Kompiuterių tinklai - Interneto tinklo sluoksnis

Septinta paskaita (5.6 skyrius),
http://computernetworks5e.org/chap05.html

lekt. Vytautas Jančauskas

Interneto tinklo sluoksnis

Interneto tinklo sluoksnio architektūra (I)

Interneto architektūriniai principai yra aprašyti RFC 1958 dokumente. Šie principai pateikti žemiau.

Užtikrinti, kad veikia Nebaigti rengti specifikacijos kol nesukurti bent keli veikiantys prototipai.

Paprastumas Jeigu kažkokio funkcionalumo gali nebūti jo neturėtų būti.

Aiškūs pasirinkimai Jeigu yra keli būdai atlikti vieną ar kitą dalyką reikia išsirinkti vieną.

Moduliškumas Pageidautina, jeigu įmanoma, suskirstyti funkcionalumą nepriklausomais moduliais kurie gali būti keičiami nepaveikiant likusių.

Atsižvelgti į heterogeneniškumą Tinklą sudarys skirtingų tipų aparatūrinė ir programinė įranga. Dėl to tinklas turi būti kuriamas bendras, paprastas ir lankstus.

Interneto tinklo sluoksnio architektūra (II)

Vengti statinių parametrų Jeigu parametrai neišvengiami, vietoje to, kad fiksuoti juos standarte, leisti dėl jų susitarti siuntėjui ir gavėjui.

Pakanka gero dizaino Jeigu projektas geras, bet žinome, kad jo neužtenka kažkokiem ribiniams atvejams apdoroti, vietoje to, kad kompromituoti dizainą, patikėti išspręsti šias problemas naudodojams su keistais poreikiais.

Griežtumas siunčiant, atlaidumas gaunant Siunčiami paketai privalo griežtai atitikti standartus, tačiau reikia atsižvelgti, kad gaunami gali ir neatitikti.

Nejautrumas masteliui Tinklas turi atlaikyti didžiulius skaičius mazgų. Dėl to reikia jį decentralizuoti.

Atsižvelgti į kainą ir efektyvumą Jei tinklas labai brangus arba neefektyvus jo niekas nenaudos.

Interneto protokolas (IP)

- Interneto pagrindas yra Interneto Protokolas (**IP**).
- Duomenų perdavimas internete veikia taip:
  1. Duomenų srautas suskaidomas paketais, kurie, teoriškai, gali būti iki 64 KB dydžio, tačiau praktikoje iki 1500 baitų dyžio, kad tilptų į vieną Ethernet duomenų kadrą.
  2. Paketai perduodami nepriklausomai vienas nuo kito. Maršrutizavimo algoritmai parenka paketui kelią pro maršrutizatorius esančius tarp siuntėjo ir gavėjo.
  3. Gavęs paketus tinklo sluoksnis juos vėl sudėlioja taip, kad būti gauti pradiniai duomenys ir perduoda juos transporto sluoksniui.

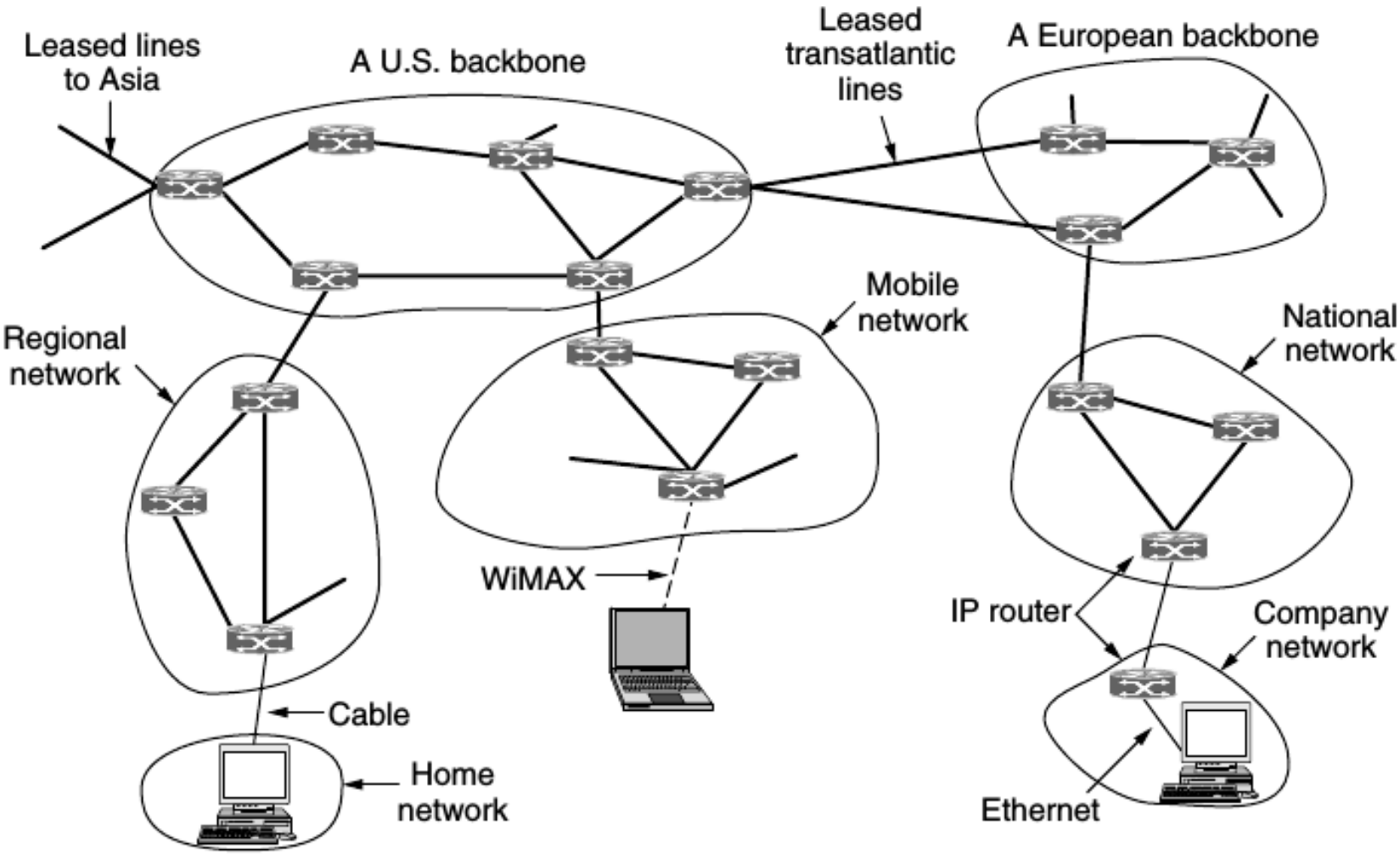


Figure 5-45. The Internet is an interconnected collection of many networks.

