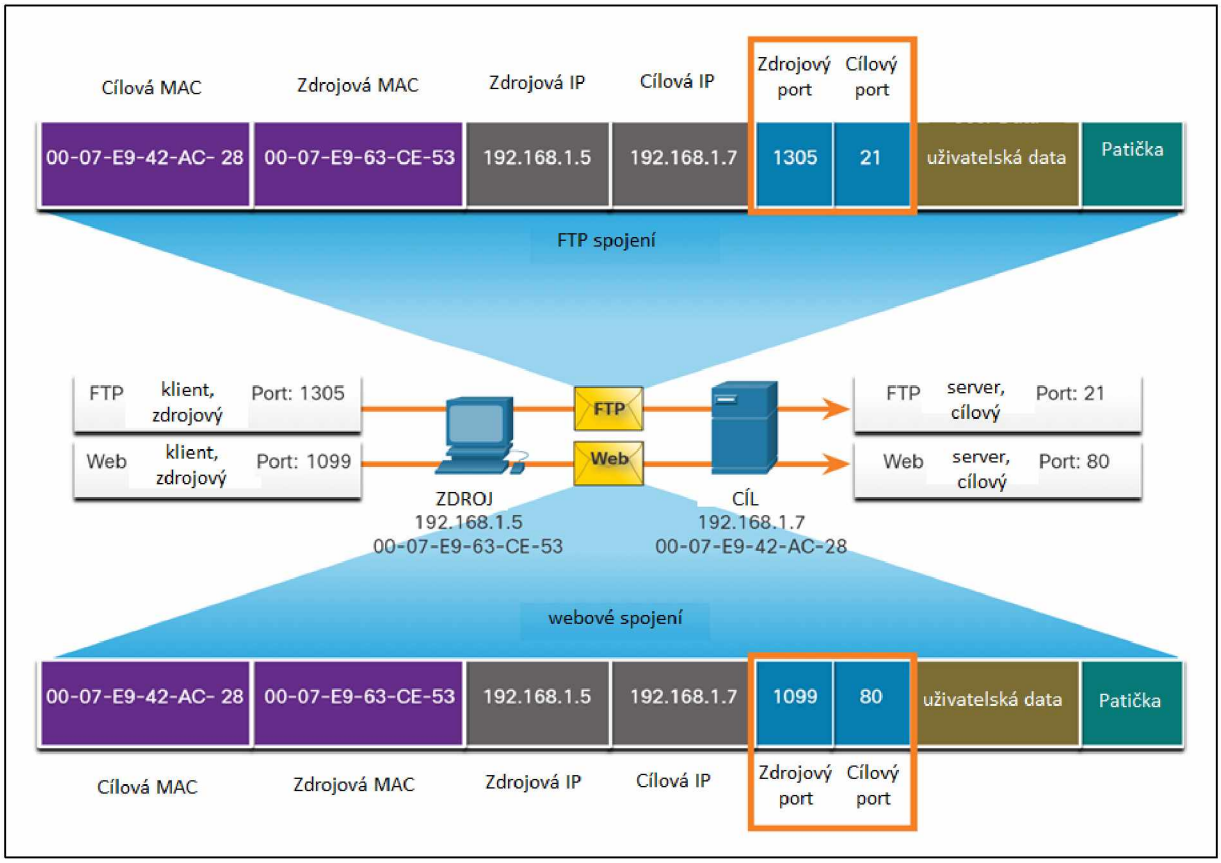
V požadavku je číslo cílového portu to, co identifikuje typ služby, která je požadována od cílového webového serveru. Například, když klient zadá port 80 v cílovém portu, server, který přijímá zprávu, ví, že jsou vyžádány webové služby.

Server může nabízet více než jednu službu současně, například webové služby na portu 80, zatímco na portu 21 nabízí navázání spojení FTP (File Transfer Protocol).

2. 14.4.2 Socketové páry

Zdrojový a cílový port jsou umístěny v rámci segmentu. Segmenty jsou pak zapouzdřeny do IP paketu. IP paket obsahuje IP adresu zdroje a cíle. Kombinace zdrojové adresy IP a čísla zdrojového portu nebo cílové adresy IP a čísla cílového portu se nazývá socket.

V příkladu na obrázku PC současně požaduje FTP a webové služby z cílového serveru.



V tomto příkladu požadavek FTP generovaný počítačem obsahuje MAC adresy vrstvy 2 a adresy IP vrstvy 3. Požadavek také identifikuje číslo zdrojového portu 1305 (tj. dynamicky generovaný hostitelem) a cílový port, identifikující služby FTP na portu 21. Hostitel také požádal o webovou stránku ze serveru pomocí stejných adres vrstvy 2 a vrstvy 3 . Používá však číslo zdrojového portu 1099 (tj. dynamicky generované hostitelem) a cílový port identifikující webovou službu na portu 80.

Socket se používá k identifikaci serveru a služby požadované klientem. Klientský socket může vypadat takto, přičemž 1099 představuje číslo zdrojového portu: 192.168.1.5:1099

Socket na webovém serveru může být 192.168.1.7:80

Společně se tyto dva sockety spojí a vytvoří pár socketů: 192.168.1.5:1099, 192.168.1.7:80

Sockety umožňují více procesům běžícím na klientovi, aby se navzájem odlišily a aby se od sebe odlišilo více připojení k procesu serveru.

Číslo zdrojového portu funguje jako zpáteční adresa pro žádající aplikaci. Transportní vrstva sleduje tento port a aplikaci, která iniciovala požadavek, takže když je vrácena odpověď, může být předána správné aplikaci.

3. 14.4.3 Skupiny čísel portů

Internet Assigned Numbers Authority (IANA) je organizace pro standardy zodpovědná za přidělování různých standardů adresování, včetně 16bitových čísel portů. 16 bitů používaných k identifikaci čísel zdrojového a cílového portu poskytuje rozsah portů od 0 do 65535.

IANA rozdělila rozsah čísel do následujících tří skupin portů.

Skupina portů	Číslo	Popis rozsahu
Známé porty	0 až 1 023	• Tato čísla portů jsou vyhrazena pro běžné nebo oblíbené služby a aplikace, jako jsou webové prohlížeče, e-mailové klienty a klienti vzdáleného přístupu. • Definované známé porty pro běžné serverové aplikace umožňují klientům snadno identifikovat požadovanou související službu.
Registrované porty	1 024 až 49 151	• Tato čísla portů přiděluje IANA žádající entitě pro použití s konkrétními procesy nebo aplikacemi. • Tyto procesy jsou primárně jednotlivé aplikace, které se uživatel rozhodl nainstalovat, spíše než běžné aplikace, které by obdržely dobře známé číslo portu. • Například společnost Cisco zaregistrovala port 1812 pro proces ověřování serveru RADIUS.
Soukromé a/nebo dynamické porty	49 152 až 65 535	• Tyto porty jsou také známé jako dočasné porty. • Operační systém klienta obvykle přiřazuje čísla portů dynamicky, když je zahájeno připojení ke službě. • Dynamický port se pak používá k identifikaci klientské aplikace během komunikace.

Poznámka: Některé klientské operační systémy mohou pro přiřazování zdrojových portů místo dynamických čísel portů používat registrovaná čísla portů.

Tabulka zobrazuje některá běžná známá čísla portů a jejich přidružené aplikace.

Číslo portu	Protokol	Aplikace
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name System (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server
68	UDP	Dynamic Host Configuration Protocol – klient
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol verze 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

Některé aplikace mohou používat TCP i UDP. DNS například používá UDP, když klienti odesílají požadavky na server DNS. Komunikace mezi dvěma servery DNS však vždy používá protokol TCP.

Chcete-li zobrazit úplný seznam čísel portů a souvisejících aplikací, vyhledejte na webu IANA registr portů.

4. 14.4.4 Příkaz netstat

Nevysvětlená připojení TCP mohou představovat velkou bezpečnostní hrozbu. Mohou indikovat, že je něco nebo někdo připojen k místnímu hostiteli. Někdy je nutné vědět, která aktivní TCP spojení jsou otevřená, a běží na síťovém hostiteli. Netstat je důležitý síťový nástroj, který lze použít k ověření těchto připojení. Jak je znázorněno níže, zadejte příkaz netstat, abyste

zobrazili seznam používaných protokolů, místní adresy a čísla portů, cizí adresy a čísla portů a stav připojení.

```
C:\> netstat

Active Connections

  Proto  Local Address          Foreign Address            State
  TCP    192.168.1.124:3126     192.168.0.2:netbios-ssn    ESTABLISHED
  TCP    192.168.1.124:3158     207.138.126.152:http       ESTABLISHED
  TCP    192.168.1.124:3159     207.138.126.169:http       ESTABLISHED
  TCP    192.168.1.124:3160     207.138.126.169:http       ESTABLISHED
  TCP    192.168.1.124:3161     sc.msn.com:http            ESTABLISHED
  TCP    192.168.1.124:3166     www.cisco.com:http         ESTABLISHED
(output omitted)
C:\>
```

Ve výchozím nastavení se příkaz netstat pokusí přeložit IP adresy na názvy domén a čísla portů na známé aplikace. Volbu -n lze použít k zobrazení IP adres a čísel portů v jejich číselné podobě.

5. 14.4.5 Zkontrolujte své znalosti – čísla portů

Ověřte si, zda rozumíte číslům portů výběrem správné odpovědi na následující otázky.

1. Předpokládejme, že hostitel s IP adresou 10.1.1.10 chce požádat o webové služby ze serveru na 10.1.1.254. Která z následujících možností zobrazí správný pár socketů?

1. 1099:10.1.1.10, 80:10.1.1.254
2. 10.1.1.10:80, 10.1.1.254:1099
3. 10.1.1.10:1099, 10.1.1.254:80
4. 80:10.1.1.10, 1099:10.1.1.254

2. Která skupina portů obsahuje čísla portů pro aplikace FTP, HTTP a TFTP?

1. dynamické porty
2. soukromé porty
3. registrované porty
4. dobře známé porty

3. Který příkaz systému Windows zobrazí používané protokoly, místní adresu a čísla portů, zahraniční adresu a čísla portů a stav připojení?

1. ipconfig /all
2. ping
3. netstat
4. traceroute

—— konec ukázky —— celý učební text je samostatně v příloze

3 Závěr

Cíl práce byl splněn, práce obsahuje návrh učebního textu v českém jazyce k vybrané kapitolu kurzu CCNA1 NetAcad, v podobě dokumentu o rozsahu 62 tiskových stran, jako podporu pro výuku počítačových sítí.

Pro zvýšení interaktivity i v tištěné verzi byla navržena technologie QR, a ke kvízům umístěn QR kód se správnými odpověďmi na kvízové otázky, aby si žák nebo student mohl sám ověřit svoje získané znalosti, s pomocí chytrého telefonu s příslušnou aplikací, což je dnes běžné vybavení, které nevyžaduje online připojení k internetu, ani podporu na serverové straně, ani dostupný jakýkoliv server vůbec.

Autor by chtěl postupně zpracovat i další klíčové kapitoly podle priorit, každá by mohla tvořit víceméně samostatnou knihu, nebo silný sešit, podobného rozsahu – v aktuální verzi kurzu CCNA1 je celkem 17 kapitol (modulů).

Dále má v úmyslu ve spolupráci s nadanými studenty například formou prací SOČ připravit i české verze videonahrávek, které jsou součástí kapitol NetAcad.

4 Použitá literatura

1) Cisco Networking Academy [online]. San Francisco: Cisco Systems, 2023 [cit. 2023-02-10]. Dostupné z: https://www.netacad.com/
2) MINISTRYNĚ KOPICOVÁ PODEPSALA MEMORANDUM O SPOLUPRÁCI SE SPOLEČNOSTÍ CISCO. *MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY* [online]. Praha: MŠMT, 2009, 14.10.2009 [cit. 2023-02-10]. Dostupné z: https://www.msmt.cz/ministerstvo/novinar/ministryne-kopicova-podepsala-memorandum-o-spolupraci-se
3) CCNA: Introduction to Networks [online]. San Jose, Kalifornie, USA: Cisco Networking Academy, 2021 [cit. 2022-05-15]. Dostupné z: https://www.netacad.com/courses/networking/ccna-introduction-networks
4) SKALKOVÁ, Jarmila. Obecná didaktika-2., rozšířené a aktualizované vydání. Grada Publishing as, 2007.
5) FOJTÍK, Rostislav. Didaktika informatiky II. Ostrava: Ostravská univerzita, 2005.
6) JONASSEN, David a Marcy DRISCOLL. *Handbook of Research on Educational Communications and Technology: A Project of the Association for Educational Communications and Technology* [online]. 2nd Edition. New York: Routledge, 2004 [cit. 2023-02-10]. ISBN 9781410609519. Dostupné z: https://doi.org/10.4324/9781410609519
7) MERRILL, M.D. *First principles of instruction.* ETR&D 50, 43–59 (2002). https://doi.org/10.1007/BF02505024
8) SPECTOR, J. Michael. *Handbook of research on educational communications and technology*. Fourth edition. New York: Springer, [2014]. ISBN 9781461431855, 1461431859. Dostupné z: https://dx.doi.org/10.1007/978-1-4614-3185-5
9) ODOM, Wendell. Počítačové sítě bez předchozích znalostí. 1. vyd. Brno : CP Books, a.s., 2005. 384 s. ISBN 80-251-0538-5.
10) PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z : technologie pro datovou, hlasovou i multimediální komunikaci. 2. aktualiz. vyd. [s.l.] : [s.n.], 2006. 430 s. ISBN 80-251-1278-0.
11) *EArchiv.cz: Archiv článků a přednášek Jiřího Peterky* [online]. Praha: Jiří Peterka, 2023 [cit. 2023-02-10]. Dostupné z: https://www.earchiv.cz/

5 Přílohy

Příloha A

Kapitola 14: Transportní vrstva

Text ke kapitole **Module 14 – Transport Layer** kurzu CCNA1 **Introduction to Networks**, online na webu **netacad.com** (podle anglického originálu). Připravil Zdeněk Drvota.

Obsah:

Transportní vrstva

14.0.1 Proč studovat tento modul?

Vítejte v Transportní vrstvě!

Transportní vrstva je místo, kde, jak název napovídá, jsou data přenášena z jednoho hostitele na druhého. Tady se vaše síť skutečně rozhýbe! Transportní vrstva používá dva protokoly: TCP a UDP. Představte si TCP jako doručení doporučeného dopisu poštou. Musíte dodání podepsat, než vám jej poštovní přepravce vydá. Tím se proces trochu zpomalí, ale odesílatel s jistotou ví, že jste dopis obdrželi a kdy jste jej obdrželi. UDP je spíše jako obyčejný, orazítkovaný dopis. Přijde do vaší poštovní schránky, a pokud ano, je pravděpodobně určen vám, ale ve skutečnosti může být pro někoho jiného, kdo tam nebydlí. Může se také stát, že do vaší poštovní schránky vůbec nedorazí. Odesílatel si nemůže být jistý, že jste jej obdrželi. Přesto jsou chvíle, kdy je protokol UDP, jako orazítkovaný dopis, potřebným protokolem. Toto téma se zabývá tím, jak TCP a UDP fungují v transportní vrstvě. Součástí tohoto modulu je několik videí, která vám pomohou porozumět těmto procesům.

14.0.2 Co se v tomto modulu naučíme?

Název modulu: Transportní vrstva

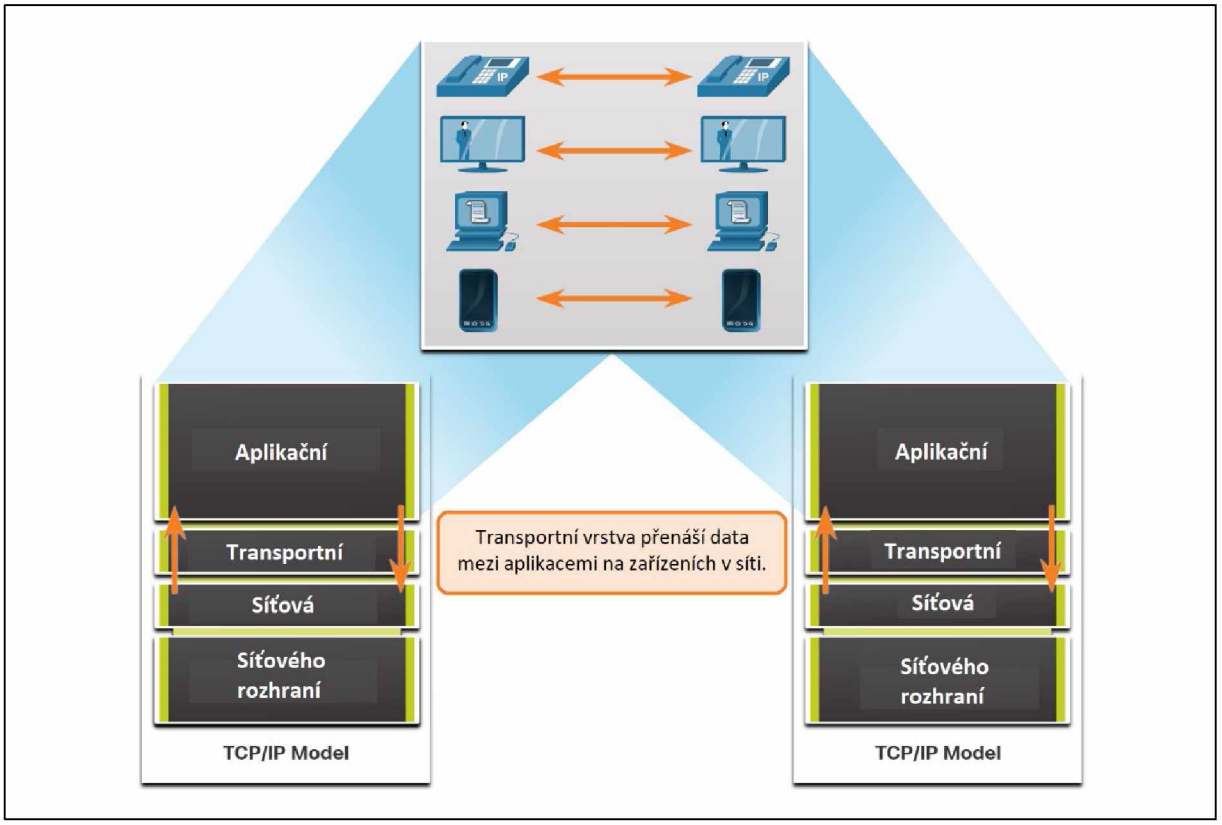
Cíl modulu: Porovnat operace protokolů transportní vrstvy při podpoře end-to-end komunikace.

Název tématu	Cíl tématu
Přenos dat	Vysvětlit účel transportní vrstvy při řízení přenosu dat v end-to-end komunikaci.
Přehled TCP	Vysvětlit vlastnosti TCP.
Přehled UDP	Vysvětlit vlastnosti UDP.
Čísla portů	Vysvětlit, jak TCP a UDP používají čísla portů.
Komunikační proces TCP	Vysvětlit, jak procesy vytvoření a ukončení relace TCP usnadňují spolehlivou komunikaci.
Spolehlivost a řízení toku	Vysvětlit, jak jsou přenášeny a potvrzovány datové jednotky protokolu TCP, aby bylo zaručeno doručení.
Komunikace UDP	Porovnat operace protokolů transportní vrstvy při podpoře end-to-end komunikace.

14.1.1 Role transportní vrstvy

Programy aplikační vrstvy generují data, která si musí vyměňovat zdrojový a cílový hostitel. Transportní vrstva je zodpovědná za logickou komunikaci mezi aplikacemi běžícími na různých hostitelích. To může zahrnovat služby, jako je vytvoření dočasné relace mezi dvěma hostiteli a spolehlivý přenos informací pro aplikaci.

Jak je znázorněno na obrázku, transportní vrstva je spojnicí mezi aplikační vrstvou a nižšími vrstvami, které jsou zodpovědné za síťový přenos.



Transportní vrstva nezná typ cílového hostitele, typ média, přes které musí data cestovat, cestu, kterou data urazí, přetížení linky nebo velikost sítě.

Transportní vrstva obsahuje dva protokoly:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

14.1.2 Odpovědnosti transportní vrstvy

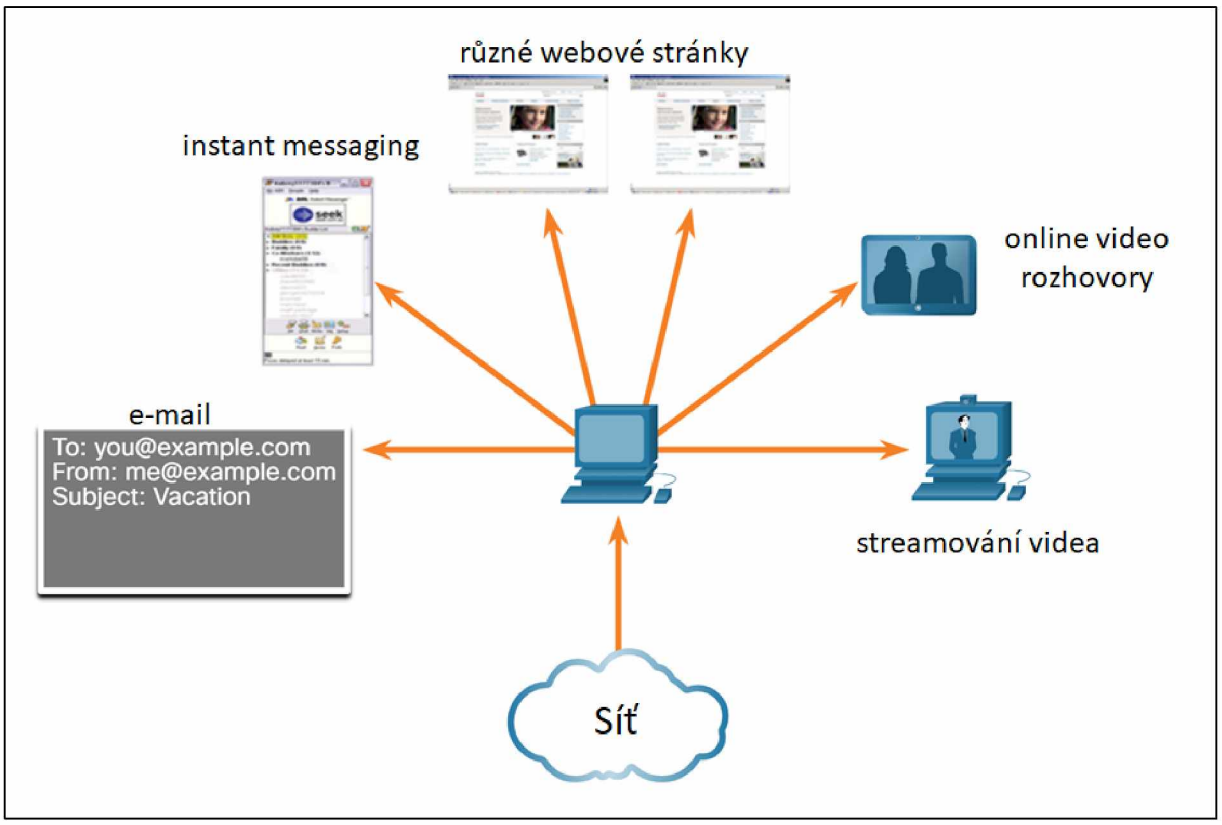
Transportní vrstva má mnoho povinností.

Na transportní vrstvě je každá sada dat proudících mezi zdrojovou aplikací a cílovou aplikací známá jako konverzace a je sledována samostatně. Za udržování a sledování těchto četných konverzací je odpovědná transportní vrstva.

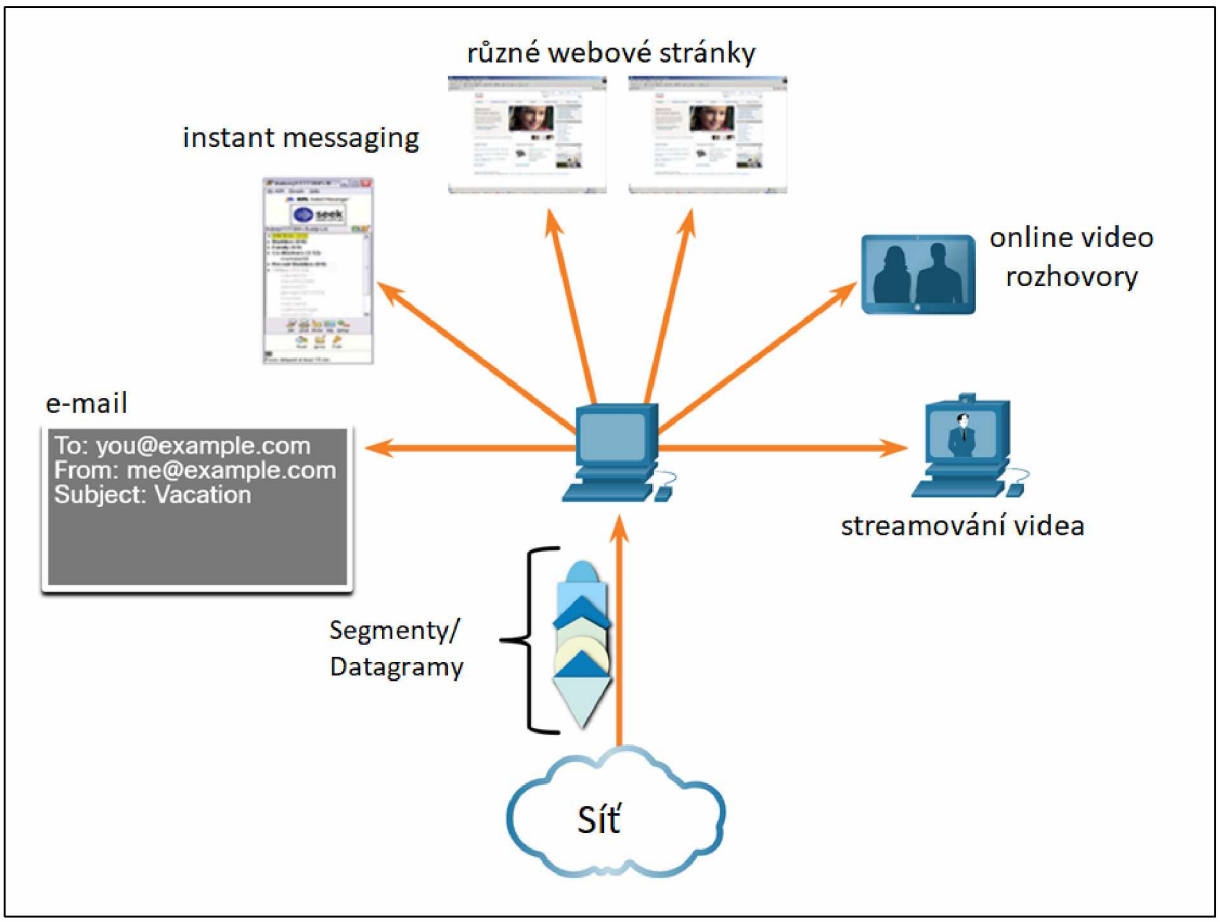
Jak je znázorněno na obrázcích, hostitel může mít více aplikací, které komunikují po síti současně.

Většina sítí má omezení na množství dat, které lze zahrnout do jednoho paketu. Data proto musí být rozdělena na zvládnutelné části.

