



SVEUČILIŠTE U ZAGREBU



Fakultet
elektrotehnike i
računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

Sigurnost podatkovnog sloja



Creative Commons



- **slobodno smijete:**

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo



- **pod sljedećim uvjetima:**

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, prerađu možete distribuirati samo pod licencom koja je ista ili slična ovoj.



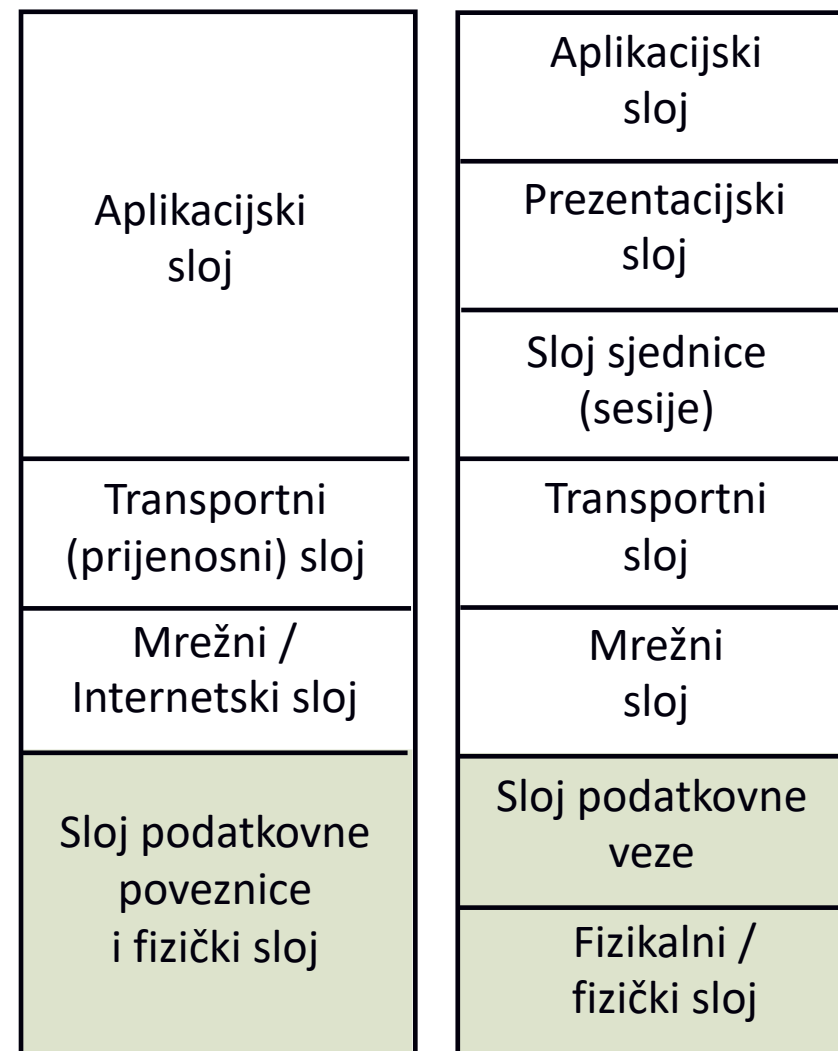
U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Sadržaj

- općenito o podatkovnom sloju
- sigurnost lokalnih mreža
- elementi lokalne mreže Ethernet
- ranjivosti
- zaštita mreže Ethernet
- osnovno o sigurnosti ostalih podatkovnih mreža

Općenito o podatkovnom sloju

- drugi sloj ISO/OSI referentnog modela
- sve „ispod Interneta”
- zadaća
 - omogućiti komunikaciju dva direktno povezana računala/mrežna uređaja
- niz bitnih i manje bitnih protokola/tehnologija
- Ethernet, xDSL, 2G/2.5G/3G/4G/5G, POTS/ISDN, WiMax, FrameRelay, ATM



Ethernet

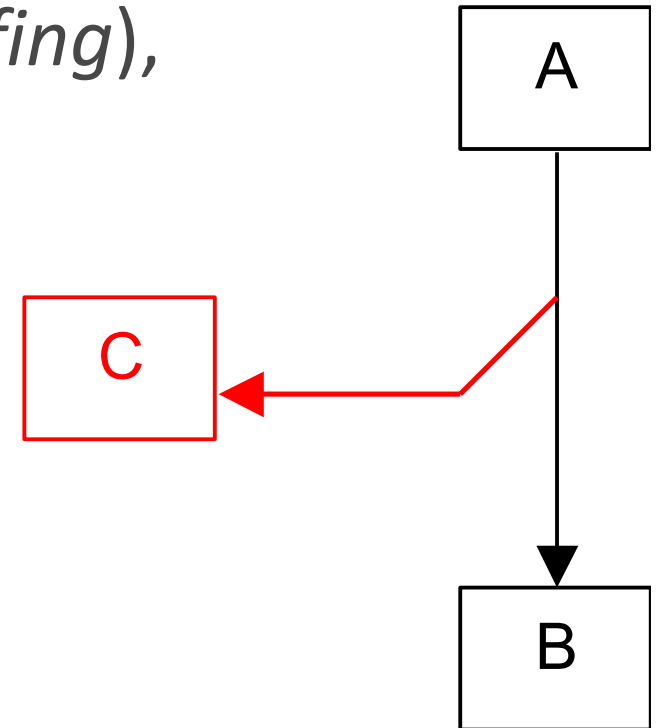
- izuzetno popularna mreža
 - u lokalnim mrežama gotovo da i nema alternative
- vrlo velik raspon brzina koje ta mreža pokriva
 - od 10 Mbps do 100 Gbps
 - razvoj 400 Gbps i planovi/potreba za Tbps brzinama
- u žičnoj (bakar i optika) i bežičnoj varijanti
 - žični i bežični Ethernet se na fizičkom sloju potpuno razlikuju, na podatkovnom manje (iz perspektive mrežnog sloja su svi identični)
- dodatna upotreba
 - povezivanje lokacija na području grada (Metro Ethernet)
 - industrijski Ethernet

