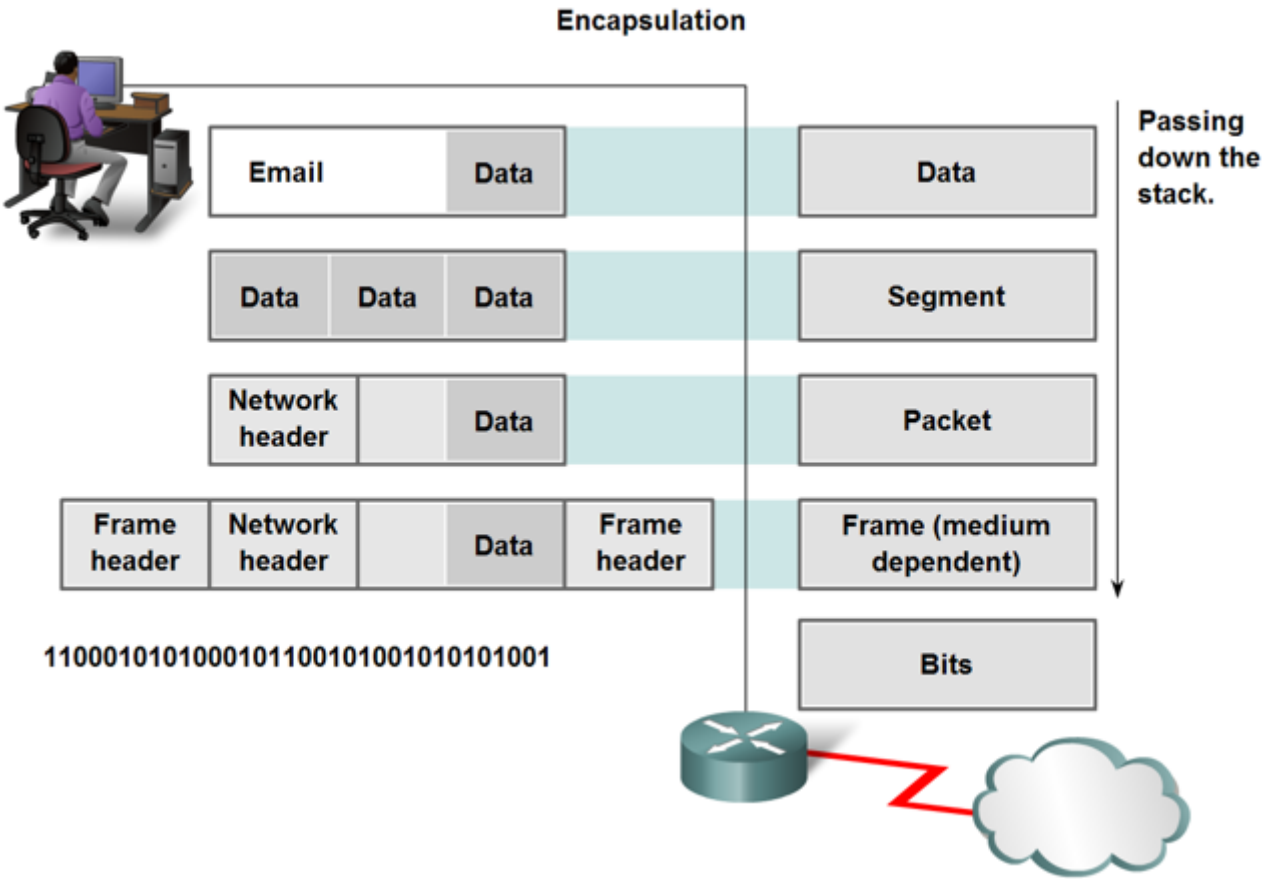
Cvicenie03

OBSAH

Úloha 3.1 - Čo vieme o modeloch sietí z druhej prednášky?

- v úvode si zopakujte formou spoločnej diskusie tému z prednášky, zamerajte sa na tieto body:
- referenčný a protokolový model, ktorý je ktorý?
- keď rozprávame o vrstvách L1, L2, ... LX..., je nám jasné na ktorý model sa odkazujeme? vždy referenčný!
- proces enkapsulácie, proces de-enkapsulácie
- PDU na jednotlivých vrstvách, čo tvorí rámec, čo paket, čo segment, čo sú to aplikačné dáta, majú aj oni nejakú hlavičku?
- v ktorej hlavičke sú logické a v ktorej fyzické adresy?
- ako odlíšime rôzne aplikačné procesy na jednom koncovom zariadení? Hint: L4, čísla/identifikátory.



