SVEUČILIŠTE U ZAGREBU

Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2023./2024.

Sigurnost transportnog 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, preradu 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.

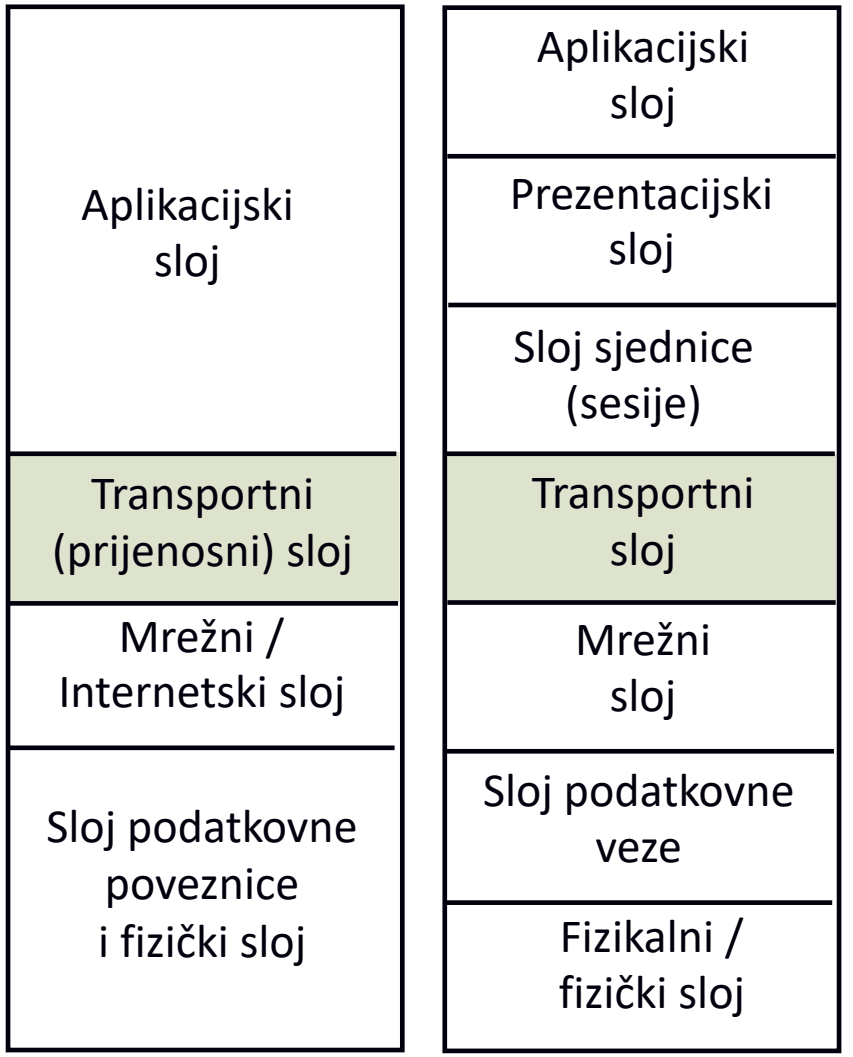
Tekst licencije preuzet je s http://creativecommons.org/.

Sadržaj

- općenito o prijenosnom sloju
- temelji protokola UDP
- napadi na protokol UDP
- temelji protokola TCP
- napadi na protokol TCP
- sigurnosna rješenja

Općenito o transportnom sloju

- omogućava komunikaciju s kraja-na-kraj
- najčešći protokoli na Internetu:
  - TCP (~70%) i UDP (~30%)
  - postoje još SCTP, DCCP, QUIC
- protokol TCP
  - upotrebljava ga niz aplikacija (web (http/https), elektronička pošta, protokoli usmjeravanja, prijenos datoteka, udaljeni rad, ...)
- sve češća upotreba protokola UDP:
  - višemedijske aplikacije, VoIP, neki sistemski protokoli Interneta (DNS)

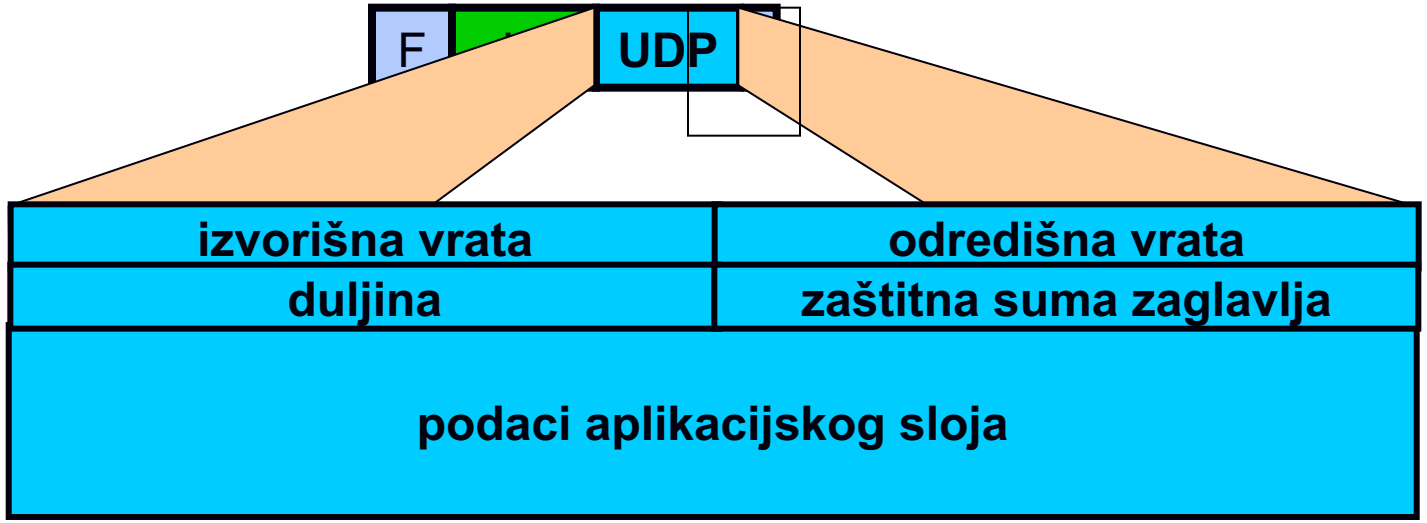


Protokol UDP

- Nespojni transportni protokol
- Nema ugrađene mehanizme za pouzdan prijenos
- Nema kontrole toka
- Često se koristi za prijenos višemedijskih podataka (efikasniji je od TCP) i za usluge temeljene na principu zahtjev / odziv (DNS, NIS, NFS, RPC)

Protokol UDP

- duljina UDP zaglavlja: 8 okteta



Napadi na UDP

- UDP obmana - (UDP *spoofing*)
  - mijenjanjem izvorišne IP adrese “predstavljamo se” kao drugo računalo
  - IP adresa je jedini način identifikacije računala u protokolu UDP
  - ne šalju se potvrde
- UDP otimanje - (UDP *hijacking*)
  - napadač sluša vezu
  - odgovara na klijentov UDP zahtjev prije poslužitelja slanjem paketa s promijenjenom izvorišnim adresom
  - klijent misli da je primio paket od poslužitelja
  - nema identifikacije paketa