Elementi mreže Ethernet

- ključne komponente žične mreže Ethernet
 - preklopnici (komutatori, engl. switch) (prije: koncentratori, engl. hub)
 - kabe - vertikalno i horizontalno kabliranje
 - bakrene žice i optika
- bežični Ethernet se temelji na pristupnim točkama
 - uglavnom se spaja na žični Ethernet
- dodatno se na mreži nalaze i drugi uređaji koji na prvi pogled ne izgledaju kao preklopnici i/ili računala
 - VoIP telefoni

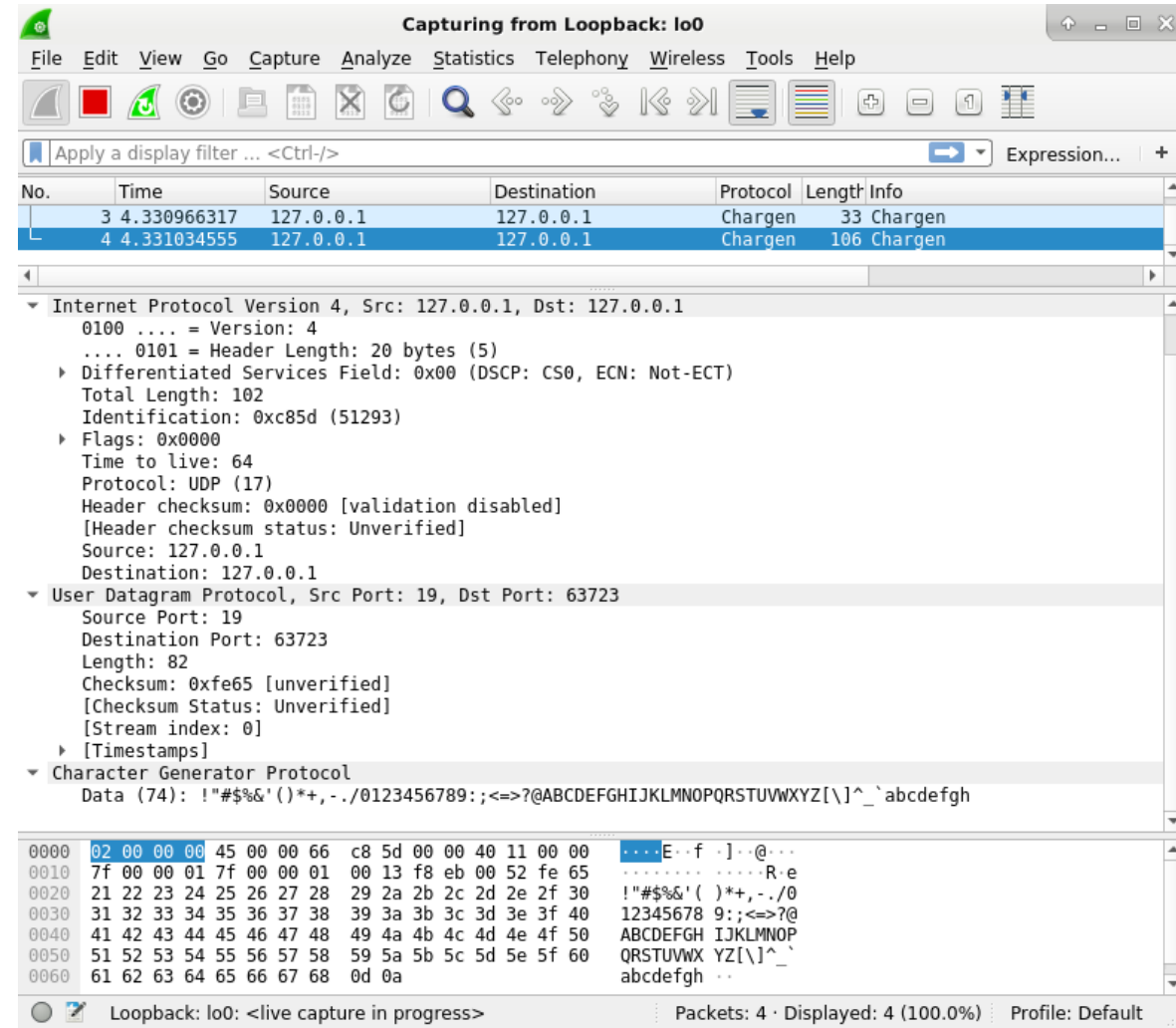
Presretanje, prisluškivanje

- **Presretanje** (*interception*), prisluškivanje (*evesdropping*), **njuškanje** mreže (*network sniffing*), prisluškivanje na vodu (*wiretapping*)
 - elektronička komunikacija se presreće i preuzima informacija
 - Potencijalne štete
 - Neovlaštena uporaba podataka
 - Potencijalno narušavanje privatnosti
- Zakonski regulirano presretanje (*lawfull interception*)



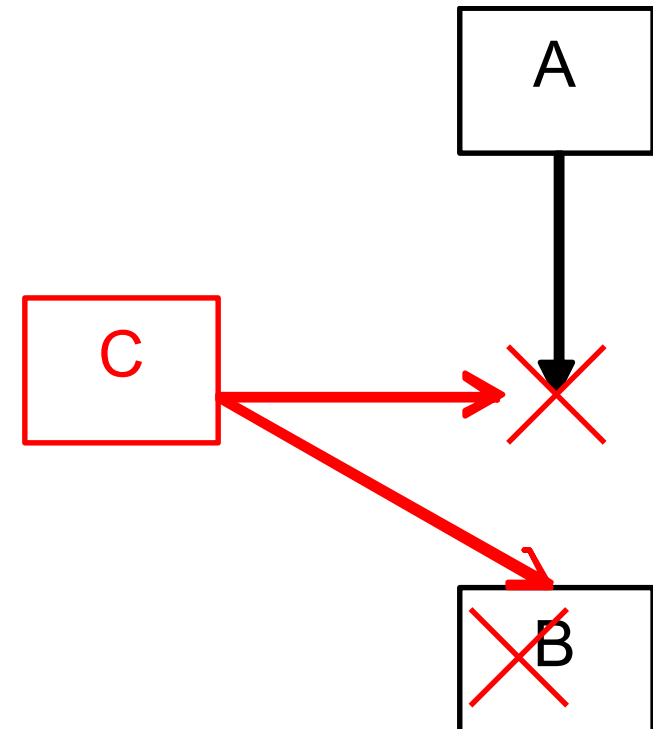
Network sniffing

- temelj za mnoge napade
 - napadač postavlja svoju mrežnu karticu u promiskuitetni način rada - vidi sav promet na tom segmentu
 - mrežna kartica predaje sve pristigle pakete IP sloju
 - mnogi protokoli prenose autentifikacijske podatke u obliku čistog teksta => username/password itd.
- alati: Wireshark, tcpdump, ...