Úloha 3.2 - Prieskum modelov TCP/IP a OSI pomocou programu Packet Tracer.

- Ciele:
  - Uvedomiť si do hĺbky proces enkapsulácie a dekapsulácie.
  - Pochopiť funkciu vrstiev TCP/IP aj OSI na praktickom príklade komunikácie web klienta s web serverom.
    - najprv s web serverom v LAN
    - potom so vzdialeným web serverom
  - Pochopiť ako sa menia informácie v hlavičkách, prečo sa menia, ktoré zariadenia ich menia, ktoré ich nemenia - pohľad zúžime iba na adresné informácie
  - Vedieť efektívne používať simulačný režim v programe Packet Tracer.

- Topológia k úlohe 3.2 (Packet Tracer) aj postup v slovenčine
- Instructions in English: PIKS_LAB_03.2_Investigation_TCP-IP_and_OSI_layers_in_PT_EN_2022_03_04_0600.docx

Úloha 3.3 - Analýza sieťovej prevádzky pomocou programu Wireshark.

- Ciele:

    - Zachytiť a analyzovať ICMP dáta vo Wiresharku pri komunikácií v lokálnej sieti
    - Zachytiť a analyzovať ICMP dáta vo Wiresharku pri vzdialenej komunikácií (mimo LAN)
    - Vedieť efektívne ovládať a pracovať v programe Wireshark

- Postup k úlohe 3.3:
    - v slovenčine: PIKS_LAB_03.3_Investigation_TCP-IP_model_in_Wireshar_SK_2022_03_04_0600.docx
    - v angličtine: PIKS_LAB_03.3_Investigation_TCP-IP_model_in_Wireshar_EN_2022_03_04_0600.docx

- Motivácia (poznámka za okraj):
    - Aj hackeri (tí etickí), využívajú Wireshark, a silu tohto nástroja, ktorou je široká škála filtrov, ktoré je možné v ňom využiť:
        - viac ako 242 000 polí v 3 000 protokoloch !!!
        - Link na zoznam filtrov:
            - z hacker-toolbelt: https://medium.com/hacker-toolbelt/wireshark-filters-list-983c49468a45
            - z oficiálnej stránky Wireshark.org: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

Úloha 3.4 - Základná konfigurácia prepínača

Siete sú tvorené tromi základnými komponentami: koncovými stanicami, prepínačmi a smerovačmi. V tejto úlohe budete pracovať v malej sieti s 2 koncovými stanicami a 2 prepínačmi.

- Nakonfigurujete základné nastavenia prepínača.
- Zabezpečíte prístup k príkazovému riadku prepínača a konzolovým portom s použitím šifrovaného aj nešifrovaného hesla.
- Nakonfigurujete správy pre používateľov logujúcich sa na daný prepínač, ktoré sa používajú na varovanie neautorizovaných osôb, ktorých prístup na dané zariadenie je zakázaný.
- Použijete show príkazy pre zobrazenie bežiacej konfigurácie, verzie IOSu a stavu jeho rozhraní.
- Použijete príkaz copy pre zálohovanie konfigurácie do trvalej pamäte.
- Koncovým staniciam nastavíte IP adresy a otestujete konektivitu v takejto sieti pomocou príkazu ping medzi koncovými stanicami.

Pri spúšťaní zadania na túto úlohu, ktorá je hodnotená, treba v okne **User profile** vyplniť svoje reálne **Priezvisko_Meno**, presne v tom tvare a **bez**

interpunkcie, nie opačne. následne Vás aplikácia upozorní, že sa zadanie resetne, potvrdíte OK, a začnete riešiť úlohu. Mail ani Additional info zadávať netreba.

- Pri ukladaní je potrebné názov **odovzdávaného súboru** .pka doplniť o Vaše priezvisko a meno presne takto: PIKS_LAB_03.4_Basic_switch_configuration_2023_03_01_**Priezvisko_Meno**.pka (priezvisko a meno musí byť bez diakritiky).
- Používajte Check Results - Assesment items - skúste získať všetky body. Kto získa plné skóre, dostane za túto úlohu 3 body, kto získa menej, dostane pomerovo také percento bodov, koľko odpovedá jeho získanému skóre.
- V Moodle máme priestor na odozvdanie tejto úlohy.