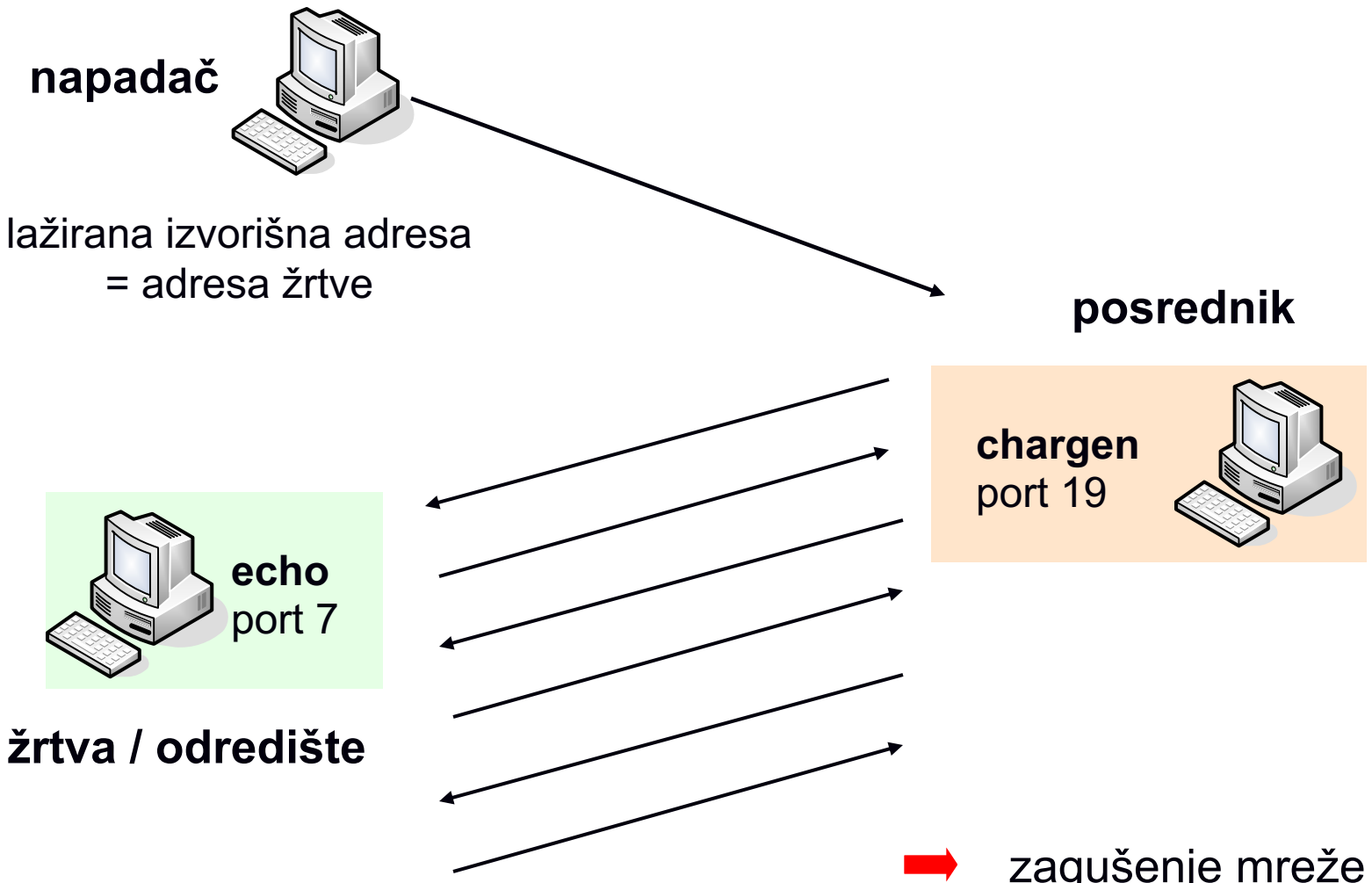
Napadi na UDP

- UDP oluje - (UDP *storms*)
  - jedan paket je dovoljan za pokretanje napada!
  - obično se pošalje nekoliko paketa kako bi se pojačalo djelovanje
  - može se koristiti bilo koji servis koji automatski odgovara na primljeni UDP datagram: echo (7), chargen (19), daytime (13), time (37), …
  - i usmjeritelji često podržavaju nekoliko dijagnostičkih usluga
  - petlja se izvodi dok jedno računalo ne završi (može biti potreban i reboot)

UDP Small Services

Naziv	*Port*	Opis usluge
echo	7/udp	server echoes the data that the client sends
daytime	13/udp	server returns the time and date in a human readable format
chargen	19/udp	server responds with a datagram containing a string of ascii characters
time	37/udp	server returns the time as a 32-bit binary number