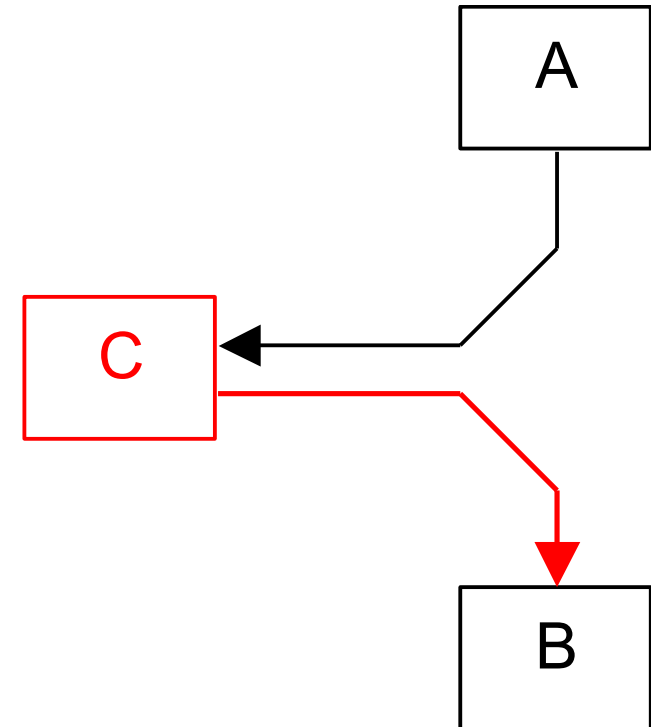
Prekidanje, uskraćivanje

- **Prekidanje** (engl. interruption)
 - prekidanje normalnog tijeka komunikacije, usluge ili aplikacije
- Uskraćivanje usluge (engl. denial of service)
 - onemogućavanje usluge izazivanjem preopterećenja mreže ili umreženog sustava



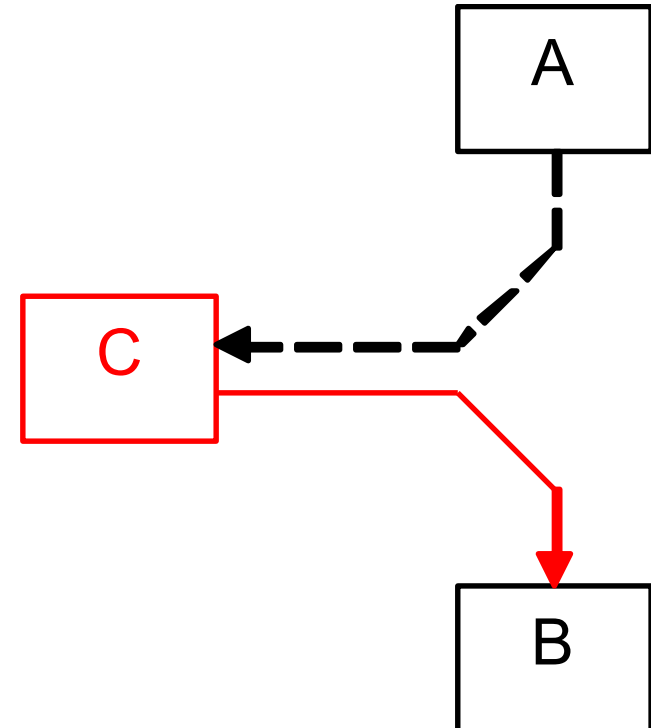
Promjena, kašnjenje

- Promjena (engl. modification, tampering)
 - Promjena ili uništenje informacije
 - Kašnjenje može izazvati isti učinak – podatak postaje nevažan



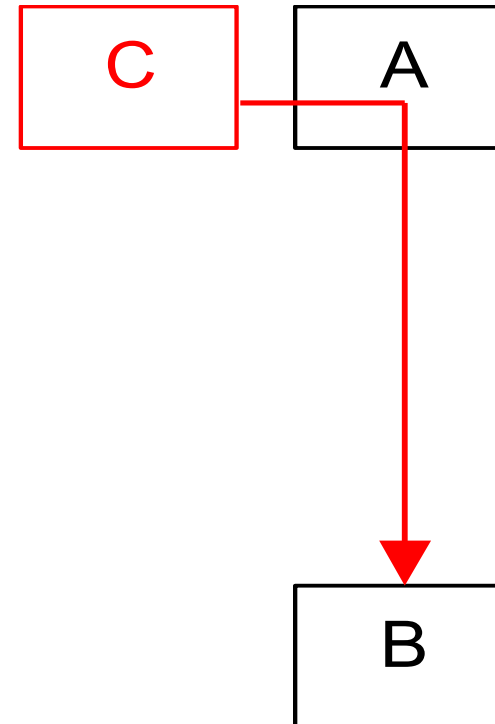
Umetanje, ponavljanje

- Umetanje, ubacivanje (engl. fabrication)
 - Ubacivanje zlonamjerne informacije
- Ponavljanje (engl. replay)
 - Ubacivanje informacije prethodno preuzete presretanjem