IPv4 protokolas

IPv4 protokolas

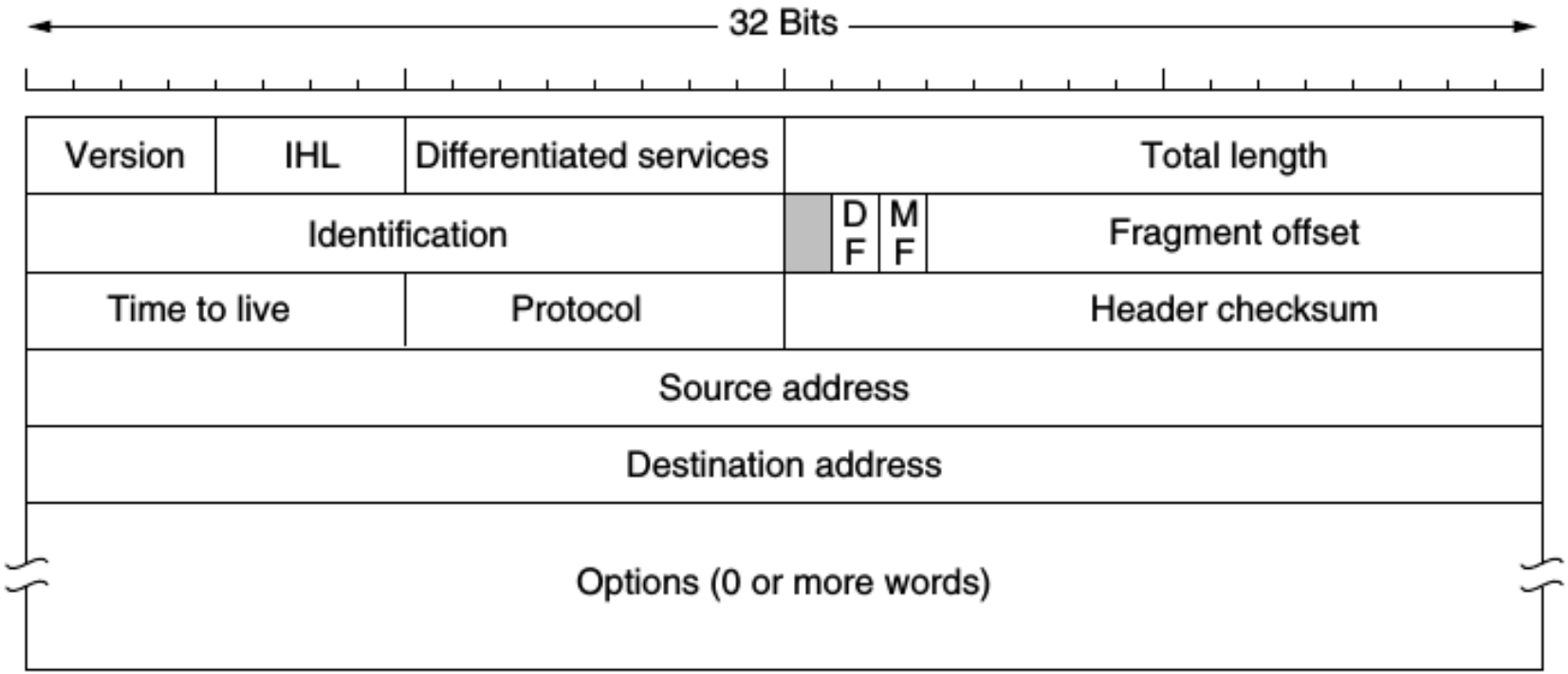


Figure 5-46. The IPv4 (Internet Protocol) header.

IPv4 paketo antraštės formatas (I)

IP antraštė saugoma “big-endian” formatu (atvirkščiai negu Intel architektūros kompiuteriuose) todėl norint naudoti “little-endian” sistemose reikia atitinkamos konvertacijos.

Version (4 bitai) Naudojamo IP protokolo versija (pvz. 4 arba 6).

IHL (4 bitai) Antraštės ilgis 32 bitų žodžiais.

Differentiated Services (8 bitai) Skirtas atskirti skirtingų paslaugų tipų paketus. Galimos įvairios patikimumo ir greičio kombinacijos.

Total Length (16 bitų) Viso paketo ilgis baitais, įskaitant antraštę.

Identification (16 bitų) Jeigu paketas buvo išskaidytas mažesniais visi fragmentai turės tą pačią Identification lauko reikšmę.

Nenaudojamas, DF, MF bitai (3 bitai) Pirmas bitas nenaudojamas (?); DF - Don’t fragment; MF - More fragments, visuose fragmentuose išskyrus paskutinį šis bitas bus vienetas.

IPv4 paketo antraštės formatas (II)

Fragment offset (13 bitų) Fragmento poslinkis atkuriant paketą baitais.

Time to live (8 bitai) Apribojamas paketo gyvavimo laikas šuoliais. Kai šis skaičius nulis, paketas nebeperduodamas ir siuntėjui išsiunčiamas įspėjamasis paketas.

Protocol (8 bitai) Naudojamas transporto lygio protokolui nustatyti. Pavyzdžiui TCP, UDP ir kai kurie kiti.

Header checksum (16 bitų) Antraštės kontrolinė suma. Turi būti perskaičiuojama po kiekvieno šuolio. Kodėl?

Source, Destination address (po 32 bitus) Siuntėjo ir gavėjo IP adresai.

Options (0 arba daugiau žodžių) Papildomi IP protokolo nustatymai. Kodėl šio lauko ilgis gali būti kintamas?

Papildomi IPv4 paketo nustatymai (I)

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Figure 5-47. Some of the IP options.

Papildomi IPv4 paketo nustatymai (II)

Papildomi nustatymai paprastai sudaryti iš vieno baito nustatymo kodo, nustatymo duomenų ilgio ir duomenų.

Strict source routing Nurodomas pilnas kelias - naudojamas jeigu buvo sugadintos maršrutizavimo lentelės arba matuojant perdavimo laiką.

Loose source routing Reikalauma, kad paketas aplankytų nurodytus maršrutizatorius. Taip galima padaryti, kad paketai keliautų per konkrečią šalį ir pan.

Record route Kiekvienas maršrutizatorius prikabina savo IP adresą. Taip galima testuoti maršrutizavimo algoritmus, ar diagnozuoti sutrikimus tinkle.

Timestamp Kiekvienas maršrutizatorius prideda ne tik savo IP adresą bet ir paketo priėmimo laiką, naudojamas matavimams tinkle.

Papildomi nustatymai dažnai maršrutizatorių visiškai ignoruojami.