UDP storm / UDP flood



➡ zagušenje mreže

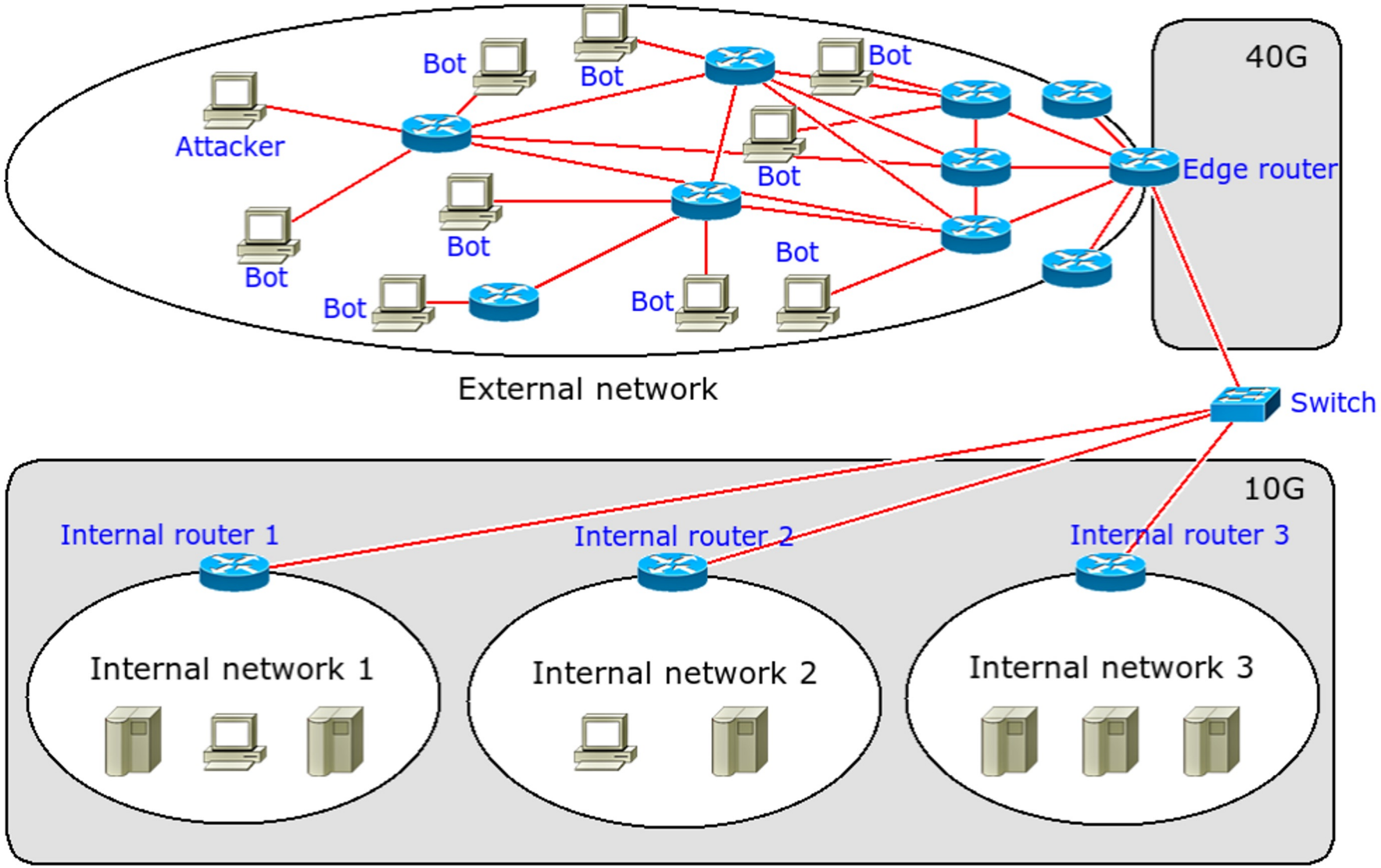
DoS - Napadi uskraćivanja usluge

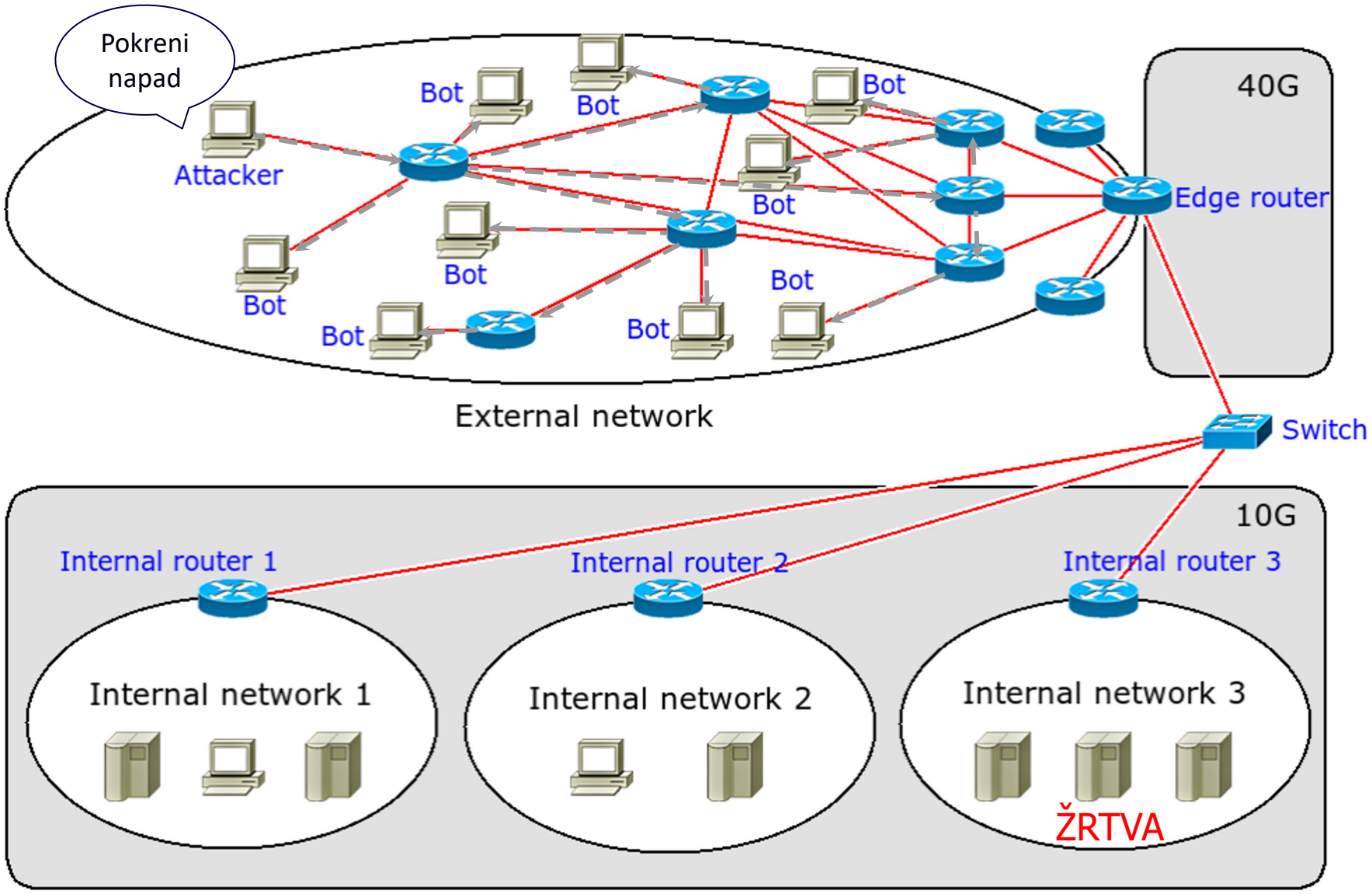
- DoS: Denial of Service / DDoS: Distributed Denial of Service
- nisu specifični za mrežni ili prijenosni sloj
  - bilo koje ograničeno sredstvo može biti cilj napada
    - pristupni link, memorija, CPU, disk, ...
  - cilj napada može biti i nekakva pogreška u aplikaciji ili protokolu
- obrana vrlo teška i ovisi o konkretnom napadu i specifičnostima samog napada
  - u određenim slučajevima nužna je suradnja s ISP-om
  - dobro je unaprijed planirati razne situacije
- posljedice napada mogu biti katastrofalne za žrtvu
  - nedostupnost ima novčane i reputacijske posljedice

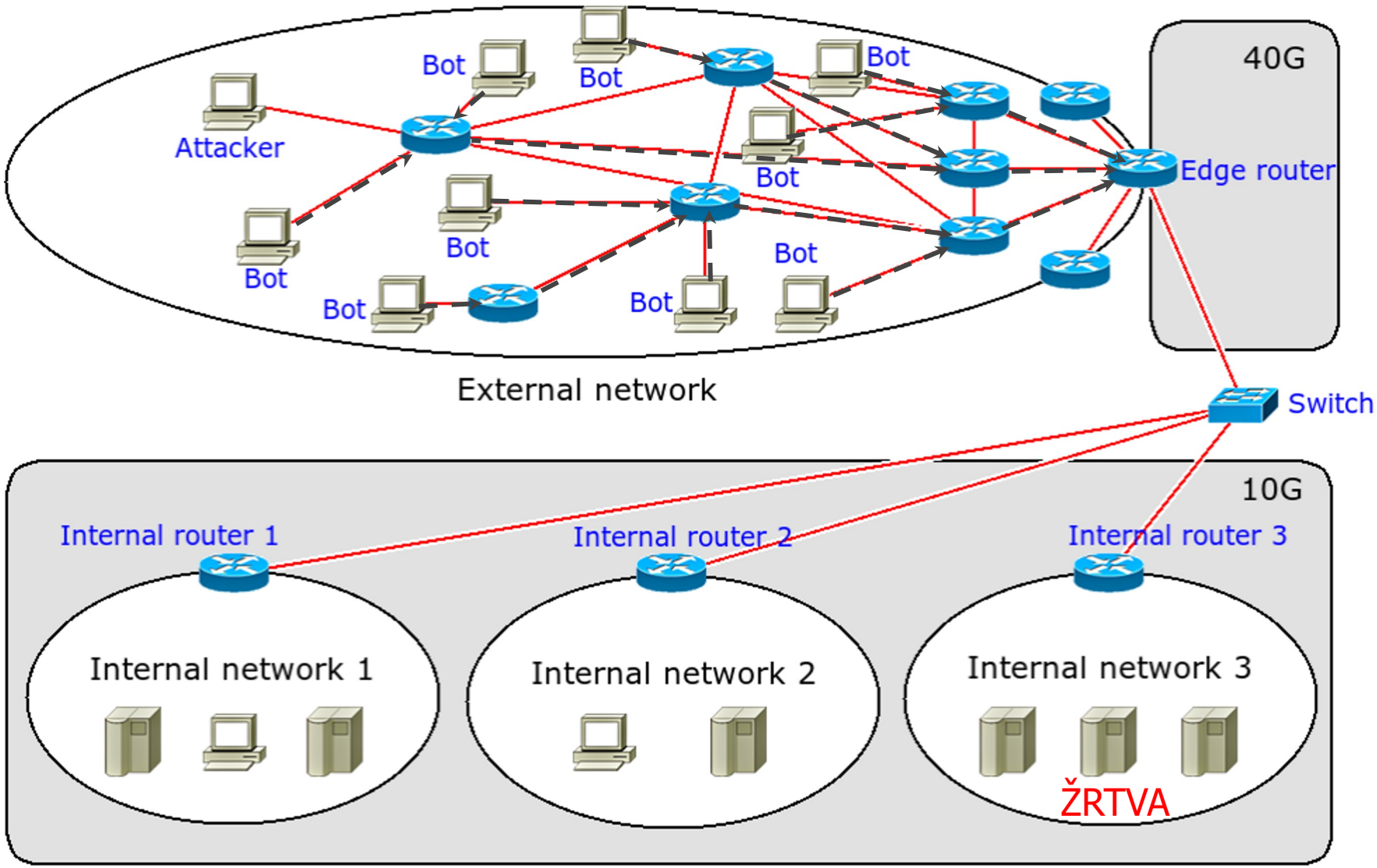
Mehanizam za provođenje napada

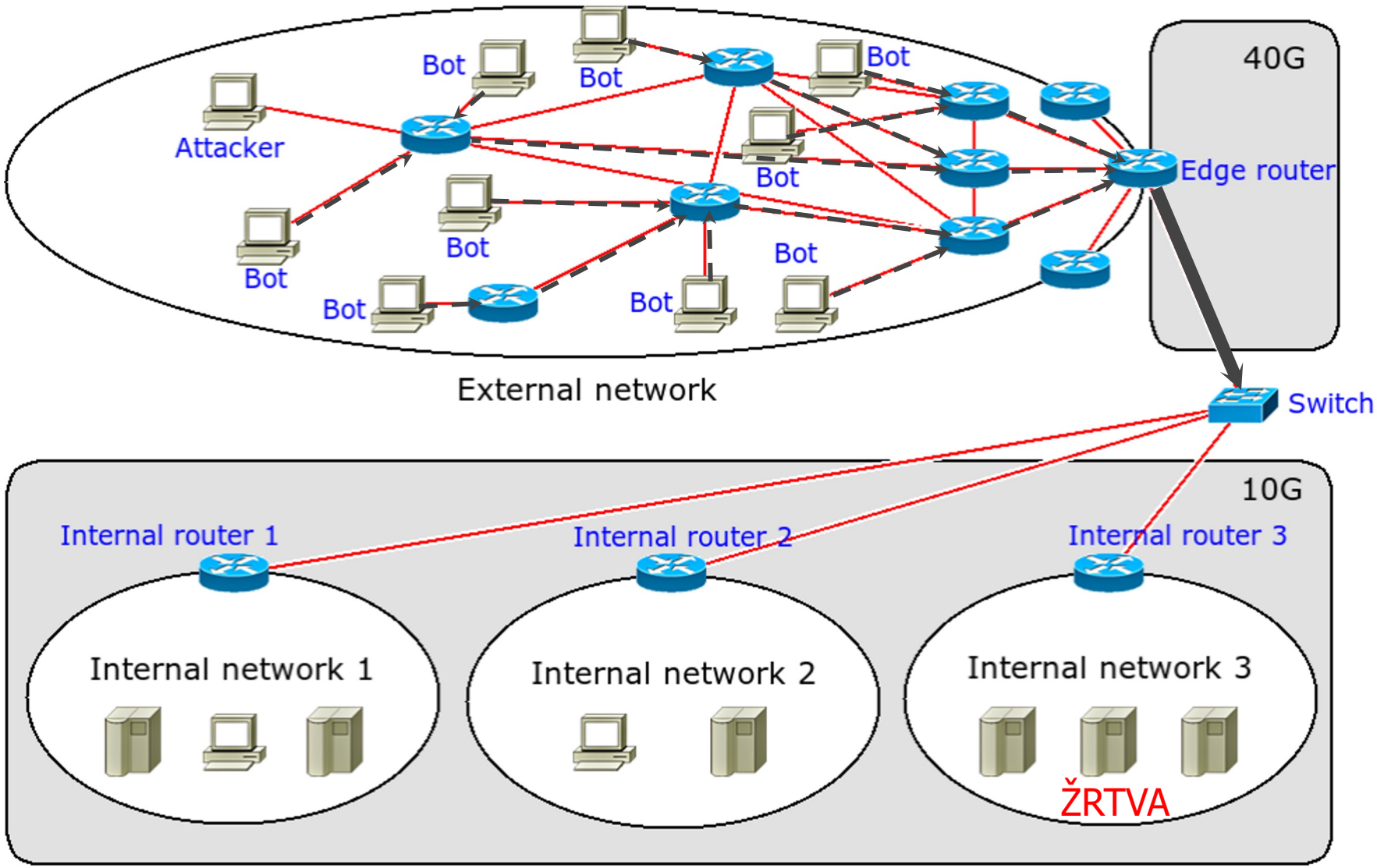
- „botmasteri” zaraze velik broj računala koja tvore „botnet”
  - može biti i više od 100,000 zaraženih računala
  - svako zaraženo računalo se naziva *bot* ili *zombie*
- komunikacija s *botnetom* se odvija preko C&C (Command and Control)
  - komunikacija između zaraženih računala i C&C odvija se putem IRC-a, HTTP-a ili P2P protokolom
- uklanjanje *bota*
  - nije moguće/nema smisla djelovati na pojedina računala
  - napadači su često prikriveni
  - preuzimanje C&C je najčešći način