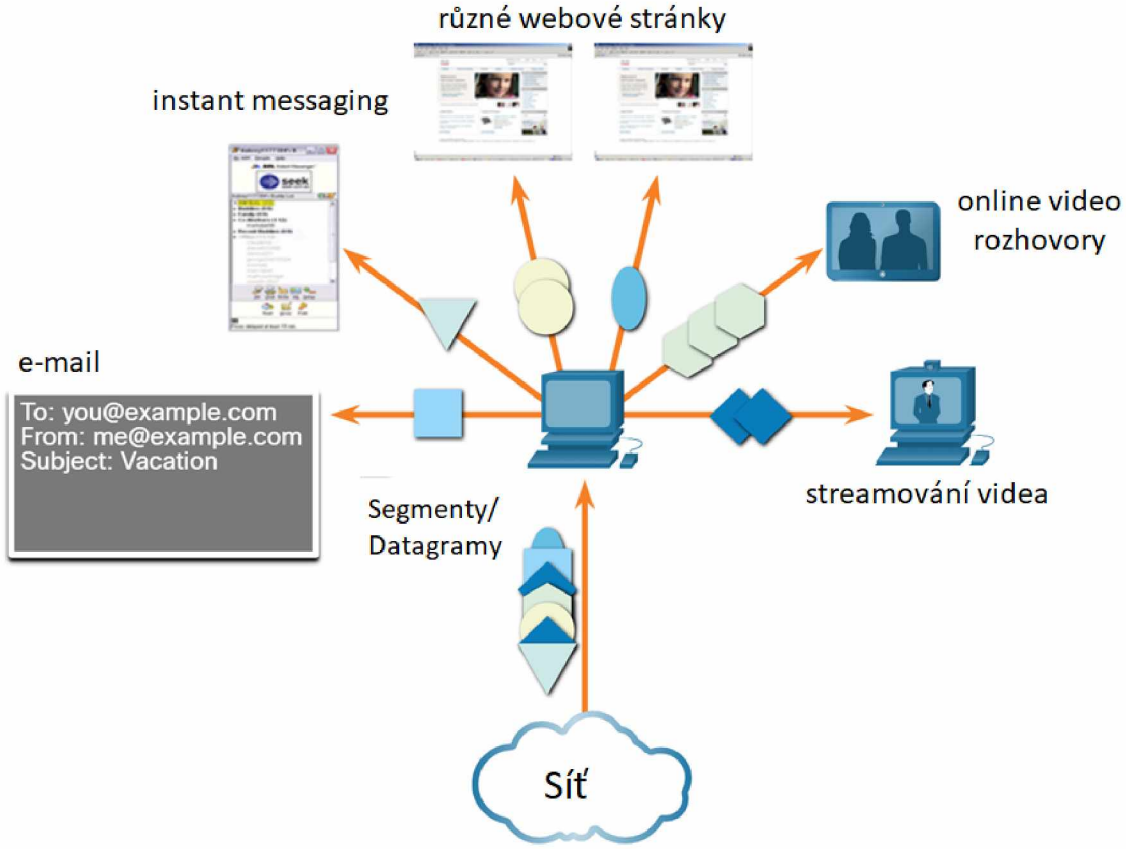
Sledování jednotlivých konverzací



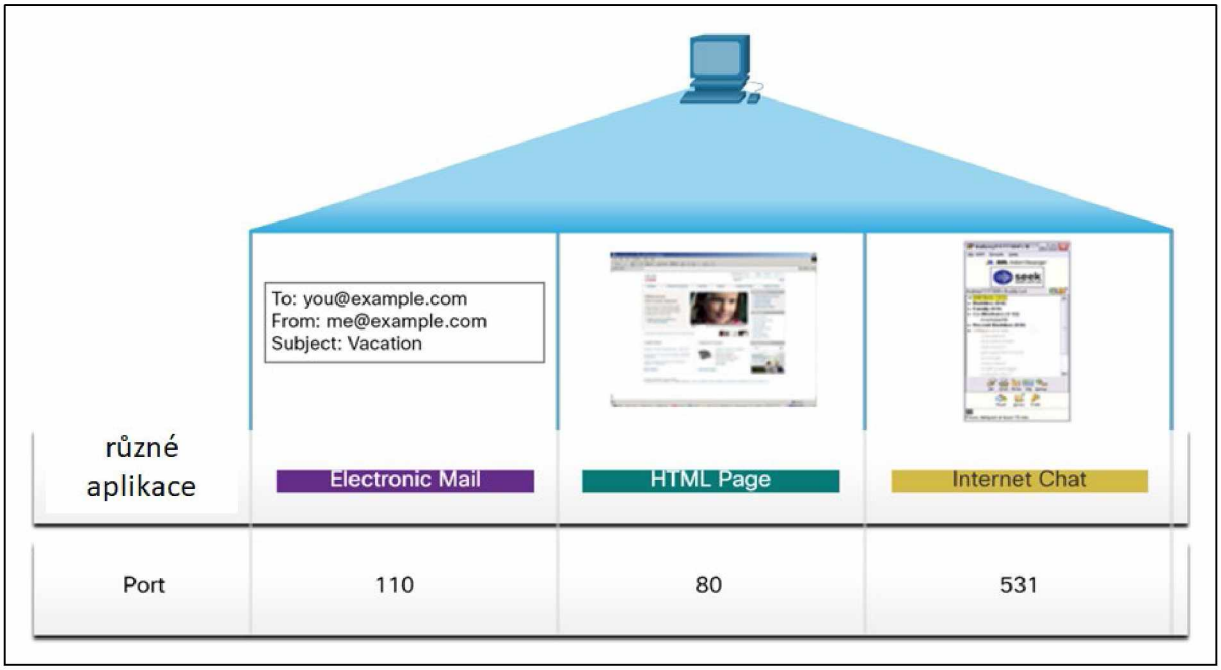
Segmentace dat a opětovné sestavení segmentů



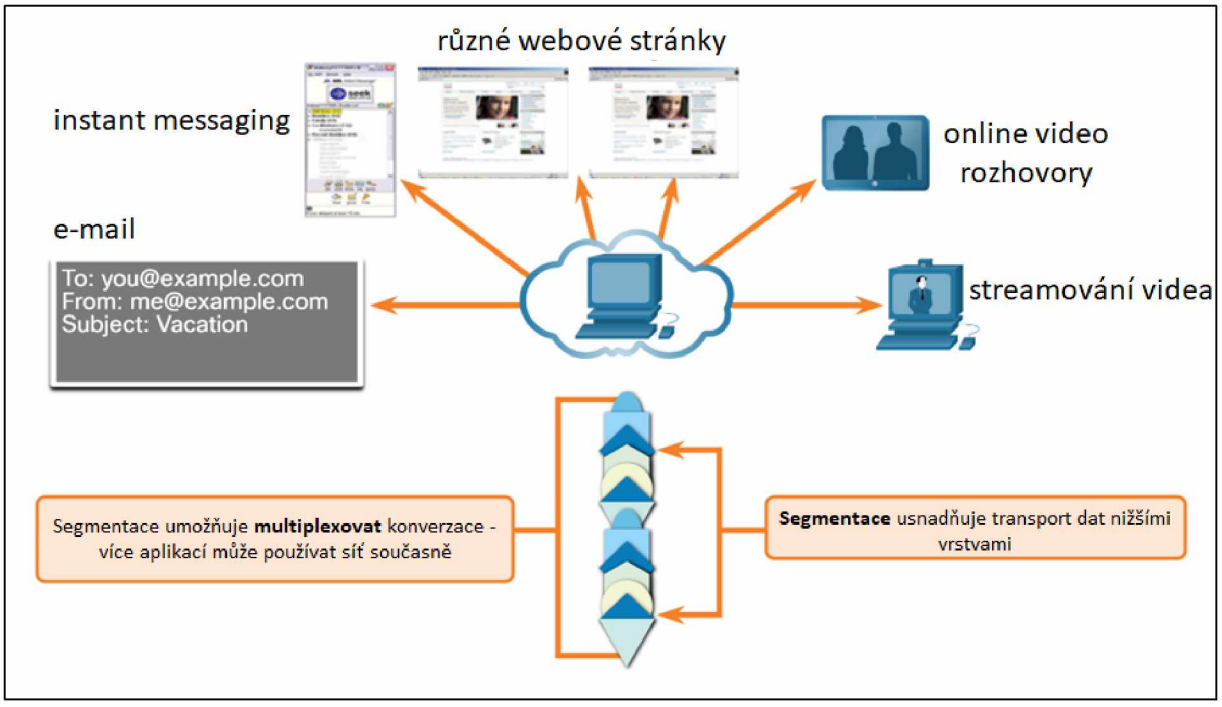
Přidat informace o záhlaví



Identifikace aplikací



Multiplexování konverzace



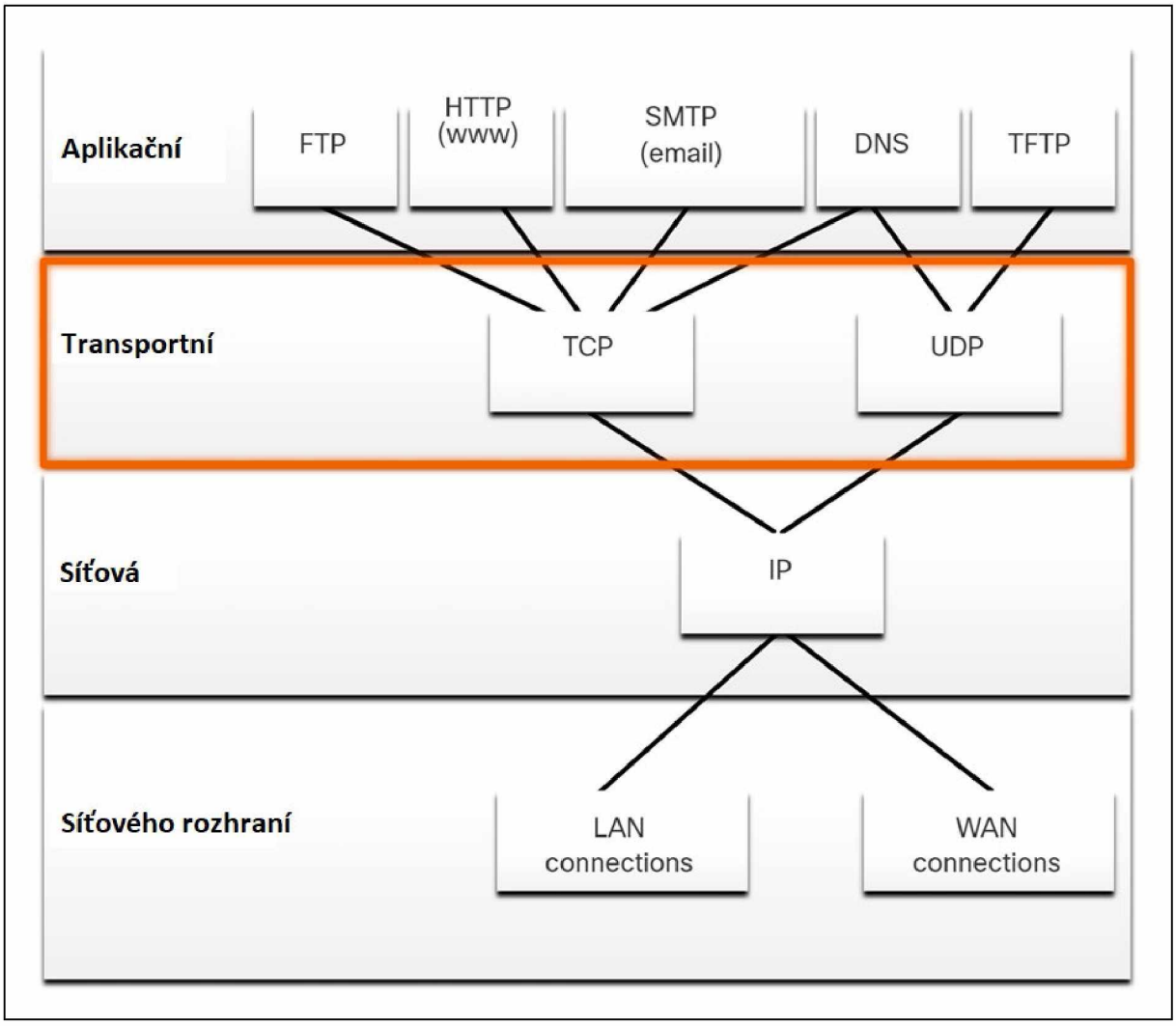
14.1.3 Protokoly transportní vrstvy

Protokol síťové vrstvy IP se zabývá pouze strukturou, adresováním a směrováním paketů. IP nespecifikuje, jak probíhá doručení nebo přeprava paketů.

Protokoly transportní vrstvy určují způsob přenosu zpráv mezi hostiteli a jsou zodpovědné za řízení požadavků na spolehlivost konverzace. Transportní vrstva zahrnuje protokoly TCP a UDP.

Různé aplikace mají různé požadavky na spolehlivost dopravy. Proto TCP/IP poskytuje dva protokoly transportní vrstvy, jak je znázorněno na obrázku.

Schéma – jak protokoly aplikační vrstvy jako FTP, HTTP, SMTP používají TCP na transportní vrstvě, a DNS a TFTP používají UDP. Jak všichni používají IP na internetové vrstvě bez ohledu na to, zda se připojují k LAN nebo WAN na úrovni síťového rozhraní



14.1.4 Transmission Control Protocol (TCP)

IP se zabývá pouze strukturou, adresováním a směrováním paketů od původního odesílatele ke konečnému cíli. IP není zodpovědná za zaručení doručení nebo určení, zda je třeba vytvořit spojení mezi odesílatelem a příjemcem.

TCP je považován za spolehlivý, plně vybavený protokol transportní vrstvy, který zajišťuje, že všechna data dorazí na místo určení. TCP zahrnuje pole, která zajišťují doručení dat aplikace. Tato pole vyžadují dodatečné zpracování odesílajícím a přijímajícím hostitelem.

Poznámka: TCP rozděluje data do segmentů.

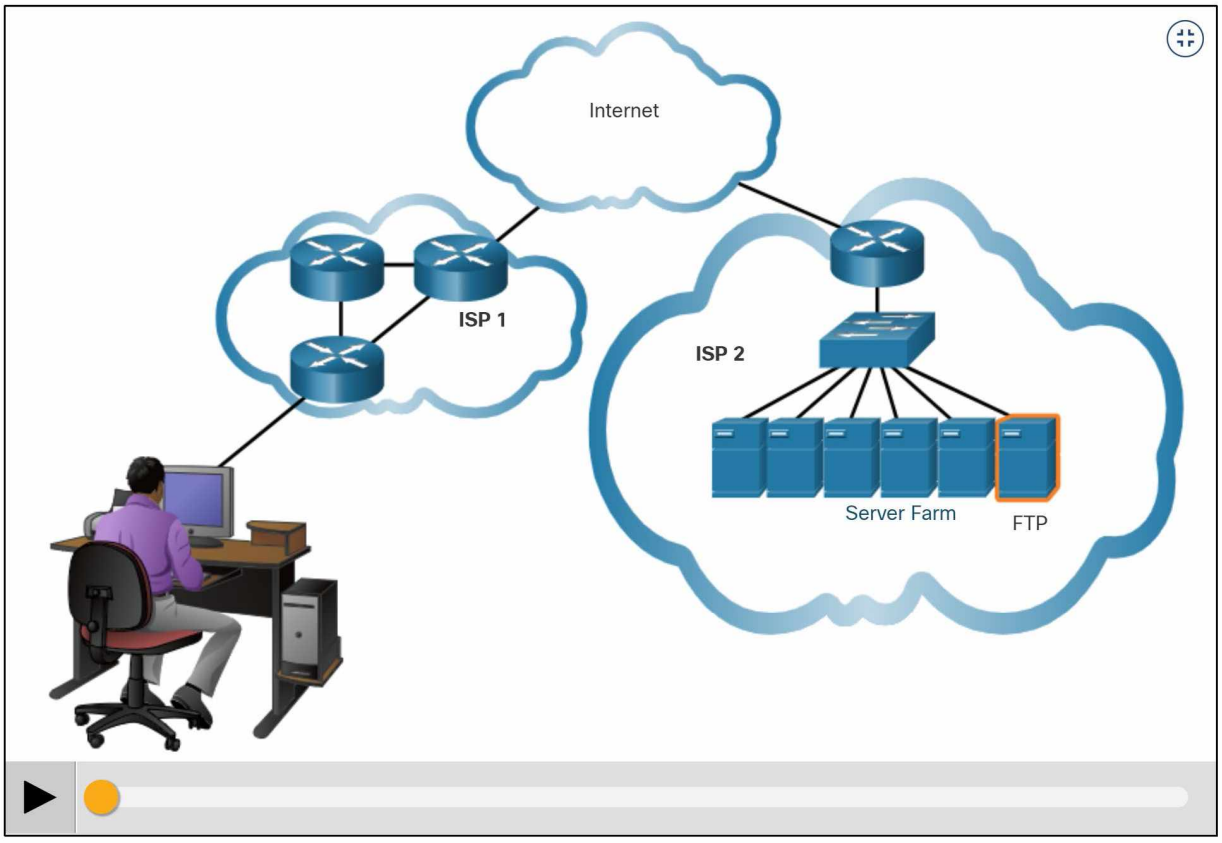
Transport TCP je analogický odesílání balíků, které jsou sledovány od zdroje k cíli. Pokud je objednávka zásilky rozdělena do několika balíků, může zákazník online zkontrolovat pořadí dodávky

TCP poskytuje spolehlivost a řízení toku pomocí těchto základních operací:

- Číslování a sledování datových segmentů přenášených na konkrétního hostitele z konkrétní aplikace
- Potvrzení přijatých dat
- Po určité době znovu odešle všechna nepotvrzená data
- Sekvenční data, která mohou přijít v nesprávném pořadí, v cíli přerovná do správného
- Odesílá data efektivní rychlostí, která je přijatelná pro příjemce

Aby bylo možné zachovat stav konverzace a sledovat informace, musí TCP nejprve navázat spojení mezi odesílatelem a příjemcem. Proto je TCP známý jako protokol spojovaný.

Klikněte na Přehrát na obrázku, abyste viděli, jak jsou TCP segmenty a potvrzení přenášeny mezi odesílatelem a příjemcem.



14.1.5 User Datagram Protocol (UDP)

UDP je jednodušší protokol transportní vrstvy než TCP. Neposkytuje spolehlivost a řízení toku, což znamená, že vyžaduje méně polí hlavičky. Protože UDP procesy odesílatele a příjemce nemusí řídit spolehlivost a řízení toku, znamená to, že datagramy UDP lze zpracovávat rychleji než

segmenty TCP. UDP poskytuje základní funkce pro doručování datagramů mezi příslušnými aplikacemi s velmi malou režií a kontrolou dat.

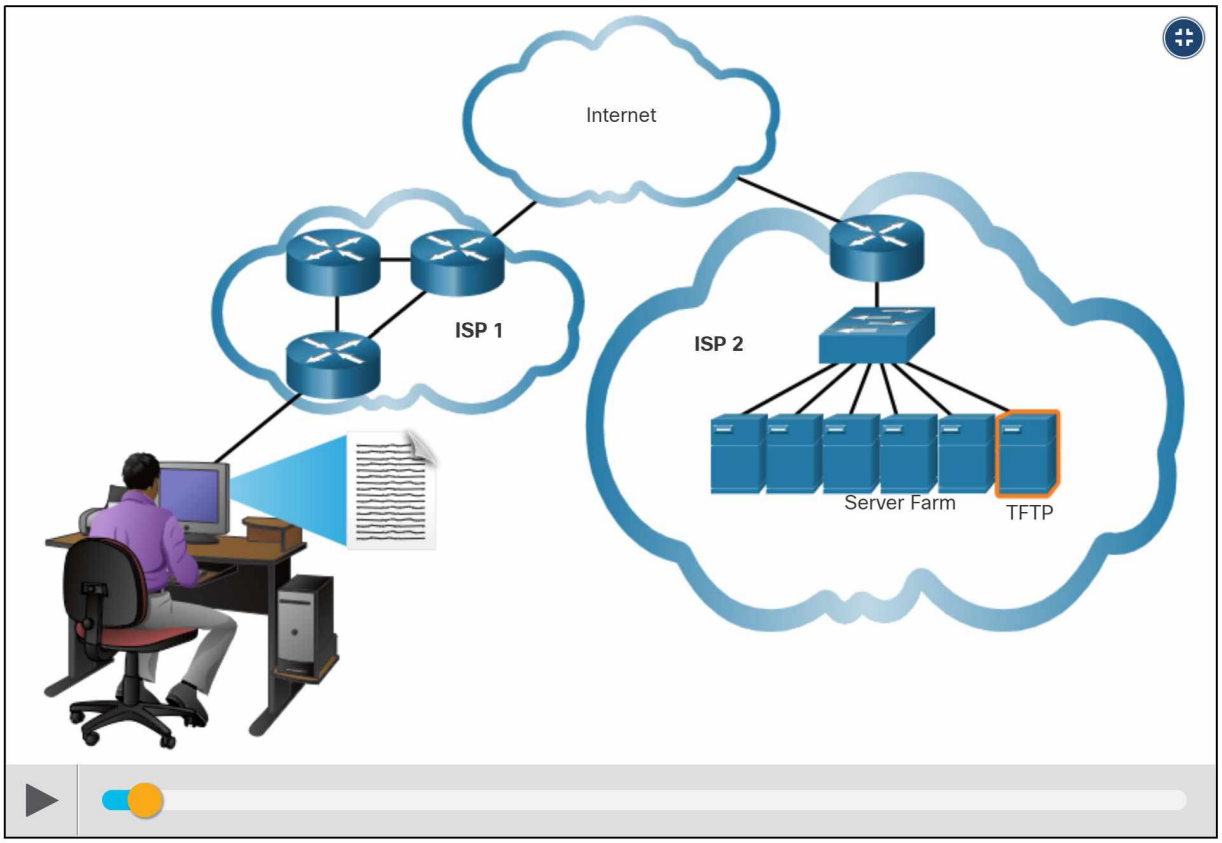
Poznámka: UDP rozděluje data do datagramů, které se někdy také označují jako segmenty (jako obecnější pojem).

UDP je protokol nespojovaný. Protože protokol UDP neposkytuje spolehlivost ani řízení toku, nevyžaduje navázané spojení. Protože UDP nesleduje informace odeslané nebo přijaté mezi klientem a serverem, UDP je také známý jako bezestavový protokol.

UDP je také známý jako protokol doručování s nejlepším úsilím (best effort), protože neexistuje žádné potvrzení, že data jsou přijata v cíli. s UDP neexistují žádné procesy transportní vrstvy, které by informovaly odesílatele o úspěšném doručení.

UDP je jako poslat obyčejný (ne doporučený) dopis poštou. Odesílatel dopisu si není vědom toho, jestli příjemce může dopis přijmout. Pošta také není odpovědná za sledování zásilky nebo informování odesílatele, pokud zásilka nedorazí do konečného místa určení.

Kliknutím na Přehrát na obrázku zobrazíte animaci UDP datagramů přenášených od odesílatele k přijímači.



14.1.6 Správný protokol transportní vrstvy pro správnou aplikaci

Některé aplikace mohou tolerovat určitou ztrátu dat během přenosu po síti, ale zpoždění přenosu jsou nepřijatelná. Pro tyto aplikace je UDP lepší volbou, protože vyžaduje menší režii sítě. UDP je

vhodnější pro aplikace, jako je Voice over IP (VoIP). Potvrzení a opakovaný přenos by zpomalily doručení a učinily by hlasovou konverzaci nepřijatelnou.

UDP je také používán aplikacemi typu request-and-reply, kde je dat minimum a opakovaný přenos lze provést rychle. Například DNS (Domain Name System) používá pro tento typ transakce UDP. Klient požaduje adresy IPv4 a IPv6 pro známý název domény ze serveru DNS. Pokud klient neobdrží odpověď v předem stanoveném čase, jednoduše odešle požadavek znovu.

Pokud se například nepodaří doručit jeden nebo dva segmenty živého videostreamu, způsobí to chvilkové narušení streamu. To se může jevit jako zkreslení obrazu nebo zvuku, ale nemusí to být pro uživatele patrné. Pokud by cílové zařízení muselo počítat se ztrátou dat, stream by se mohl zpozdit při čekání na opakovaný přenos, což by způsobilo výrazné zhoršení obrazu nebo zvuku. v tomto případě je lepší vykreslit nejlepší možné médium (obraz, zvuk) jen s přijatými segmenty a vzdát se spolehlivosti.

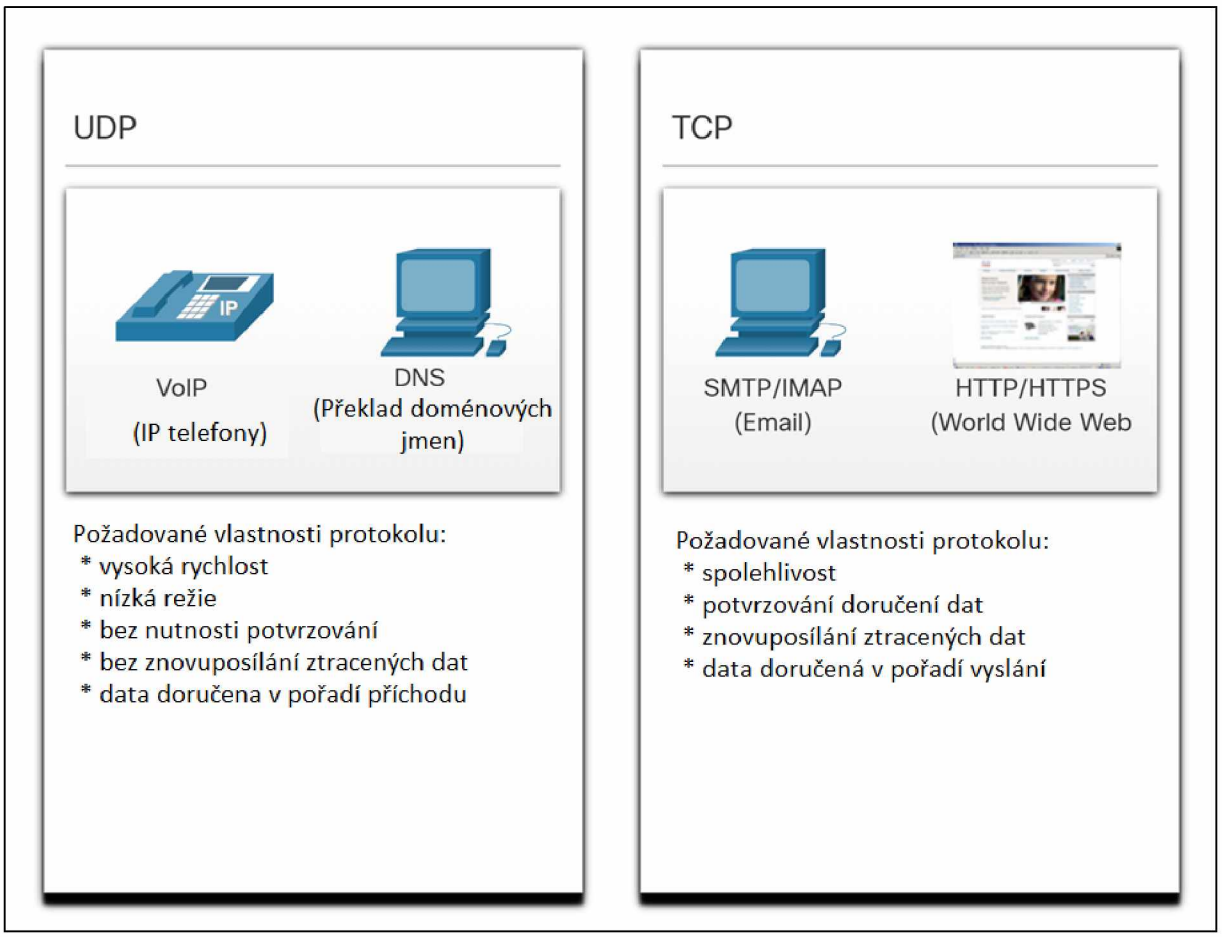
Pro ostatní aplikace je důležité, aby všechna data dorazila a mohla být zpracována ve správném pořadí. Pro tyto typy aplikací se jako přenosový protokol používá TCP. Například aplikace, jako jsou databáze, webové prohlížeče a e-mailové klienty, vyžadují, aby všechna odesílaná data dorazila na místo určení v původním stavu. Jakákoli chybějící data by mohla poškodit komunikaci a učinit ji neúplnou nebo nečitelnou. Například při přístupu k bankovním informacím přes web je důležité zajistit, aby byly všechny informace odeslány a přijaty správně.

Vývojáři aplikací si musí vybrat, který typ transportního protokolu je vhodný na základě požadavků aplikací. Video může být odesláno přes TCP nebo UDP. Aplikace, které streamují uložené audio a video, obvykle používají TCP. Aplikace používá TCP k provádění ukládání do vyrovnávací paměti, zkoumání šířky pásma a řízení zahlcení, aby bylo možné lépe řídit kvalitu uživatelova prožitku.

Video a hlas v reálném čase obvykle používají UDP, ale mohou také používat TCP, nebo obojí – UDP i TCP. Aplikace pro videokonference může standardně používat protokol UDP, ale protože mnoho firewallů blokuje protokol UDP, lze aplikaci provozovat obvykle také přes TCP.

Aplikace, které streamují uložený zvuk a video, používají TCP. Pokud například vaše síť náhle nemůže podporovat šířku pásma potřebnou ke sledování filmu na vyžádání, aplikace pozastaví přehrávání. Během pauzy se může zobrazit zpráva např. „načítání...“, zatímco TCP pracuje na obnovení streamu. Když jsou všechny segmenty v pořádku a obnoví se minimální úroveň šířky pásma, obnoví se vaše TCP relace a přehrávání filmu pokračuje.

Obrázek shrnuje rozdíly mezi UDP a TCP.



14.1.7 Ověřte si své znalosti – přenos dat

Ověřte své znalosti transportní vrstvy výběrem správné odpovědi na následující otázky.

1. Která vrstva je zodpovědná za vytvoření dočasné komunikační relace mezi zdrojovou a cílovou hostitelskou aplikací?

a: aplikační vrstva
b: vrstva síťového rozhraní
c: síťová vrstva
d: fyzická vrstva
e: transportní vrstva

2. Které tři volby jsou odpovědnosti transportní vrstvy? (Vyberte tři.)

a: multiplexování konverzace
b: identifikace rámce
c: identifikace směrovací informace
d: segmentování dat a opětovné sestavení segmentů
e: sledování jednotlivých konverzací

3. Které prohlášení protokolu transportní vrstvy je pravdivé?

a: TCP má méně polí než UDP.
b: TCP je rychlejší než UDP.
c: UDP je doručovací protokol s nejvyšší snahou.
d: UDP poskytuje spolehlivost.

4. Který protokol transportní vrstvy by byl použit pro aplikace VoIP?

a: Session Information Protocol (SIP)
b: Transmission Control Protocol (TCP)
c: User Datagram Protocol (UDP)
d: VoIP přenosový protokol

14.2.1 Vlastnosti TCP

V předchozím tématu jste se dozvěděli, že TCP a UDP jsou dva protokoly transportní vrstvy. Toto téma se zabývá podrobněji tím, co TCP dělá a kdy je vhodné jej používat místo UDP.

Pro pochopení rozdílů mezi TCP a UDP je důležité poznat, jak každý protokol implementuje specifické funkce spolehlivosti a jak každý protokol sleduje konverzace.