IPv4 adresavimas

- Visi IPv4 adresai yra 32 bitų ilgio.
- Kiekvienas kompiuteris ir maršrutizatorius tinkle turi IP adresą.
- IP adresai skiriami tinklo interfeisams. Jeigu kompiuteris prijungtas prie dviejų tinklų jis turės du IP adresus. Maršrutizatorius taip pat dažnai turės kelis adresus.
- IP adresai yra hierarchiniai. Jie užrašomi dešimtainiais skaičiais su taškais. Pvz. jeigu adreso reikšmė yra 80D00297, jis bus užrašytas 128.209.2.151.

IPv4 prefiksai

- IP adreso aukštesnės eilės bitai sudaro tinklo dalį, žemesnės eilės - host'o dalį.
- Tinklo dalis yra vienoda visiems kompiuteriams esantiems viename tinkle - pvz. Ethernet vietiniame tinkle.
- Tinklo prefiksą sudaro žemiausias tinklo adresas ir kiek bitų skirta tinklo prefiksui, pvz. 128.209.0.0/24, reiškia, kad tinklo daliai skirti pirmi 24 bitai.
- Potinklio kaukė gaunama pažymint tinklo prefikso bitus vienetais, o host dalį nuliais. Mūsų pavyzdžio atveju, potinklio kaukė būtų 255.255.255.0.
- Naudojant hierarchinį adresavimą, maršrutizatoriams savo lentelėse užtenka saugoti apie 300000 prefiksų.

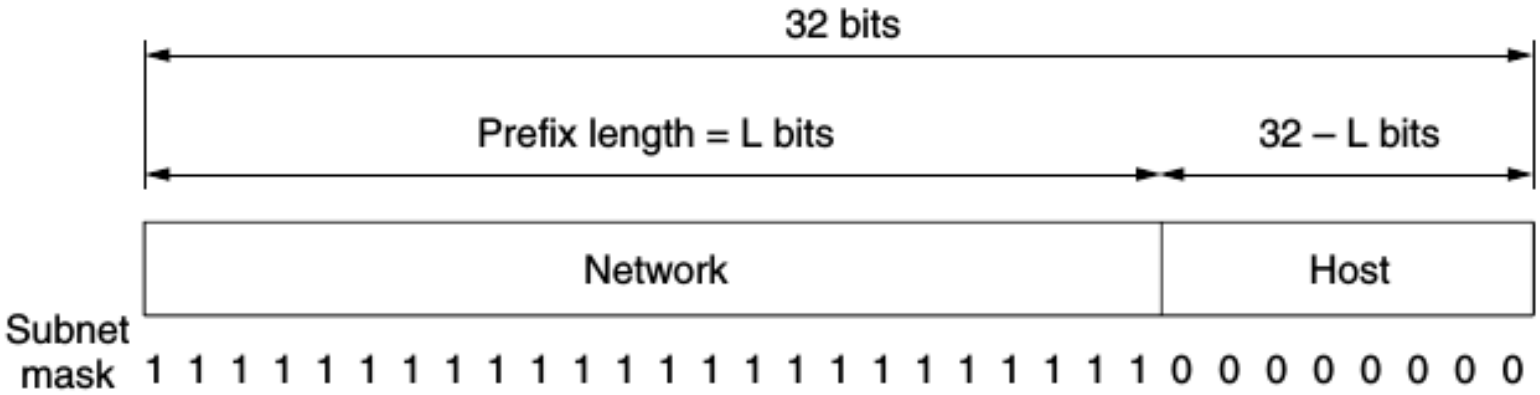


Figure 5-48. An IP prefix and a subnet mask.

IPv4 potinkliai

- Tinklo numerius centralizuotai skirsto **ICANN (Internet Corporation for Assigned Names and Numbers)** organizacija, taip išvengiama konfliktų.
- **ICANN** skiria adresų erdvės dalis įvairioms regioninėms agentūroms, kurios savo ruožtu skirsto juos interneto paslaugų tiekėjams.
- Potinkliai (angl. **subnets**) leidžia organizacijoms padalinti savo adresų bloką smulkiau. Pavyzdžiu kiekvienam įmonės departamentui gali būti skiriamas savo blokas. To bloko nariai sudarys to departamento tinklą.
- Gavęs paketą maršrutizatorius gali atlikti OR operaciją su potinklių kaukėmis ir tikrinti ar gaunamas prefiksas atitinka potinklio prefiksą.
- Naudojant potinklius nebūtina iš naujo kreiptis į **ICANN** ar kitą organizaciją.

Computer Science:	10000000	11010000	1|xxxxxxx	xxxxxxxx
Electrical Eng.:	10000000	11010000	00|xxxxxx	xxxxxxxx
Art:	10000000	11010000	011|xxxxx	xxxxxxxx

Here, the vertical bar (|) shows the boundary between the subnet number and the host portion.

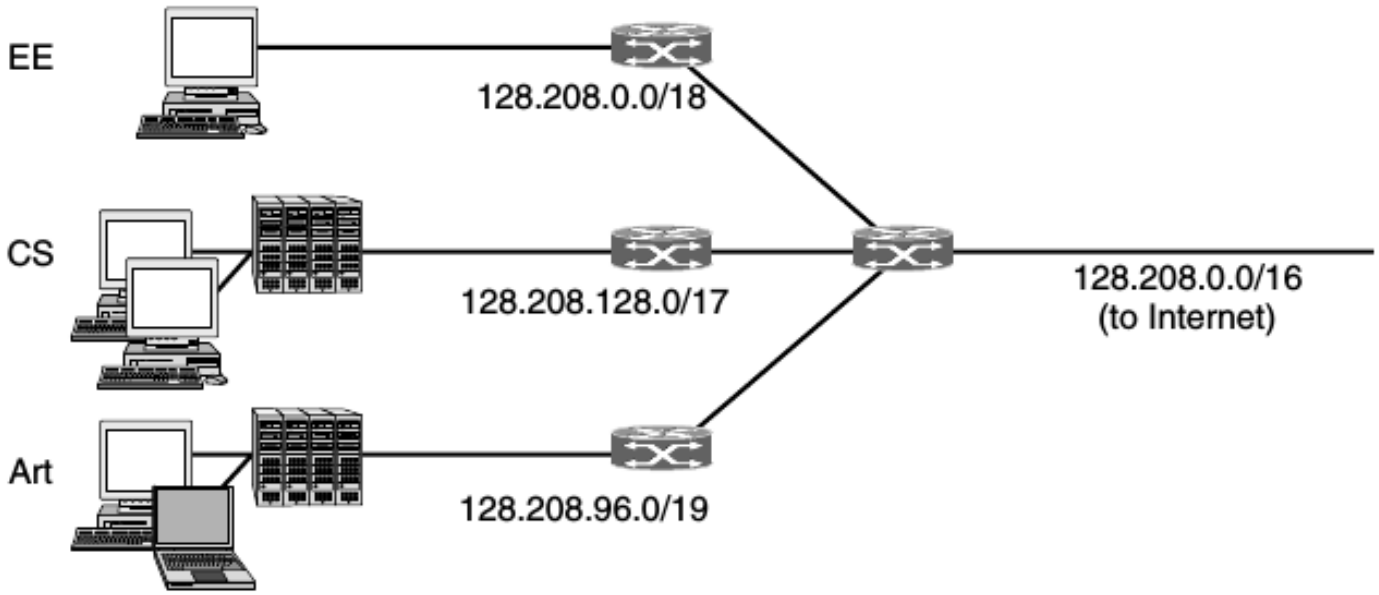


Figure 5-49. Splitting an IP prefix into separate networks with subnetting.