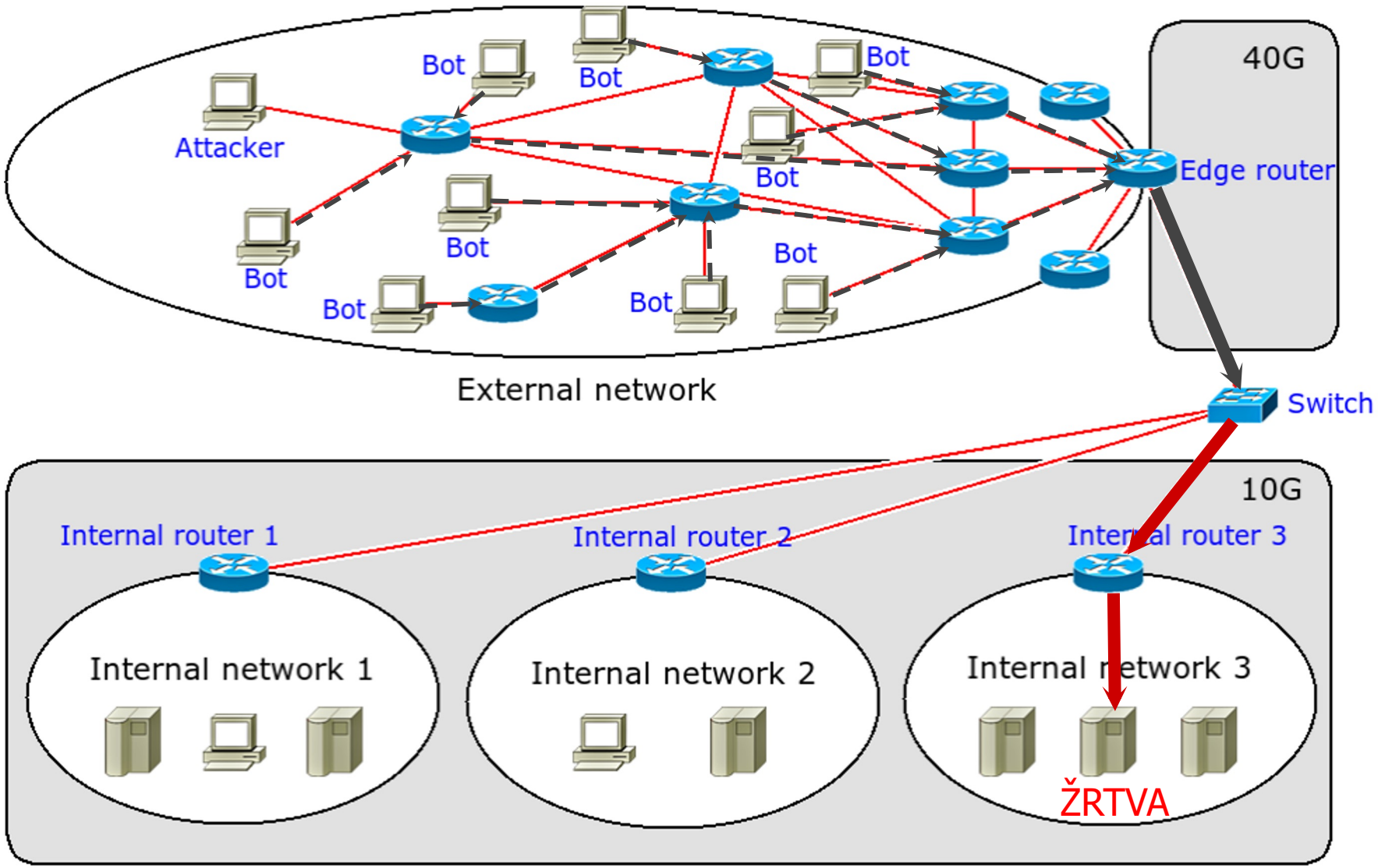
DDoS napadi (Distributed Denial-of-Service)

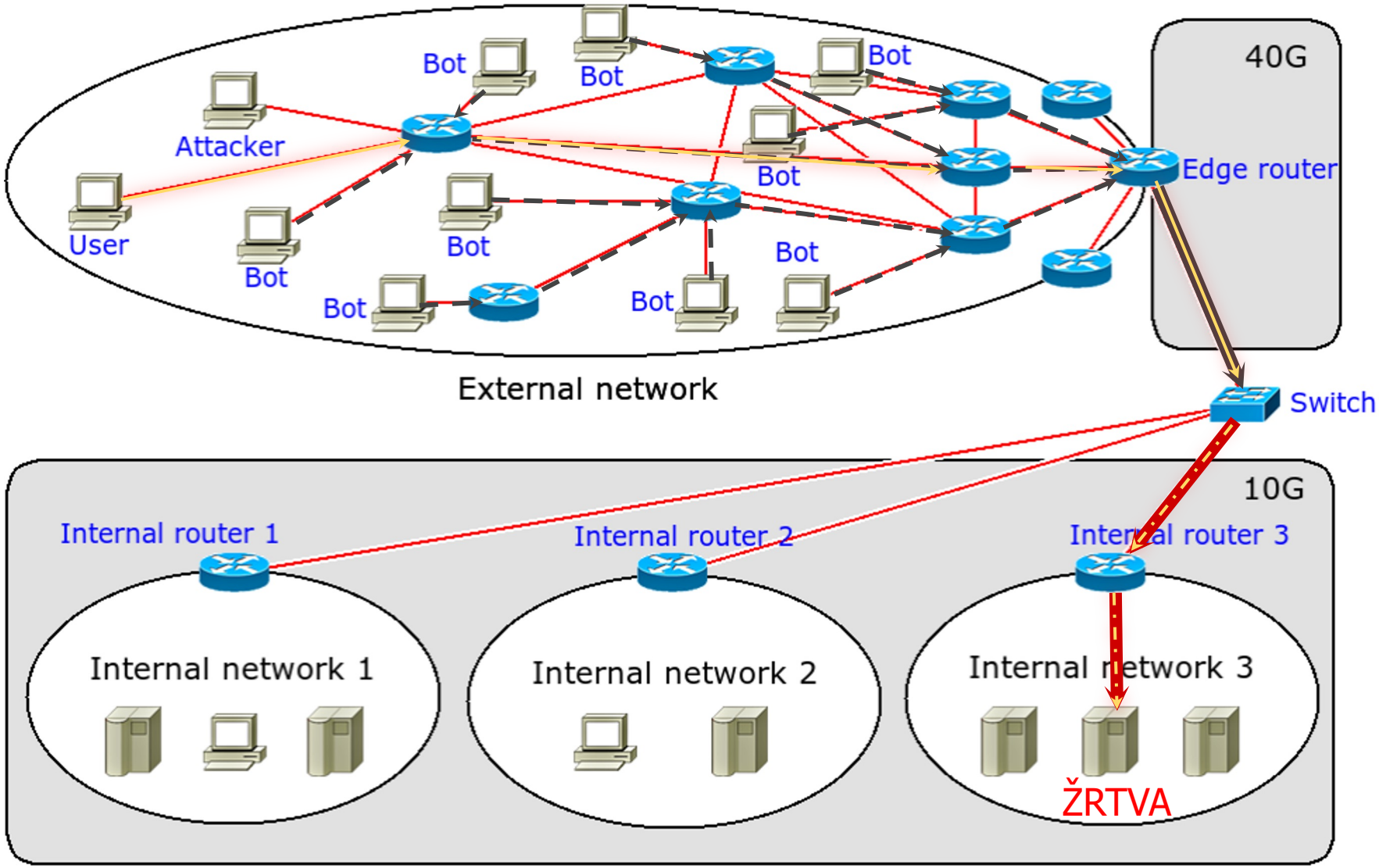



Pokreni napad
Attacker
Bot
Bot
Bot
Bot
Bot
Bot
Bot
Bot
40G
Edge router
External network
Switch
10G
Internal router 1
Internal router 2
Internal router 3
Internal network 1
Internal network 2
Internal network 3
ŽRTVA