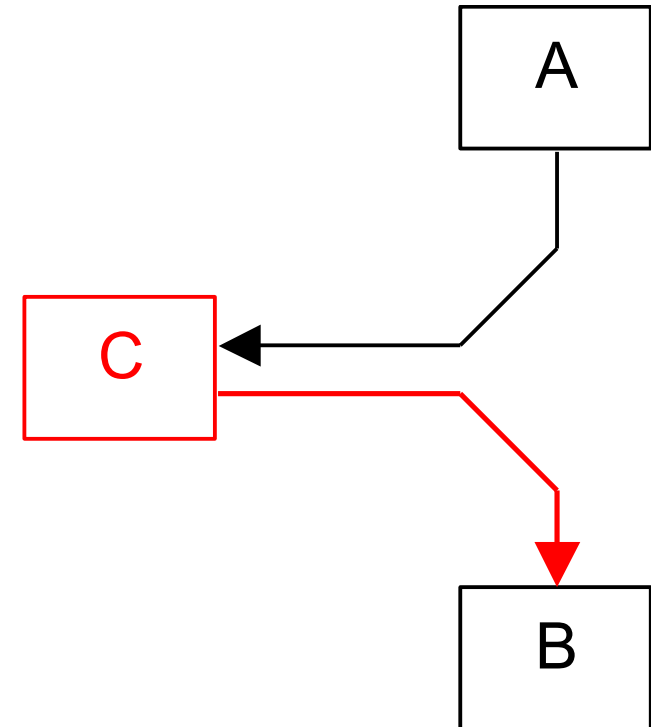
Lažno predstavljanje

- Lažno predstavljanje
 - Maskiranje (engl. masquerade)
 - Lažno predstavljanje (engl. impersonation)
 - Preuzimanje identiteta i uloge korisnika



„Čovjek u sredini”

- Često se u kontekstu komunikacija govori o napadu „čovjek u sredini”
 - engl. Man in the Middle, MITM
- To je situacija u kojoj su prisutne sve prethodno spomenute prijetnje
 - Kako bi sve navedene prijetnje bile ostvarive napadač se mora nalaziti negdje na putu kojim se prenose podaci
- Najbolji položaj za napadača i najgori za branitelja



Cilj napadača u slučaju mreže Ethernet

- neovlašteni pristup mreži
 - manipulacija prometom na mreži
- sve to je vrlo vjerojatno tek **međukorak** u nekom **složenijem napadu**
 - pristupiti lokalnoj mreži ili preuzeti kontrolu nad njom i ne činiti ništa nema baš nekog smisla(!)
- neke mogućnosti zloupotrebe pristupa Ethernet mreži
 - preuzimanje kontrole nad preklopticima
 - enumeracija, **praćenje prometa** i aktivnosti na mreži
 - **pretvaranje** da se radi o nekome drugome

Preduvjeti napada na Ethernet mrežu

- računalu s odgovarajućim ovlastima na mreži
- pristup mreži
 - fizički pristup nekoj komponenti mreže
 - žicama, mrežnim priključnicama, preklopnici (+konzola)
 - omogućavaju direktan pristup mreži
 - pristup putem Interneta
 - pristup preklopnici preko usmjernika
 - pristup nekom računalu već spojenom na mrežu
 - trojanci
 - udaljeni rad (VNC, RDP, TeamViewer, ssh)

Fizički pristup lokalnoj mreži (1)

- manipulacija žica
 - bakrene vodiče (UTP CATn) je vrlo jednostavno manipulirati
 - optiku je puno teže manipulirati, ali ne i nemoguće
 - posebno problematično vertikalno povezivanje (*backbone*)
- pristup mrežnim utičnicama
 - priključivanje vlastitih računala
 - posebno problematične utičnice koje se nalaze u javnim prostorima!

Fizički pristup lokalnoj mreži (2)

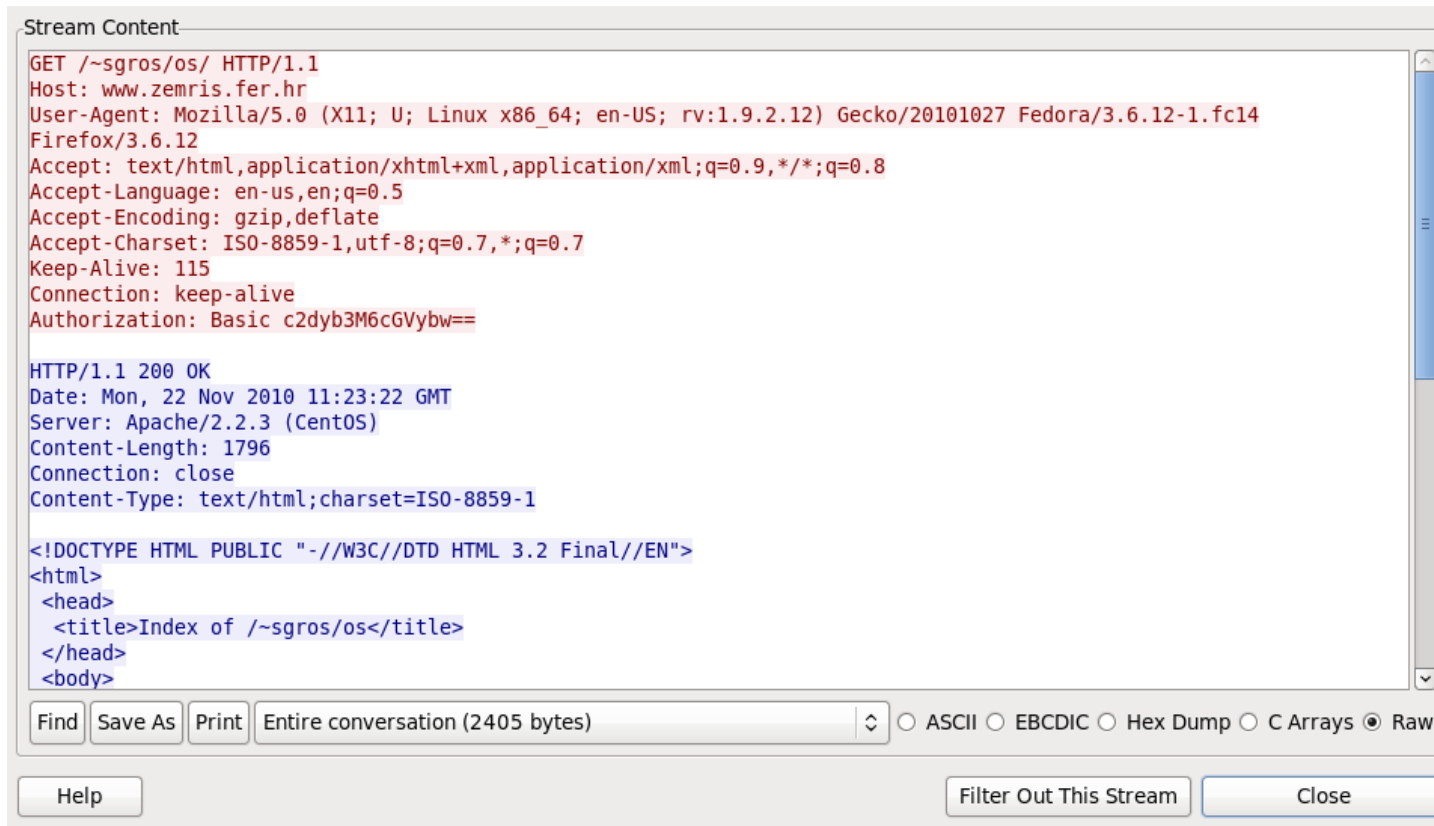
- pristup preklopticima
 - direktno spajanje na preklopnike i pristup linkovima za vertikalno povezivanje
 - zamjena preklopnika i manipulacija njegovim OS-om
 - pristup konzoli
 - telnet(!), web(!), ssh
 - jednostavni DoS napadi