CIDR - Classless InterDomain Routing

- Jeigu organizacijų tinklams, kad nusiųsti paketą bet kam internete užtenka turėti maršrutizavimo lentelėje ISP maršrutizatoriaus adresą, Tier 1 tinklai tokios prabangos sau leisti negali.
- Augant internetui, interneto stuburą sudarantys maršrutizatoriai turi apdoroti milijardus paketų o lentelėse yra milijonai įrašų.
- Tokie maršrutizatoriai sudaro Interneto **default-free zone**.
- Tam reikia specializuotos aparatūros, be to toks adresavimas tampa nebeefektyvus.
- Sprendžiant šias problemas sukurtas **CIDR - Classless InterDomain Routing**, kurio paskutinis standartas aprašytas RFC 4632.

CIDR iliustruojantis pavyzdys (I)

- Tarkime turime 8192 IP adresų bloką prasidedantį nuo 194.24.0.0.
- Kembridžo universitetui reikia 2048 adresų ir jam paskirti adresas nuo 194.24.0.0 iki 194.24.7.255, o kaukė yra 255.255.258.0. Tai yra /21 prefiksas.
- Oksfordo universitetui reikia 4096 adresų. Jam skiriami adresai nuo 194.24.16.0 iki 194.24.31.255 ir kaukė 255.255.240.0.
- Edinburgo universitetui reikia 1024 adresų, jam paskiriami adresai nuo 194.24.8.0 iki 194.24.11.255 ir kaukė 255.255.252.0.

University	First address	Last address	How many	Prefix
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12.0/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

Figure 5-50. A set of IP address assignments.

CIDR iliustruojantis pavyzdys (II)

- Tarkime informacija apie šių tinklų IP adresus perduodama į **default-free** zonos maršrutizatorius.
- Maršrutizatoriai esantys netoli universitetų (pvz. Londone) naudos po vieną įrašą kiekvienam prefiksui.
- Įsivaizduokime maršrutizatorių esantį toli, pvz. Niujorke. Visi paketai skirti šių universitetų tinklams bus perduodami per Londono maršrutizatorių.
- Londono maršrutizatorius tai žino, todėl visus tris prefiksus apjungia į vieną - 194.24.0.0/19 ir perduoda Niujorko maršrutizatoriui, kad jis įrašytų į savo lentelę.
- Tokiu būdu maršrutizavimo lentelės sumažinamos iki maždaug 200000 įrašų.

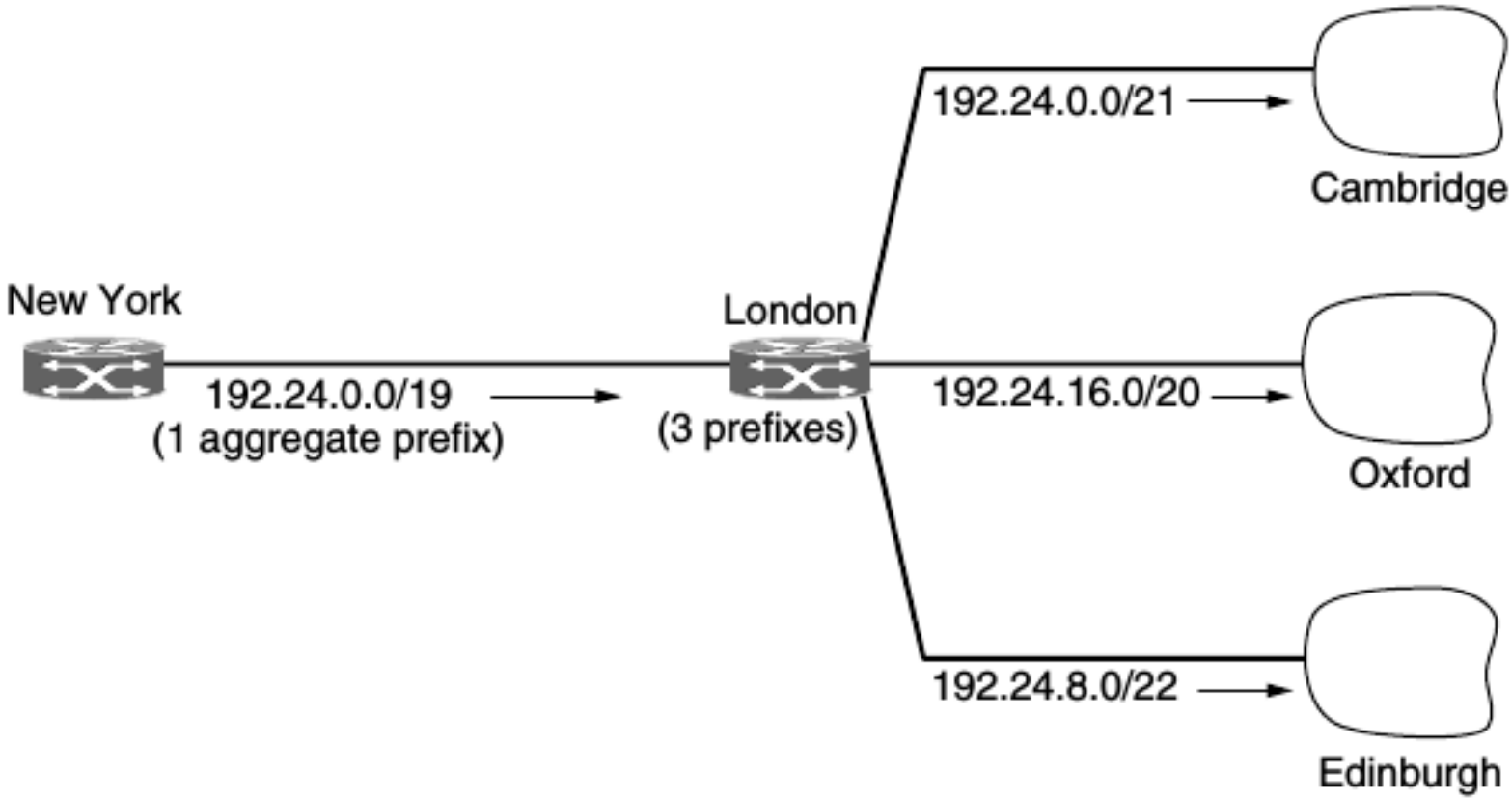


Figure 5-51. Aggregation of IP prefixes.