Bot
Bot
Bot
Attacker
Bot
Bot
Bot
Bot
Bot
40G
Edge router
External network
Switch
10G
Internal router 1
Internal router 2
Internal router 3
Internal network 1
Internal network 2
Internal network 3
ŽRTVA


Bot
Bot
Bot
Attacker
Bot
Bot
Bot
Bot
Bot
40G
Edge router
External network
Switch
10G
Internal router 1
Internal router 2
Internal router 3
Internal network 1
Internal network 2
Internal network 3
ŽRTVA


Bot
Bot
Bot
Attacker
Bot
Bot
Bot
Bot
Bot
40G
Edge router
External network
Switch
10G
Internal router 1
Internal router 2
Internal router 3
Internal network 1
Internal network 2
Internal network 3
ŽRTVA


Bot
Bot
Bot
Attacker
Bot
User
Bot
Bot
Bot
Bot
Bot
40G
Edge router
External network
Switch
10G
Internal router 1
Internal router 2
Internal router 3
Internal network 1
Internal network 2
Internal network 3
ŽRTVA

DDoS napadi (Distributed Denial-of-Service)

2016. – deseci milijuna jedinstvenih IP adresa izvorišta (623 Gbps; Mirai botnet)

2020. – 2.3 Tbps (CLDAP DDoS refl. & amp.)

2020. – 167 Mpps spoofanih datagrama prema 180.000 CLDAP, DNS, SMTP

2018. – 1.35 Tbps (memcached; tisuće AS)

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

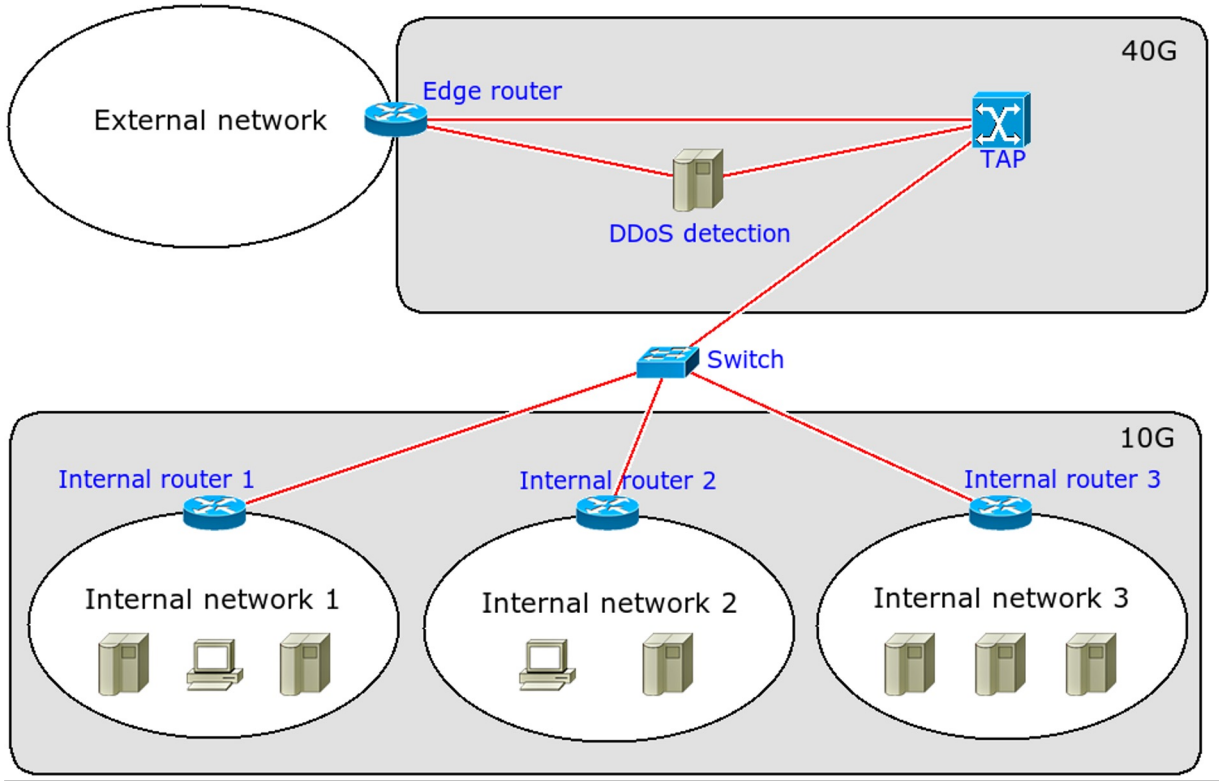
izvor: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Zaštita od volumetričkih uskraćivanja usluge

- promatrani sustav sastoji se od izvora napada, komunikacijskih puteva te žrtve
- obrana je moguća na svakom od tih mjesta
- zaštita od napada ovisi o konkretnoj situaciji
  - nužno je dobro poznavanje vlastite infrastrukture i karakteristika napada
  - nužno je uspostaviti dobar odnos sa svojim ISP-om
    - ISP može filtrirati promet na svojim usmjernicima
    - primjer: za napad temeljen na UDP-u moguće je blokirati UDP (pripaziti na DNS koji koristi UDP)
    - primjer: paketi dolaze izvan Hrvatske, moguće blokiranje vanjskog prometa (vatrozid, ili BGP)
- višestruki pristup Internetu
  - korištenje ADSL-a i sličnih metoda
  - korištenje BGP usmjeravanja

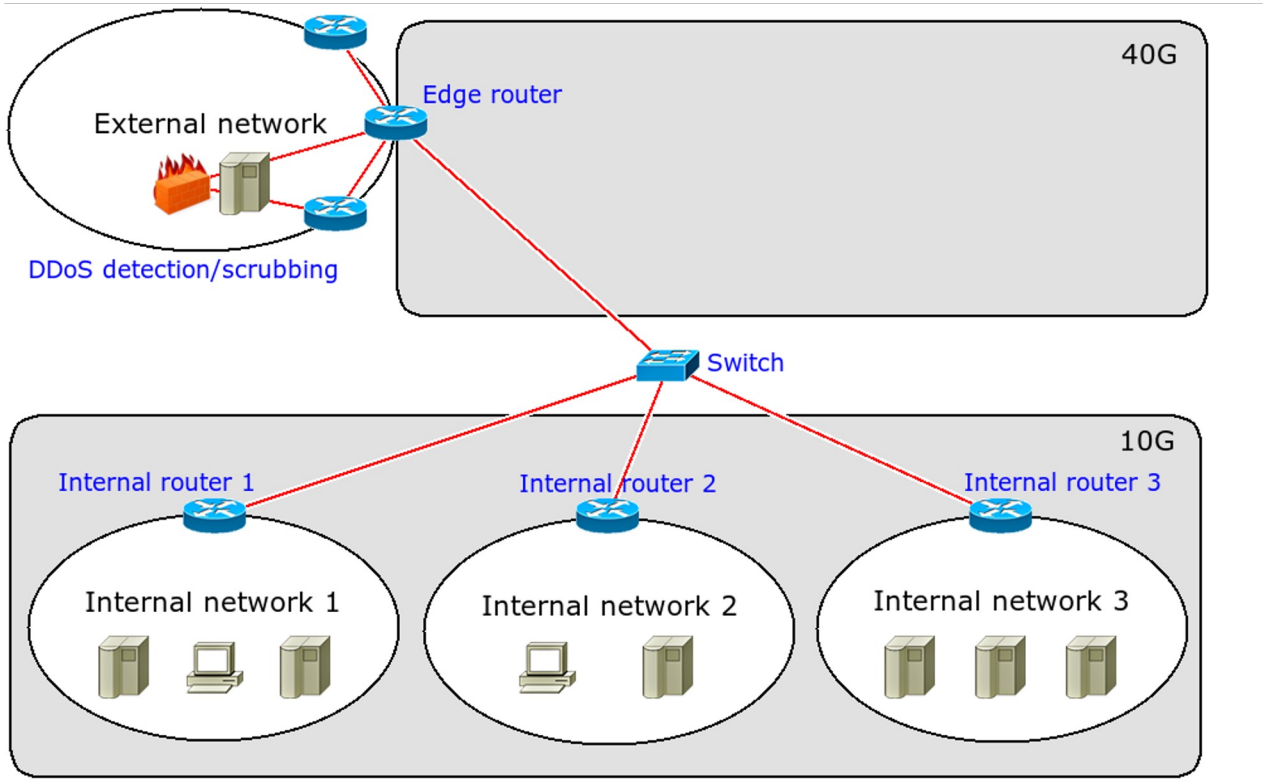
Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