Kromě podpory základních funkcí segmentace dat a opětovného sestavení poskytuje TCP také následující služby:

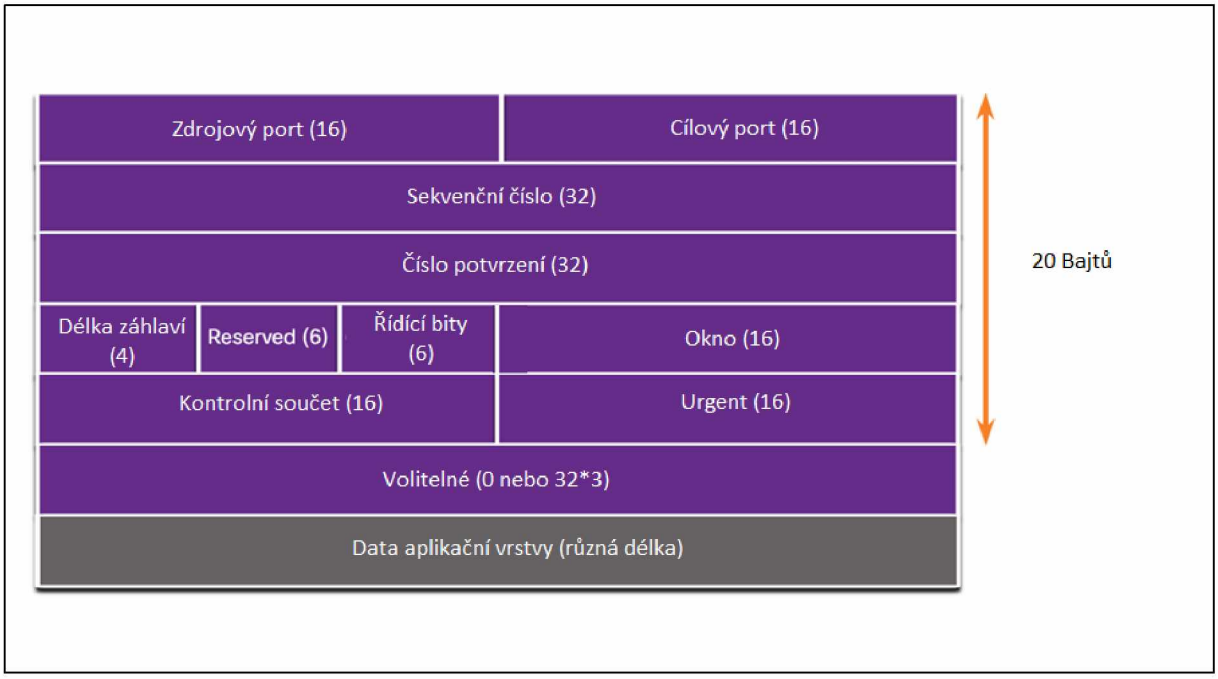
- Navazuje relaci – TCP je protokol spojovaný, který vyjednává a vytváří trvalé spojení (neboli relaci) mezi zdrojovým a cílovým zařízením před provedením jakéhokoli přenosu dat. Prostřednictvím navázání relace si zařízení vyjednají objem provozu, který lze v daném čase předat, a komunikační parametry se mezi nimi dohodnou.
- Zajišťuje spolehlivé doručení – z mnoha důvodů je možné, že se segment při přenosu po síti poškodí nebo úplně ztratí. TCP zajišťuje, že každý segment odeslaný zdrojem dorazí do cíle.
- Poskytuje doručení ve stejném pořadí – protože sítě mohou poskytovat více cest, které mohou mít různé přenosové rychlosti, data mohou dorazit v nesprávném pořadí. Očíslováním a sekvenčním řazením segmentů TCP zajišťuje, že segmenty jsou v cíli znovu sestaveny do správného pořadí.
- Podporuje Flow Control – Síťoví hostitelé mají omezené zdroje (tj. paměť a výpočetní výkon). Když si TCP uvědomí, že tyto prostředky jsou přetíženy, může požádat odesílající aplikaci, aby snížila rychlost toku dat. To se provádí TCP regulací množství dat, které zdroj přenáší. Řízení toku může zabránit potřebě opakovaného přenosu dat, když jsou zdroje přijímajícího hostitele zahlceny.

Pro více informací o TCP si vyhledejte na internetu RFC 793.

14.2.2 TCP záhlaví

TCP je stavový protokol, což znamená, že sleduje stav komunikační relace. Pro sledování stavu relace TCP zaznamenává, které informace odeslal a které informace byly potvrzeny. Stavová relace začíná vytvořením relace a končí ukončením relace.

Segment TCP přidává 20 bajtů (tj. 160 bitů) režie při zapouzdření dat aplikační vrstvy. Obrázek ukazuje pole v hlavičce TCP.



14.2.3 Pole záhlaví TCP

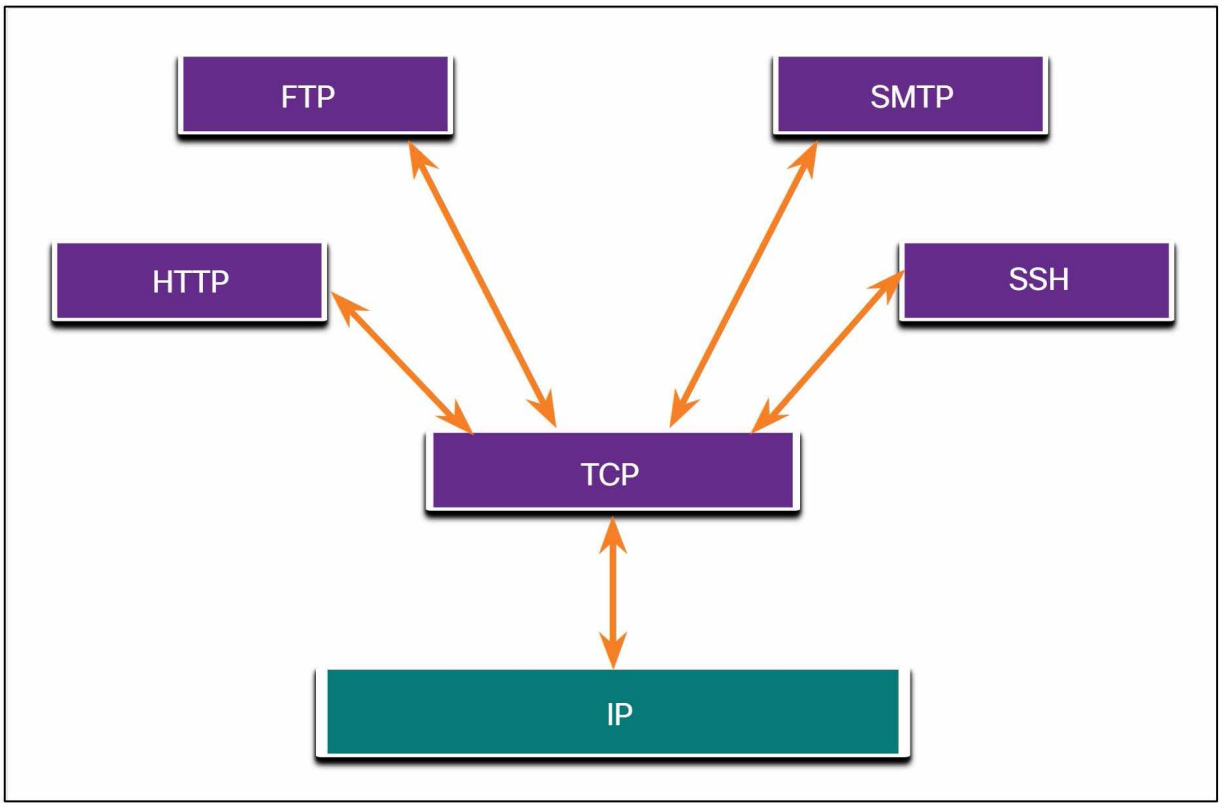
Tabulka identifikuje a popisuje deset polí v hlavičce TCP.

Pole záhlaví TCP	Popis
Zdrojový port	16bitové pole používané k identifikaci zdrojové aplikace podle čísla portu.
Cílový port	16bitové pole používané k identifikaci cílové aplikace podle čísla portu.
Sekvenční číslo	32bitové pole používané pro účely opětovného sestavení dat.
Číslo potvrzení	32bitové pole používané k označení přijetí dat a dalšího očekávaného bajtu ze zdroje.
Délka záhlaví	4bitové pole známé jako "datový offset", které udává délku záhlaví segmentu TCP.
Reserved	6bitové pole, které je rezervováno pro budoucí použití.
Řídící bity	6bitové pole, které obsahuje bitové kódy nebo příznaky, které označují účel a funkci segmentu TCP.
Velikost okna	16bitové pole používané k označení počtu bajtů, které lze najednou přijmout.
Kontrolní součet	16bitové pole používané pro kontrolu chyb hlavičky segmentu a dat.
Urgent	16bitové pole používané k označení, zda jsou obsažená data naléhavá.

14.2.4 Aplikace, které používají TCP

TCP je dobrým příkladem toho, jak různé vrstvy sady protokolů TCP/IP mají specifické role. TCP zpracovává všechny úkoly spojené s rozdělením datového toku do segmentů, poskytuje spolehlivost, řídí tok dat a mění pořadí segmentů. TCP osvobozuje aplikaci od nutnosti spravovat

kteroukoli z těchto úloh. Aplikace, jako jsou ty zobrazené na obrázku, mohou jednoduše posílat datový tok do transportní vrstvy a využívat služeb TCP.



14.2.5 Zkontrolujte si, jak rozumíte výkladu – Přehled TCP

Ověřte si své znalosti TCP výběrem správné odpovědi na následující otázky.

1. Který protokol transportní vrstvy zajišťuje spolehlivé doručení se zachováním stejného pořadí?

a: ICMP
b: IP
c: TCP
d: UDP

2. Které tvrzení o TCP záhlaví je pravdivé?

a: Skládá se ze 4 polí v 8bajtovém záhlaví.
b: Skládá se z 8 polí v 10bajtovém záhlaví.
c: Skládá se z 10 polí ve 20bajtovém záhlaví.
d: Skládá se z 20 polí ve 40bajtovém záhlaví.

3. Které dvě aplikace by používaly protokol transportní vrstvy TCP? (Vyberte dvě.)

a: FTP
b: HTTP
c: ICMP

d: TFTP
e: VoIP

14.3.1 Funkce UDP

Tato část se bude zabývat UDP, co dělá a kdy je vhodné jej použít místo TCP. UDP je „best effort" přenosový protokol. UDP je odlehčený transportní protokol, který nabízí stejnou segmentaci dat a opětovné sestavení jako TCP, ale bez spolehlivosti TCP a řízení toku.

UDP je tak jednoduchý protokol, že je obvykle popsán z hlediska toho, co nedělá ve srovnání s TCP.

Mezi funkce UDP patří následující:

- Data jsou rekonstruována v pořadí, v jakém byla přijata.
- Žádné ztracené segmenty nebudou znovu odeslány.
- Nedochází k vytvoření relace – spojení.
- Odesílající není informován o dostupnosti zdroje.

Pro další informace o UDP vyhledejte na internetu příslušné RFC.

14.3.2 Hlavička UDP

UDP je bezestavový protokol, což znamená, že ani klient, ani server nesledují stav komunikační relace. Pokud je při použití protokolu UDP jako transportního protokolu vyžadována spolehlivost, musí ji zpracovat aplikace.

Jedním z nejdůležitějších požadavků pro poskytování živého videa a hlasu po síti je, aby data pokračovala rychle. Živé video a hlasové aplikace mohou tolerovat určitou ztrátu dat s minimálním nebo žádným znatelným efektem a dokonale se hodí pro UDP.

Bloky komunikace v UDP se nazývají datagramy nebo segmenty. Tyto datagramy jsou odesílány protokolem transportní vrstvy s nejlepší snahou (best effort).

Hlavička UDP je mnohem jednodušší než hlavička TCP, protože má pouze čtyři pole a vyžaduje 8 bajtů (tj. 64 bitů). Obrázek ukazuje pole v hlavičce UDP.

14.3.3 Pole záhlaví UDP

Tabulka identifikuje a popisuje čtyři pole v záhlaví (hlavičce) UDP.

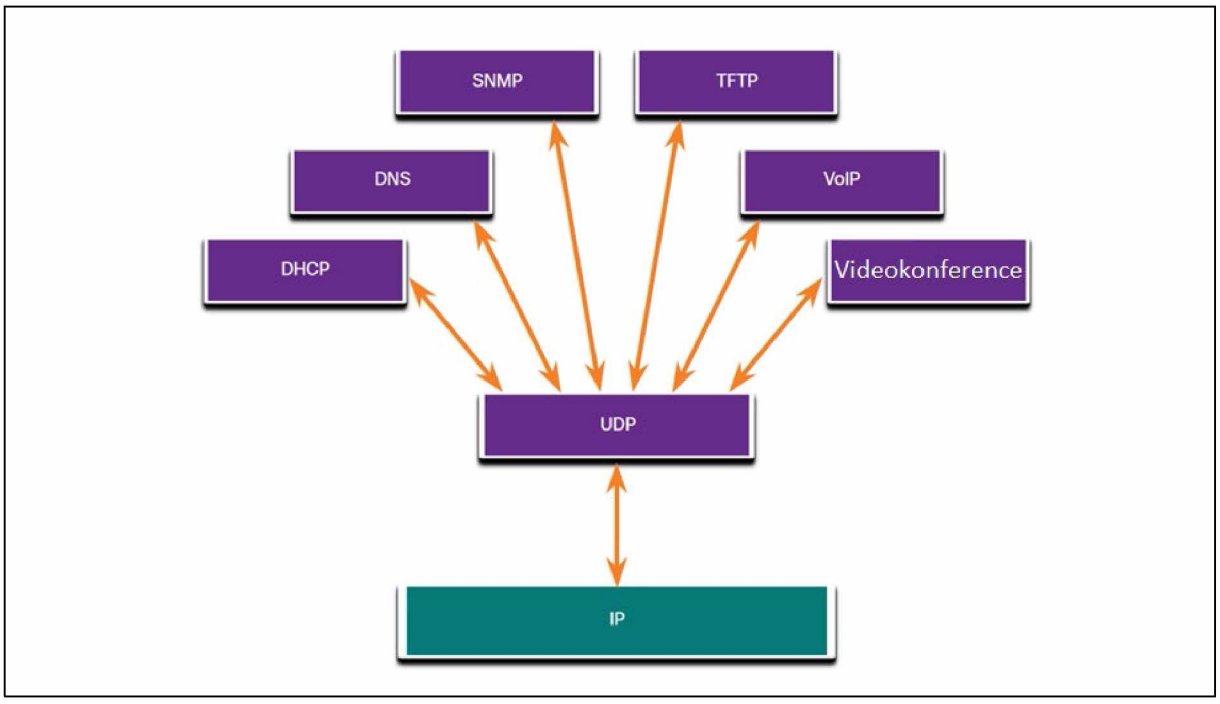
Pole záhlaví UDP	Popis
Zdrojový port	16bitové pole používané k identifikaci zdrojové aplikace podle čísla portu.
Cílový port	16bitové pole používané k identifikaci cílové aplikace podle čísla portu.
Délka	16bitové pole, které udává délku záhlaví datagramu UDP.
Kontrolní součet	16bitové pole používané pro kontrolu chyb hlavičky a dat datagramu.

14.3.4 Aplikace, které používají UDP

Existují tři typy aplikací, pro které je nejvhodnější UDP:

- Živé video a multimediální aplikace – Tyto aplikace mohou tolerovat určitou ztrátu dat, ale vyžadují malé nebo žádné zpoždění. Příklady zahrnují VoIP a živé streamování videa.
- Jednoduché aplikace žádostí a odpovědí – Aplikace s jednoduchými transakcemi, kde hostitel odešle požadavek a může nebo nemusí obdržet odpověď. Příklady zahrnují DNS a DHCP.
- Aplikace, které samy zvládají spolehlivost – Jednosměrná komunikace, kde řízení toku, detekce chyb, potvrzování a obnova chyb nejsou vyžadovány, nebo je může zpracovat až aplikační vrstva. Příklady zahrnují SNMP a TFTP.

Obrázek identifikuje aplikace, které vyžadují UDP.



Ačkoli DNS a SNMP standardně používají protokol UDP, oba mohou také používat TCP. DNS použije TCP, pokud je požadavek DNS nebo odpověď DNS delší než 512 bajtů, například když odpověď DNS obsahuje mnoho překladů názvů. Podobně v některých situacích může chtít správce sítě nakonfigurovat SNMP pro použití TCP.

14.3.5 Zkontrolujte si své znalosti – přehled UDP

Ověřte si, zda rozumíte UDP výběrem správné odpovědi na následující otázky.

1. Který z následujících protokolů je bezestavový protokol transportní vrstvy s nejlepším úsilím?

a: ICMP
b: IP
c: TCP
d: UDP

2. Které prohlášení hlavičky UDP je pravdivé?

a: Skládá se ze 4 polí v 8bajtovém záhlaví.
b: Skládá se z 8 polí v 10bajtovém záhlaví.
c: Skládá se z 10 polí ve 20bajtovém záhlaví.
d: Skládá se z 20 polí ve 40bajtovém záhlaví.

3. Které dvě aplikace by používaly protokol transportní vrstvy UDP? (Vyberte dvě.)

a: FTP
b: HTTP
c: ICMP
d: TFTP
e: VoIP

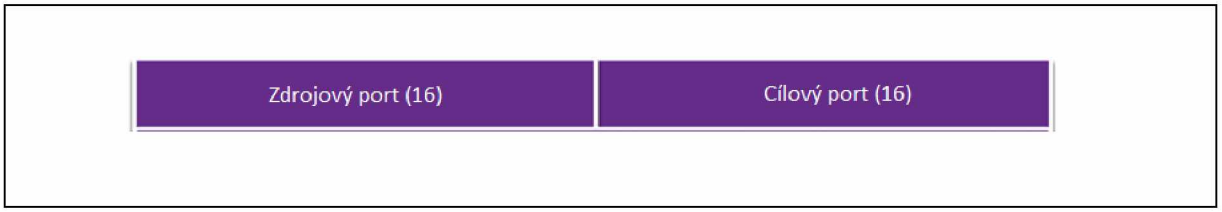
4. Která dvě pole jsou stejná v hlavičce TCP a UDP? (Vyberte dvě.)

a: Kontrolní bity
b: Číslo cílového portu
c: Pořadové číslo
d: Číslo zdrojového portu
e: Dobře známé číslo portu

14.4.1 Vícenásobná samostatná komunikace

Jak jste se dozvěděli, existují některé situace, ve kterých je TCP správným protokolem pro danou úlohu, a jiné situace, ve kterých by měl být použit protokol UDP. Bez ohledu na to, jaký typ dat se přenáší, TCP i UDP používají čísla portů.

Protokoly transportní vrstvy TCP a UDP používají čísla portů ke správě více současných konverzací. Jak je znázorněno na obrázku, pole záhlaví TCP a UDP identifikují číslo portu zdrojové a cílové aplikace.



Číslo zdrojového portu je přidruženo ke zdrojové aplikaci na místním hostiteli, zatímco číslo cílového portu je přidruženo k cílové aplikaci na vzdáleném hostiteli.

Předpokládejme například, že hostitel iniciuje požadavek na webovou stránku z webového serveru. Když hostitel zahájí požadavek webové stránky, hostitel dynamicky generuje číslo zdrojového portu, aby jednoznačně identifikoval konverzaci. Každý požadavek vygenerovaný hostitelem bude používat jiné dynamicky vytvořené zdrojové číslo portu. Tento proces umožňuje více konverzací současně.

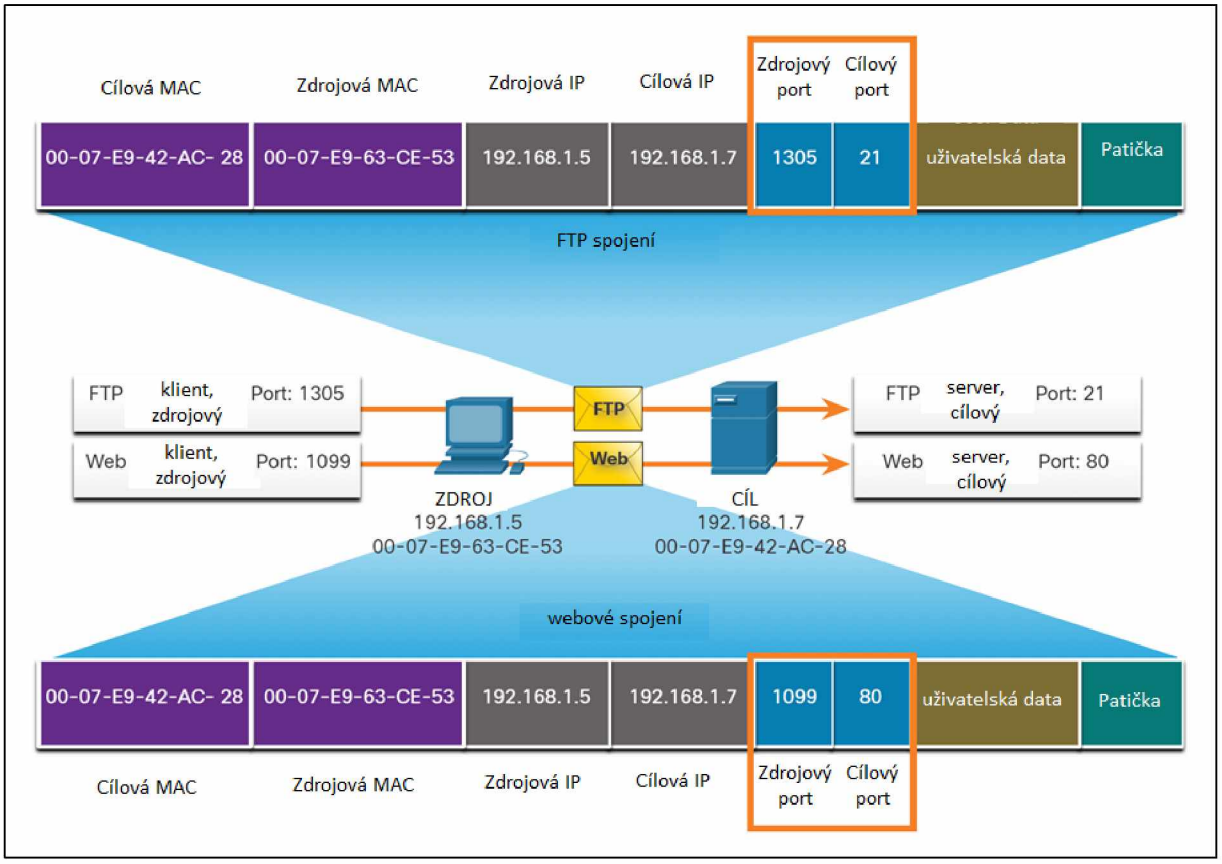
V požadavku je číslo cílového portu to, co identifikuje typ služby, která je požadována od cílového webového serveru. Například, když klient zadá port 80 v cílovém portu, server, který přijímá zprávu, ví, že jsou vyžádány webové služby.

Server může nabízet více než jednu službu současně, například webové služby na portu 80, zatímco na portu 21 nabízí navázání spojení FTP (File Transfer Protocol).

14.4.2 Socketové páry

Zdrojový a cílový port jsou umístěny v rámci segmentu. Segmenty jsou pak zapouzdřeny do IP paketu. IP paket obsahuje IP adresu zdroje a cíle. Kombinace zdrojové adresy IP a čísla zdrojového portu nebo cílové adresy IP a čísla cílového portu se nazývá socket.

V příkladu na obrázku PC současně požaduje FTP a webové služby z cílového serveru.



V tomto příkladu požadavek FTP generovaný počítačem obsahuje MAC adresy vrstvy 2 a adresy IP vrstvy 3. Požadavek také identifikuje číslo zdrojového portu 1305 (tj. dynamicky generovaný hostitelem) a cílový port, identifikující služby FTP na portu 21. Hostitel také požádal o webovou stránku ze serveru pomocí stejných adres vrstvy 2 a vrstvy 3 . Používá však číslo zdrojového portu 1099 (tj. dynamicky generované hostitelem) a cílový port identifikující webovou službu na portu 80.

Socket se používá k identifikaci serveru a služby požadované klientem. Klientský socket může vypadat takto, přičemž 1099 představuje číslo zdrojového portu: 192.168.1.5:1099

Socket na webovém serveru může být 192.168.1.7:80

Společně se tyto dva sockety spojí a vytvoří pár socketů: 192.168.1.5:1099, 192.168.1.7:80

Sockety umožňují více procesům běžícím na klientovi, aby se navzájem odlišily a aby se od sebe odlišilo více připojení k procesu serveru.

Číslo zdrojového portu funguje jako zpáteční adresa pro žádající aplikaci. Transportní vrstva sleduje tento port a aplikaci, která iniciovala požadavek, takže když je vrácena odpověď, může být předána správné aplikaci.

14.4.3 Skupiny čísel portů

Internet Assigned Numbers Authority (IANA) je organizace pro standardy zodpovědná za přidělování různých standardů adresování, včetně 16bitových čísel portů. 16 bitů používaných k identifikaci čísel zdrojového a cílového portu poskytuje rozsah portů od 0 do 65535.

IANA rozdělila rozsah čísel do následujících tří skupin portů.

Skupina portů	Číslo	Popis rozsahu
Známé porty	0 až 1 023	• Tato čísla portů jsou vyhrazena pro běžné nebo oblíbené služby a aplikace, jako jsou webové prohlížeče, e-mailové klienty a klienti vzdáleného přístupu. • Definované známé porty pro běžné serverové aplikace umožňují klientům snadno identifikovat požadovanou související službu.
Registrované porty	1 024 až 49 151	• Tato čísla portů přiděluje IANA žádající entitě pro použití s konkrétními procesy nebo aplikacemi. • Tyto procesy jsou primárně jednotlivé aplikace, které se uživatel rozhodl nainstalovat, spíše než běžné aplikace, které by obdržely dobře známé číslo portu. • Například společnost Cisco zaregistrovala port 1812 pro proces ověřování serveru RADIUS.
Soukromé a/nebo dynamické porty	49 152 až 65 535	• Tyto porty jsou také známé jako dočasné porty. • Operační systém klienta obvykle přiřazuje čísla portů dynamicky, když je zahájeno připojení ke službě. • Dynamický port se pak používá k identifikaci klientské aplikace během komunikace.

Poznámka: Některé klientské operační systémy mohou pro přiřazování zdrojových portů místo dynamických čísel portů používat registrovaná čísla portů.

Tabulka zobrazuje některá běžná známá čísla portů a jejich přidružené aplikace.

Číslo portu	Protokol	Aplikace
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name System (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server
68	UDP	Dynamic Host Configuration Protocol – klient
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol verze 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

Některé aplikace mohou používat TCP i UDP. DNS například používá UDP, když klienti odesílají požadavky na server DNS. Komunikace mezi dvěma servery DNS však vždy používá protokol TCP.

Chcete-li zobrazit úplný seznam čísel portů a souvisejících aplikací, vyhledejte na webu IANA registr portů.

14.4.4 Příkaz netstat

Nevysvětlená připojení TCP mohou představovat velkou bezpečnostní hrozbu. Mohou indikovat, že je něco nebo někdo připojen k místnímu hostiteli. Někdy je nutné vědět, která aktivní TCP spojení jsou otevřená, a běží na síťovém hostiteli. Netstat je důležitý síťový nástroj, který lze použít k ověření těchto připojení. Jak je znázorněno níže, zadejte příkaz netstat, abyste zobrazili seznam používaných protokolů, místní adresy a čísla portů, cizí adresy a čísla portů a stav připojení.

```
C:\> netstat

Active Connections

  Proto  Local Address          Foreign Address            State
  TCP    192.168.1.124:3126     192.168.0.2:netbios-ssn    ESTABLISHED
  TCP    192.168.1.124:3158     207.138.126.152:http       ESTABLISHED
  TCP    192.168.1.124:3159     207.138.126.169:http       ESTABLISHED
  TCP    192.168.1.124:3160     207.138.126.169:http       ESTABLISHED
  TCP    192.168.1.124:3161     sc.msn.com:http            ESTABLISHED
  TCP    192.168.1.124:3166     www.cisco.com:http         ESTABLISHED
(output omitted)
C:\>
```

Ve výchozím nastavení se příkaz netstat pokusí přeložit IP adresy na názvy domén a čísla portů na známé aplikace. Volbu -n lze použít k zobrazení IP adres a čísel portů v jejich číselné podobě.

14.4.5 Zkontrolujte své znalosti – čísla portů

Ověřte si, zda rozumíte číslům portů výběrem správné odpovědi na následující otázky.

1. Předpokládejme, že hostitel s IP adresou 10.1.1.10 chce požádat o webové služby ze serveru na 10.1.1.254. Která z následujících možností zobrazí správný pár socketů?

a: 1099:10.1.1.10, 80:10.1.1.254
b: 10.1.1.10:80, 10.1.1.254:1099
c: 10.1.1.10:1099, 10.1.1.254:80
d: 80:10.1.1.10, 1099:10.1.1.254

2. Která skupina portů obsahuje čísla portů pro aplikace FTP, HTTP a TFTP?

a: dynamické porty
b: soukromé porty
c: registrované porty
d: dobře známé porty

3. Který příkaz systému Windows zobrazí používané protokoly, místní adresu a čísla portů, zahraniční adresu a čísla portů a stav připojení?

a: ipconfig /all
b: ping
c: netstat
d: traceroute

14.5.1 Procesy TCP serveru

Základy TCP již znáte. Pochopení role čísel portů vám pomůže pochopit podrobnosti komunikačního procesu TCP. v tomto tématu se také dozvíte o procesech třícestného navázání spojení TCP a ukončení relace.

Každý proces aplikace běžící na serveru je nakonfigurován tak, aby používal číslo portu. Číslo portu je buď automaticky přiřazeno nebo konfigurováno ručně správcem systému.