CIDR iliustruojantis pavyzdys (III)

- Prefiksai gali persidengti.
- Mūsų pavyzdyje galime panaudoti nepanaudotą adresų erdvės bloką kitoms reikmėms.
- Maršrutizatorius gavęs paketą išrenka prefiksą kurio ilgis yra didžiausias, kitaip tariant jis padengia mažiausią adresų kiekį, arba dar kitaip tariant yra labiausiai specifinis.
- Jeigu paketas atitinka prefiksus /20 ir /24, bus naudojamas /24.
- Peržiūrima visa lentelė kol randamas ilgiausias adresą atitinkantis prefiksas. Tam yra sukurti specialūs greiti algoritmai.

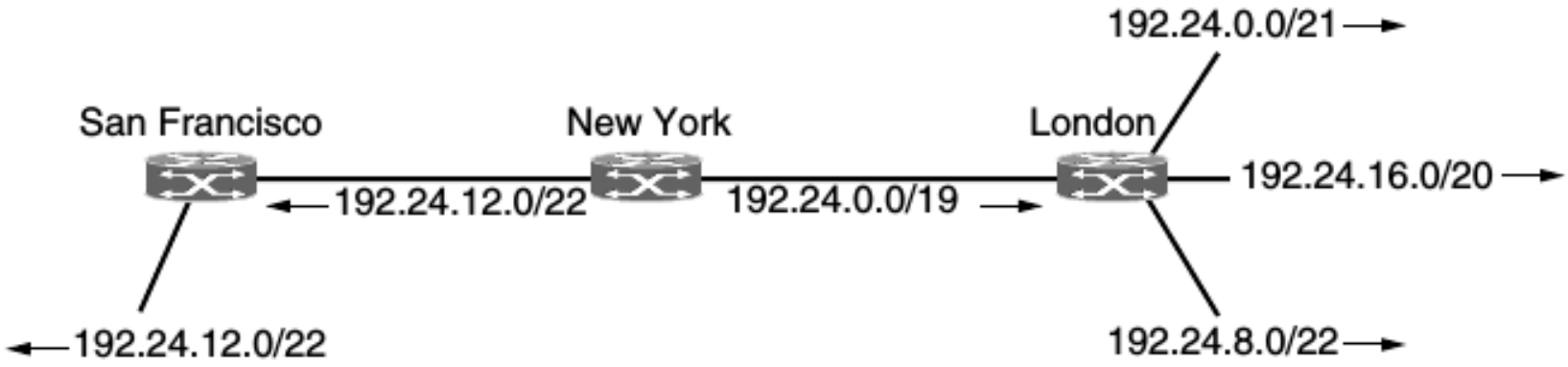


Figure 5-52. Longest matching prefix routing at the New York router.

Classful and Special Addressing

- Prie 1993 (prieš **CIDR**) adresai buvo suskirstyti į penkias klases - A, B, C, D ir E.
  - A - 128 tinklai iki 16 milijonų kompiuterių.
  - B - 16384 tinklai iki 65536 kompiuterių.
  - C - 2 milijonai tinklų iki 256 kompiuterių.
  - D - multicast.
  - E - rezervuota ateičiai.
- Kompanijos greit išgraibstė B klasės tinklus nes A buvo per dideli o C per maži.
- Žinoma, buvo galima naudoti potinklius, bet ir tai neužtikrina efektyvaus adresų paskirstymo augant Internetui.

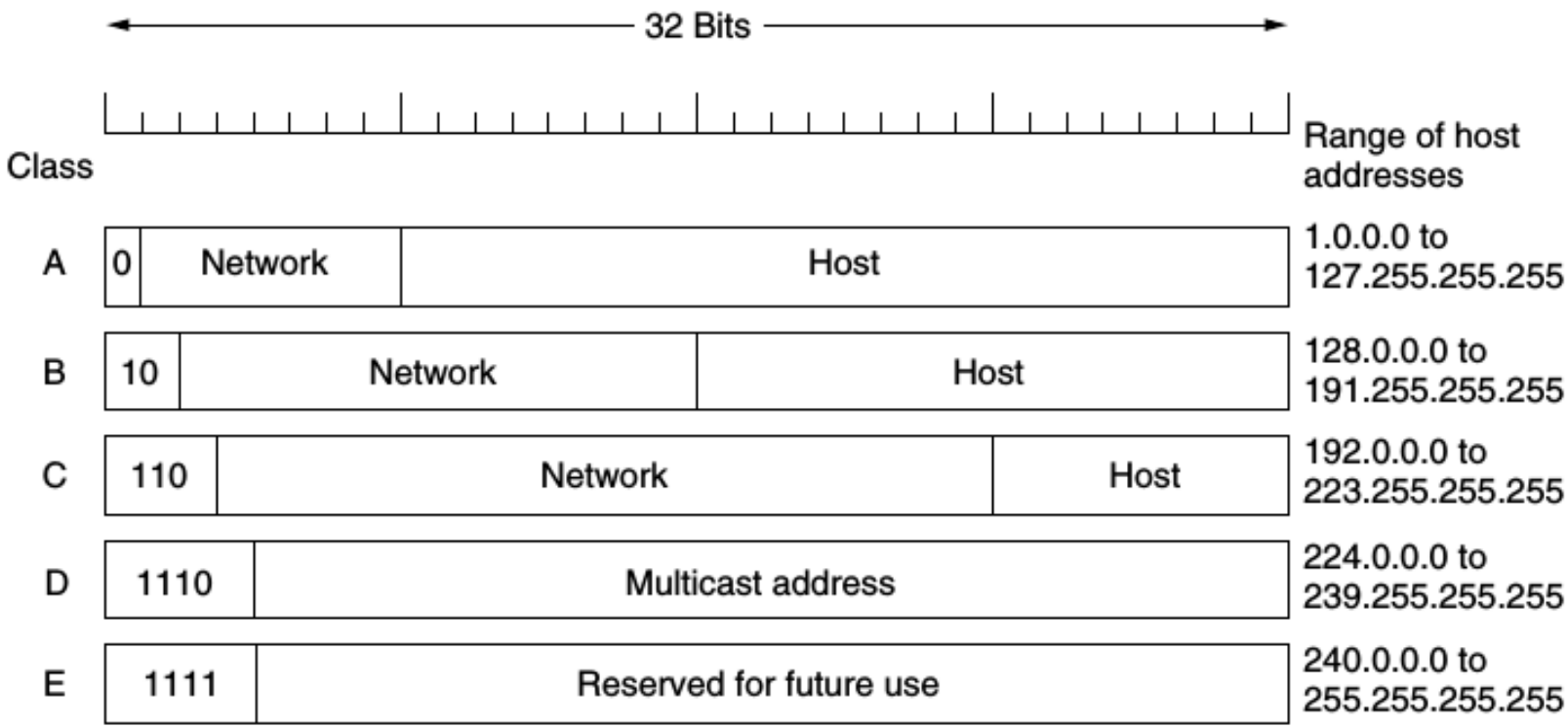


Figure 5-53. IP address formats.