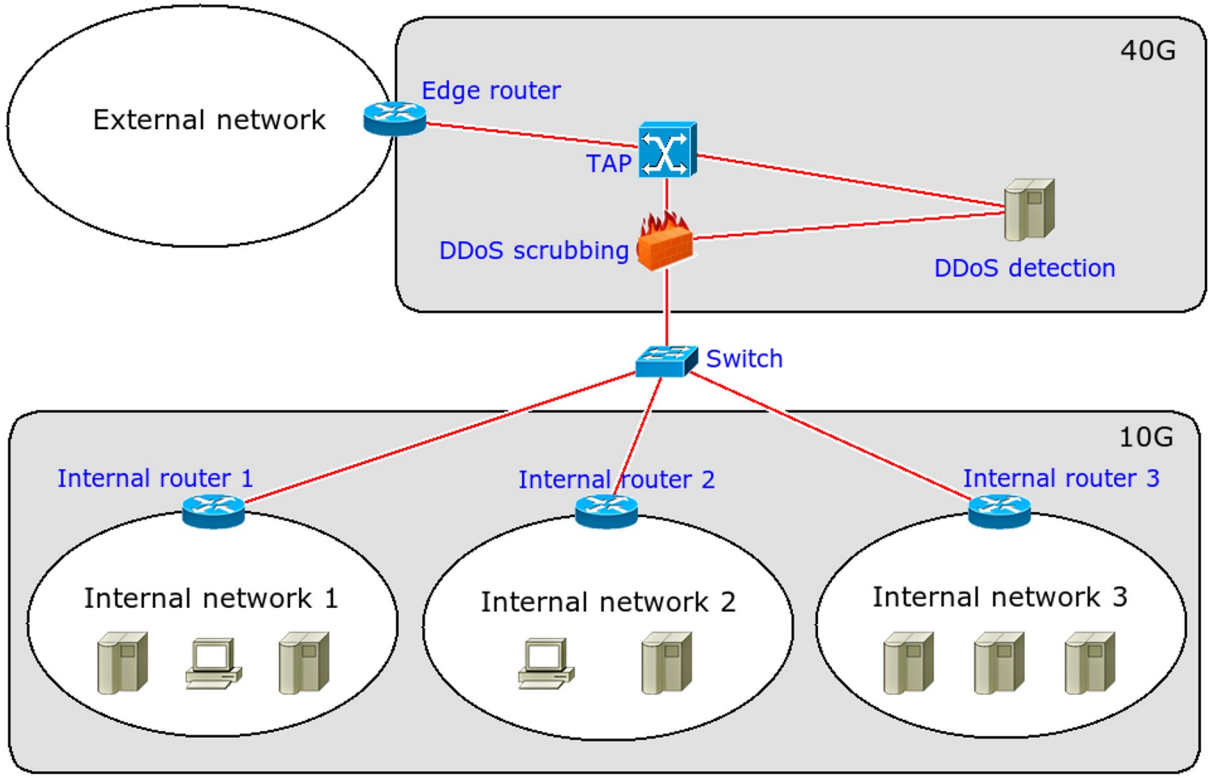
Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



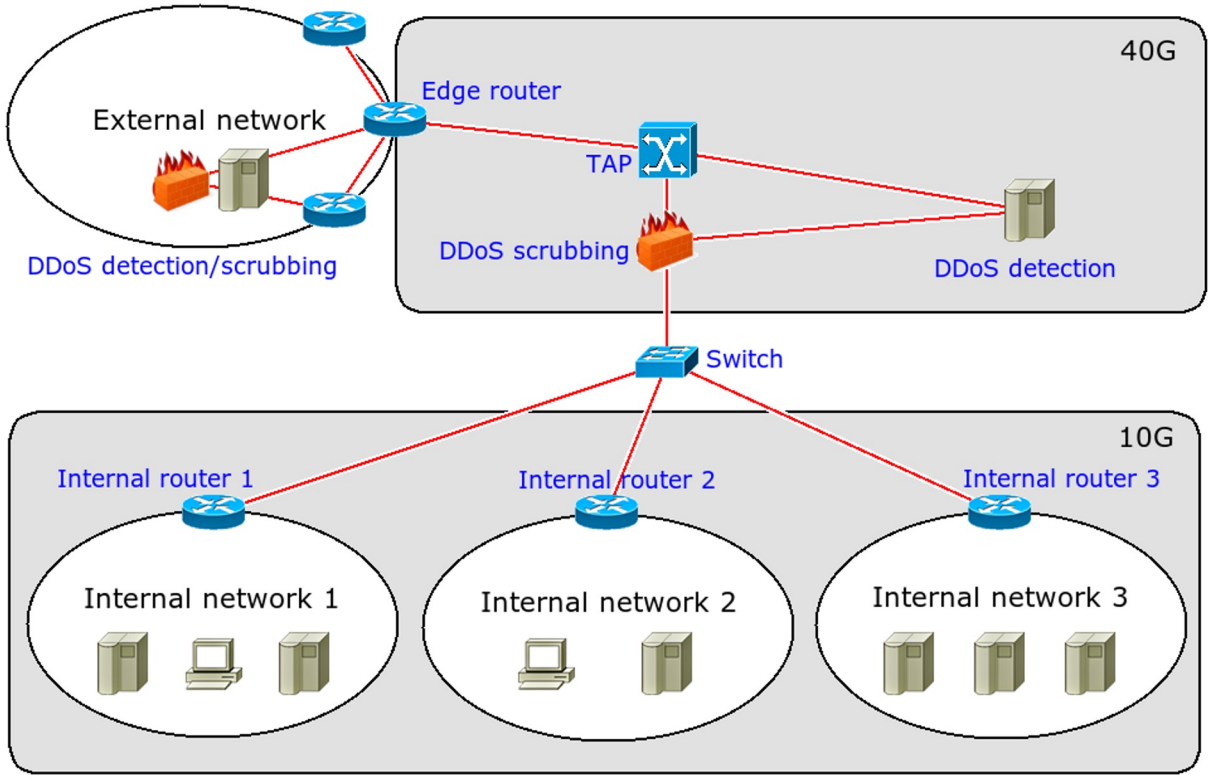
Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



Zaštita od DDoS napada

- „blackholing”
- „off-site” detekcija i filtriranje
- „on-site” detekcija i filtriranje
- hibridna „on-site/off-site” detekcija i filtriranje



Zaštita od DDoS napada: HW

- ASIC, FPGA (složeno i uglavnom nefleksibilno)
  - teško je modificirati i nadograđivati
  - energetski neučinkovito (TCAM)
  - vlasnička programska podrška (*proprietary*)
  - ograničena memorija
  - skupo!
  - brzo!

AntiDDoS8030

AntiDDoS8080

AntiDDoS8160

izvor: HUAWEI AntiDDoS8000 DDoS Protection System
https://carrier.huawei.com/~/media/cnbg/downloads/product/fixed%20network/carrier%2012700/pdf/huawei%20antiddos8000%20ddos%20protection%20system%20datasheet.pdf

Zaštita od DDoS napada: SW

- programsko filtriranje
  - fleksibilno, relativno jednostavna modifikacija i nadogradnja
  - jeftino, „off-the-shelf”
  - ne toliko brzo?
- standardni „firewall”
  - iptables, ipfw, …
  - IPset – hash za pohranu IP adresa
- korišteni programski okviri (*framework*) i tehnologije:
  - netmap
  - eBPF/XDP
  - DPDK – Intel

10 Gbps / 40 Gbps / 100 Gbps?

- najmanji ethernet okvir: 84 okteta
  - 7 okteta MAC preambula + 1 oktet „start frame delimiter“
  - eth. adresa odredišta: 6 okteta + eth. adresa izvorišta: 6 okteta + tip: 2 okteta
  - minimalni „payload“: 46 okteta
  - CRC: 4 okteta; razmak između ethernet okvira: 12 okteta („inter-frame gap“)
- najveći ethernet okvir: 1538 okteta, (12) + (7+ 1) + (6 + 6 + 2) + MTU je 1500 + 4
- ako se koristi danas standardna mreža brzine 10 Gbit/s, za najmanji ethernet okvir:

$$\frac{10 \cdot 10^9\ bit/s}{84\ okteta \cdot 8\ bita} = 14.880.952\ pps\ (packets\ per\ second) = 14{,}88\ Mpps$$

- vrijeme dostupno za obradu svakog paketa pri brzini 14.88 Mpps: $\frac{1}{14.880.952} = 67{,}2\ ns$
- ako CPU radi na 3 GHz i izvodi samo jednu instrukciju po ciklusu: 201 CPU ciklus po paketu
- 100 Gbps, 148,8 Mpps, CPU 4 Ghz: ~27 CPU ciklusa po paketu
- „cache-misses”: 32 ns; vrijeme pristupa L2: 4,3 ns; vrijeme pristupa L3: 7,9 ns; sistemski poziv na Linuxu: minimalno 41,85 ns

Usluge zaštite specijaliziranih tvrtki (1)