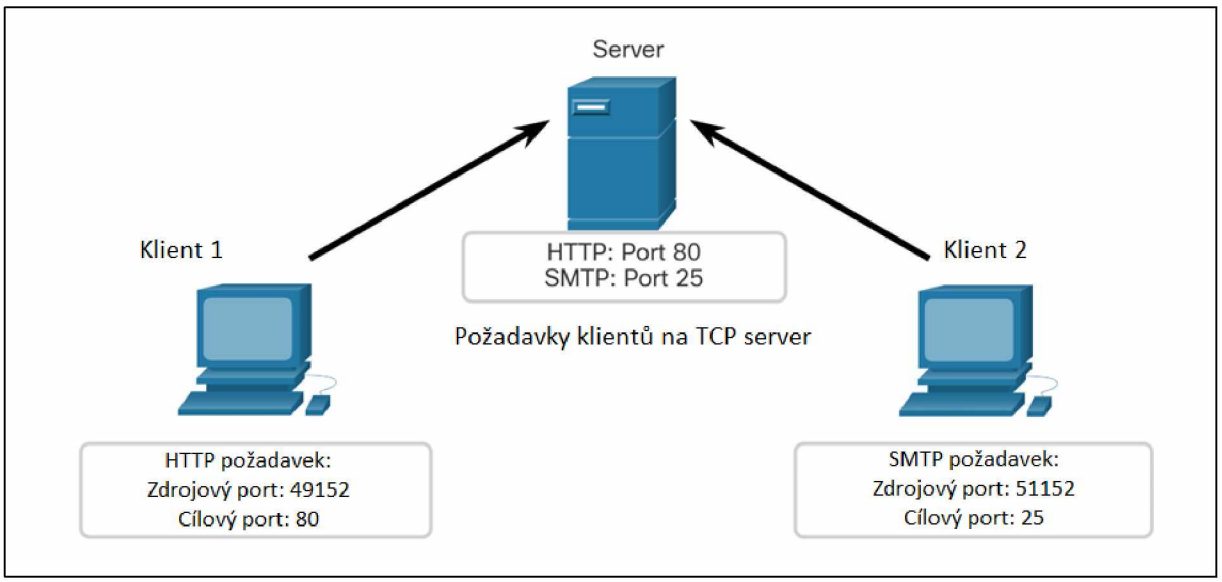
Jednotlivý server nemůže mít dvě služby přiřazené ke stejnému číslu portu v rámci stejné služby transportní vrstvy. Například hostitel, na kterém je spuštěna aplikace webového serveru a aplikace pro přenos souborů, nemohou mít obě nakonfigurované pro použití stejného portu, jako je port TCP 80.

Aktivní serverová aplikace přiřazená ke konkrétnímu portu je považována za otevřenou, což znamená, že transportní vrstva přijímá a zpracovává segmenty adresované tomuto portu. Jakýkoli příchozí požadavek klienta adresovaný správnému socketu je přijat a data jsou předána serverové aplikaci. Na serveru může být současně otevřeno mnoho portů, jeden pro každou aktivní serverovou aplikaci.

Výběrem jednotlivých karet získáte další informace o procesech serveru TCP.

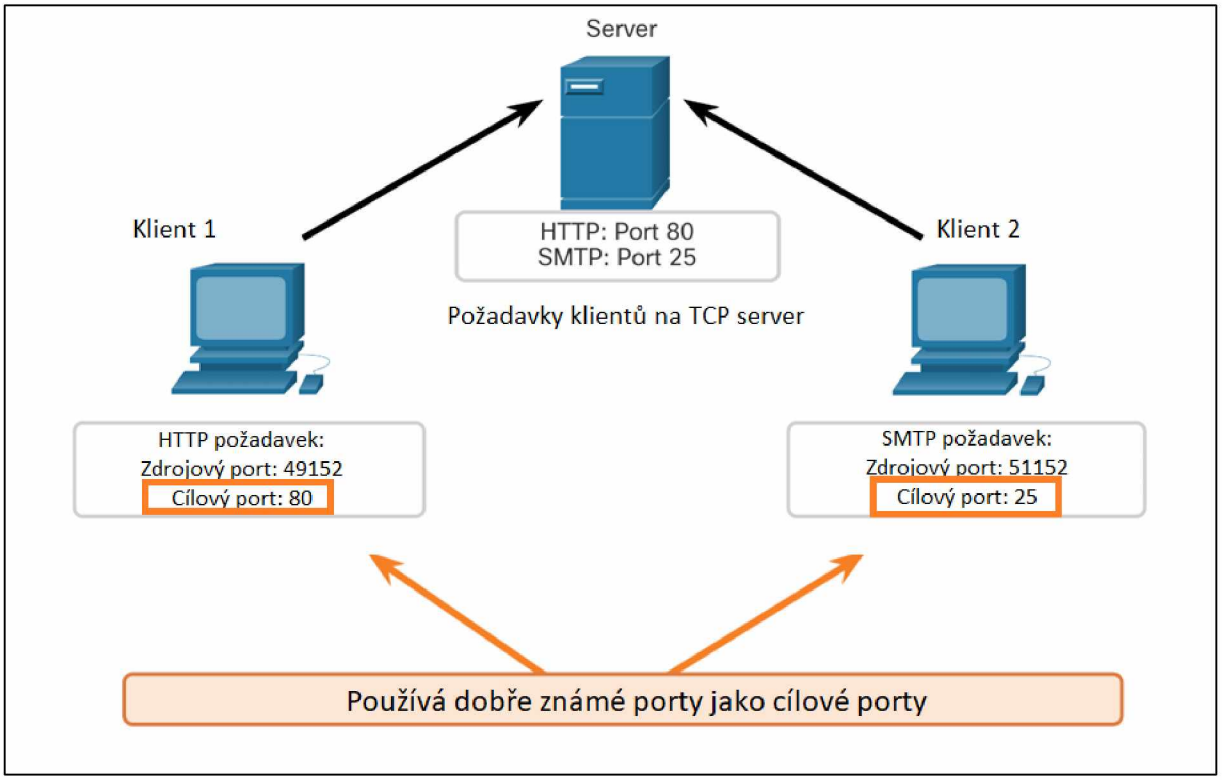
Klienti odesílající požadavky TCP

Klient 1 požaduje webové služby a Klient 2 požaduje e-mailovou službu stejného serveru.



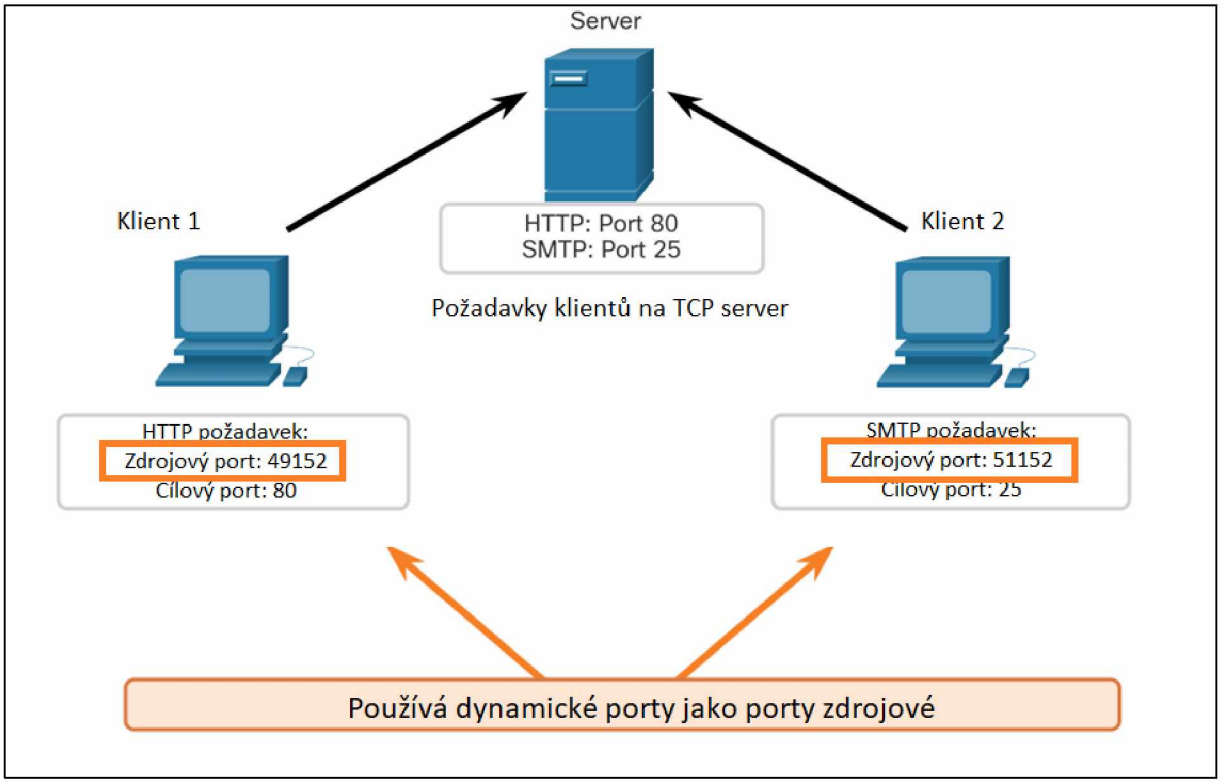
Cílové porty požadavku

Klient 1 požaduje webové služby pomocí známého cílového portu 80 (HTTP) a Klient 2 požaduje e-mailovou službu pomocí známého portu 25 (SMTP).



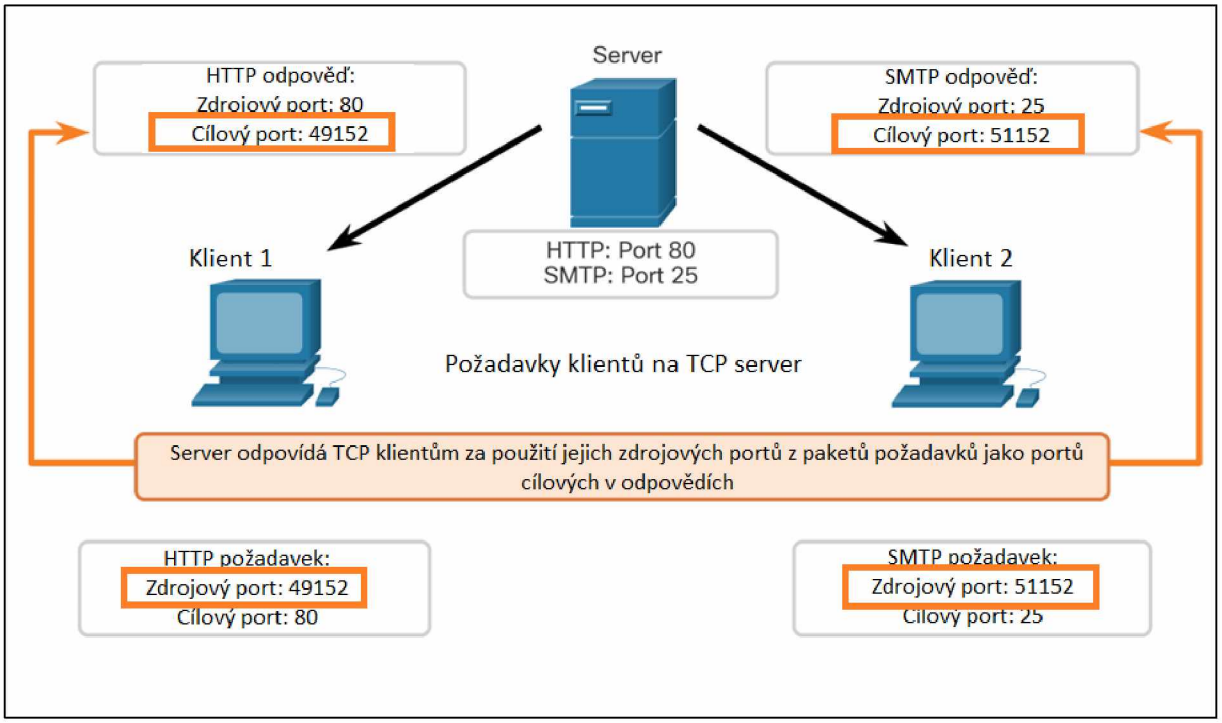
Zdrojové porty požadavku

Požadavky klienta dynamicky generují číslo zdrojového portu. v tomto případě Klient 1 používá zdrojový port 49152 a Klient 2 používá zdrojový port 51152.



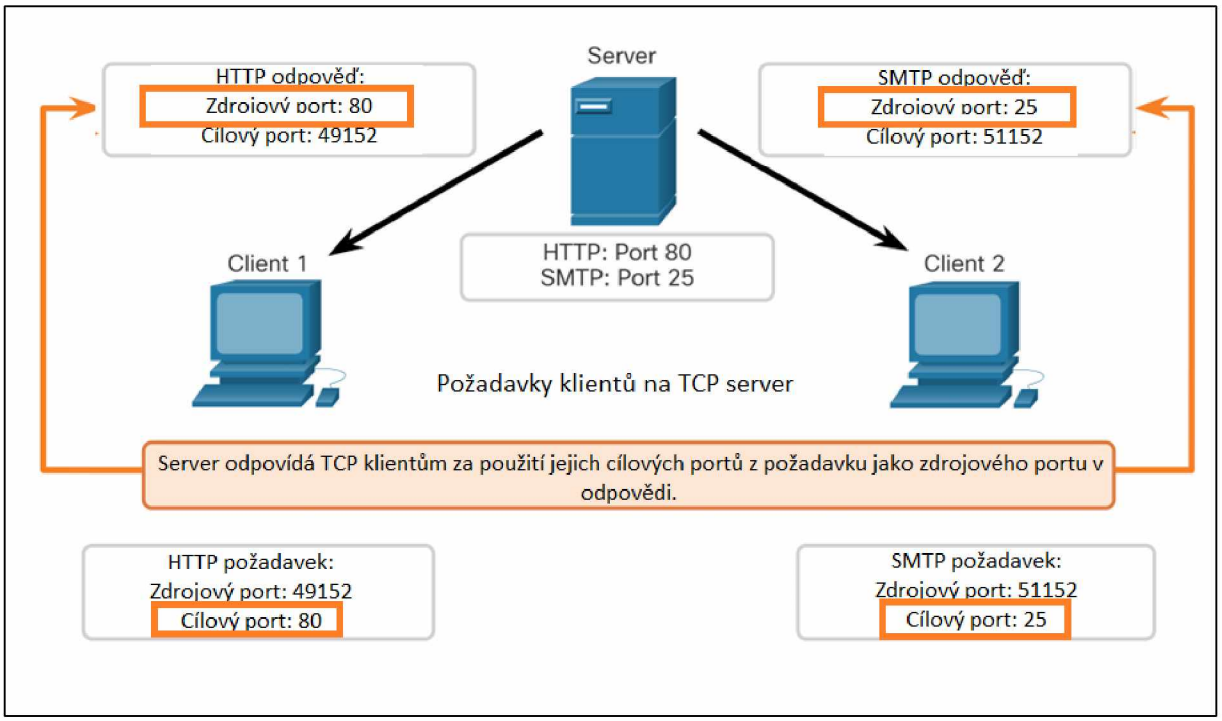
Cílové porty odpovědi

Když server odpoví na požadavky klienta, obrátí cílový a zdrojový port původního požadavku. Všimněte si, že odpověď serveru na webový požadavek má nyní cílový port 49152 a e-mailová odpověď má nyní cílový port 51152.



Zdrojové porty odpovědi

Zdrojový port v odpovědi serveru je původní cílový port v počátečních požadavcích.



14.5.2 Navázání spojení TCP

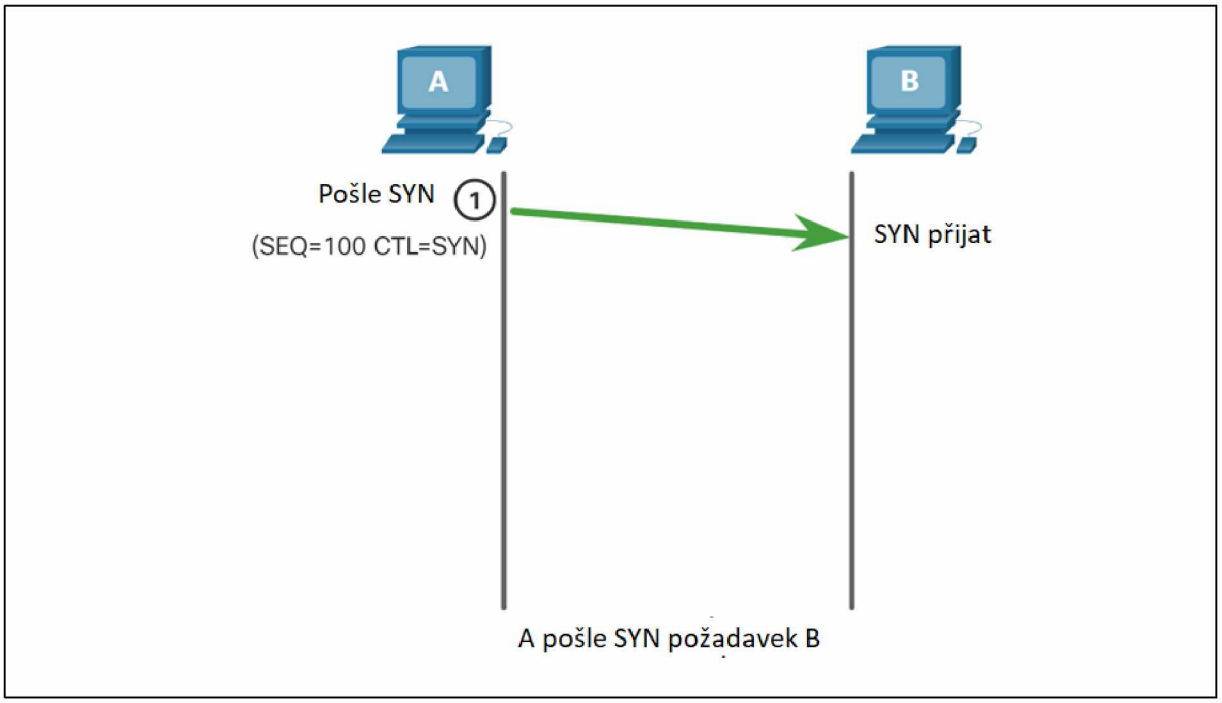
V některých kulturách, když se dva lidé setkají, často se pozdraví potřesením rukou. Obě strany chápou akt podání ruky jako signál přátelského pozdravu. Síťová připojení jsou podobná. v TCP spojení naváže hostitelský klient spojení se serverem pomocí třícestného procesu třesení rukou – handshake.

Výběrem jednotlivých karet získáte další informace o každém kroku navázání spojení TCP.

Krok 1. SYN | Krok 2. ACK a SYN | Krok 3. ACK

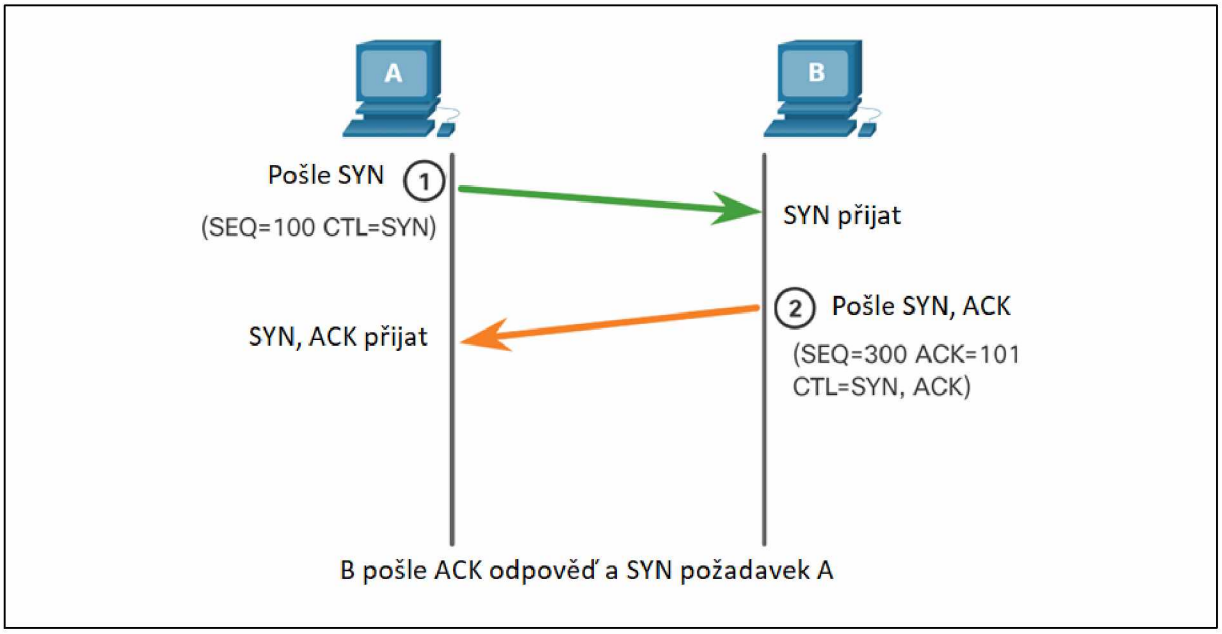
Krok 1. SYN

Iniciující klient požaduje komunikační relaci klient-server se serverem.



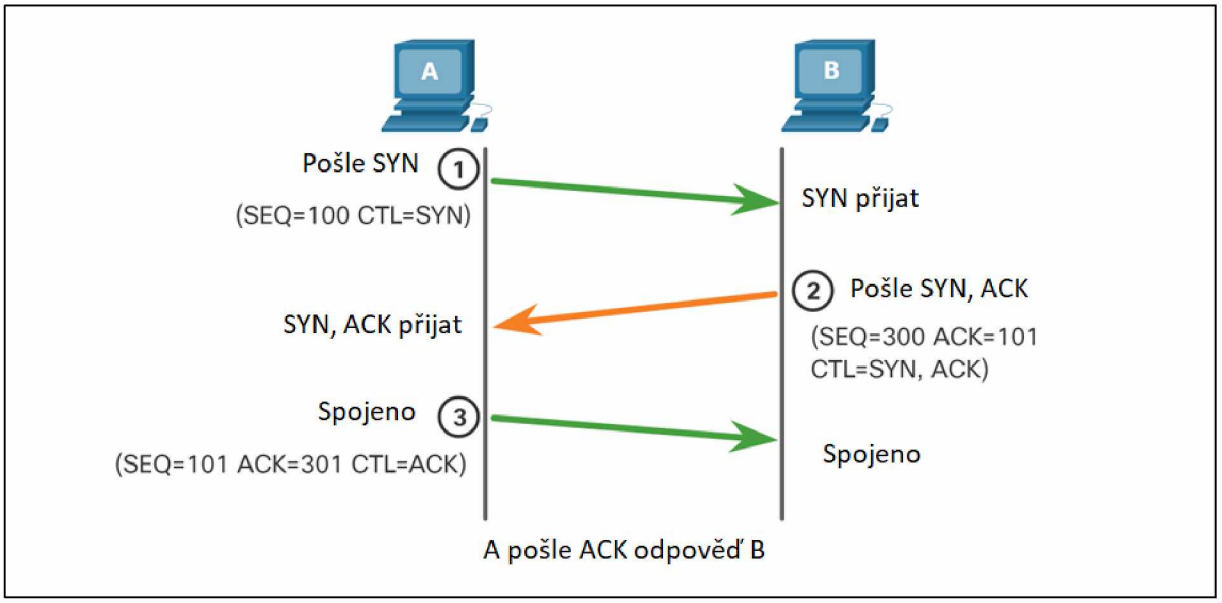
Krok 2. ACK a SYN

Server potvrdí komunikační relaci mezi klientem a serverem a požádá o komunikační relaci server-klient.



Krok 3. ACK

Iniciující klient potvrdí relaci komunikace server-klient.



Třícestný handshake ověří, že cílový hostitel je k dispozici pro komunikaci. v tomto příkladu hostitel A ověřil, že hostitel B je dostupný.

14.5.3 Ukončení relace

Chcete-li ukončit připojení, musí být v záhlaví segmentu nastaven ovládací příznak Finish (FIN). k ukončení každé jednosměrné TCP relace se používá obousměrný handshake, který se skládá ze

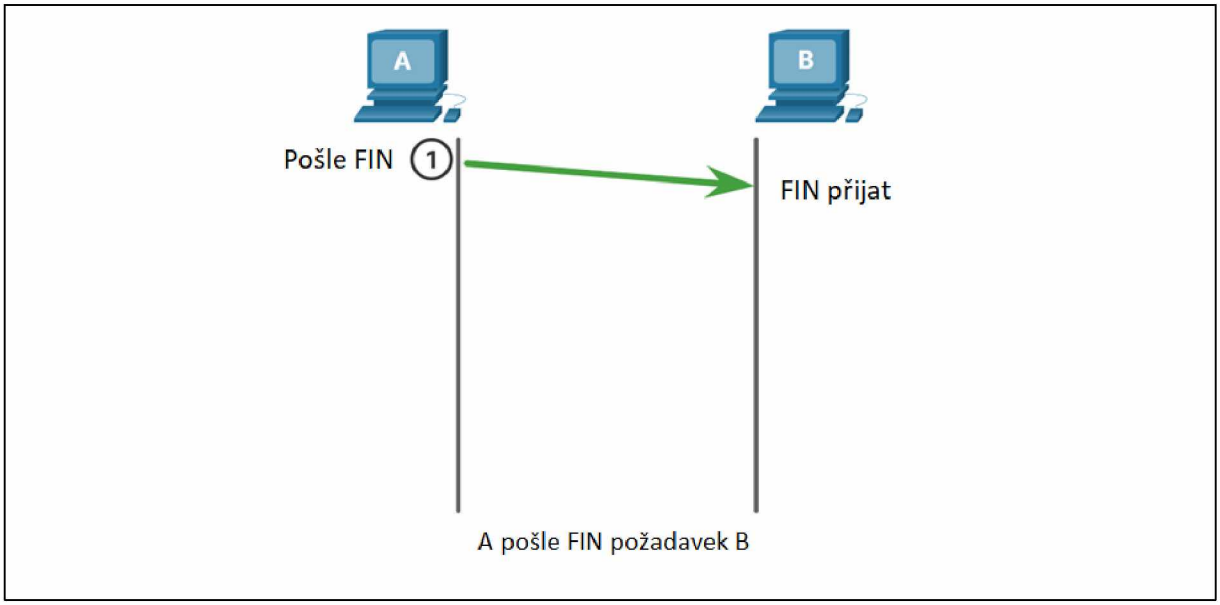
segmentu FIN a segmentu potvrzení (ACK). Proto k ukončení jedné konverzace podporované protokolem TCP jsou k ukončení obou relací potřeba čtyři výměny. Ukončení může iniciovat klient nebo server.

V tomto příkladu jsou termíny klient a server použity pro zjednodušení jako reference, ale proces ukončení mohou zahájit libovolní dva hostitelé, kteří mají otevřenou relaci.

Výběrem jednotlivých karet získáte další informace o krocích ukončení relace.

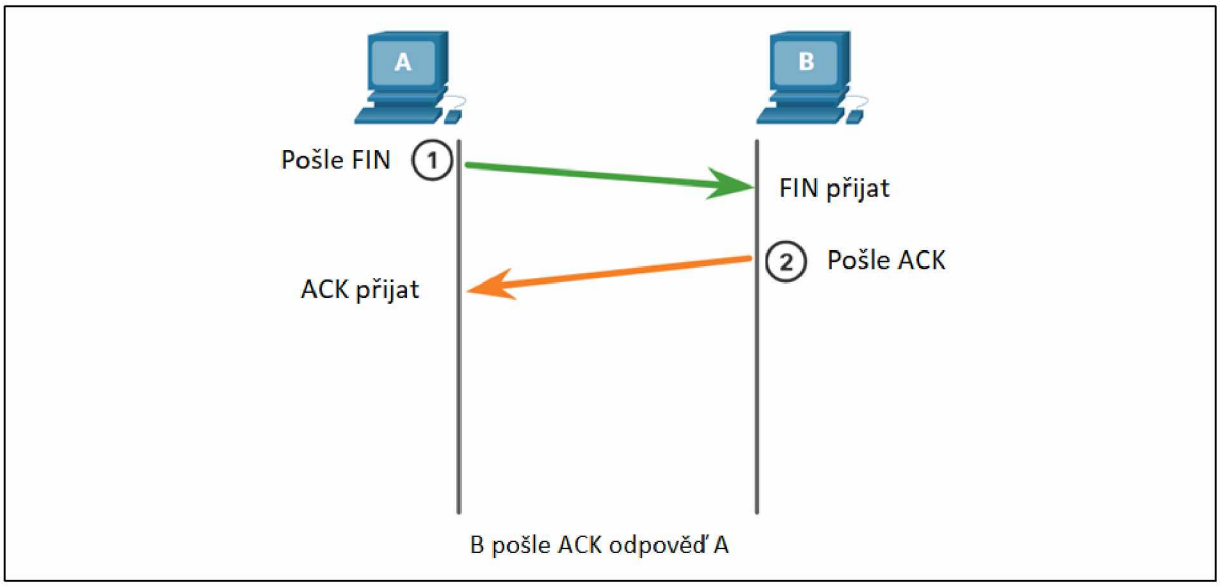
Krok 1. FIN

Když klient nemá žádná další data k odeslání v proudu, odešle segment s nastaveným příznakem FIN.



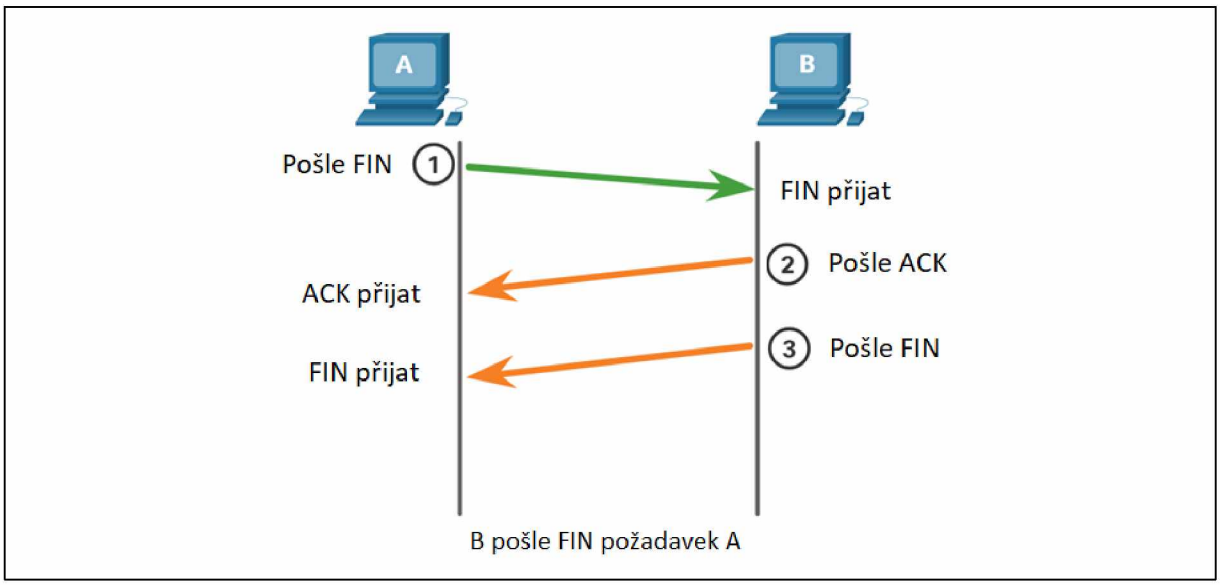
Krok 2. ACK

Server odešle ACK pro potvrzení přijetí FIN pro ukončení relace od klienta k serveru.