Specialūs IP adresai

0.0.0.0	Kompiuteriai naudoja kraudamiesi, jis reiškia “šis tinklas” ir leidžia kompiuteriams kreiptys į savo tinklą nežinant jo numerio.
255.255.255.255	Reiškia visus tinklo kompiuterius ir naudojamas transliuojant lokaliam tinkle.
127.xx.yy.zz	Naudojami **loopback** testavimui. Tokie paketai nesiunčiami tinklui o apdorojami lokaliai kaip įeinantys paketai.

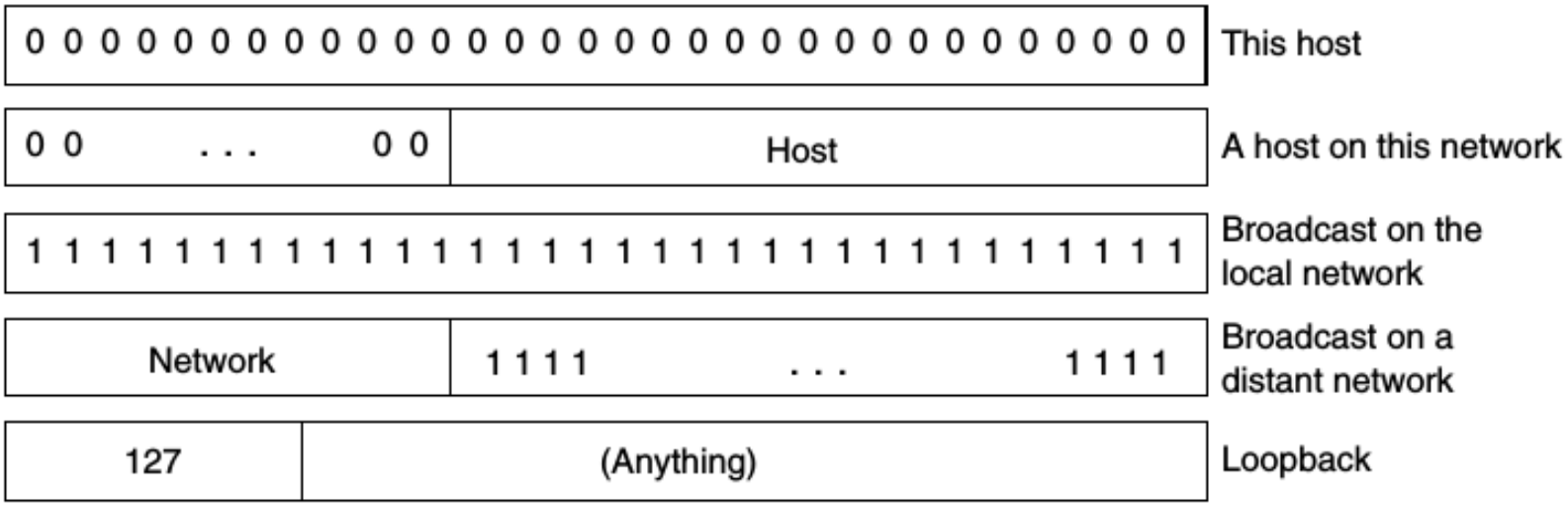


Figure 5-54. Special IP addresses.

NAT - Network Address Translation (I)

- IPv4 adresų trūksta. Tarkime jeigu ISP gauna 65534 adresų bloką, o turi 10000 klientų reikia kažkaip suktis.
- Vienas iš būdų yra adresus paskirti dinamiškai kiekvieną kartą prisijungus naudotojui.
- Kitas būdas yra **NAT**. Kiekvienam naudotojui ar nedidelei įmonei duodamas vienas adresas. Naudotojas tinkle naudoja vidinius IP kurie iš išorės nematomi.
- Išeinantys paketai pereiną per specialų prietaisą vadinamą **NAT box** kuris dabar dažnai yra maršrutizatoriaus dalis. Paketų vidiniai IP adresai tiesiog pakeičiami į tam klientui ISP duotą adresą.

NAT - Network Address Translation (II)

- Šiuo metu vidiniams potinkliams yra rezervuoti šie adresų ruožai:
  - 10.0.0.0 - 10.255.255.255 (16777216 kompiuterių)
  - 172.16.0.0 - 172.31.255.255 (1048576 kompiuterių)
  - 192.168.0.0 - 192.168.255.255 (65536 kompiuterių)
- Šie adresai negali pasirodyti už vidinių tinklų ribų - internete kaip tokiame. Jie negali būti naudojami taip vadinamiems išoriniams adresams.

NAT - Network Address Translation (III)

- O ką daryti su įeinančiais duomenimis? Jeigu IP pakeičiamas NAT įrenginio kaip kiti Interneto naudotojai žino kuriam iš vidinio tinklo kompiuterių perduoti duomenis? Jie juk mato tik vieną išorinį adresą.
- Panaudojamas TCP/UDP protokolų portas. Kitaip tariant portas naudojamas kaip adreso praplėtimas.
- Gavęs paketą, maršrutizatorius pagal portą iš lentelės paima andresą atitinkantį tą portą.
- Kaip tai pažeidžia sluoksninės architektūros kūrimo principus?
- Ką daryti jeigu noriu vidiniame tinkle paleisti pvz. žaidimų serverį, prie kurio naudotojai, norės jungtis per konkretų portą?
- NAT problemos nagrinėjamos RFC 2993.