Prisluškivanje prometa (1)

- najjednostavnije je prisluškivati promet (engl. sniffing)
 - pasivni napad
 - mrežne kartice prihvaćaju samo određeni promet
 - s odgovarajućim ovlastima to možemo promijeniti
 - tzv. *promiscuous mode*
- što se postiže na taj način?
 - praćenje prometa na mreži
 - dohvat povjerljivih informacija (npr. lozinke)
- koliko je to teško?
 - izuzetno jednostavno!
 - alati npr. tcpdump, wireshark, ngrep,...

Prisluškivanje prometa (2) - primjer

- promet snimljen tijekom prijave na HTTP Web stranicu i rekonstruiran u jednostavni tekst



```
Stream Content
GET /~sgros/os/ HTTP/1.1
Host: www.zemris.fer.hr
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.12) Gecko/20101027 Fedora/3.6.12-1.fc14
Firefox/3.6.12
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Authorization: Basic c2dyb3M6cGVybW==

HTTP/1.1 200 OK
Date: Mon, 22 Nov 2010 11:23:22 GMT
Server: Apache/2.2.3 (CentOS)
Content-Length: 1796
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /~sgros/os</title>
</head>
<body>
```

Find Save As Print Entire conversation (2405 bytes) ☐ ASCII ☐ EBCDIC ☐ Hex Dump ☐ C Arrays ☒ Raw

Help Filter Out This Stream Close

Prisluškivanje prometa (3)

- problem za napadača
 - ethernet mreža je preklapana mreža
 - ne stiže **sav promet** do **svih mrežnih** kartica
 - krajnja računala promet vide samo pod određenim uvjetima
- "rješenje": zlorabiti lošu implementaciju
 - ograničen spremnik MAC adresa
 - primjerice HP ProCurve 2600 serija

	horizontal surface mounting only	horizontal surface mounting only
Performance		
Latency	< 13.3 μ s (LIFO)	< 12 μ s (LIFO)
Throughput	up to 10.1 million pps	up to 10.1 million pps
Routing/Switching capacity	13.6 Gbps	13.6 Gbps
MAC address table size	8000 entries	8000 entries
Environment		

Prisluškivanje prometa (4)

- uobičajen rad preklopnika
 - uči položaj MAC adresa na temelju izvorišne adrese
 - zaboravlja nakon nekog vremena naučene adrese
- napad na preklopnik u kojemu se generira mnoštvo lažnih MAC adresa
 - u trenutku kad se MAC tablica prepuni, preklopnik se degenerira u koncentrator (moguće pratiti sav promet)
- zaštita
 - ograničenje broja MAC adresa po portu
 - fiksiranje nekih kritičnijih MAC adresa

Sigurnost protokola ARP

- protokol ARP služi za povezivanje IP i MAC adresa
 - vrlo jednostavan i nezaštićen protokol
- ideja napada – slati lažirane ARP odgovore
- mogućnosti koje napadač ima na raspolaganju
 - otimanje komunikacije (engl. hijacking)
 - praćenje i izmjena prometa koji prolazi između dvije strane koje komuniciraju
 - pretvarati se da smo izvor informacija
 - uskraćivanje usluge

Ranjivost protokola ARP

- ARP - protokol za pretvaranje 32 bitnih IP adresa u 48 bitne Ethernet (MAC) adrese
- ako računalo A želi poslati IP datagram računalu B ili usmjeritelju u lokalnoj mreži, tada ono mora znati njegovu MAC adresu
- A šalje broadcast ARP zahtjev na mrežu (uključujući svoje preslikavanje)
- B odgovara računalu A, porukom ARP odziv
- preslikavanje se lokalno pohranjuje u svakom računalu u ARP cache:
\$ arp -an

Ranjivost protokola ARP

tip hardvera (2 okteta)		tip protokola (2 okteta)
duljina hw adrese (1 oktet)	duljina prot. adr. (1 oktet)	kod operacije (2 okteta)
hardverska (ethernet, MAC) adresa pošiljatelja (6 okteta)		
IP adresa pošiljatelja (4 okteta)		
hardverska (ethernet, MAC) adresa primatelja / cilja (6 okteta)		
ciljna IP adresa (4 okteta)		

- ovisno o tipu poruke, određena polja su prazna:
 - za ARP: odredišna HW adresa,
 - za RARP: sve osim izvorišne HW adrese.