- Topológia k úlohe 3.4 (Packet Tracer) + postup v slovenčine
- Instruction in English: PIKS_LAB_03.4_Basic_switch_configuration_EN_2022_03_04_0600.docx

---

Úloha 3.5: Preskúmať posielanie správy adresovanej ako unicast, broadcast a multicast.

Aktivita pre rýchlejšie skupiny.

Otvorte si pripravenú topológiu siete s 5 smerovačmi, prepojenými 1 prepínačom a sledujte v simulačnom móde prechod správ typu unicast, broadcast a multicast.

Topológia k úlohe 3.5 (Packet Tracer)

Úloha 3.6 - Prieskum štandardizačných organizácií

- Aktivita pre rýchlejšie skupiny.
- Ciele:
  - Vysvetliť význam štandardizačných organizácii a protokolov v sieťach.
  - Vyhľadať hlavné štandardizačné organizácie (Networking Standards Organizations).
  - Zamyslieť sa nad možnosťami internetu a počítačových sieti.

- Postup k úlohe 3.6:
  - v slovenčine: PIKS_LAB_03.6_Investigation_of_standardization_organizations_SK_2022_03_04_0600.docx
    v angličtine: TBD

Celosemestrálny projekt [úloha 02+03]: Analýza zabezpečenia prístupu k sieťovým zariadeniam vo svojej sieti

Inštrukcie k forme spracovania, hodnoteniu a kde nájsť priestor na odovzdanie: v sekcii Moodle pre 8. týždeň semestra nájdete odkaz: Semestrálny projekt

1. Preskúmajte a spíšte výsledky svojho prieskumu vo svojej domácej sieti (resp. v sieti, ktorú ste si zvolili pre svoj celosemestrálny projekt na 1. cvičení) pre každé sieťové zariadenie:

- akú formu konfigurácie Vám umožňujú vaše zariadenia - grafické prostredie (GUI), príkazový riadok (CLI), iné? ako sa dá pristúpiť ku konfigurácii daných zariadení? (konzola/vty/ssh/aux/web prehliadač/iné?)
    - popíšte bližšie, ako k nim pristupujete
- akú úroveň zabezpečenia viete nakonfigurovať na zariadeniach z hľadiska prístupu k nim?
    - máte zabezpečený prístup k manažmentu zariadenia heslom? menom a heslom? inak?
        - používate predvolené nastavenia od výrobcu? Ak áno, pokúste sa zmeniť tieto nastavenia a popíšte úspešnosť výsledku
- aký operačný systém (prípadne aký firmware) majú vaše zariadenia? (rozlíšenie týchto pojmov, OS vs. firmware možno prečítať napr. tu)
    - je aktuálny?
        - ak nie, viete ho aktualizovať (update/upgrade)?
        - prečo je dôležité mať najaktuálnejší OS/firmware?
    - je open-source alebo proprietárny?

2. Prvá analýza sieťovej prevádzky z/do vašej domácej siete

- Nainštalujte si doma program Wireshark na svojom PC a použite ho na odchytenie dát, ktoré prichádzajú alebo odchádzajú z vašej sieťovej karty.
    - Pre Linux je Wireshark už súčasťou štandardného balíčka, viď info na stránke uvedenej vyššie (treba sa prerolovať úplne dole)
    - Pre Windows - Ak ste pri inštalácii vo Windws zvolili Npcap, a program WireShark nepracuje, tak odinštalujte Npcap a zopakujte inštaláciu, ale pri zvoľte Winpcap namiesto Npcap.
- Analyzujte, aké protokoly (stĺpec Protocol vo Wiresharku v prvom okne) je vidieť pri odchytávaní dát prechádzajúcich z/do vašej domácej siete
    - Analyzujte zapúzdrenie dát - hlavičky L2, L3, L4, L7 ISO OSI (v TCP/IP sú to L1, L2, L3, L4)
        - Ktorý protokol má viditeľné hlavičky všetkých 4 vrstiev? Aké?
        - Ktorý protokol má viditeľné iba niektoré nižšie vrtsvy? Aké?
        - Ktorý protokol u vás v zachytených dátach prevažuje?

- vo Wireshark menu je možné nájsť aj zobrazenie si Štatistík - Statistics -: Protocol Hierarchy, -> I/O graphs (počty paketov za sekundy vstupujúce/vystupujúce vašou NIC)
- Pozrite si aj iné položky v menu Statistics vo Wireshark-u, zaujala Vás niektorá z nich, resp. pohľad na dáta ktoré vám poskytuje? Ak áno, čo vás na tom zaujalo?