- na tržištu postoje specijalizirane tvrtke koje pružaju zaštitu
  - Akamai, CenturyLink, CloudFlare, DOSarrest, F5 Networks, Incapsula, Level3, Neustar, Verisign, cratis.hr
  - opće naziv: „DDoS Protection Service – DPS”
- usluga nije samo protiv volumetričkih napada već i semantičkih
- dva temeljna načina implementacije tih usluga
  - zaštita se nalazi u oblaku
  - u mrežu klijenta instalira se uređaj za zaštitu
  - hibridni pristup kombinira oblak i uređaj u mreži klijenta

Usluge zaštite specijaliziranih tvrtki (2)

- način korištenja usluga DPS-a: DNS i BGP
- promjene u DNS i primjena reverznog posredničkog poslužitelja (proxy)
  - prikladno za pojedine Web stranice/portale
  - kada je moguće koristiti reverzni posrednički poslužitelj
- korištenjem protokola BGP tvrtka za zaštitu šalje obavijesti o mreži klijenta
  - promet stiže do DPS-a, filtrira se te se tunelima šalje do klijenta
  - prikladno za zaštitu cijelih mreža ili kada reverzni posrednički poslužitelj nije moguće koristiti

Taksonomija DDoS napada (UDP)

- RioRey: „Taxonomy of DDoS Attacks” https://www.riorey.com/types-of-ddos-attacks/
- UDP:
  - UDP Flood
  - Fragmentation
  - DNS Flood
  - VoIP Flood
  - Media Data Flood
  - Non-Spoofed UDP Flood

UDP amplification, *UDP reflection*

- servisu koji koristi UDP (bez autentifikacije) pošalje se upit s lažiranom izvorišnom adresom a njegov odziv sadrži više podataka od upita
- „UDP-Based Amplification Attacks”
  - https://www.us-cert.gov/ncas/alerts/TA14-017A
- „Weaponizing Middleboxes for TCP Reflected Amplification”
  - https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/

Primjeri *UDP amplification*, *UDP reflection*

- „DNS amplification” – 28 do 54 puta
- „NTP amplification” – 556.9 puta
  - Network Time Protocol – protokol za sinkronizaciju vremena
  - loša konfiguracija omogućava slanje upita poslužitelju o posljednjih 600 sinkroniziranih računala
- „SNMP amplification” – teoretski do 650 puta
- SSDP - 30.8 puta
- CharGEN - 358.8 puta

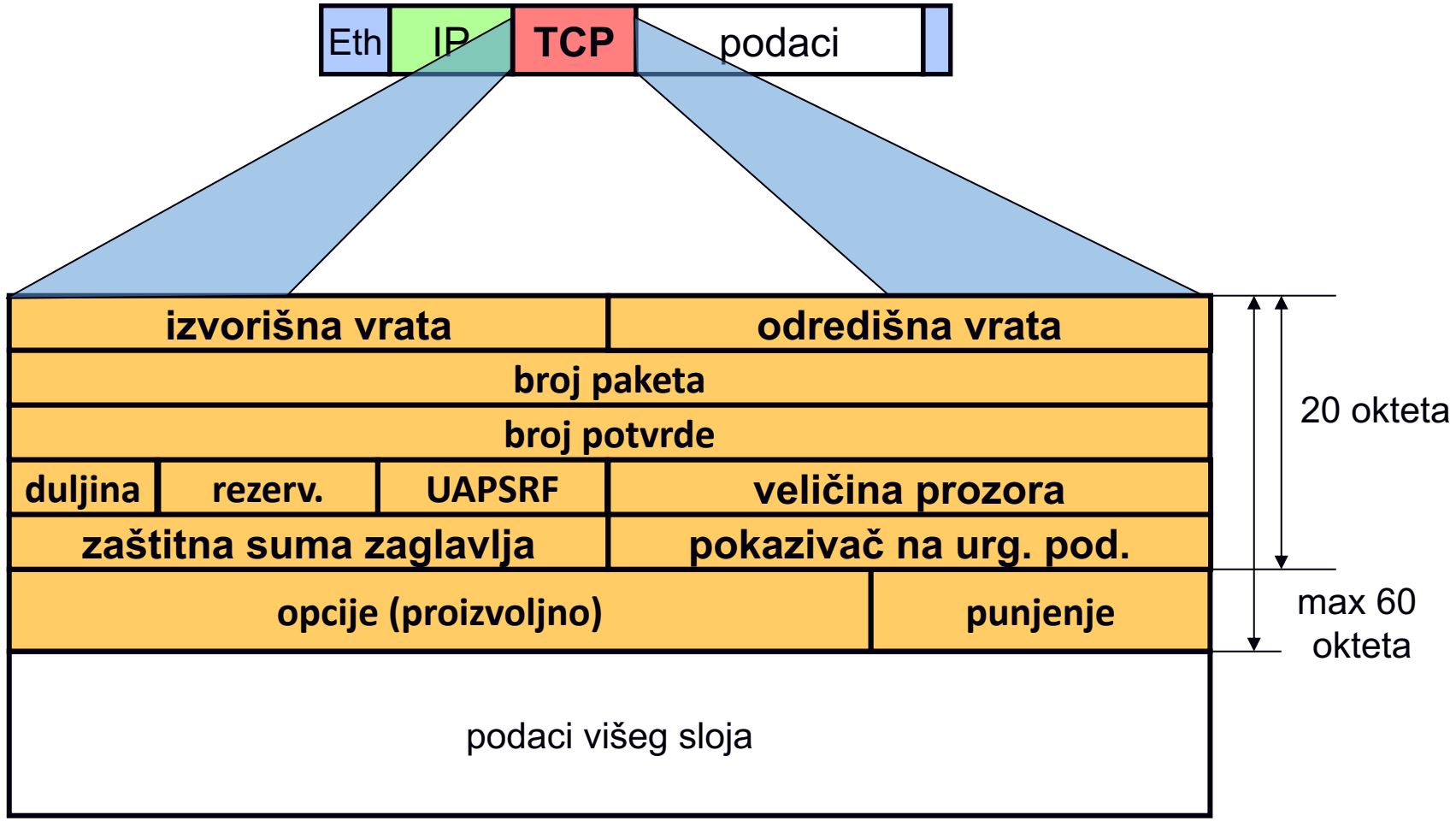
Primjeri *UDP amplification*, *UDP reflection*

- akamai's [state of the internet] / security Q2 2016 report
  - https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf
  - https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf
- DDoS korištenjem DNS
  - 2012. godine, 65 Gbit/s
  - 2013. godine, 300 Gbit/s
- DDoS korištenjem NTP (Network Time Protocol)
  - 2014. godine, 100 Gbit/s
  - 2014. godine, 400 Gbit/s (CloudFlare)

Protokol TCP

- Konekcijski (spojno) orijentirani transportni protokol
- Pouzdan
  - istek vremenske kontrole (*timeout*) i retransmisija
  - potvrde
  - nema dupliciranja
  - slaže pakete
  - kontrolni zbroj
  - omogućuje kontrolu toka
- Obostrana veza