Napad na ARP

- ARP nema ugrađene mehanizme autentifikacije
- moguće je poslati odgovor prije pravog računala te vratiti lažno preslikavanje adresa (IP/HW)
- lažni ARP odgovori mogu se koristiti za spremanje krivih ARP preslikavanja na računalu kome su upućeni
- ARP poruke mogu se slati kontinuirano kako bi se (lažni) podaci zadržali u *cacheu*

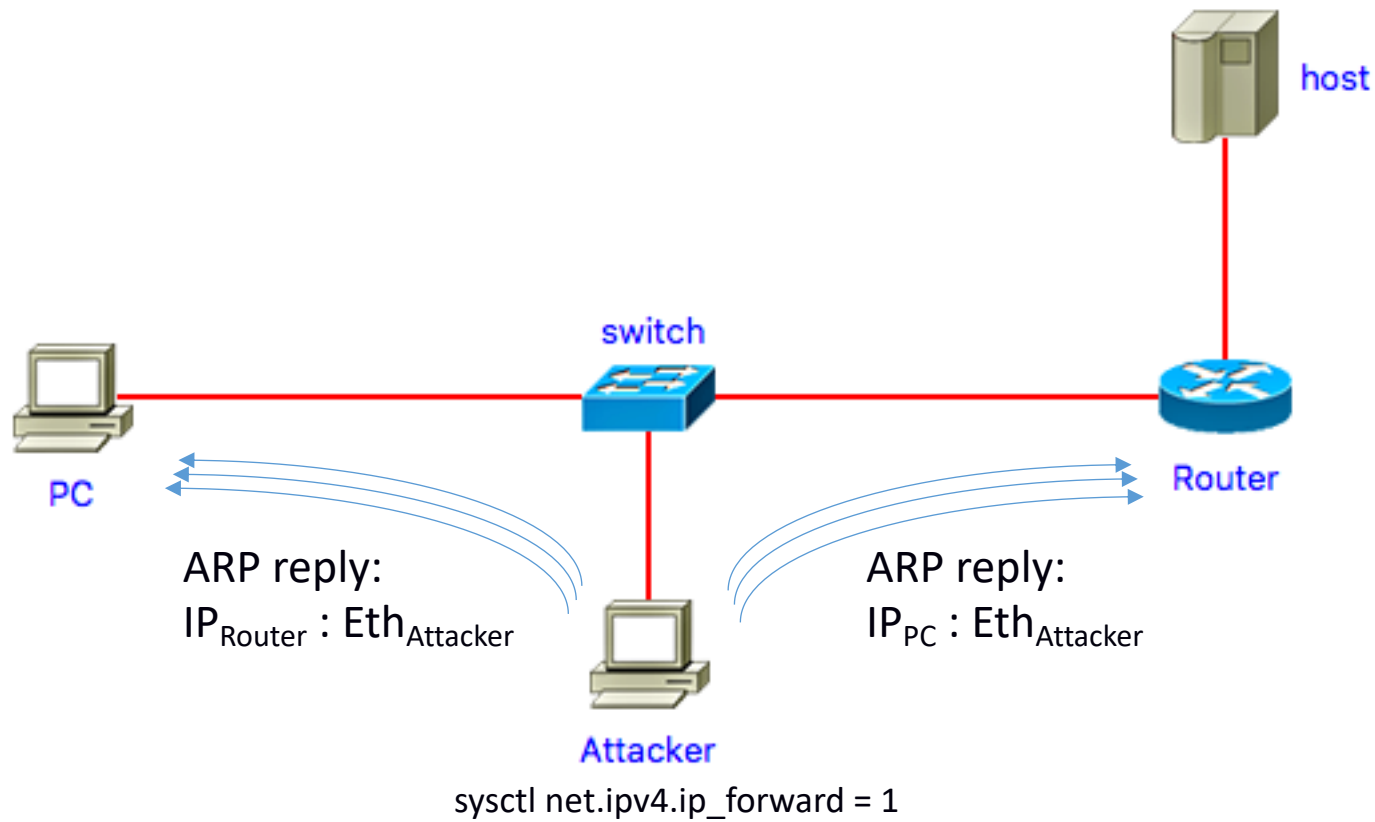
Napadi mogući iskorištavanjem protokola ARP

- slanje nepostojećih MAC adresa za IP adrese
 - nemogućnost komunikacije - uskraćivanje usluge (DoS)
- ubacivanje između lokalnog usmjernika/poslužitelja i žrtve
 - napadač može pratiti svu komunikaciju i snimati tajne podatke
 - utjecati na komunikaciju
- skeniranje mreže u potrazi za aktivnim uređajima
 - arping, nmap
- vrlo poznat alat ettercap za provođenje napada
 - slobodno dostupan na Internetu
 - sadrži i GUI te omogućava „point-and-click” napade

Napad na ARP

- Cilj:
 - Prisluškivanje prometa (preklopnik, komutator (switch) prosljeđuje ethernet okvire između mrežnih sučelja na temelju ethernet adrese odredišta)
 - Prekidanje: lažno preslikavanje IP adrese usmjeritelja na nepostojeću MAC adresu (DoS napad)
 - Promjena
 - Ometanje
- alati: arpoison, ettercap, dsniff, parasite

Napad na ARP



Napad na ARP - otkrivanje i zaštita

- ako je preuzimanje bilo uspješno, malo je vjerojatno da će korisnici napadnutog računala išta primijetiti
- najjednostavniji način: ispis *ARP cachea*
 - ako se MAC adresa od određene IP adrese promijenila napadačevo računalo se identificira s pomoću te MAC adrese te po mogućnosti fizički odspaja s mreže
- može se detektirati s nekog trećeg računala, na kojem se njuška mreža i traže lažni ARP odzivi
- u slučaju DoS napada, lagano je ustanoviti da nešto nije u redu