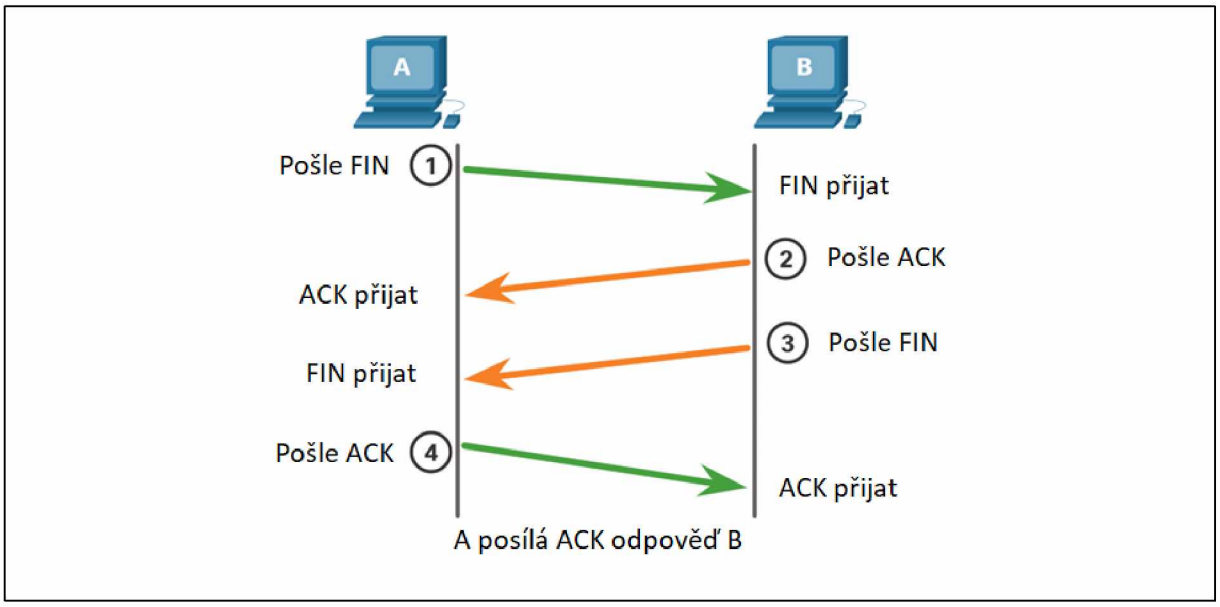
Krok 3. FIN

Server odešle FIN klientovi, aby ukončil relaci mezi serverem a klientem.



Krok 4. ACK

Klient odpoví ACK pro potvrzení FIN ze serveru.



Po potvrzení všech segmentů je relace uzavřena.

14.5.4 Analýza třícestného handshake TCP

Hostitelé udržují stav, sledují každý datový segment v rámci relace a vyměňují si informace o přijatých datech pomocí informací v hlavičce TCP. TCP je plně duplexní protokol, kde každé spojení představuje dvě jednosměrné komunikační relace. k navázání spojení hostitelé provedou třícestný handshake. Jak je znázorněno na obrázku, řídicí bity v hlavičce TCP indikují průběh a stav připojení.

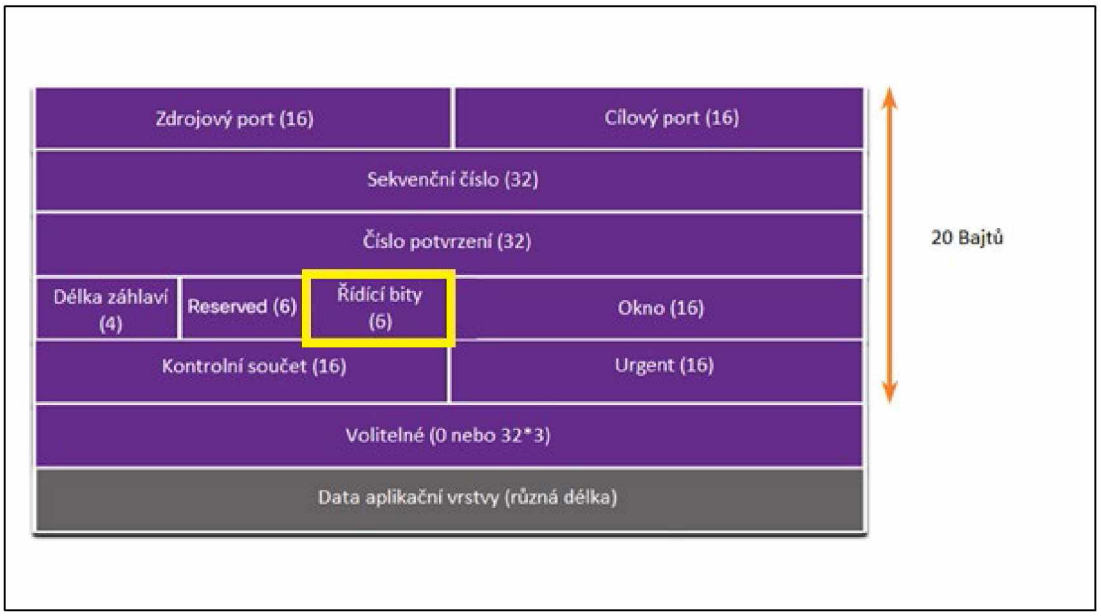
Toto jsou funkce třícestného „podání ruky“:

- Zjistí, že cílové zařízení je přítomno v síti.
- Ověřuje, že cílové zařízení má aktivní službu a přijímá požadavky na číslo cílového portu, které hodlá použít iniciující klient.
- Informuje cílové zařízení, že zdrojový klient zamýšlí navázat komunikační relaci na tomto čísle portu.

Po dokončení komunikace se relace ukončí a spojení se ukončí. Mechanismy připojení a relace umožňují funkci spolehlivosti TCP.

Schéma – pole záhlaví segmentu TCP se zvýrazněným polem řídicích bitů o 6 bitech

Pole řídicích bitů



Šest bitů v poli řídící bity (Control Bits) hlavičky TCP segmentu je také známo jako příznaky. Příznak je bit, který je buď zapnutý (1), nebo vypnutý (0).

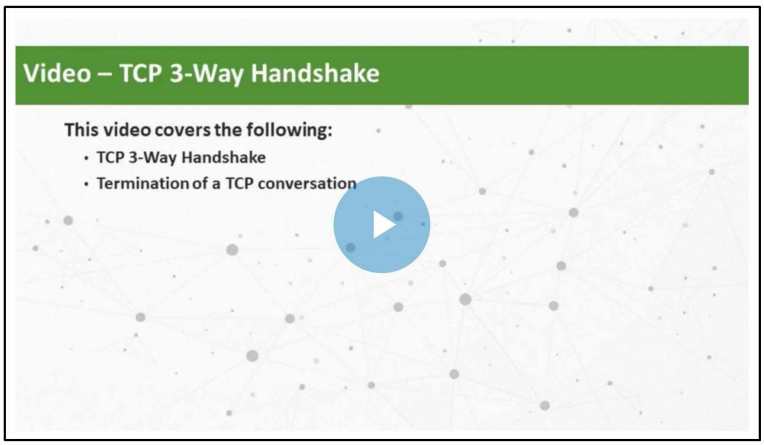
Šest příznaků řídicích bitů je následujících:

- URG – naléhavé (URGENT) pole ukazatele významnosti
- ACK – příznak potvrzení používaný při navazování spojení a ukončení relace
- PSH – funkce Push
- RST – resetuje připojení, když dojde k chybě nebo vypršení časového limitu
- SYN – synchronizace pořadových čísel, používá se při navazování spojení
- FIN – žádná další data od odesílatele, a používá se při ukončení relace

Prohledejte internet a zjistěte více o příznacích (flags) PSH a URG.

14.5.5 Video – TCP Třícestný handshake

Kliknutím na Přehrát na obrázku zobrazíte videoukázku TCP 3-Way handshake pomocí Wireshark.



14.5.6 Ověřte si své znalosti – proces komunikace TCP

Ověřte si své znalosti o procesu komunikace TCP výběrem správné odpovědi na následující otázky.

1. Které z následujících by byly platné zdrojové a cílové porty pro hostitele připojujícího se k e-mailovému serveru?

a: Zdroj: 25, Cíl: 49152
b: Zdroj: 80, Cíl: 49152
c: Zdroj: 49152, Cíl: 25
d: Zdroj: 49152, Cíl: 80

2. Které příznaky řídicího bitu se používají během třícestného handshake?

a: ACK a FIN
b: FIN a RESET
c: RESET a SYN
d: SYN a ACK

3. Kolik výměn je potřeba k ukončení obou relací mezi dvěma hostiteli?

a: jedna výměna
b: dvě výměny
c: tři výměny
d: čtyři výměny
e: pět výměn

14.6.1 Spolehlivost TCP – zaručené doručení a doručení ve správném pořadí

Důvodem, proč je TCP pro některé aplikace vhodnějším protokolem, je to, že na rozdíl od UDP znovu odesílá zahozené (ztracené) pakety a čísluje pakety, aby před jejich zkompletováním znal jejich správné pořadí. TCP může také pomoci udržovat tok paketů, aby nedošlo k přetížení zařízení. Toto téma podrobně popisuje tyto funkce TCP.

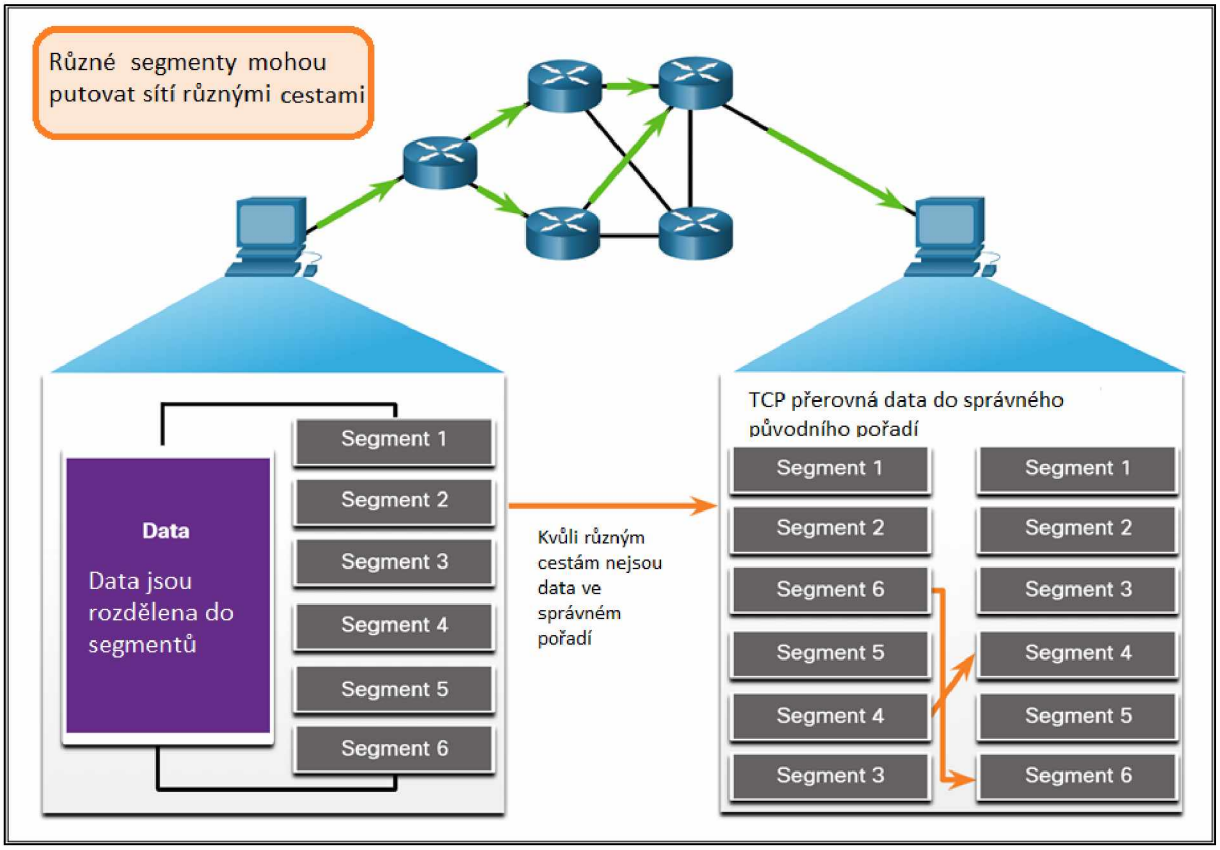
Mohou nastat situace, kdy segmenty TCP nedorazí do cíle. Jindy mohou segmenty TCP dorazit mimo pořadí. Aby původní zpráva byla příjemci srozumitelná, musí být přijata všechna data a data v těchto segmentech musí být znovu sestavena do původního pořadí. k dosažení tohoto cíle jsou v záhlaví každého paketu přiřazena sekvenční čísla. Pořadové číslo představuje první datový bajt segmentu TCP.

Během nastavování relace je nastaveno počáteční pořadové číslo (ISN). Toto ISN představuje počáteční hodnotu bajtů, které jsou přenášeny do přijímající aplikace. Jak jsou data přenášena během relace, pořadové číslo se zvyšuje o počet bajtů, které byly přeneseny. Toto sledování datových bajtů umožňuje jedinečně identifikovat a potvrdit každý segment. Poté lze identifikovat chybějící segmenty.

ISN nezačíná na jedničce, ale v podstatě jde o náhodné číslo. To má zabránit určitým typům škodlivých útoků. Pro jednoduchost budeme pro příklady v této kapitole používat ISN 1.

Pořadová čísla segmentů udávají, jak znovu sestavit a uspořádat přijaté segmenty, jak je znázorněno na obrázku.

Schéma – i když se segmenty mohou ubírat různými cestami a do cíle dorazit mimo pořadí, TCP má schopnost změnit pořadí segmentů. Segmenty TCP se v cíli znovu uspořádají:

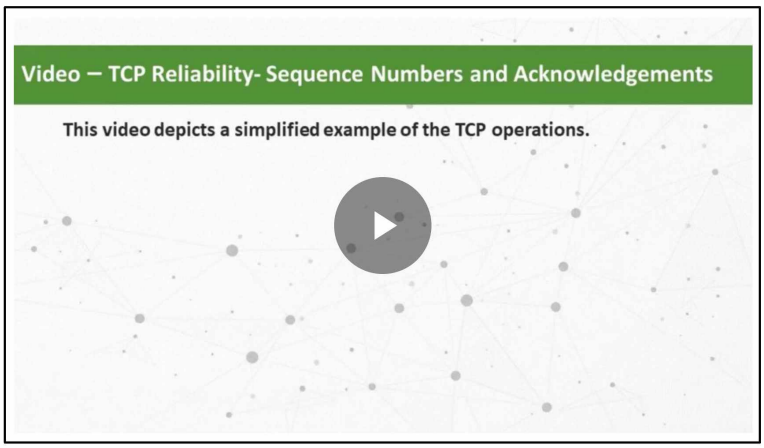


Přijímající proces TCP umístí data ze segmentu do přijímací vyrovnávací paměti. Segmenty jsou poté umístěny ve správném pořadí a po opětovném sestavení jsou předány aplikační vrstvě. Všechny segmenty, které dorazí s pořadovými čísly, která jsou mimo pořadí, jsou uchovány pro pozdější zpracování. Poté, když dorazí segmenty s chybějícími bajty, jsou tyto segmenty doplněny, zkompletovány a zpracovány ve správném pořadí.

14.6.2 Video – TCP Spolehlivost – Sekvenční čísla a potvrzení

Jednou z funkcí TCP je zajistit, aby každý segment dosáhl svého cíle. Služby TCP na cílovém hostiteli potvrzují data, která byla přijata zdrojovou aplikací.

Kliknutím na Přehrát na obrázku zobrazíte lekci o sekvenčních číslech TCP a potvrzeních.



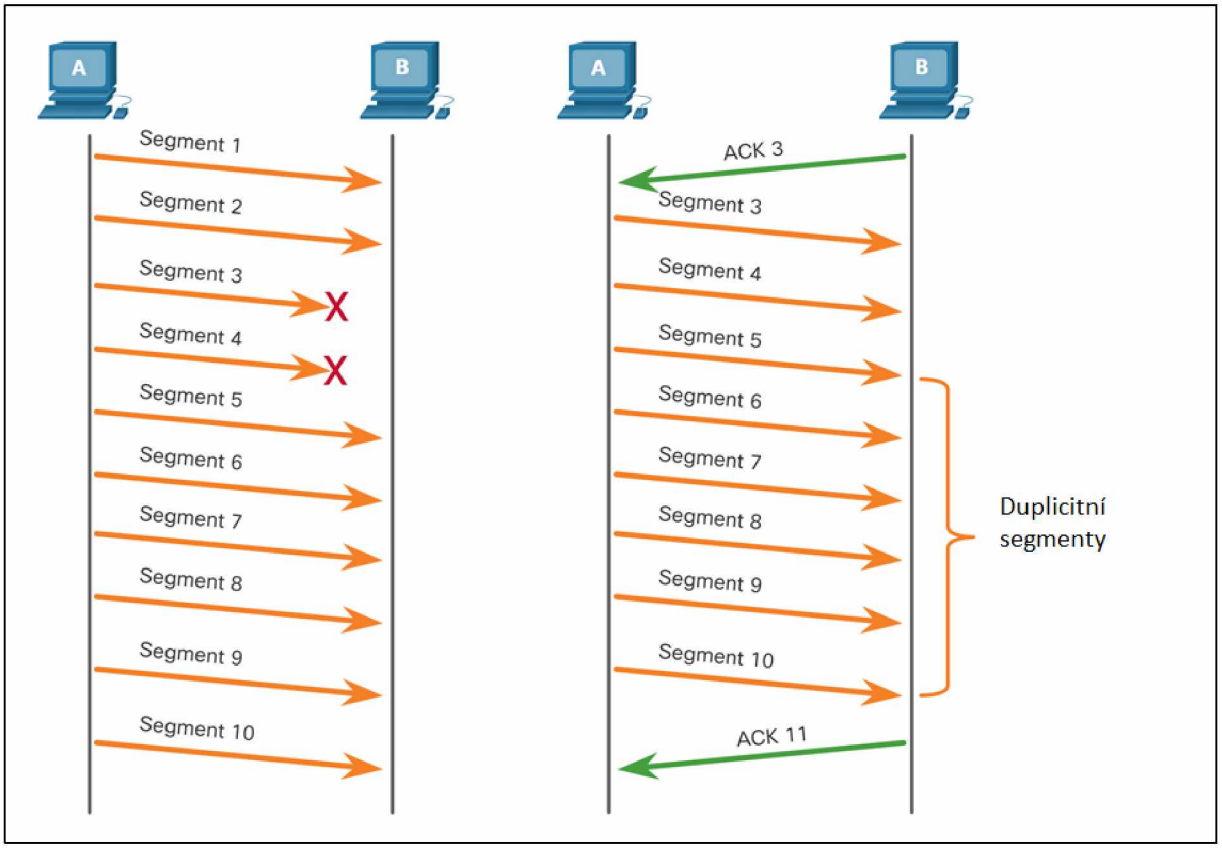
14.6.3 Spolehlivost TCP – ztráta dat a opakovaný přenos

Bez ohledu na to, jak dobře je síť navržena, občas dochází ke ztrátě dat. TCP poskytuje metody řízení těchto ztrát segmentů. Mezi nimi je mechanismus pro opakované vysílání segmentů pro nepotvrzená data.

Sekvenční (SEQ) číslo a potvrzovací (ACK) číslo se používají společně k potvrzení příjmu bajtů dat obsažených v přenášených segmentech. Číslo SEQ identifikuje první bajt dat v přenášeném segmentu. TCP používá číslo ACK odeslané zpět do zdroje k označení dalšího bajtu, který přijímač očekává, že přijme. Říká se tomu „expectational acknowledgement".

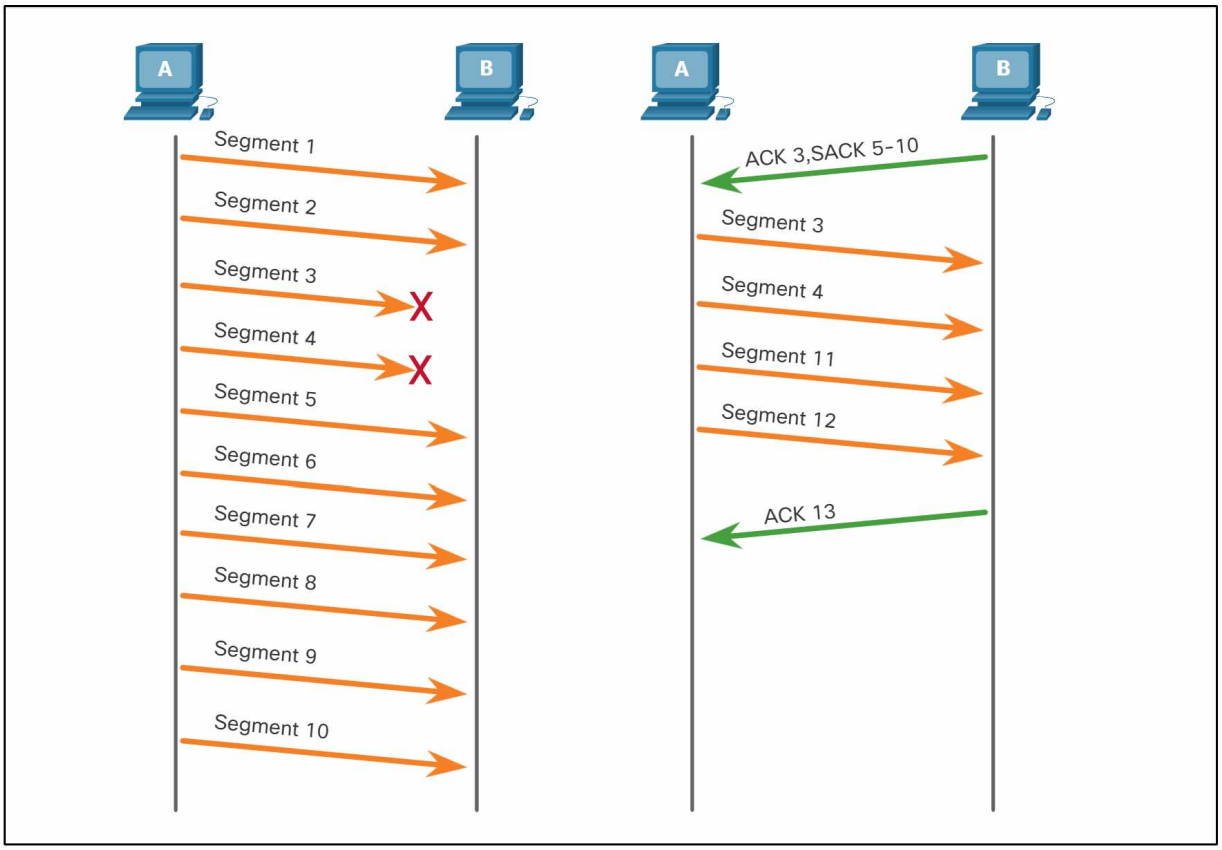
Před pozdějšími vylepšeními mohl TCP potvrdit pouze další očekávaný bajt. Například na obrázku s použitím čísel segmentů pro zjednodušení odesílá hostitel a segmenty 1 až 10 hostiteli B. Pokud dorazí všechny segmenty kromě segmentů 3 a 4, hostitel B odpoví potvrzením, že dalším očekávaným segmentem je segment 3. Hostitel a nemá tušení, zda dorazily nějaké další segmenty nebo ne. Hostitel a by proto znovu odeslal segmenty 3 až 10. Pokud by všechny znovu odeslané segmenty dorazily úspěšně, segmenty 5 až 10 by byly duplicitní. To může vést ke zpožděním, přetížení a neefektivitě.

Schéma – PCA posílá 10 segmentů na PCB, ale segmenty 3 a 4 nedorazí. Takže počínaje segmentem 3 PCA znovu odešle segmenty 3 až 10, i když PCB potřeboval pouze segmenty 3 a 4



Hostitelské operační systémy dnes obvykle využívají volitelnou funkci TCP nazvanou selektivní potvrzení (SACK), vyjednanou během třístranného handshake. Pokud oba hostitelé podporují SACK, přijímač může explicitně potvrdit, které segmenty (bajty) byly přijaty, včetně všech nesouvislých segmentů. Odesílající hostitel by tedy musel znovu odeslat pouze chybějící data. Například na dalším obrázku, pro zjednodušení opět s použitím čísel segmentů, hostitel a posílá segmenty 1 až 10 hostiteli B. Pokud dorazí všechny segmenty kromě segmentů 3 a 4, hostitel B může potvrdit, že přijal segmenty 1 a 2 (ACK 3) a selektivně potvrdí segmenty 5 až 10 (SACK 5-10). Hostitel a by musel znovu odeslat pouze segmenty 3 a 4.

Schéma – PCA odesílá 10 segmentů na PCB, ale segmenty 3 a 4 nedorazí. Tentokrát PCB pošle ack 3 a sack 5-10, čímž dá PCA vědět, že má znovu odeslat chybějící segmenty 3 a 4 a pokračovat segmentem 11



Poznámka: TCP obvykle odesílá potvrzení ACK pro každý druhý paket, ale toto chování mohou změnit další faktory, které přesahují rámec tohoto tématu.

TCP používá časovače, aby věděl, jak dlouho čekat před opětovným odesláním segmentu. Na obrázku si přehrajte video a kliknutím na odkaz stáhněte soubor PDF. Video a soubor PDF zkoumají ztrátu dat TCP a opakovaný přenos.

14.6.4 Video – TCP spolehlivost – Ztráta dat a znovuposílání

Kliknutím na Přehrát na obrázku zobrazíte lekci o opakovaném přenosu TCP.

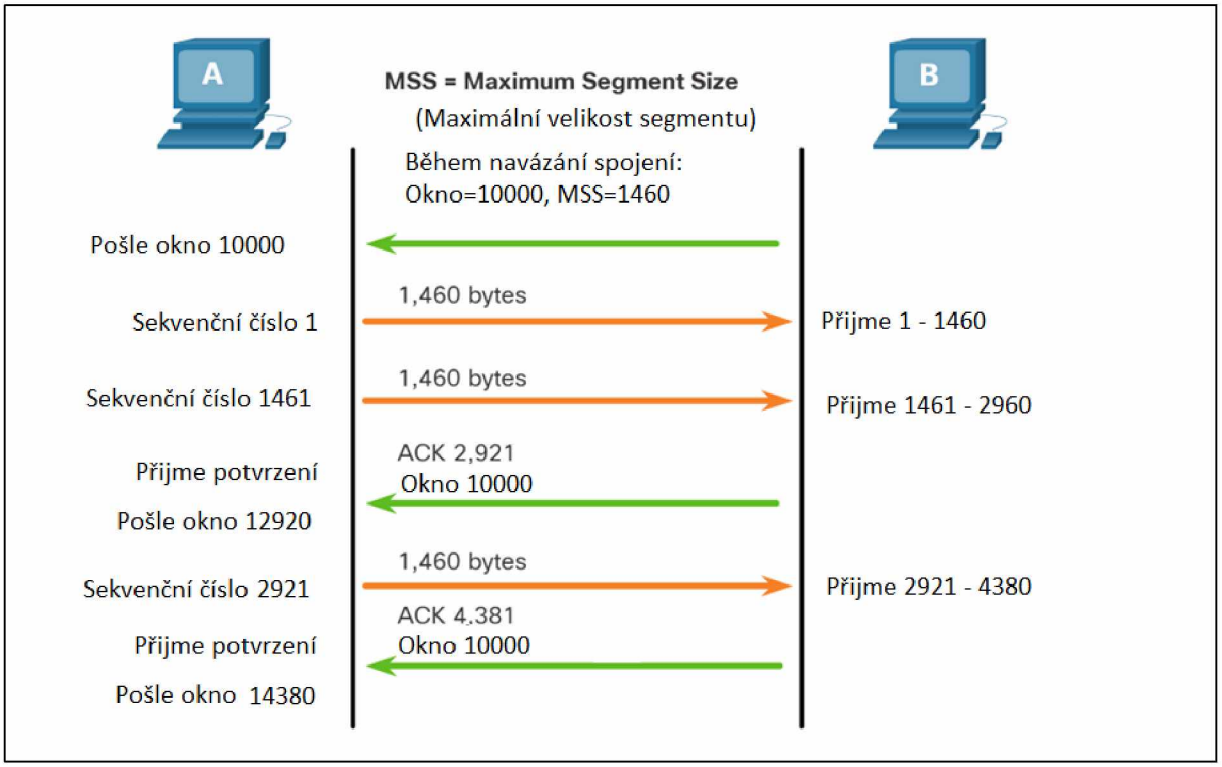
14.6.5 Řízení toku TCP – velikost okna a potvrzení

TCP také poskytuje mechanismy pro řízení toku. Řízením toku je určeno množství dat, které může cíl spolehlivě přijmout a zpracovat. Řízení toku pomáhá udržovat spolehlivost přenosu TCP úpravou rychlosti toku dat mezi zdrojem a cílem pro danou relaci. Aby toho bylo dosaženo, obsahuje hlavička TCP 16bitové pole nazývané velikost okna.