Format TCP segmenta



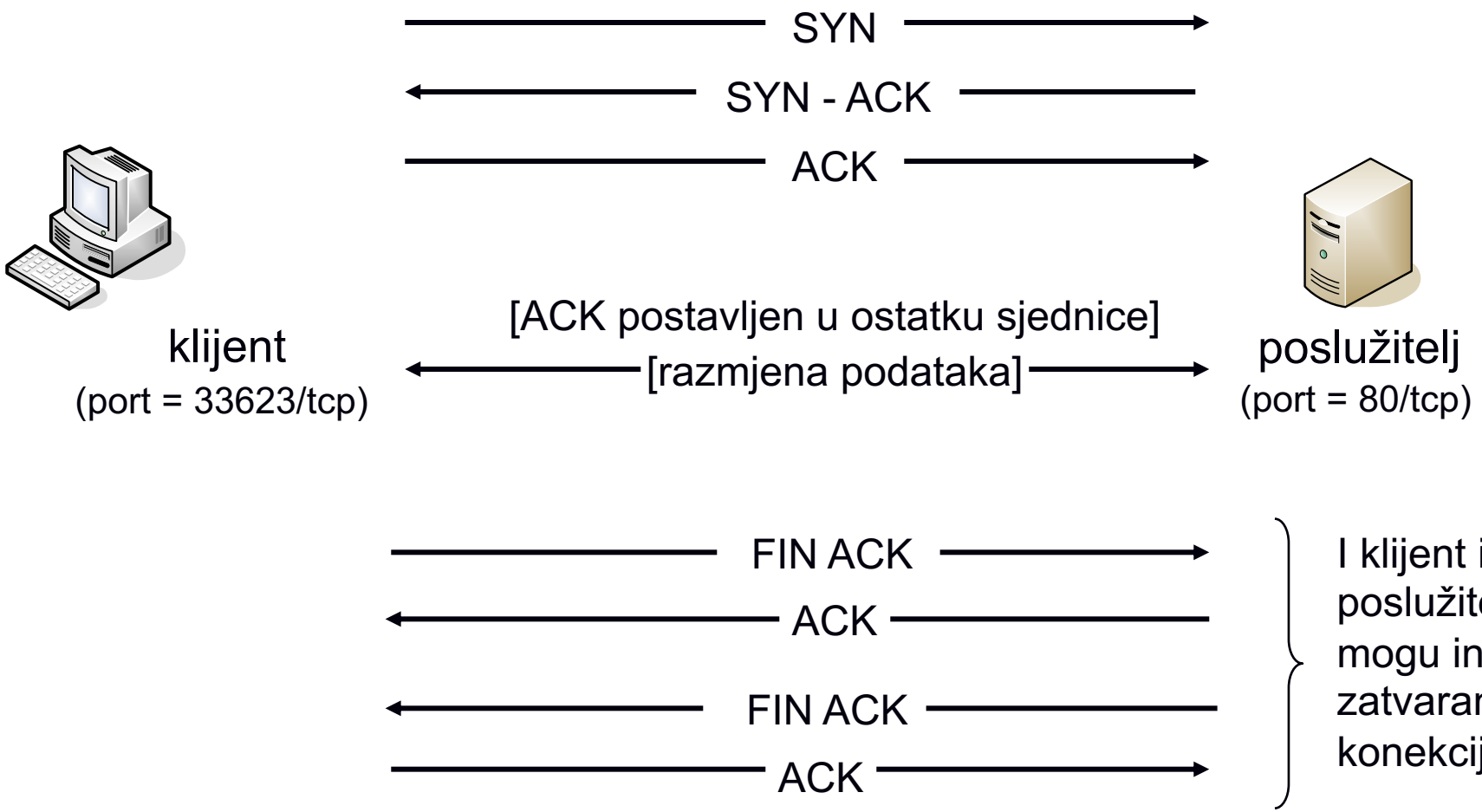
Slijedni brojevi i brojevi potvrde

- SEQ
  - slijedni broj („*Sequence number*”)
  - označava redni broj prvog okteta koji se prenosi u korisničkim podacima
- ACK
  - broj potvrde („*Acknowledgment number*”)
  - označava redni broj okteta koji pošiljatelj ove potvrde očekuje primiti
  - ujedno potvrđuje da su svi podaci do tog okteta primljeni

TCP zastavice

- SYN dogovaranje početnih brojeva pri uspostavi veze
- FIN završeno slanje podataka
- ACK broj potvrde je postavljen
- URG postavljen je „*urgent pointer*”
- PSH primatelj treba predati podatke aplikaciji što je prije moguće
- RST resetira vezu

Primjer TCP sjednice



Slanje podataka i kontrola toka

- u paketu se šalje potvrda o zadnjim ispravno primljenim podacima
- paket se prihvaća samo ako je unutar veličine predajnog prozora („transmission window”)
- za potvrdu se može koristiti i prazni segment (segment bez podataka)
- paketi sa zastavicama SYN ili FIN povećavaju slijedni broj iako ne sadrže podatke
- protokol kliznog prozora („Sliding Window Protocol”)
  - omogućava slanje više paketa prije nego što dođe potvrda o prispijeću paketa
  - veći protok podataka u odnosu na protokol „stop-and-wait”

Napadi na protokol TCP

- za napad je bitan položaj napadača
- na putu kojim prolaze TCP segmenti (engl. on path)
  - MITM napad, napadač može pratiti i mijenjati komunikaciju
  - jedina potpuna zaštita je IPsec
  - TLS ne štiti od napada uskraćivanja usluge
- van puta kojim prolaze TCP segmenti (engl. off path)
  - napadač ne može pratiti komunikaciju i mora pogađati određene parametre
  - manje mogućnosti napada, ali s propusnošću veze raste prijetnja

Taksonomija DDoS napada (TCP)

- RioRey: „Taxonomy of DDoS Attacks”
  https://www.riorey.com/types-of-ddos-attacks/
- TCP:
  - SYN Flood
  - SYN-ACK Flood
  - ACK&PUSH Flood
  - Fragmented ACK
  - RST or FIN Flood
  - Synonymous IP
  - Fake Session
  - Session Attack
  - Missused Application

Napad TCP SYN flood (1)

- Poslužitelj po primitku SYN segmenta rezervira resurse
  - veza je u poluotvorenom stanju koje traje neko vrijeme
  - dopušten je samo određen broj poluotvorenih veza
- "Problem" za napadača
  - Računalo koje primi SYN+ACK, a nije poslalo SYN, odgovara s RST
  - Napadač mora koristiti adresu s koje neće stići odgovor!

Napad TCP SYN flood (2)

$ **netstat -anf inet**

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp4	0	0	10.0.1.10.22	192.168.1.182.11008	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.225.28014	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.175.44828	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.184.28987	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.0.10303	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.237.25561	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.186.48231	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.53.20148	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.14.60914	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.68.35857	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.74.57236	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.156.2794	SYN_RCVD
tcp4	0	0	10.0.1.10.22	192.168.1.217.59919	SYN_RCVD

. . .

- CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
- Defining Strategies to Protect Against TCP SYN Denial of Service Attacks
  - https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/14760-4.html

Napad TCP SYN flood (3)

- Ne postoji standardizirana niti potpuna zaštita
- Neke metode zaštite
  - Povećanje broja dozvoljenih poluotvorenih veza
  - Skraćenje trajanja poluotvorene veze
  - Smanjenje količine stanja poluotvorene veze (SYN cache)
- Zaštita uz pomoć kolačića (SYN cookies)
  - Za inicijalni SYN se uopće ne čuva stanje
    - Stanje se rekonstruira iz završnog odgovora
  - “kolačić” je posebno odabran 32 bitni slijedni broj
    - ISN klijenta, MSS klijenta, vremenski brojač, adresa i pristup

Napad TCP SYN flood (4)

- Zaštita uz pomoć kolačića (nastavak)
  - Problem nedovoljne količine prostora u TCP zaglavlju
  - Niz opcija nije podržan, primjerice skaliranje prozora, različite veličine MSS-a (3 bita)
- SYN napad je lekcija za sve novije protokole
- Amplificirani napad
  - Poslužitelju se šalje SYN segment s lažiranom adresom žrtve
  - Server obavlja retransmisiju SYN+ACK segmenta

Primjer TCP DDoS napada

- „Record-breaking DDoS reportedly delivered by >145k hacked cameras”
  - http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/
  - rujan 2016.
  - 145607 kamere / dvr (1-30 Mbps po IP)
  - > 1.5 Tbps DDoS
  - tcp/ack, tcp/ack+psh, tcp/syn

RST i FIN napadi na protokol TCP

- Prema TCP specifikaciji po primitku ispravnog RST segmenta potrebno je raskinuti vezu
- RST napad
  - Slanje segmenta s postavljenom RST zastavicom
  - Problem je pogoditi parametre TCP veze
    - slijedni broj (unutar prozora!), izvorišna i odredišna IP adresa, izvorišni i odredišni pristup (port)
    - 1Mbps, MSS=1500, 100ms latencije, 15 skokova, WIN 35000
    - 1:57000, 40 okteta RST, 20s (na 1Mbps)
    - za 16384 pristupa, 91 sat
- FIN napad
  - Sličan RST napadu jedino se zatvara pojedini kraj veze

Zaštita od RST i FIN napada

- TCP MD5/AO
- (Ručno) ograničenje maksimalne veličine prozora
  - Napadač u tom slučaju mora napraviti više pokušaja
- Ograničenje slijednog broja u RST segmentima
  - Dodatno slanje ACK segmenta
- Druga rješenja koja modificiraju ponašanje TCP-a

ICMP napadi na protokol TCP

- ICMP je mrežni protokol
  - Na temelju podataka iz višeg sloja se obavlja demultipleksiranje
    - Zaglavlje mrežnog sloja i prvih 64 bita višeg sloja [RFC793]
    - Što više podataka, ali manje od 576 okteta [RFC1812]
- Konkretni napadi
  - ICMP poruke o greškama uzrokuju prekid veze
  - Port ili protokol nedostižni, fragmentacija potrebna a DF bit postavljen
  - ICMP poruka o zakrčenju (ICMP Source Quench)
- Zaštita prijenosnog sloja
  - Provjera ispravnih slijednih brojeva

Sigurnosna rješenja

- TCP-MD5 (RFC2385) / TCP-AO (RFC5925)
  - Uglavnom za zaštitu protokola BGP
    - BGP koristi i TTL zaštitu
  - Valjani RST, kada nema druge strane, će biti ignoriran
  - Problematično zbog dijeljene tajne, kripto-algoritmi usporavaju poslužitelje/usmjernike,
  - TCP MD5 zamijenjen s TCP AO jer koristi problematičan algoritam, nema zaštite od ponavljanja, ne podržava IPv6, zamjena dijeljene tajne je problematična (nema načina signalizacije promjene dijeljene tajne)
- IPsec – lako potpuno, nije skalabilno rješenje
- TLS

TCP „reflected amplification attack”?

- TCP uspostavlja vezu (3-way handshake)
- „IP spoofing” se može koristiti samo za napade tipa SYN-flood?
- „Weaponizing Middleboxes for TCP Reflected Amplification”
  - https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/