Napad na ARP - zaštita

- ako postoji neobično ponašanje u mreži korisno je pogledati ARP *cache*
- korištenje hardvera koji će učiniti takve napade nemogućima ili više vidljivima
 - korištenje komutatora, *switch*, s mogućnošću “zaključavanja” priključaka (*port security*)
- onemogućavanje ARP-a i njegova ručna konfiguracija

Zaštita od manipulacija korištenjem protokola ARP

- ograničenja manipulacije protokolom ARP
 - radi isključivo unutar jedne difuzne (engl. broadcast) domene
 - napadnuto računalo mora već imati zapis MAC-IP za računalo s kojim mu želimo prekinuti komunikaciju
- zaštita
 - statički zapisi
 - praćenje ARP prometa
 - preklopnici mogu pratiti promjene u suradnji s DHCP poslužiteljem/protokolom

IPv6 – NDP

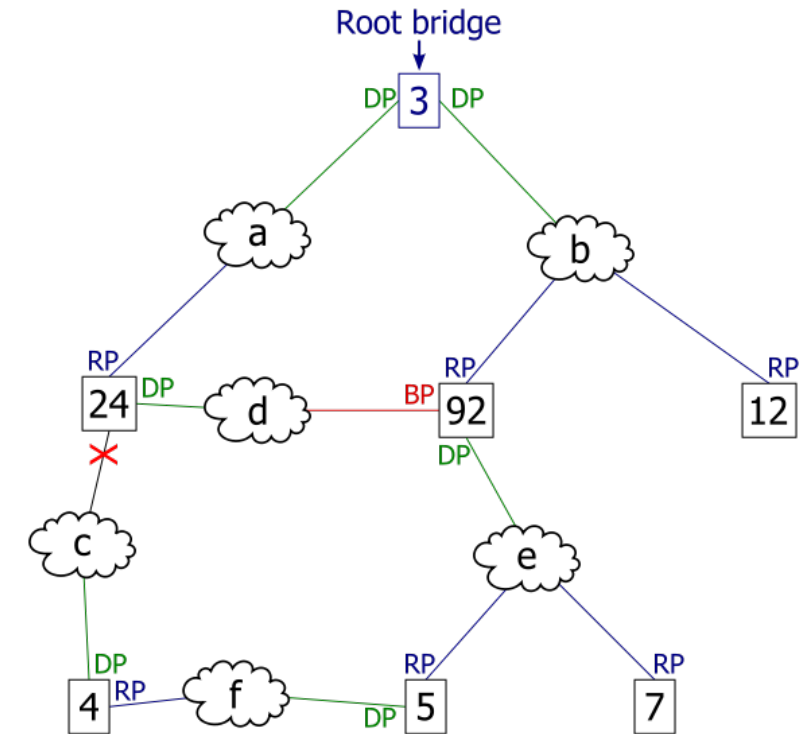
- ARP je zamijenjen protokolom NDP - "Neighbor Discovery Protocol" (ICMPv6)
 - nema autentifikacije (kao ni ARP)
 - statički zapisi prepisuju se dinamičkim
 - ARP Spoofing ---> NDP Spoofing
- dostupni alati
 - "THC – The Hacker Choice": Parasit6, Fakerouter6, ...

IPv6 – SEND

- protokol SEND - "Secure Neighbor Discovery"
 - NDP + kriptografska zaštita
- CGA - Cryptographically Generated Addresses (RFC 3972)
 - svaki uređaj ima par RSA ključeva (ne treba certifikat)
 - valjanost se djelomično provjerava
 - zaštita od NDP *spoofinga*, onemogućen *spoofing* valjane CGA adrese
- nedostaci:
 - usmjeritelji moraju obavljati puno kriptografskih operacija (dio se može odraditi unaprijed)
 - potencijalni DoS jer usmjeritelj mora čuvati puno stanja
 - dostupno na Unixoidnim sustavima (Windows ?)

Protokol R/STP

- Ethernet mreža je izuzetno automatizirana
 - učenje MAC adresa
 - redundantni putovi (petlje)
 - mogu u potpunosti zagušiti mrežu
- protokoli Spanning Tree Protocol (STP, 802.1D) i Rapid Spanning Tree Protocol (RSTP, 802.1w)
 - koriste algoritam razapinjućeg stabla (engl. spanning tree):
 - razmjenjuju BPDU podatkovne jedinice (engl. bridge protocol data unit)
 - parametri: identifikatori i težine, prenosnika i pristupa
 - cilj: ostvariti topologiju stabla s najjačim preklopnici u centru



Ranjivosti protokola R/STP (1)

- faze protokola
 - odabir korijenskog premostnika (engl. root bridge)
 - odabir korijenskih pristupa (engl. root ports)
 - odabir odabranih pristupa (engl. designated ports)
 - promjena stanja pristupa
- stanja pristupa
 - onemogućen (engl. disabled)
 - blokirajući – samo prihvata BPDU-ove (20s)
 - osluškuje – prihvata i proslijeđuje BPDU-ove (15s)
 - učenje – tablica proslijeđivanja se izgrađuje (15s)
 - proslijeđuje – podatkovni promet se proslijeđuje

Ranjivosti protokola R/STP (2)

- namjerna **modifikacija topologije**
 - radi uskraćivanja usluge (stalno u procesu otkrivanja topologije)
 - radi preusmjeravanja prometa
- izvršenje napada je relativno jednostavno
 - unutar Linux operacijskog sustava nalazi se implementiran protokol STP
 - vrlo je jednostavno napraviti **premosnik koristeći** operacijski sustav Linux
- problem (za napadača!)
 - **velika količina** prometa

Ranjivosti protokola R/STP (3)

- zaštita
 - zabraniti protokol STP na priključnicama gdje su krajnje stanice
 - Cisco terminologija: BPDU Guard
- zabraniti pristupima da postanu korijenski pristupi
 - Cisco terminologija: Root Guard