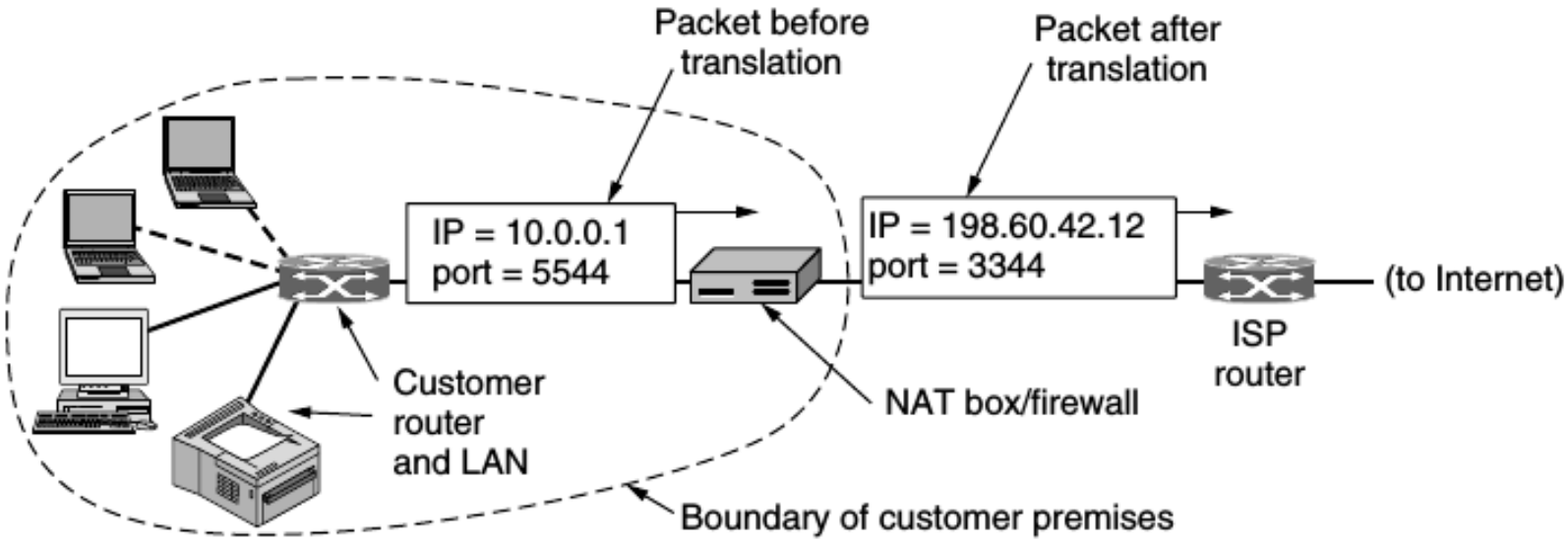


Figure 5-55. Placement and operation of a NAT box.

IPv6 protokolas (I)

IPv4 adresų trūkumas augant Internetui yra didelė problema. Vienintelis ilgalaikis jos sprendimo būdas (CIDR ir NAT yra trumpalaikiai būdai) yra naudoti ilgesnius adresus. IPv6 naudoja 128 bitų adresus. Kuriant IPv6 buvo keliami tokie tikslai:

1. Palaikyti milijardus tinklo naudotojų, netgi esant neefektyvioms adresavimo schemoms.
2. Sumažinti maršrutizavimo lentelių dydį.
3. Supaprastinti protokolus, leisti apdoroti paketus greičiau.
4. Geresnis saugumas.
5. Skirti daugiau dėmesio paslaugos tipui.
6. Padėti perduoti duomenis multicasting būdu.
7. Leisti kompiuteriui keisti buvimo vietą nekeičiant adreso.
8. Atsižvelgti į ateityje galimus pakeitimus.
9. Leisti naujam ir senam protokolams egzistuoti kartu metų metus.

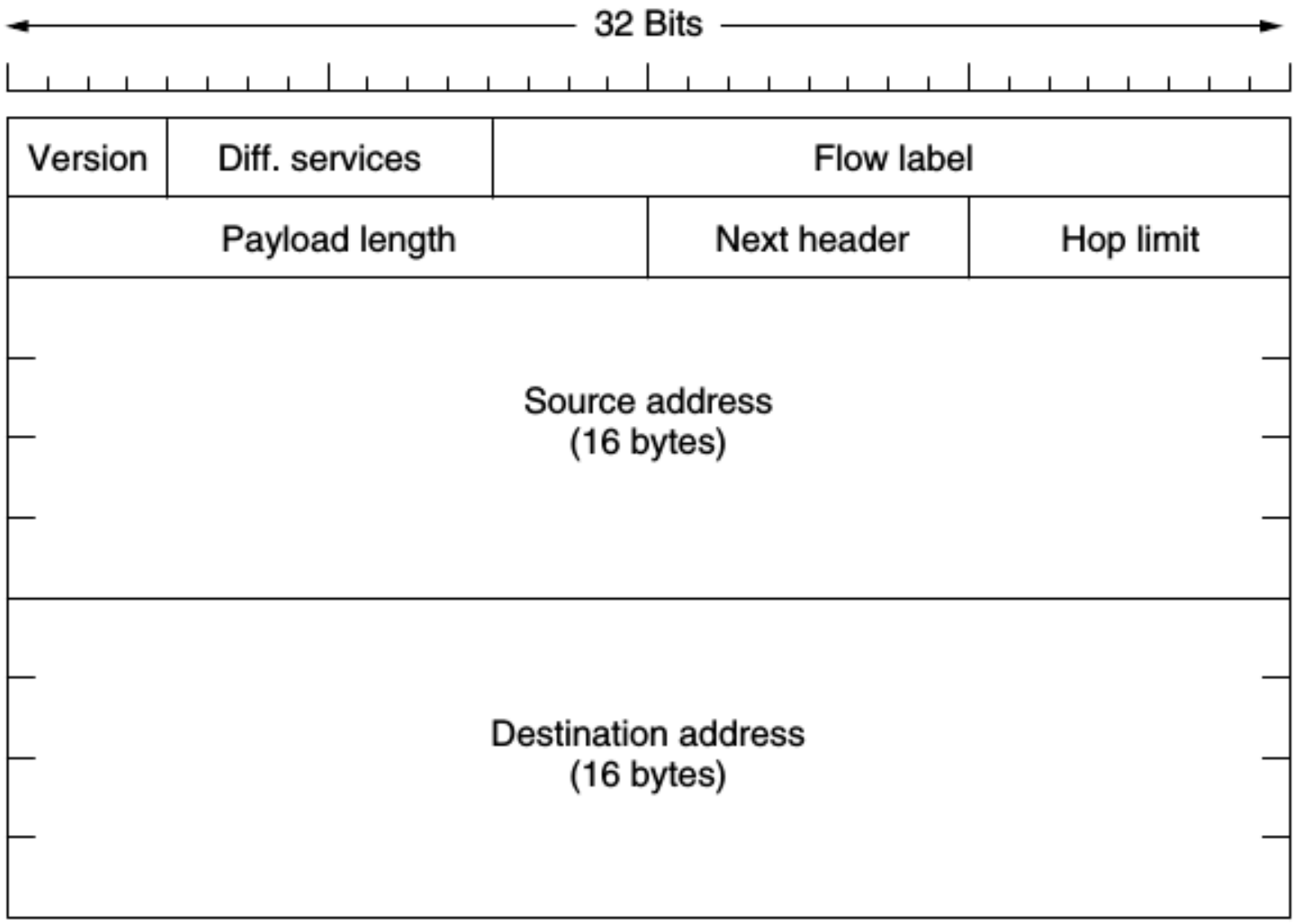


Figure 5-56. The IPv6 fixed header (required).