Obrázek ukazuje příklad velikosti okna a potvrzení.

Schéma – PCB odesílající PCA sjednanou velikost okna 10 000 bajtů a maximální velikost segmentu 1460 bajtů. PCA začne odesílat segmenty začínající pořadovým číslem 1. Potvrzení

z PCB lze odeslat bez čekání na dosažení velikosti okna a velikost okna lze upravit pomocí PCA vytvořením posuvného okna. Příklad velikosti okna TCP.



Velikost okna určuje počet bajtů, které lze odeslat, než se očekává potvrzení. Číslo potvrzení ACK je číslo dalšího očekávaného bajtu.

Velikost okna je počet bajtů, které může cílové zařízení relace TCP přijmout a zpracovat najednou. v tomto příkladu je počáteční velikost okna PC B pro relaci TCP 10 000 bajtů. Počínaje prvním bajtem, byte číslo 1, poslední bajt, který může PC a odeslat bez přijetí potvrzení, je bajt 10 000. Toto je známé jako okno odesílání PC A. Velikost okna je zahrnuta v každém segmentu TCP, takže cíl může velikost okna kdykoli upravit v závislosti na dostupnosti vyrovnávací paměti.

Počáteční velikost okna je dohodnuta při navázání TCP relace během třícestného handshake. Zdrojové zařízení musí omezit počet bajtů odeslaných do cílového zařízení na základě velikosti okna cíle. Teprve poté, co zdrojové zařízení obdrží potvrzení, že bajty byly přijaty, může pokračovat v odesílání dalších dat pro relaci. Cíl obvykle nebude čekat na přijetí všech bajtů pro jeho velikost okna, než odpoví potvrzením. Jakmile jsou bajty přijímány a zpracovávány, cíl bude průběžně odesílat potvrzení, aby informoval zdroj, že může pokračovat v odesílání dalších bajtů.

Například je typické, že PC B nebude čekat, dokud nebude přijato všech 10 000 bajtů, než odešle potvrzení. To znamená, že PC a může upravit své vysílací okno, když přijímá potvrzení z PC B. Jak je znázorněno na obrázku, když PC a obdrží potvrzení s číslem potvrzení 2 921, což je další očekávaný bajt. Okno odeslání PC a se zvýší o 2 920 bajtů. Tím se změní okno odesílání z 10 000 bajtů na 12 920. PC a může nyní pokračovat v odesílání až dalších 10 000 bajtů do PC B, pokud neodešle více, než je jeho nové okno odesílání na 12 920.

Potvrzení odesílání cíle při zpracování přijatých bajtů a neustálé nastavování okna pro odesílání zdroje se nazývá posuvná okna (sliding windows). v předchozím příkladu se okno odesílání PC a zvýší nebo posune o dalších 2 921 bajtů z 10 000 na 12 920.

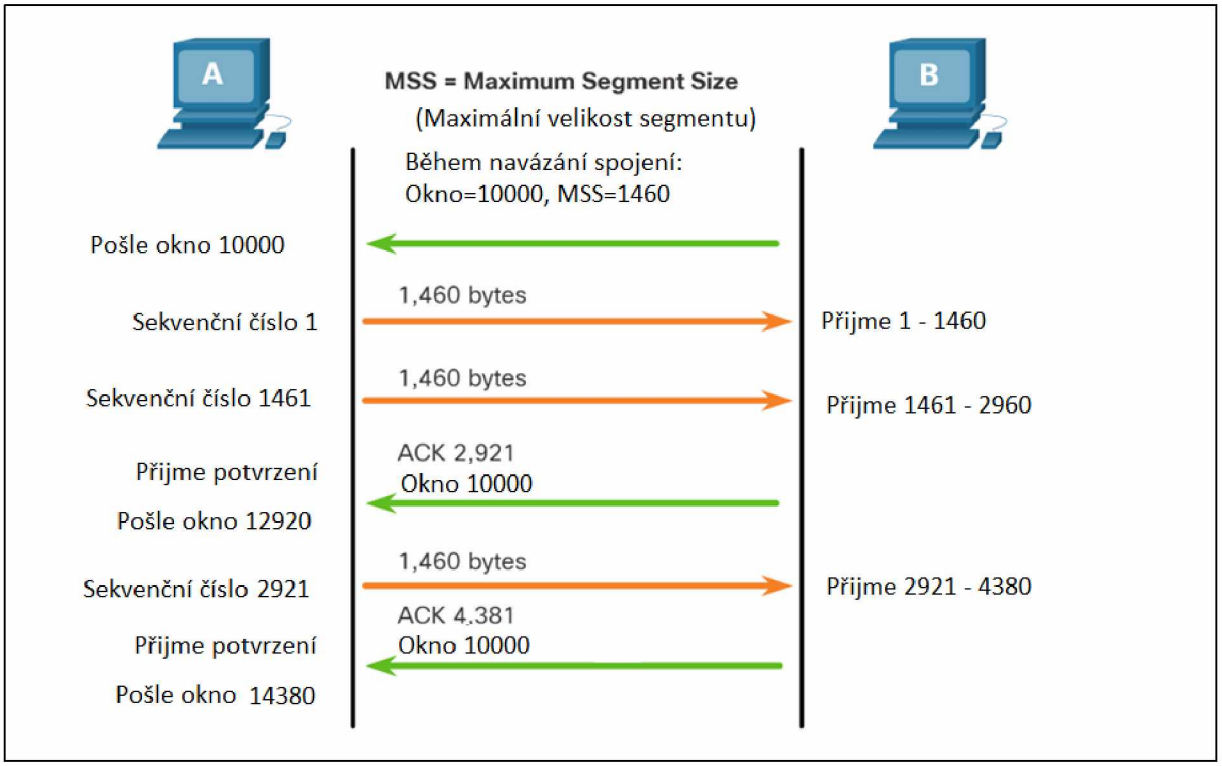
Pokud se dostupnost vyrovnávací paměti cíle sníží, může zmenšit velikost okna, aby informoval zdroj, aby snížil počet bajtů, které by měl odeslat, aniž by obdržel potvrzení.

Poznámka: Zařízení dnes používají protokol posuvných oken. Přijímač obvykle posílá potvrzení po každých dvou přijatých segmentech. Počet segmentů přijatých před potvrzením se může lišit. Výhoda posuvných oken spočívá v tom, že umožňuje odesílateli nepřetržitě vysílat segmenty, pokud přijímač potvrzuje předchozí segmenty. Detaily posuvných oken jsou nad rámec tohoto kurzu.

14.6.6 Řízení toku TCP – maximální velikost segmentu (MSS)

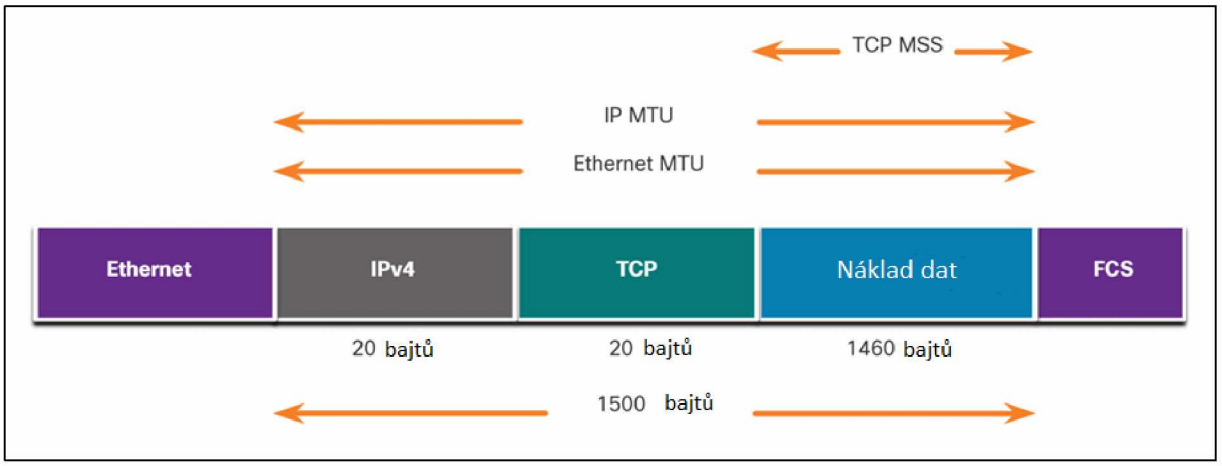
Na obrázku zdroj přenáší 1 460 bajtů dat v každém segmentu TCP. Obvykle se jedná o maximální velikost segmentu (MSS), kterou může cílové zařízení přijímat. MSS je součástí pole voleb v hlavičce TCP, které určuje největší množství dat v bajtech, které může zařízení přijmout v jednom segmentu TCP. Velikost MSS nezahrnuje hlavičku TCP. MSS je obvykle součástí třícestného handshake.

Schéma – stejný diagram jako dříve, ale důraz je kladen na MSS o maximální velikosti segmentu 1460



Běžná MSS je 1460 bajtů při použití IPv4. Hostitel určí hodnotu svého pole MSS odečtením hlaviček IP a TCP od ethernetové maximální přenosové jednotky (MTU). Na rozhraní Ethernet je výchozí MTU 1500 bajtů. Po odečtení hlavičky IPv4 o 20 bajtech a hlavičky TCP o 20 bajtech bude výchozí velikost MSS 1460 bajtů, jak je znázorněno na obrázku.

Schéma – diagram celého ethernetového rámce, jehož MTU je 1500 bajtů, přičemž 20 bajtů je hlavička IP a 20 bajtů je hlavička TCP, zbývá 1460 bajtů, což je maximální velikost segmentu TCP MSS



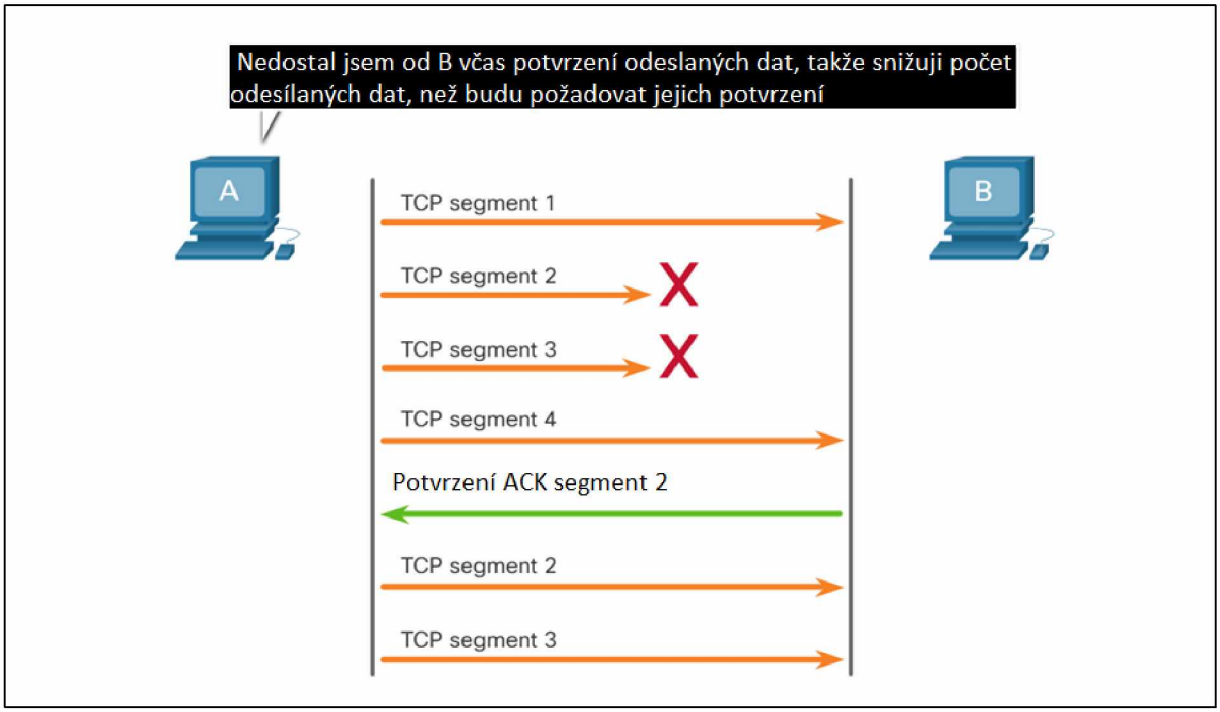
14.6.7 Řízení toku TCP – zamezení přetížení

Dojde-li v síti k zahlcení, dojde k zahození paketů přetíženým směrovačem. Když pakety obsahující segmenty TCP nedosáhnou svého cíle, zůstanou nepotvrzené. Určením rychlosti, kterou jsou segmenty TCP odesílány, ale už nejsou potvrzeny, může zdroj předpokládat určitou úroveň zahlcení sítě.

Kdykoli dojde k zahlcení, dojde k opětovnému přenosu ztracených segmentů TCP ze zdroje. Pokud opakovaný přenos není řádně řízen, může dodatečné opakované vysílání TCP segmentů zahlcení ještě zhoršit. Nejen, že jsou do sítě zaváděny nové pakety se segmenty TCP, ale k přetížení také přispěje zpětnovazební efekt znovu přenesených segmentů TCP, které byly ztraceny. Aby se zabránilo a kontrolovalo zahlcení, TCP využívá několik mechanismů, časovačů a algoritmů pro zpracování zahlcení.

Pokud zdroj zjistí, že segmenty TCP buď nejsou potvrzeny, nebo nejsou potvrzeny včas, může snížit počet bajtů, které odešle před přijetím potvrzení. Jak je znázorněno na obrázku, PC a detekuje přetížení, a proto snižuje počet bajtů, které odešle před přijetím potvrzení od PC B.

Schéma – PCA odesílající segmenty na PCB, kde ztracené segmenty a opakovaný přenos mohou způsobit zahlcení. Řízení přetížení TCP.



Čísla potvrzení ACK platí ve skutečnosti pro další očekávaný bajt, nikoli pro segment. Použitá čísla segmentů jsou pro ilustraci zjednodušená.

Všimněte si, že je to zdroj, který snižuje počet nepotvrzených bajtů, které odesílá, a nikoli velikost okna určená cílem.

Poznámka: Vysvětlení skutečných mechanismů, časovačů a algoritmů zvládání přetížení je nad rámec tohoto kurzu.

14.6.8 Ověřte si své znalosti – spolehlivost a řízení toku

Ověřte si, zda rozumíte procesu spolehlivosti TCP a řízení toku, výběrem správné odpovědi na následující otázky.

1. Jaké pole používá cílový hostitel k opětovnému sestavení segmentů do původního pořadí?

a: Kontrolní bity
b: Cílový port
c: Pořadové číslo
d: Zdrojový port
e: Velikost okna

2. Jaké pole se používá k řízení toku?

a: Kontrolní bity
b: Cílový port

c: Pořadové číslo
d: Zdrojový port
e: Velikost okna

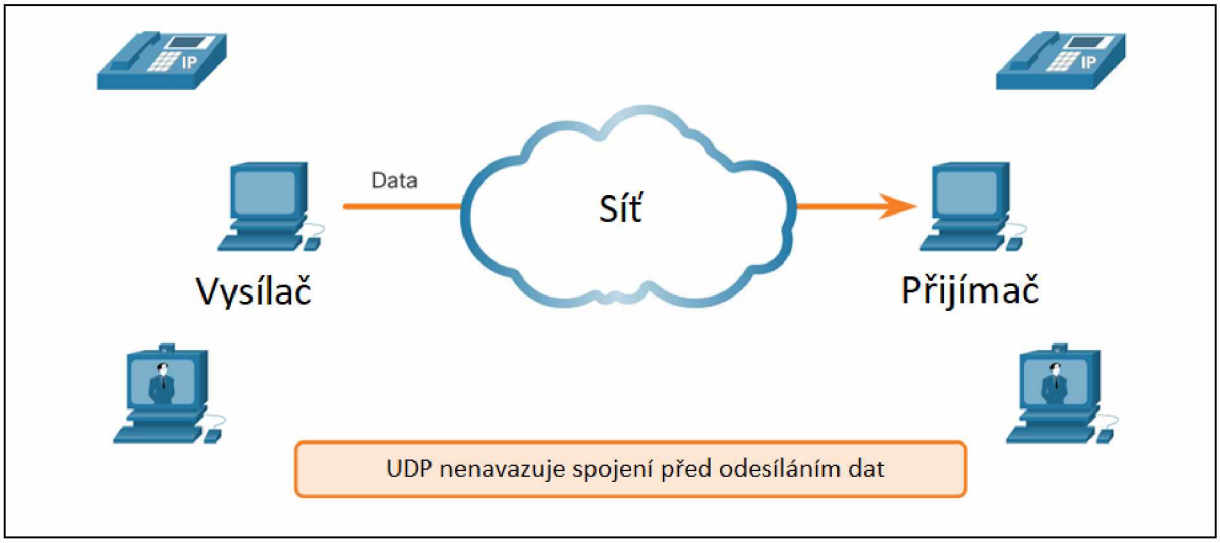
3. Co se stane, když odesílající hostitel zjistí, že došlo k přetížení?

a: Přijímající hostitel zvýší počet bajtů, které odešle, než obdrží potvrzení od odesílajícího hostitele.
b: Přijímající hostitel snižuje počet bajtů, které odesílá, než obdrží potvrzení od odesílajícího hostitele.
c: Odesílající hostitel zvýší počet bajtů, které odešle, než obdrží potvrzení od cílového hostitele.
d: Odesílající hostitel snižuje počet bajtů, které odesílá, než obdrží potvrzení od cílového hostitele.

14.7.1 UDP Nízká režie versus spolehlivost

Jak bylo vysvětleno dříve, UDP je ideální pro komunikaci, která musí být rychlá, jako je VoIP. Toto téma podrobně vysvětluje, proč je UDP ideální pro některé typy přenosů. Jak je znázorněno na obrázku, UDP nenavazuje spojení. UDP poskytuje nízkou režii přenosu dat, protože má malou hlavičku datagramu a žádný provoz správy sítě.

Schéma – hostitel odesílatele, který potřebuje odeslat hlasová a obrazová data, odesílaná pomocí protokolu UDP, nevyžaduje žádné předem dohodnuté připojení

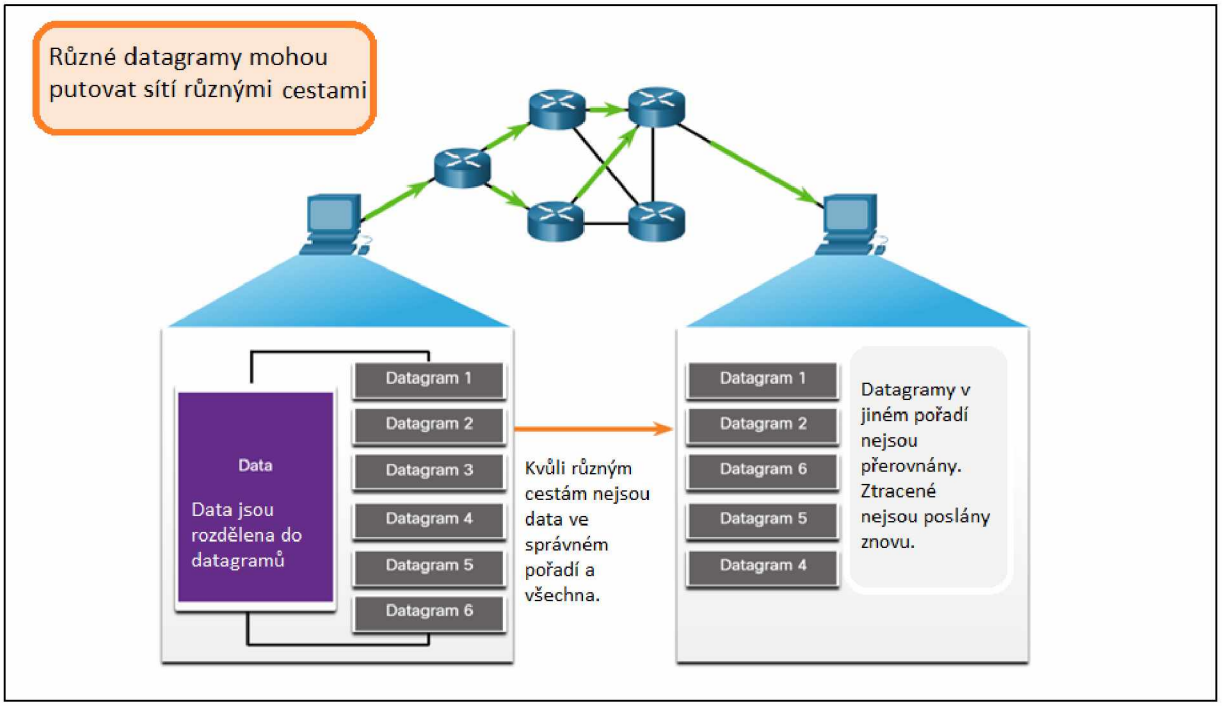


14.7.2 Znovusestavení UDP datagramů

Stejně jako segmenty s TCP, když jsou datagramy UDP odesílány na místo určení, často se ubírají různými cestami a přicházejí ve špatném pořadí. UDP nesleduje pořadová čísla jako TCP. UDP nemá žádný způsob, jak změnit pořadí datagramů do jejich pořadí přenosu, jak je znázorněno na obrázku.

Proto UDP jednoduše znovu sestaví data v pořadí, v jakém byla přijata, a předá je aplikaci. Pokud je posloupnost dat pro aplikaci důležitá, musí aplikace určit správnou posloupnost a určit, jak by měla být data zpracována.

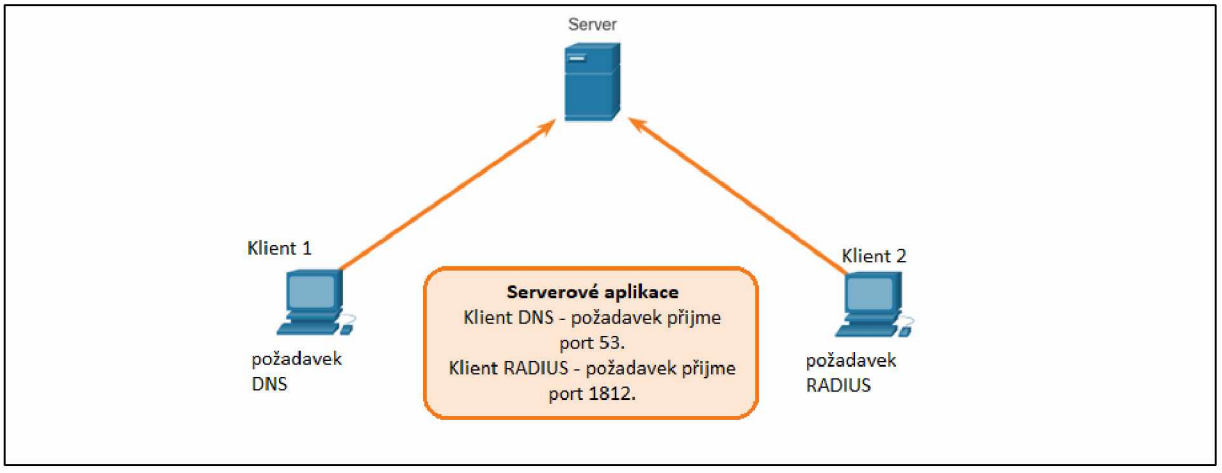
Schéma – datagramy UDP, které jsou odesílány v původním pořadí, ale přicházejí mimo pořadí kvůli možnosti různých cest k dosažení cíle. UDP: Bez připojení a nespolehlivé



14.7.3 Procesy a požadavky serveru UDP

Stejně jako aplikacím založeným na TCP jsou serverovým aplikacím založeným na UDP přiřazena známá nebo registrovaná čísla portů, jak je znázorněno na obrázku. Když tyto aplikace nebo procesy běží na serveru, přijímají data odpovídající přiřazenému číslu portu. Když UDP přijme datagram určený pro jeden z těchto portů, předá data aplikace příslušné aplikaci na základě čísla portu.

Schéma – aplikace serveru RADIUS používá UDP k naslouchání požadavkům na portu 1812, DNS na 53. UDP server naslouchá požadavkům.



Poznámka: Server RADIUS (Remote Authentication Dial-in User Service) zobrazený na obrázku poskytuje služby autentizace, autorizace a účtování (AAA) pro správu přístupu uživatelů. Provoz RADIUS je nad rámec tohoto kurzu.

14.7.4 Klientské procesy UDP

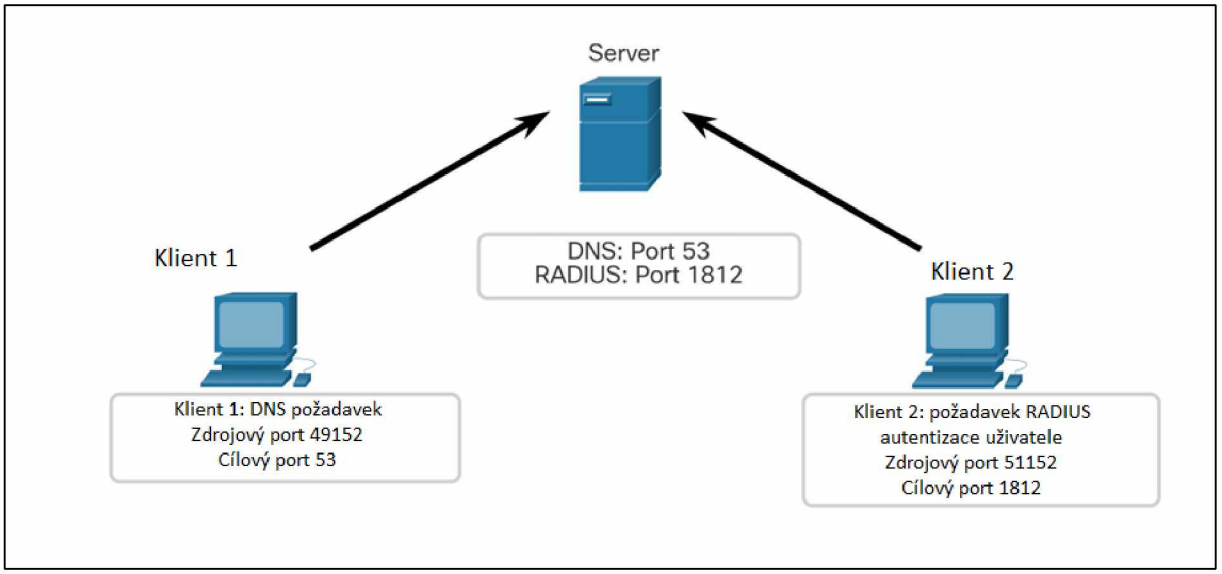
Stejně jako u TCP je komunikace mezi klientem a serverem zahájena klientskou aplikací, která požaduje data z procesu serveru. Proces klienta UDP vybírá číslo portu z rozsahu čísel dynamických portů a používá jej jako zdrojový port pro konverzaci. Cílový port je obvykle dobře známé nebo registrované číslo portu přiřazené procesu serveru.

Poté, co klient vybere zdrojový a cílový port, použije se stejný pár portů v hlavičce všech datagramů v transakci. u dat vracejících se klientovi ze serveru jsou čísla zdrojového a cílového portu v hlavičce datagramu obrácena.

Vyberte jednotlivé karty pro ilustraci dvou hostitelů požadujících služby z ověřovacího serveru DNS a RADIUS.

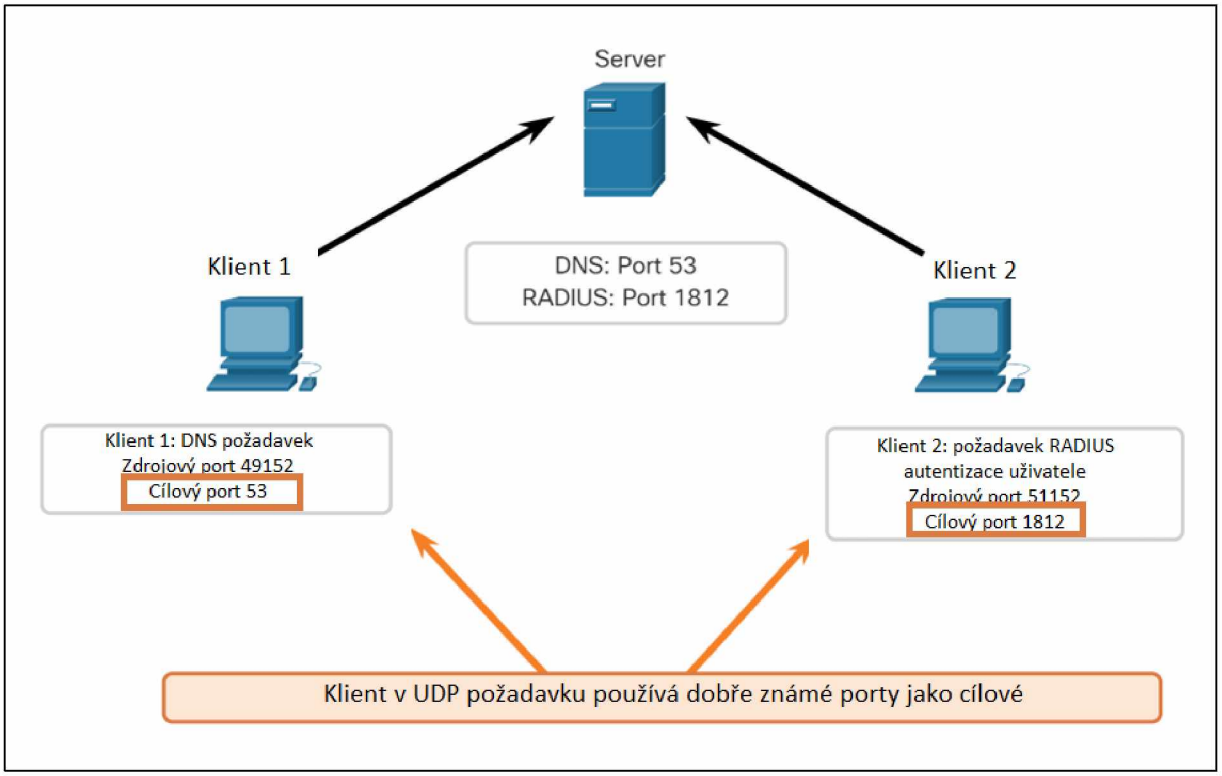
Klienti odesílající požadavky UDP

Klient 1 odesílá požadavek DNS, zatímco Klient 2 požaduje ověřovací služby RADIUS stejného serveru.