Implementacija virtualnih LAN mreža

- IEEE 802.1Q, (Dot1q): virtual LANs (VLANs)
- vrlo popularna metoda za izolaciju prometa
- dodatno 32-bitno polje u zaglavlju; između izvorišne MAC adrese i polja EtherType
- komunikacija između VLAN-ova isključivo preko usmjernika/vatrozida
- jedan preklopnik poslužuje više virtualnih LAN mreža
 - VLAN za goste (samo pristup Internetu), VLAN za knjigovodstvo, poslužitelje, ...
- preklopnici se međusobno povezuju „trunkovima”
- svaki pristup preklopnika može
 - biti isključivo u jednom VLAN-u
 - biti u više VLAN-ova
 - biti u više VLAN-ova s podrazumijevanim VLAN-om

Napadi na VLAN mreže (1)

- problem s automatskim povezivanjem više VLAN-ova (engl. dynamic trunking); napad „switch spoofing”
 - dodavanje računala koje se predstavlja kao preklopnik
- dvostruko označavanje (engl. double tagging)
 - napadač šalje okvir s dvije oznake
 - prvi preklopnik uklanja prvu oznaku i šalje okvir prema drugom preklopniku putem *trunk* porta (po prvom VLAN-u)
 - drugi preklopnik vidi drugu oznaku VLAN-a

Napadi na VLAN mreže (2)

- kako bi napad dvostrukog označavanja radio potrebno je
 - napadač i žrtva moraju biti na različitim preklopnicima
 - napadač mora znati MAC adresu žrtve
 - napadač ima isti VLAN ID kao i podrazumijevani na trunku
- zaštita
 - ne koristiti nativni VLAN
- potencijalno VLAN preskakanje uz pomoć usmjernika
 - usmjerniku se šalje okvir s njegovom MAC adresom i odredišnom adresom žrtve u drugom VLAN-u

Dinamičko konfiguriranje računala

- dodjela IP adresa nekad:
 - Reverse ARP, RARP - samo IP adresa, bez adresa DNS poslužitelja
 - i Bootstrap Protocol, BOOTP (dodatni podaci za bootanje preko mreže)
- Dynamic Host Configuration Protocol, DHCP
 - kompatibilan s BOOTP, koristi iste portove
 - može efikasno dodjeljivati adrese iz skupa raspoloživih adresa
 - IP adresa može biti fiksirana uz MAC adresu
 - standardno na svim operacijskim sustavima (za IPv4)
 - ograničen na jednu podmrežu ali usmjeritelji mogu podržavati "relay" agente
- DHCPv6

Protokol DHCP

- Služi za automatsku dodjelu adresa i mrežnih parametara
 - Klijent šalje svima na mreži poruku DHCPDISCOVER
 - Klijent u tom trenutku ne zna adresu
 - Poslužitelji odgovaraju klijentu s porukom DHCPOFFER
 - Klijent odabire poslužitelj i šalje svima DHCPREQUEST
 - Poslužitelj odgovara s DHCPACK
- Fiksiranje adresa na temelju MAC adrese radi kontrole pristupa
 - Moguće i na temelju identifikatora

Protokol DHCP

- klijent šalje UDP zahtjev na broadcast adresu 255.255.255.255 port 67
- DHCP poslužitelj šalje ponudu adrese
 - u pravilu treba biti jedan DHCP poslužitelj u podmreži
 - u ponudi se standardno nalazi puno dodatnih podataka: *default router*, adrese DNS poslužitelja

Problemi protokola DHCP

- Nema nikakve zaštite poruka
 - Bilo tko može slati i primiti DHCP poruke
- Lažni DHCP poslužitelji na mreži
 - Napadi uskraćivanja usluga
 - Preusmjerenje prometa
- Bilo koji klijent može zatražiti parametre
 - Lako se zaobilazi MAC/ID zaštita
 - Moguće iscrpljivanje svih raspoloživih adresa („DHCP Starvation attack“)

Ostali mogući problemi u lokalnoj mreži Ethernet

- protokol **SNMP**
 - davanje informacija o preklopniku
 - mogućnost promjene podataka u preklopniku
- protokoli **LLDP** (Link Layer Discovery Protocol) i CDP (Cisco Discovery Protocol)
 - davanje podataka o topologiji mreže
- udaljen pristup preklopniku (telnet/ssh/Web)
 - napadi pogađanjem lozinke
 - korištenje zasebnog VLAN-a

Zaštita lokalne mreže Ethernet (1)

- fizička infrastruktura mora biti zaštićena
 - vertikalno kabliranje u kanalicama
 - horizontalno kabliranje posebno zaštićeno
 - mrežne utičnice koje se dulje ne koriste moraju biti isključene
 - preklopnici u zaključanim ormarićima pod odgovarajućim nadzorom
- koristiti upravljive preklopnike
 - ispravna autentikacija pristupa upravljačkom modulu
 - izoliranje prometa po VLAN-ovima
 - autentikacija prije pristupa mreži (802.1x)
 - ograničenje broja MAC adresa po pristupu
 - isključiti upravljačke protokole na pristupima gdje se ne očekuju drugi preklopnici
 - neupravljivi preklopnici ne nude nikakvu zaštitu
 - treba ih izbjegavati!

Zaštita lokalne mreže Ethernet (2)

- računala i aplikacije
 - korisnici na računalima bez administratorskih ovlasti
 - spriječena instalacija programa i manipuliranje podatkovnim slojem
 - antivirusni alati radi zaštite od malicioznog koda
 - strogi nadzor i kontrola udaljenog pristupa
 - korištenje kriptiranja radi zaštite integriteta, tajnosti i autentičnosti podataka (SSL, IPsec)

Ostali protokoli podatkovne veze

- ADSL se uzima za pristup Internetu
 - ekonomski najisplativija opcija za surfanje
 - moguć vektor ulaska u zaštićenu mrežu
- primjer ranjivosti
 - D-Link „backdoor”
- krivo podešeni ADSL usmjernici mogu propustiti napadače u lokalnu mrežu
- modemski pristup
 - danas se vrlo rijetko koriste
 - potencijalna opasnost od njihova otkrivanja i ulaska u mrežu