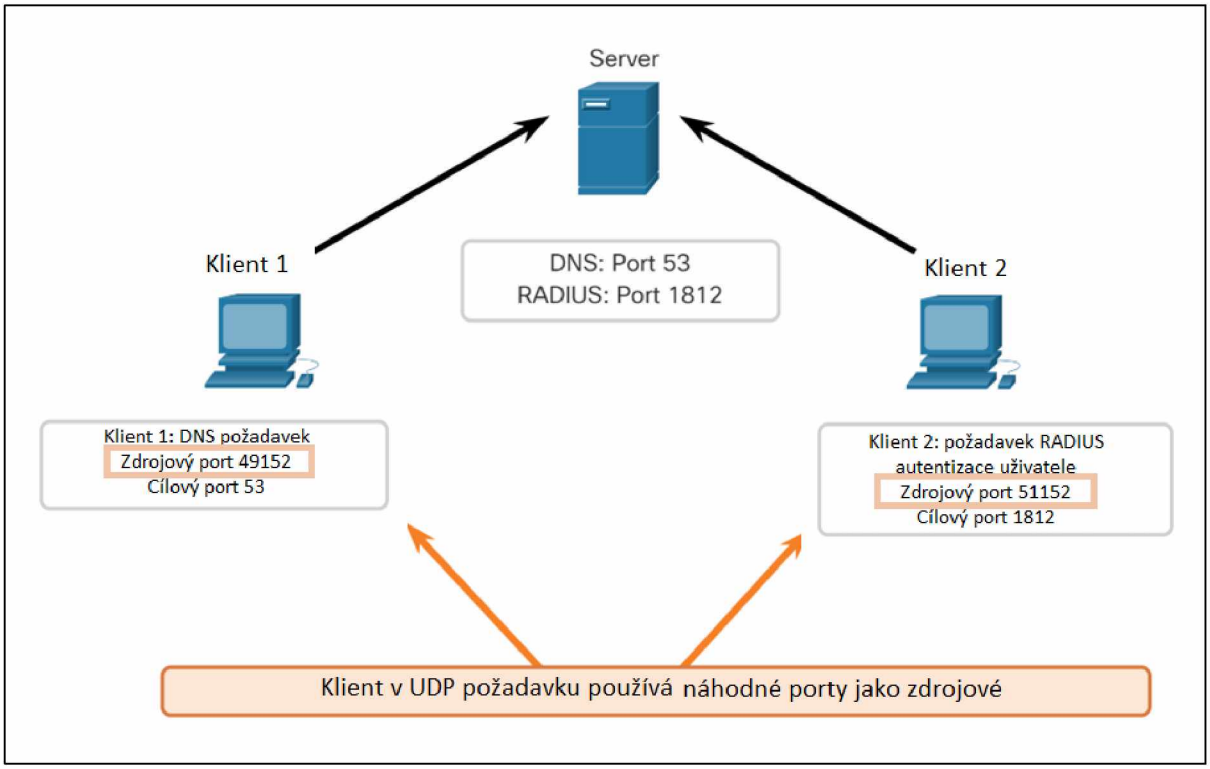
Cílové porty požadavku UDP

Klient 1 odesílá požadavek DNS pomocí dobře známého cílového portu 53, zatímco klient 2 požaduje ověřovací služby RADIUS pomocí registrovaného cílového portu 1812.



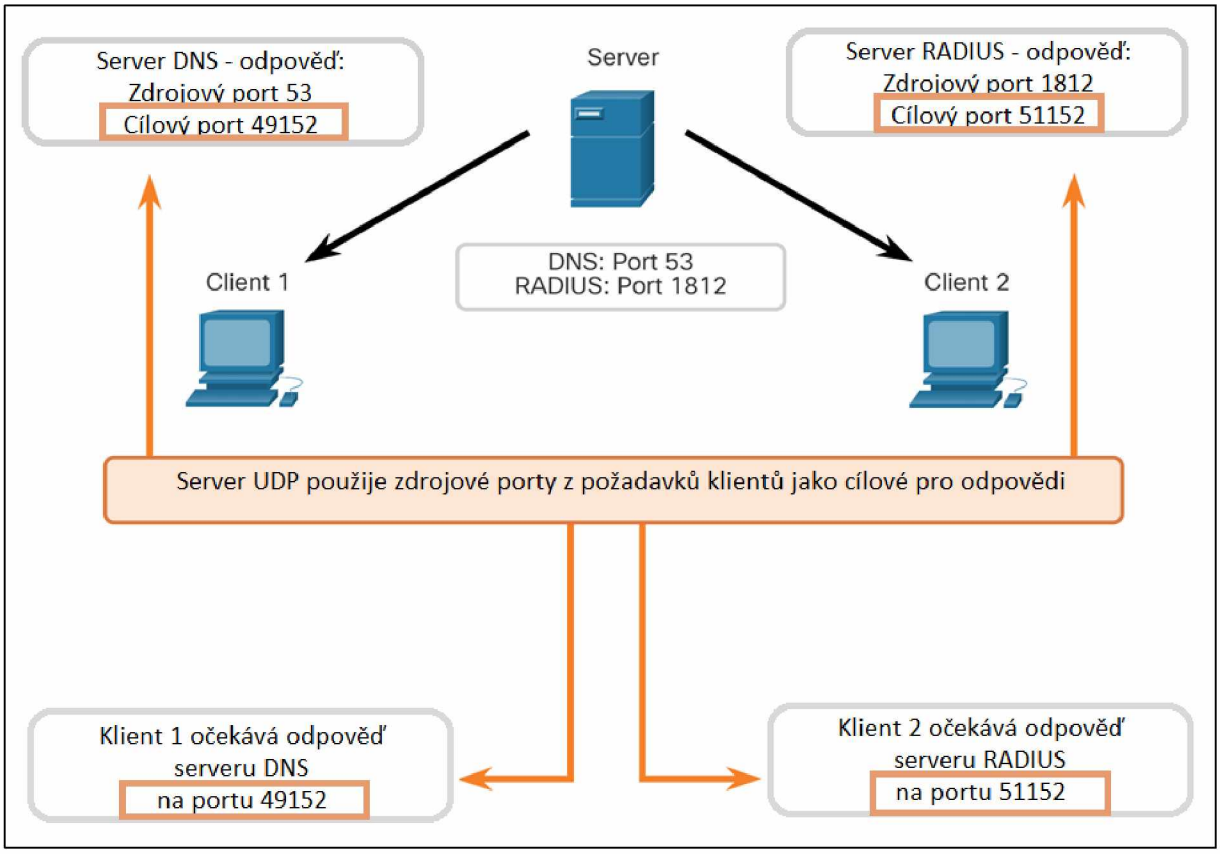
Porty zdroje požadavku UDP

Požadavky klientů dynamicky generují čísla zdrojových portů. v tomto případě Klient 1 používá zdrojový port 49152 a Klient 2 používá zdrojový port 51152.



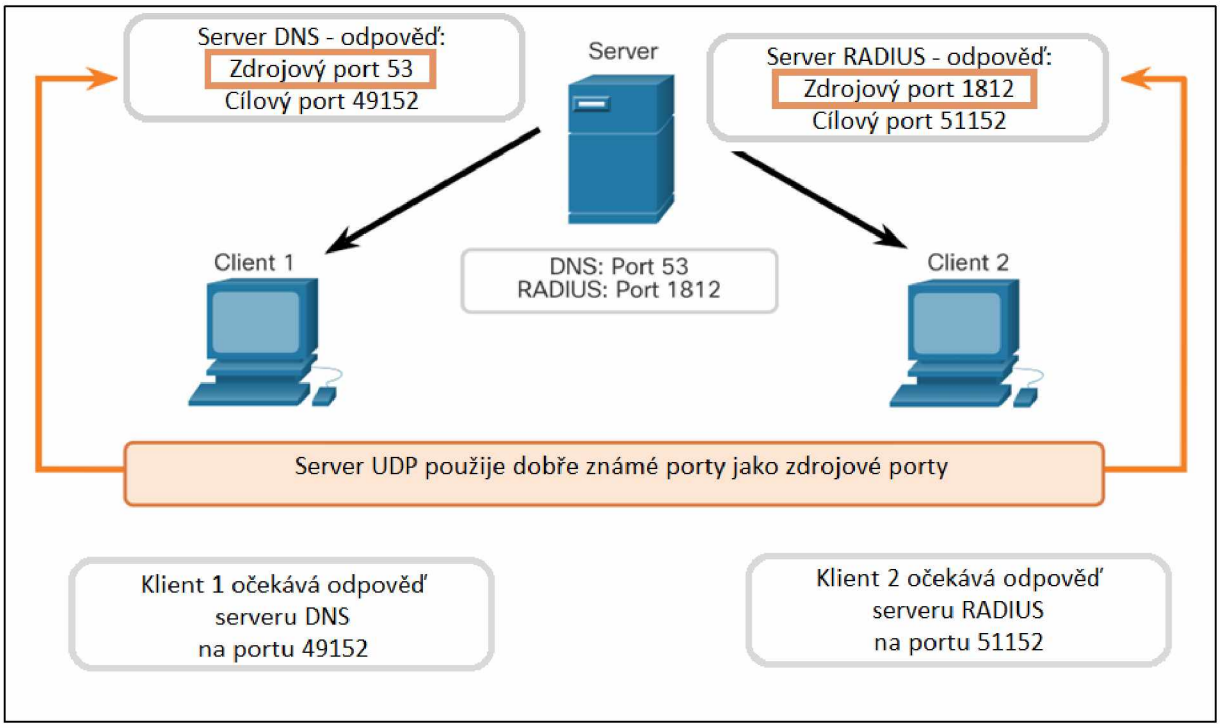
Cíl odpovědi UDP

Když server odpoví na požadavky klienta, obrátí cílový a zdrojový port původního požadavku. v odpovědi serveru na požadavek DNS je nyní cílový port 49152 a odpověď na ověření RADIUS je nyní cílový port 51152.



Porty zdroje odpovědi UDP

Zdrojové porty v odpovědi serveru jsou původní cílové porty v počátečních požadavcích.



14.7.5 Ověřte si své znalosti – komunikace UDP

Ověřte si, zda rozumíte komunikaci UDP výběrem správné odpovědi na následující otázky.

1. Proč je UDP žádoucí pro protokoly, které provádějí jednoduché transakce požadavků a odpovědí?

a: Řízení toku
b: Nízká režie
c: Spolehlivost
d: Doručení podle stejné objednávky

2. Které prohlášení o opětovném sestavení datagramů UDP je pravdivé?

a: UDP data znovu nesestaví.
b: UDP znovu sestaví data v pořadí, v jakém byla přijata.
c: UDP znovu sestaví data pomocí řídicích bitů.
d: UDP znovu sestaví data pomocí pořadových čísel.

3. Které z následujících by byly platné zdrojové a cílové porty pro hostitele připojujícího se k serveru DNS?

a: Zdroj: 53, Cíl: 49152
b: Zdroj: 1812, Cíl: 49152
c: Zdroj: 49152, Cíl: 53
d: Zdroj: 49152, Cíl: 1812


?ŘEŠ
ENÍ?

14.8.1 Packet Tracer - TCP a UDP komunikace

V této aktivitě prozkoumáte funkčnost protokolů TCP a UDP, multiplexování a funkci čísel portů při určování, která místní aplikace data požaduje nebo která data odesílá.

- Komunikace TCP a UDP

14.8.2 Co jsme se v tomto modulu naučili?

Přeprava dat

Transportní vrstva je spojením mezi aplikační vrstvou a nižšími vrstvami, které jsou zodpovědné za síťový přenos. Transportní vrstva je zodpovědná za logickou komunikaci mezi aplikacemi běžícími na různých hostitelích. Transportní vrstva zahrnuje TCP a UDP. Protokoly transportní vrstvy určují způsob přenosu zpráv mezi hostiteli a zodpovídají za správu požadavků na spolehlivost konverzace. Transportní vrstva je zodpovědná za sledování konverzací (relací), segmentaci dat a opětovné sestavení segmentů, přidávání informací v záhlaví, identifikaci aplikací a multiplexování konverzací. TCP je stavový, spolehlivý, potvrzuje data, znovu odesílá ztracená data a dodává data v sekvenčním pořadí. Použijte TCP pro e-mail a web. UDP je bezestavový, rychlý, má nízkou režii, nevyžaduje potvrzení, neposílá znovu ztracená data a dodává data v pořadí, v jakém dorazí. Použijte UDP pro VoIP a DNS.

Přehled TCP

TCP vytváří relace, zajišťuje spolehlivost, poskytuje doručení ve stejném pořadí a podporuje řízení toku. Segment TCP přidává 20 bajtů režie jako informace záhlaví při zapouzdření dat aplikační vrstvy. Pole záhlaví TCP jsou Zdrojový a Cílový port, Sekvenční číslo, Číslo potvrzení, Délka záhlaví, Rezervováno, Řídicí bity, Velikost okna, Kontrolní součet a Urgent (naléhavé). Aplikace, které používají TCP, jsou HTTP, FTP, SMTP a Telnet.

Přehled UPD

UDP rekonstruuje data v pořadí, v jakém jsou přijata, ztracené segmenty nejsou znovu odesílány, není vytvořena relace a UPD neinformuje odesílatele o dostupnosti zdrojů. Pole záhlaví UDP jsou Zdrojový a Cílový port, Délka a Kontrolní součet. Aplikace, které používají UDP, jsou DHCP, DNS, SNMP, TFTP, VoIP a videokonference.

Čísla portů

Protokoly transportní vrstvy TCP a UDP používají čísla portů ke správě více současných konverzací. To je důvod, proč pole hlavičky TCP a UDP identifikují číslo portu zdrojové a cílové aplikace. Zdrojový a cílový port jsou umístěny v rámci segmentu. Segmenty jsou pak zapouzdřeny do IP paketu. IP paket obsahuje IP adresu zdroje a cíle. Kombinace zdrojové adresy IP a čísla zdrojového portu nebo cílové adresy IP a čísla cílového portu se nazývá socket. Socket se používá k identifikaci serveru a služby požadované klientem. Existuje rozsah čísel portů od 0 do 65535. Tento rozsah je rozdělen do skupin: Známé porty, Registrované porty, Soukromé a/nebo Dynamické porty. Existuje několik známých čísel portů, která jsou vyhrazena pro běžné aplikace, jako jsou FTP, SSH, DNS, HTTP a další. Někdy je nutné vědět, která aktivní TCP spojení jsou

otevřená a běží na síťovém hostiteli. Netstat je důležitý síťový nástroj, který lze použít k ověření těchto připojení.

Komunikační proces TCP

Každý proces aplikace běžící na serveru je nakonfigurován tak, aby používal číslo portu. Číslo portu je buď automaticky přiřazeno nebo konfigurováno ručně správcem systému. Procesy TCP serveru jsou následující: klienti odesílají požadavky TCP, požadují cílové porty, požadují zdrojové porty, reagují na požadavky cílového portu a zdrojového portu. k ukončení jedné konverzace podporované protokolem TCP jsou k ukončení obou relací potřeba čtyři výměny. Ukončení může iniciovat klient nebo server. Třícestný handshake zjistí, že cílové zařízení je přítomno v síti, ověří, že cílové zařízení má aktivní službu a přijímá požadavky na číslo cílového portu, které hodlá použít iniciující klient, a informuje cílové zařízení, že zdroj klient zamýšlí navázat komunikační relaci na tomto čísle portu. Šest příznaků řídicích bitů je: URG, ACK, PSH, RST, SYN a FIN.

Spolehlivost a řízení toku

Aby původní zpráva byla příjemci srozumitelná, musí být přijata všechna data a data v těchto segmentech musí být znovu sestavena do původního pořadí. Pořadová čísla jsou přiřazena v záhlaví každého paketu. Bez ohledu na to, jak dobře je síť navržena, občas dochází ke ztrátě dat. TCP poskytuje způsoby, jak řídit ztráty segmentů. Existuje mechanismus pro opakované vysílání segmentů pro nepotvrzená data. Hostitelské operační systémy dnes obvykle využívají volitelnou funkci TCP nazvanou selektivní potvrzení (SACK), vyjednanou během třístranného handshake. Pokud oba hostitelé podporují SACK, přijímač může explicitně potvrdit, které segmenty (bajty) byly přijaty, včetně všech nesouvislých segmentů. Odesílající hostitel by tedy potřeboval pouze znovu odeslat chybějící data. Řízení toku pomáhá udržovat spolehlivost přenosu TCP úpravou rychlosti toku dat mezi zdrojem a cílem. Aby toho bylo dosaženo, obsahuje hlavička TCP 16bitové pole nazývané velikost okna. Proces potvrzení odesílání cíle při zpracování přijatých bajtů a neustálé nastavování okna odesílání zdroje se nazývá posuvná okna. Zdroj může přenášet 1 460 bajtů dat v rámci každého segmentu TCP. Toto je typická MSS, kterou může cílové zařízení přijímat. Aby se zabránilo a kontrolovalo přetížení, TCP využívá několik mechanismů pro manipulaci s přetížením. Je to zdroj, který snižuje počet nepotvrzených bajtů, které odesílá, a nikoli velikost okna určená cílem.

Komunikace UPD

UDP je jednoduchý protokol, který poskytuje základní funkce transportní vrstvy. Když jsou datagramy UDP odeslány do cíle, často se ubírají různými cestami a dorazí ve špatném pořadí. UDP nesleduje pořadová čísla jako TCP. UDP nemá žádný způsob, jak změnit pořadí datagramů do jejich pořadí přenosu. UDP jednoduše znovu sestaví data v pořadí, v jakém byla přijata, a předá je aplikaci. Pokud je posloupnost dat pro aplikaci důležitá, musí aplikace sama určit správnou posloupnost a určit, jak by měla být data zpracována. Serverovým aplikacím založeným na UDP jsou přiřazena známá nebo registrovaná čísla portů. Když UDP přijme datagram určený pro jeden z těchto portů, předá data aplikace příslušné aplikaci na základě čísla portu. Proces klienta UDP dynamicky vybírá číslo portu z rozsahu čísel portů a používá jej jako zdrojový port pro konverzaci. Cílový port je obvykle dobře známé nebo registrované číslo portu přiřazené procesu serveru. Poté, co klient vybere zdrojový a cílový port, použije se stejný pár portů v hlavičce všech datagramů použitých v transakci. u dat vracejících se klientovi ze serveru jsou čísla zdrojového a cílového portu v hlavičce datagramu obrácena.

14.8.3 Modulový kvíz – Transportní vrstva

1. Která funkce transportní vrstvy se používá k vytvoření relace orientované na připojení?

a: TCP třícestný handshake
b: Pořadové číslo UDP
c: UDP ACK příznak
d: Číslo TCP portu

2. Jaká je kompletní řada známých portů TCP a UDP?

a: 1024 - 49151
b: 0 až 255
c: 256 - 1023
d: 0 až 1023

3. Co je to socket?

a: kombinace zdrojové a cílové sekvence a potvrzovacích čísel
b: kombinace zdrojových a cílových pořadových čísel a čísel portů
c: kombinaci zdrojové IP adresy a čísla portu nebo cílové IP adresy a čísla portu
d: kombinaci zdrojové a cílové IP adresy a zdrojové a cílové ethernetové adresy

4. Jak síťový server spravuje požadavky více klientů na různé služby?

a: Každý požadavek je sledován prostřednictvím fyzické adresy klienta.
b: Server používá IP adresy k identifikaci různých služeb.
c: Každý požadavek má kombinaci čísel zdrojového a cílového portu a jedinečných IP adres.
d: Server odesílá všechny požadavky přes výchozí bránu.

5. Co se stane, když část zprávy FTP není doručena na místo určení?

a: Část zprávy FTP, která byla ztracena, je znovu odeslána.
b: Zdrojový hostitel FTP odešle dotaz cílovému hostiteli.
c: Celá zpráva FTP je znovu odeslána.
d: Zpráva je ztracena, protože FTP nepoužívá spolehlivý způsob doručení.

6. Jaké typy aplikací jsou nejvhodnější pro použití UDP?

a: aplikace citlivé na zpoždění
b: aplikace, které vyžadují spolehlivé doručení
c: aplikace, které vyžadují opakovaný přenos ztracených segmentů
d: aplikace, které jsou citlivé na ztrátu paketů

7. Přetížení sítě vedlo ke ztrátě segmentů TCP, které byly odeslány do cíle. Jakým způsobem to protokol TCP řeší?

a: Cíl posílá méně potvrzovacích zpráv, aby se šetřila šířka pásma.
b: Zdroj snižuje množství dat, která přenáší, než obdrží potvrzení od cíle.
c: Zdroj zmenší velikost okna, aby se snížila rychlost přenosu z cíle.
d: Cíl zmenší velikost okna.

8. Které dvě operace zajišťuje TCP, ale ne UDP? (Vyberte dvě.)

a: identifikaci jednotlivých rozhovorů
b: opakovaný přenos jakýchkoli nepotvrzených dat
c: rekonstrukci dat v obdržené objednávce
d: identifikaci aplikací
e: potvrzení přijatých dat

9. Jaký je účel použití čísla zdrojového portu v komunikaci TCP?

a: pro sledování více konverzací mezi zařízeními
b: k dotazu na nepřijatý segment
c: k sestavení segmentů, které dorazily mimo pořadí
d: pro upozornění vzdáleného zařízení, že konverzace skončila

10. Které dva příznaky v hlavičce TCP se používají při třícestném navázání spojení TCP k navázání spojení mezi dvěma síťovými zařízeními? (Vyberte dva.)

a: ACK
b: PSH
c: URG
d: SYN
e: RST
f: FIN

11. Jaký mechanismus TCP se používá ke zvýšení výkonu tím, že umožňuje zařízení nepřetržitě posílat stálý proud segmentů, pokud zařízení také přijímá nezbytná potvrzení?

a: Socketový pár
b: Obousměrné podání ruky
c: Posuvné okno
d: Třícestné podání ruky

12. Jakou akci provádí klient při navazování komunikace se serverem pomocí UDP na transportní vrstvě?

a: Klient nastaví velikost okna pro relaci.
b: Klient náhodně vybere číslo zdrojového portu.
c: Klient odešle ISN na server, aby zahájil 3-cestný handshake.
d: Klient odešle synchronizační segment pro zahájení relace.

13. Které dvě služby nebo protokoly používají preferovaný protokol UDP pro rychlý přenos a nízkou režii? (Vyberte dva)

a: DNS
b: VoIP
c: HTTP
d: FTP
e: POP3

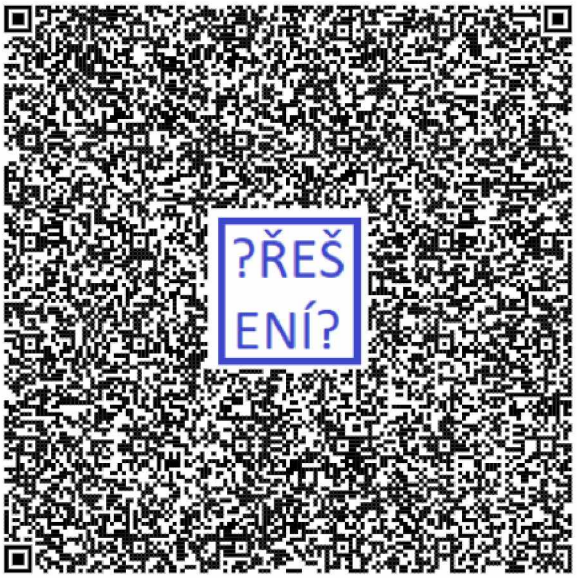
14. Které číslo nebo sada čísel představuje socket?

a: 21
b: 10.1.1.15
c: 192.168.1.1:80

d: 01-23-45-67-89-AB

15. Jaká je odpovědnost protokolů transportní vrstvy?

a: poskytování přístupu k síti
b: převod soukromých IP adres na veřejné IP adresy
c: určení nejlepší cesty k předání paketu
d: sledování jednotlivých konverzací



Příloha B

UNIVERZITA PARDUBICE
FAKULTA FILOZOFICKÁ

VÝZKUMNÁ ZPRÁVA Z PŘEDMĚTU METODOLOGIE
POUŽÍVÁNÍ E-LEARNINGOVÝCH NÁSTROJŮ

DPS 25. běh 20.5.2022 Ing. Zdeněk Drvota

Abstrakt

Práce se zabývá tématem používání e-learningových nástrojů Cisco Netacad a jiných studijních materiálů při výuce počítačových sítí. Sledována je míra používání studijních materiálů v anglickém (AJ) nebo českém jazyce (ČJ) v závislosti na schopnosti komunikace v AJ, a na odborných znalostech (studijním oboru).

Ve výzkumu byl použit kvantitativní výzkumný design. Výzkumný soubor tvoří žáci střední odborné školy (DELTA) , a studenti předmětu Počítačové sítě denního a kombinovaného studia vysoké školy (UPCE). Pro získání dat byla zvolena metoda dotazníkového šetření, nástrojem dotazník vlastní konstrukce. Účast byla dobrovolná, dotazník byl předložen v elektronické podobě frekventantům kurzů Cisco Netacad.

Výsledky výzkumu budou využity při další výuce počítačových sítí.

Klíčová slova: Cisco Netacad, e-learning, studijní materiály, počítačové sítě, anglický jazyk.

Obsah

Úvod

Výuka počítačových sítí probíhá na řadě středních a vysokých škol s využitím e-learningových kurzů síťové akademie Cisco (Cisco Netacad). Studijní materiály jsou dostupné mimo jiné v jazyce anglickém, nikoliv však v českém. Stejně tak i kvízy, testové otázky a další nástroje.

Tento výzkum by měl pomoci lektorům s výběrem doplňkových materiálů, a především zjistit, jak jsou využívány studijní texty.

V práci bude popsána metodologie výzkumu, uvedena prezentaci výsledků výzkumu na základě dat sesbíraných dotazníkem a ověřených statistickými metodami. Na závěr budou uvedeny získané poznatky, v příloze text použitého dotazníku.

1 Popis metodologie výzkumu

1.1 Cíl práce

Cílem práce je zjistit míru používání e-learningových nástrojů Cisco Netacad a jiných studijních materiálů při výuce počítačových sítí v anglickém (AJ) nebo českém jazyce (ČJ) v závislosti na schopnosti komunikace v AJ, a na odborných znalostech (studijním oboru).

1.2 Formulace hypotéz

Na základě provedeného dotazníkového šetření se bude práce věnovat třem stanoveným hypotézám:

1.2.1 Hypotéza 1:

Studenti IT oboru/zaměření považují Netacad kurz za snadnější než studenti jiných oborů

H_{01}: Hodnocení obtížnosti kurzu je stejné v různých studijních oborech

H_{A1}: Hodnocení obtížnosti kurzu se liší v různých studijních oborech

1.2.2 Hypotéza 2:

Studenti s menšími předchozími odbornými znalostmi počítačových sítí (IT) používají e-learningové materiály více

H_{01}: Používání e-learningových materiálů je stejné bez ohledu na předchozí odborné znalosti

H_{A1}: Používání e-learningových materiálů se liší podle předchozích odborných znalostí

1.2.3 Hypotéza 3:

Studenti s menšími jazykovými znalostmi AJ používají doplňkové materiály v českém jazyce více

H_{01}: Používání doplňkových materiálů v českém jazyce je stejné bez ohledu na předchozí jazykové znalosti

H_{A1}: Používání doplňkových materiálů v českém jazyce se liší vzhledem k předchozím jazykovým znalostem

1.3 Popis výzkumného souboru

Výzkumný soubor tvoří žáci druhého, třetího a čtvrtého ročníku střední odborné školy (DELTA - Střední škola informatiky a ekonomie, s.r.o.), a studenti volitelného předmětu Počítačové sítě denního a kombinovaného studia DFJP Univerzity Pardubice, ve kterých jsou používány kurzy Cisco Netacad. Dotazník předán formou odkazu na elektronickou formu. Z oslovených bylo získáno 90 vyplněných dotazníků od respondentů.

1.4 Popis použitých metod a technik sběru dat

Ve svém výzkumu byla použita metoda kvantitativního dotazníkového šetření. Bylo využito otázek uzavřených, otevřených, a metody škálování.

Dotazník vlastní byl rozeslán v online formě, a to odkazem do skupin žáků a studentů v emailu, nebo prostřednictvím Cisco Netacad. Dotazník byl vytvořen na platformě Google Forms. Dotazník je uveden v příloze.

1.5 Realizace výzkumu

Odpovědi byly sbírány od od 26.4.2022 do 19.5.2022. Účast byla dobrovolná a dotazník byl zaslán pouze účastníkům kurzů Cisco Netacad.

2 Výsledky výzkumu

2.1 Prezentace dat

Pro výzkum bylo získáno 90 odpovědí, z toho od 7 od studentů vysoké školy a 83 od žáků střední školy, odpovědi slovní, číselné, škálované. Pro výzkumný problém a ověření tří hypotéz v této práci byly zpracovány slovní a škálované odpovědi, s absolutní četností. Pro statistické ověření byl zvolen chí-kvadrát test, který se používá ke zjištění, zdali mezi diskrétními kvantitativními veličinami existuje prokazatelně výrazný vztah. Odpovědi a grafy byly zpracovány pomocí programu Microsoft Excel.

2.2 Verifikace hypotéz (statistické zpracování, grafy)

2.2.1 Hypotéza 1:

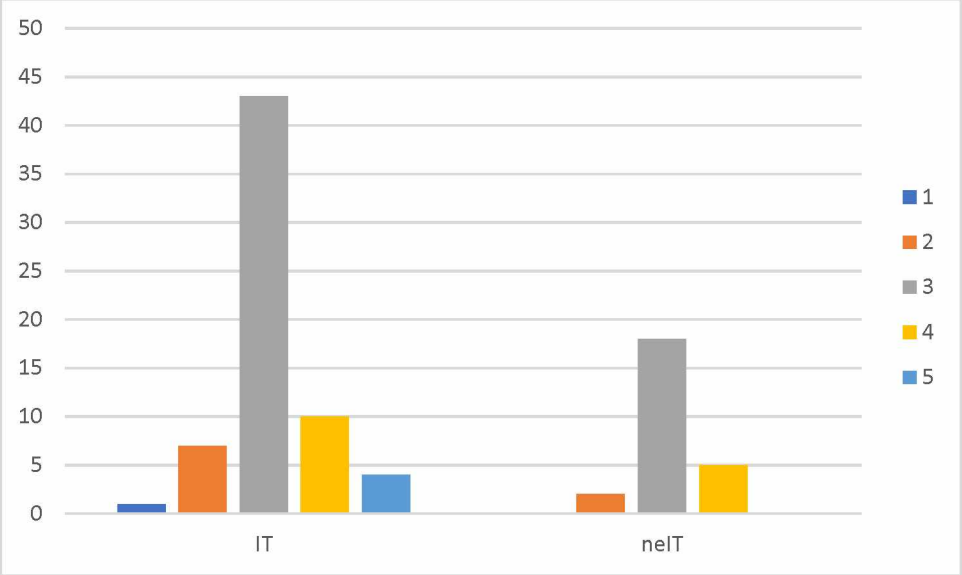
Studenti IT oboru/zaměření považují Netacad kurz za snadnější než studenti jiných oborů

H_{01}: Hodnocení obtížnosti kurzu je stejné v různých studijních oborech

H_{A1}: Hodnocení obtížnosti kurzu se liší v různých studijních oborech

Z odborného (IT) hlediska považuji aktuální (nebo poslední absolvovaný) kurz NETACAD za:

(1. lehký, 2. spíše lehký, 3. přiměřeně náročný, 4. spíše těžký, 5. těžký)



Graf 1 Obor - náročnost

U této otázky byla využita metoda škálování s lichým počtem stupňů. Pro malý počet respondentů byly sečteny odpovědi (1+2) a (4+5), pro další zpracování. Získaná data byla statisticky ověřena chí kvadrátem na hladině významnosti 5 %.

Tabulka 1 Empirické četnosti – H1

	1-2	3	4-5	Celkový součet
IT	8	43	14	65
neIT	2	18	5	25
Celkový součet	10	61	19	90

Tabulka 2 Teoretické četnosti – H1

	1-2	3	4-5	Celkový součet
IT	7,222222	44,05556	13,72222	65
neIT	2,777778	16,94444	5,277778	25
Celkový součet	10	61	19	90

α = 0,05 (hladina významnosti)

TK = 0,412828035 (testové kritérium)

KH = 5,991464547 (kritická hodnota

p-hodnota= 0,813496205

Testovací kritérium není větší než kritická hodnota, H_{01} se nezamítá

Hodnocení obtížnosti kurzu je stejné v různých studijních oborech

2.2.2 Hypotéza 2:

Studenti s menšími předchozími odbornými znalostmi počítačových sítí (IT) používají e-learningové materiály v AJ více

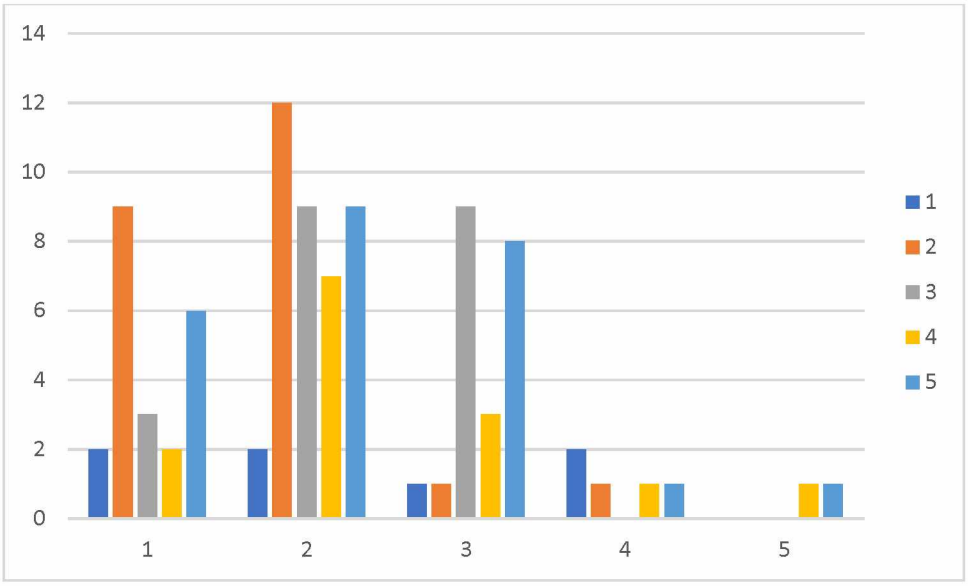
H_{01}: Používání e-learningových materiálů v AJ je stejné bez ohledu na předchozí odborné znalosti

H_{A1}: Používání e-learningových materiálů v AJ se liší podle předchozích odborných znalostí

Při samostudiu používám studijní materiály kurzu NETACAD v anglickém jazyce:

(1. Laik – jen uživatel, 2. Základní, 3. Střední, 4. Pokročilé, 5. Expert)

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. stále)



Graf 2 Odborné znalosti - používání materiálů v AJ

U této otázky byla využita metoda škálování s lichým počtem stupňů. Pro malý počet respondentů byly sečteny odpovědi (1+2) a (4+5), pro další zpracování. Získaná data byla statisticky ověřena chí kvadrátem na hladině významnosti 5 %.

Tabulka 3 Empirické četnosti – H2

	1-2	3	4-5	Celkový součet
IT	25	12	24	61
neIT	2	9	11	22
Celkový součet	3		4	7

Tabulka 4 Teoretické četnosti – H2

	1-2	3	4-5	Celkový součet
IT	20,33333333	14,23333333	26,43333333	61
neIT	7,333333333	5,133333333	9,533333333	22
Celkový součet	2,333333333	1,633333333	3,033333333	7

Byla použita Yatesova korekce pro výpočet chí-kvadrát.

$\alpha = 0,05$ (hladina významnosti)

TK = 7,568041736 (testové kritérium)

KH = 9,487729037 (kritická hodnota

p-hodnota= 0,057199145

Testovací kritérium není větší než kritická hodnota, H_{01} se nezamítá

Používání e-learningových materiálů v AJ je stejné bez ohledu na předchozí odborné znalosti

2.2.3 Hypotéza 3:

Studenti s menšími jazykovými znalostmi AJ používají doplňkové materiály v českém jazyce více

H_{01}: Používání doplňkových materiálů v českém jazyce je stejné bez ohledu na předchozí jazykové znalosti

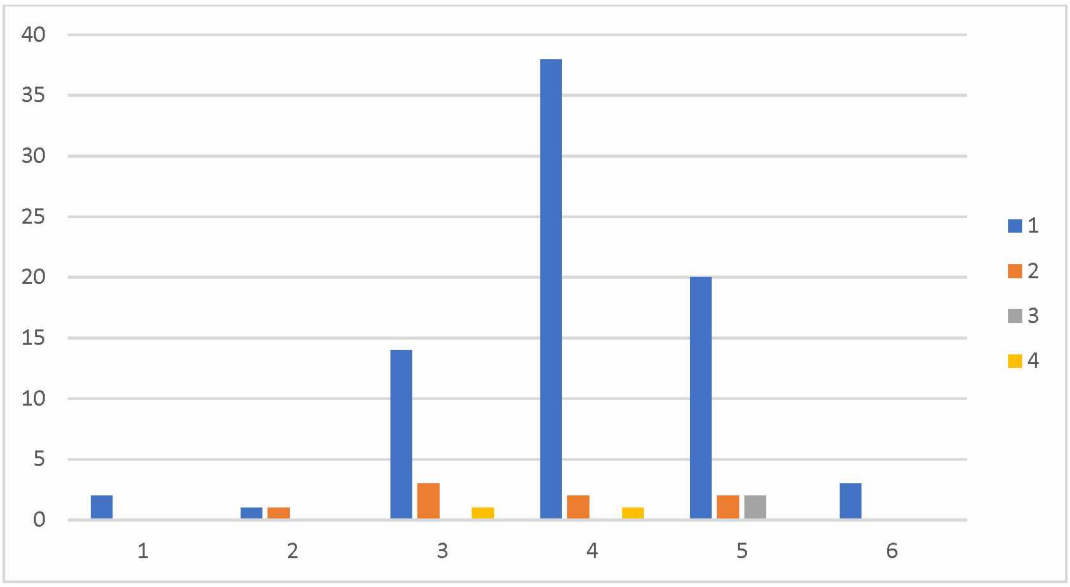
H_{A1}: Používání doplňkových materiálů v českém jazyce se liší vzhledem k předchozím jazykovým znalostem

Kromě materiálů kurzu NETACAD používám i materiály v českém jazyce:

PETERKA, Jiří. Peterkův archiv http://www.earchiv.cz/;

(A1 – Začátečník, A2 – Pokročilý začátečník, B1 – Mírně pokročilý, B2 – Pokročilý, C1 – Velmi pokročilý, C2 – Expert)

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. stále)



Graf 3 Znalost AJ - české materiály Peterka

Tabulka 5 *Empirické četnosti – H3 Peterka*

	1	2	3	4	5	Celkový součet
1	2					2
2	1	1				2
3	14	3		1		18
4	38	2		1		41
5	20	2	2			24
6	3					3
Celkový součet	78	8	2	2	0	90

Tabulka 6 *Teoretické četnosti – H3 Peterka*

	1	2	3	4	5	Celkový součet
1	1,733333333	0,177778	0,044444	0,044444		2
2	1,733333333	0,177778	0,044444	0,044444		2
3	15,6	1,6	0,4	0,4		18
4	35,53333333	3,644444	0,911111	0,911111		41
5	20,8	2,133333	0,533333	0,533333		24
6	2,6	0,266667	0,066667	0,066667		3
Celkový součet	78	8	2	2	0	90

Byla použita Yatesova korekce pro výpočet chí-kvadrát.

$\alpha = 0,05$ (hladina významnosti)

TK = 29,04456399 (testové kritérium)

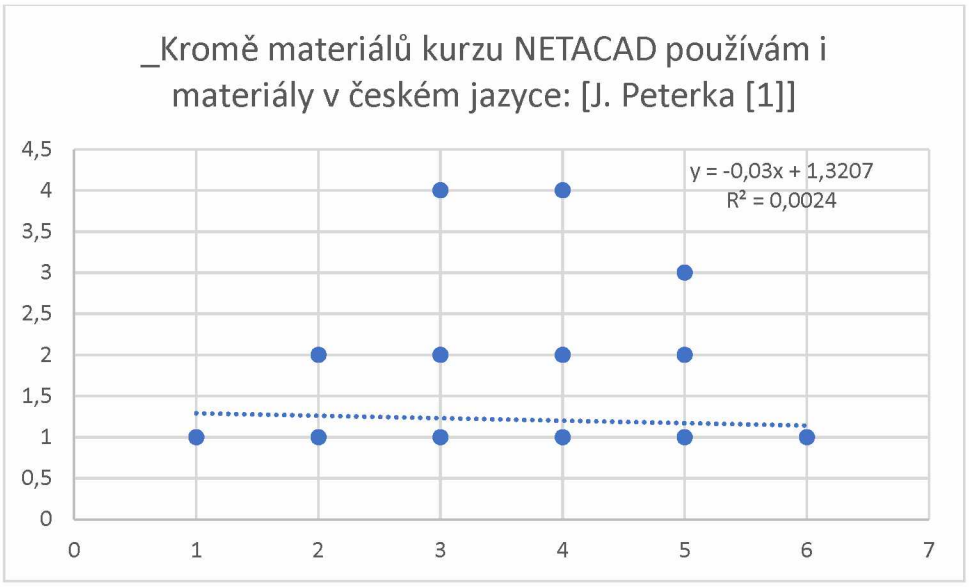
KH = 24,99579014 (kritická hodnota

p-hodnota= 0,057199145

Testovací kritérium je větší než kritická hodnota, H_{01} se zamítá

Používání doplňkových materiálů v českém jazyce se liší vzhledem k předchozím jazykovým znalostem

Korelace mezi znalostmi AJ a používáním materiálů (Peterka) je však zanedbatelná, korelační koeficient je téměř nulové hodnoty.



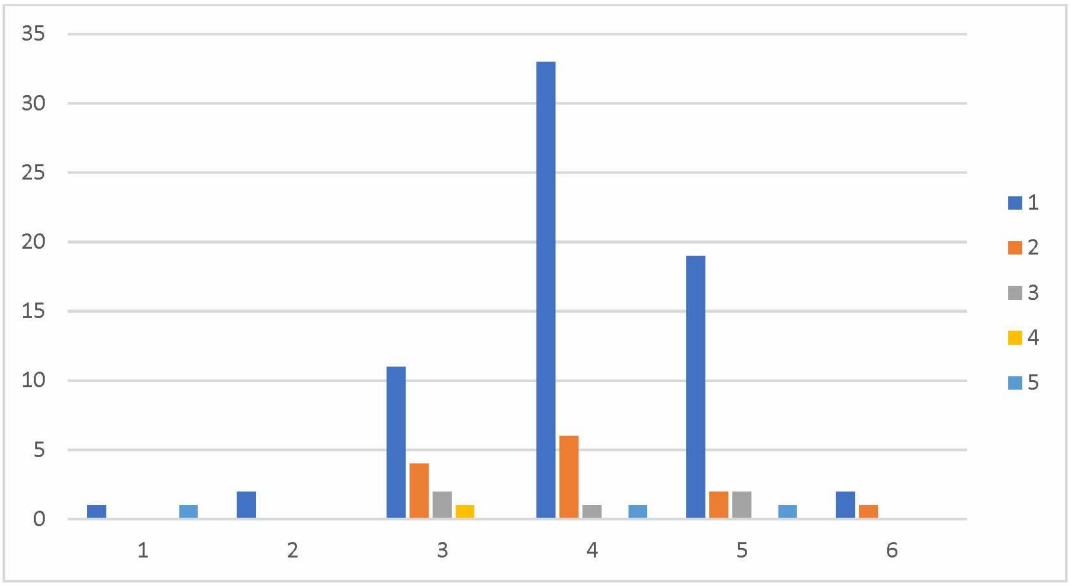
Graf 4 Závislost užívání materiálu v ČJ (Peterka) na znalostech AJ

Kromě materiálů kurzu NETACAD používám i materiály v českém jazyce:

jiné

(A1 – Začátečník, A2 – Pokročilý začátečník, B1 – Mírně pokročilý, B2 – Pokročilý, C1 – Velmi pokročilý, C2 – Expert)

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. stále)



Graf 5 Znalost AJ - české materiály jiné

Tabulka 7 *Empirické četnosti – H3 Jiné*

	1	2	3	4	5	Celkový součet
1	1				1	2
2	2					2
3	11	4	2	1		18
4	33	6	1		1	41
5	19	2	2		1	24
6	2	1				3
Celkový součet	68	13	5	1	3	90

Tabulka 8 *Teoretické četnosti – H3 Jiné*

	1	2	3	4	5	Celkový součet
1	1,511111111	0,288889	0,111111	0,022222	0,066667	2
2	1,511111111	0,288889	0,111111	0,022222	0,066667	2
3	13,6	2,6	1	0,2	0,6	18
4	30,97777778	5,922222	2,277778	0,455556	1,366667	41
5	18,13333333	3,466667	1,333333	0,266667	0,8	24
6	2,266666667	0,433333	0,166667	0,033333	0,1	3
Celkový součet	68	13	5	1	3	90

Byla použita Yatesova korekce pro výpočet chí-kvadrát.

$\alpha = 0,05$ (hladina významnosti)

TK = 40,39775147 (testové kritérium)

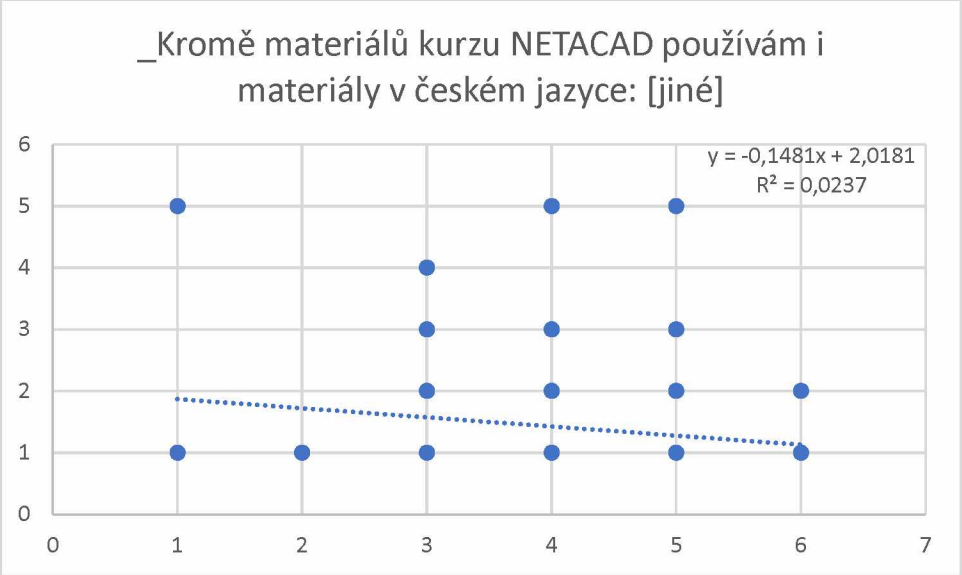
KH = 31,41043284 (kritická hodnota

p-hodnota= 0,057199145

Testovací kritérium je větší než kritická hodnota, H_{01} se zamítá

Používání doplňkových materiálů v českém jazyce se liší vzhledem k předchozím jazykovým znalostem

Korelace mezi znalostmi AJ a používáním materiálů (Peterka) je však zanedbatelná, korelační koeficient je téměř nulové hodnoty.



Graf 6 Závislost užívání materiálu v ČJ (Jiné) na znalostech AJ

2.3 Interpretace dat

2.3.1 Hypotéza 1

U hypotézy 1 se předpokládalo, že hodnocení obtížnosti kurzů bude rozdílné, a obtížnější bude pro účastníky s menšími odbornými znalostmi, pro obory jiného než IT zaměření.

Statisticky se však potvrdilo, že pro všechny obory nebo studijní zaměření se jeví obtížnost studia kurzů Cisco Netacad jako stejná.

2.3.2 Hypotéza 2

U hypotézy 2 se předpokládalo, že účastníci kurzů s menšími předchozími odbornými znalostmi počítačových sítí (IT) používají základní e-learningové materiály v AJ více

Statisticky se však potvrdilo, že Cisco Netacad materiály používají bez ohledu na úroveň odborných znalostí stejnou mírou.

2.3.3 Hypotéza 3

U hypotézy 3 se předpokládalo, že účastníci kurzů s menšími jazykovými znalostmi AJ používají doplňkové materiály v českém jazyce více.

Statisticky se však potvrdilo, že sice není na stanovené hladině významnosti míra používání materiálů v ČJ stejná pro různé znalosti AJ, nicméně korelace je prakticky zanedbatelné hodnoty.

3 Diskuze

Ze získaných statistických dat se jeví, že účastníkům kurzů Cisco Netacad zpravidla postačuje e-learnignový materiál v AJ, jiné zdroje používají spíše sporadicky, pravděpodobně jim postačuje k Cisco Netacad výklad v ČJ, a komentáře v ČJ k úlohám v AJ.

Lektoři Cisco Netacad předpokládají určitou nemalou míru používání materiálů při samostudiu, zdá se však, že reálně je mnohem menší, i přes vysokou úspěšnost v testech znalostí v kurzech.

4 Závěr

V práci byla popsána metodologie výzkumu, uvedena prezentaci výsledků výzkumu na základě dat sesbíraných dotazníkem a ověřených statistickými metodami. Na závěr jsou uvedeny získané poznatky, v příloze text použitého dotazníku

Cílem práce bylo zjistit míru používání e-learningových nástrojů Cisco Netacad a jiných studijních materiálů při výuce počítačových sítí v anglickém (AJ) nebo českém jazyce (ČJ) v závislosti na schopnosti komunikace v AJ, a na odborných znalostech (studijním oboru).

Z výzkumného šetření vyplynulo, že intuitivní předpoklady o míře využívání e-learningových materiálů a doplňkových materiálů, vzhledem k odborným nebo jazykovým znalostem, nebyly správné. Dle výsledků jsou míry používání materiálů prakticky nezávislé na odborných nebo jazykových znalostech.

Získané informace budou použity k optimalizaci výuky počítačových sítí, a používání kurzů Cisco Netacad obecně.

V dotazníkovém šetření bylo použito více otázek, jejichž vyhodnocení a statistické ověření bude předmětem dalšího zpracování.

Seznam použitých zdrojů

1. GAVORA, P. Úvod do pedagogického výzkumu. Brno: Paido, 2000. ISBN 80-85931-79-6.
2. CHRÁSKA, M. Metody pedagogického výzkumu. Olomouc: Univerzita Palackého, Pedagogická fakulta, 2016. ISBN: 978-80-247-5326-3.

Seznam použitých zkratek

AJ – anglický jazyk

ČJ – český jazyk

DELTA - DELTA – Střední škola informatiky a ekonomie, s.r.o.

DFJP – Dopravní fakulta Jana Pernera

IT – informační technologie

KH – kritická hodnota

TK – testovací kritérium

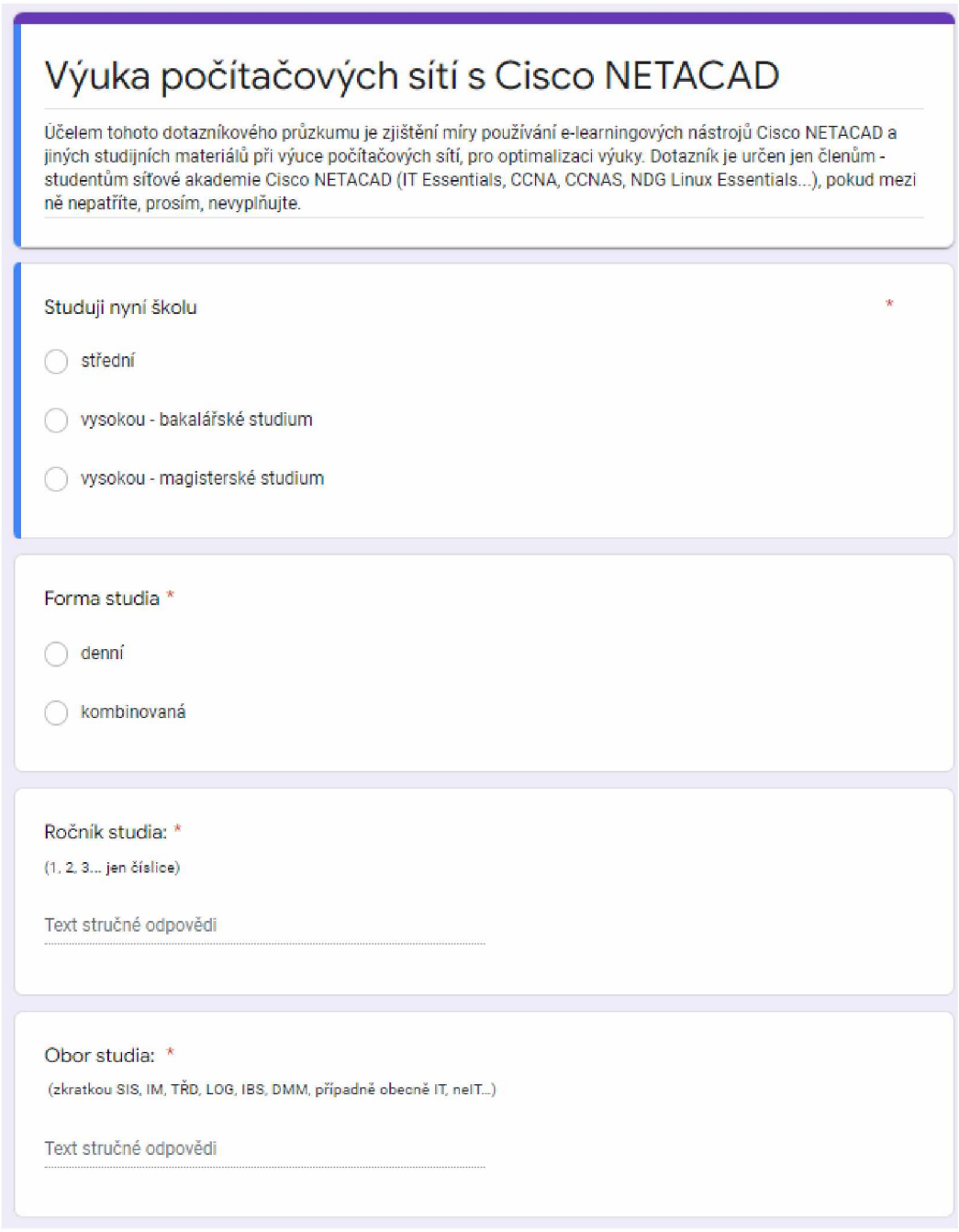
UPCE – Univerzita Pardubice

Seznam grafů

Seznam tabulek

Přílohy

Dotazník



Výuka počítačových sítí s Cisco NETACAD

Účelem tohoto dotazníkového průzkumu je zjištění míry používání e-learningových nástrojů Cisco NETACAD a jiných studijních materiálů při výuce počítačových sítí, pro optimalizaci výuky. Dotazník je určen jen členům - studentům síťové akademie Cisco NETACAD (IT Essentials, CCNA, CCNAS, NDG Linux Essentials...), pokud mezi ně nepatříte, prosím, nevyplňujte.

Studuji nyní školu *

- střední
- vysokou - bakalářské studium
- vysokou - magisterské studium

Forma studia *

- denní
- kombinovaná

Ročník studia: *

(1, 2, 3... jen číslice)

Text stručné odpovědi

Obor studia: *

(zkratkou SIS, IM, TŘD, LOG, IBS, DMM, případně obecně IT, nelT...)

Text stručné odpovědi

Kolik je mi let: *

(číslo)

Text stručné odpovědi

Kolik let školní výuky anglického jazyka (AJ) mám absolvováno: *

(číslo)

Text stručné odpovědi

Svoje všeobecné jazykové schopnosti v AJ hodnotím: *

(A1 – Začátečník, A2 – Pokročilý začátečník, B1 – Mírně pokročilý, B2 – Pokročilý, C1 – Velmi pokročilý, C2 – Expert)

	1	2	3	4	5	6	
A1 – Začátečník	○	○	○	○	○	○	C2 – Expert

Svoje předchozí znalosti (před kurzy NETACAD) v oblasti počítačových sítí hodnotím na úrovni: *

(1. Laik – jen uživatel, 2. Základní, 3. Střední, 4. Pokročilé, 5. Expert)

	1	2	3	4	5	
Laik – jen uživatel	○	○	○	○	○	Expert

Kolikátý kurz NETACAD nyní absolvuji, nebo již mám dokončený: *

(číslo)

Text stručné odpovědi

Při samostudiu používám studijní materiály kurzu NETACAD v anglickém jazyce: *

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. stále)

	1	2	3	4	5	
nikdy	○	○	○	○	○	stále

Na texty studijních materiálů (v AJ), kvízy, nebo testy kurzu NETACAD musím používat translátor: *

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. vždy)

	1	2	3	4	5	
nikdy	○	○	○	○	○	vždy

Z odborného (IT) hlediska považuji aktuální (nebo poslední absolvovaný) kurz NETACAD za: *

(1. lehký, 2. spíše lehký, 3. přiměřeně náročný, 4. spíše těžký, 5. těžký)

	1	2	3	4	5	
lehký	○	○	○	○	○	těžký

Úlohy kurzu NETACAD pro simulátor Packet Tracer samostatně zpracovávám: *

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. vždy)

	1	2	3	4	5	
nikdy	○	○	○	○	○	vždy

Kvízy a aktivity kurzu NETACAD samostatně zpracovávám: *

(1. nikdy, 2. občas, 3. často, 4. velmi často, 5. vždy)

	1	2	3	4	5	
nikdy	○	○	○	○	○	vždy

Kromě materiálů kurzu NETACAD používám i materiály v českém jazyce: *

(1. PETERKA, Jiří. Peterkův archiv http://www.earchiv.cz/; 2. PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z : technologie pro datovou, hlasovou i multimediální komunikaci. 2. aktualiz. vyd. [s.l.] : [s.n.], 2006. 430 s. ISBN 80-251-1278-0.; 3. ODOM, Wendell. Počítačové sítě bez předchozích znalostí. 1. vyd. Brno : CP Books, a.s., 2005. 384 s. ISBN 80-251-0538-5.)

	nikdy	občas	často	velmi často	stále
J. Peterka [1]	○	○	○	○	○
R.Pužmanová [2]	○	○	○	○	○
W.Odom [3]	○	○	○	○	○
jiné	○	○	○	○	○

Pokud používám jiné materiály - které to jsou:

(uveďte název, autora, knihu, web...)

Text stručné odpovědi

Celkově (z jazykového i odborného hlediska) považuji aktuální (poslední absolvovaný) kurz NETACAD za: *

(1. lehký, 2. spíše lehký, 3. přiměřeně náročný, 4. spíše těžký, 5. těžký)

	1	2	3	4	5	
lehký	○	○	○	○	○	těžký

Jiná sdělení nebo poznámky k Cisco NETACAD kurzům:

(volitelně)

Text dlouhé odpovědi