IPv6 antraštės formatas

Version Versija (4 arba 6) (4 bitai).

Differentiated services Skirtas nustatyti paslaugos tipui (8 bitai).

Flow label Nustato ar paketui reikia kažkokio specialaus apdorojimo. Taip įgyvendinamos paslaugos su pseudosujungimu (20 bitų).

Payload length - Kiek baitų užima informacija (16 bitų).

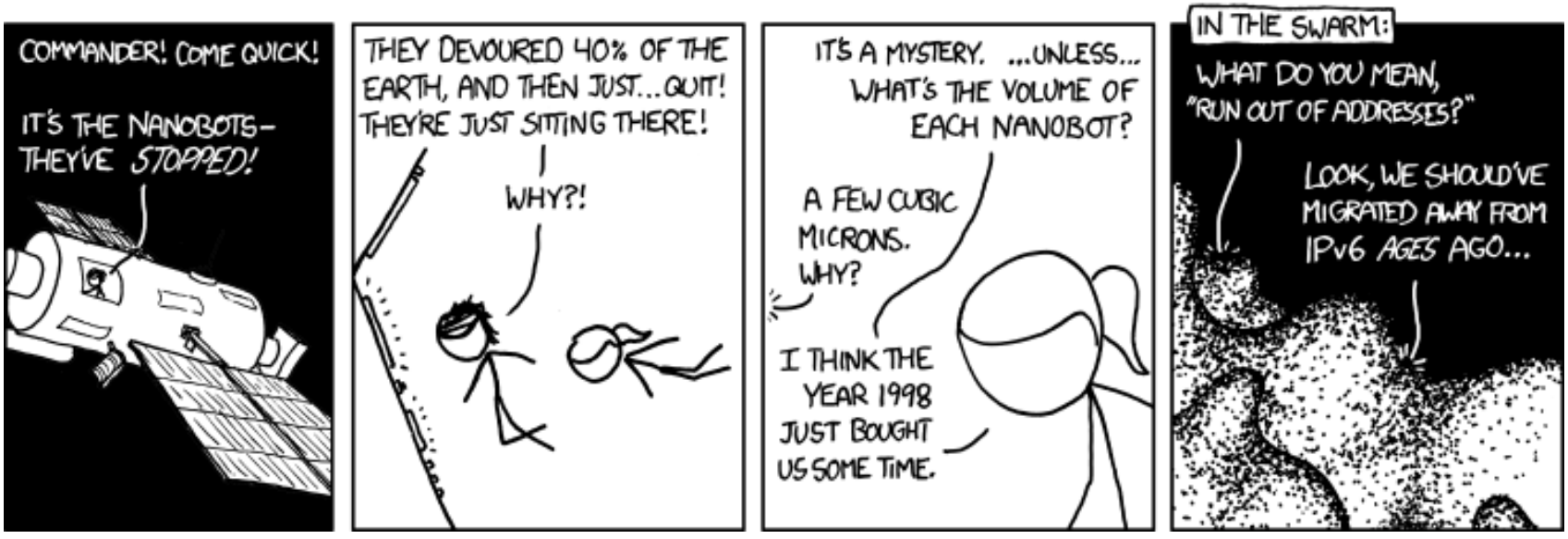
Next header - Kiek praplėtimo antraščių naudojama.

Hop limit - Kiek peršokimų iki paketas nebeperduodamas.

Source ir Destination address - Siuntėjo ir gavėjo 16 baitų adresai.

IPv6 adresas

- Adresai užrašomi kaip aštuonios keturių šešioliktainių skaitmenų grupės atskirtos dvitaškiais, pvz.: 8000:0000:0000:0000:0123:4567:89AB:CDEF.
- Jeigu skaičius prasideda nuliu jį galima praleisti. Kadangi daug adresų turės savyje daug nulių galima vietoje daug iš eilės einančių nulių rašyti du dvitaškius, pvz.: 8000::123:4567:89AB:CDEF
- IPv4 adresai rašomi prieš juos parašius du dvitaškius, pvz.: ::192.31.20.46.


COMMANDER! COME QUICK!
IT'S THE NANOBOTS- THEY'VE STOPPED!
THEY DEVOURED 40% OF THE EARTH, AND THEN JUST...QUIT! THEY'RE JUST SITTING THERE!
WHY?!
IT'S A MYSTERY. ...UNLESS... WHAT'S THE VOLUME OF EACH NANOBOT?
A FEW CUBIC MICRONS. WHY?
I THINK THE YEAR 1998 JUST BOUGHT US SOME TIME.
IN THE SWARM:
WHAT DO YOU MEAN, "RUN OUT OF ADDRESSES?"
LOOK, WE SHOULD'VE MIGRATED AWAY FROM IPv6 AGES AGO...

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

Figure 5-57. IPv6 extension headers.

IPv6 praplėtimai

Hop-by-hop Informacija visiems maršrutizatoriams, dabar naudojama kai reikia paketų didesnių negu 64 KB.

Destination Skirta papildomai informacijai gavėjui.

Routing Jei norima nurodyti kokius maršrutizatorius būtina aplankyti.

Fragmentation Naudojama kai paketas suskaidytas į kelis fragmentus.

Authentication Jei reikia, kad gavėjas galėtų patikrinti kas siuntė paketą.

Encrypted security payload Leidžia užkoduoti duomenis.

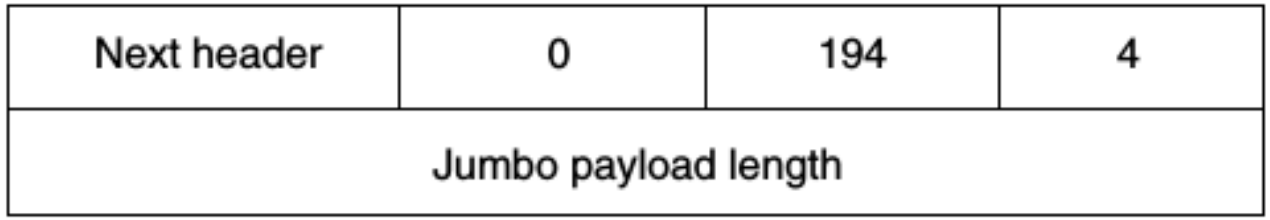


Figure 5-58. The hop-by-hop extension header for large datagrams (jumbograms).

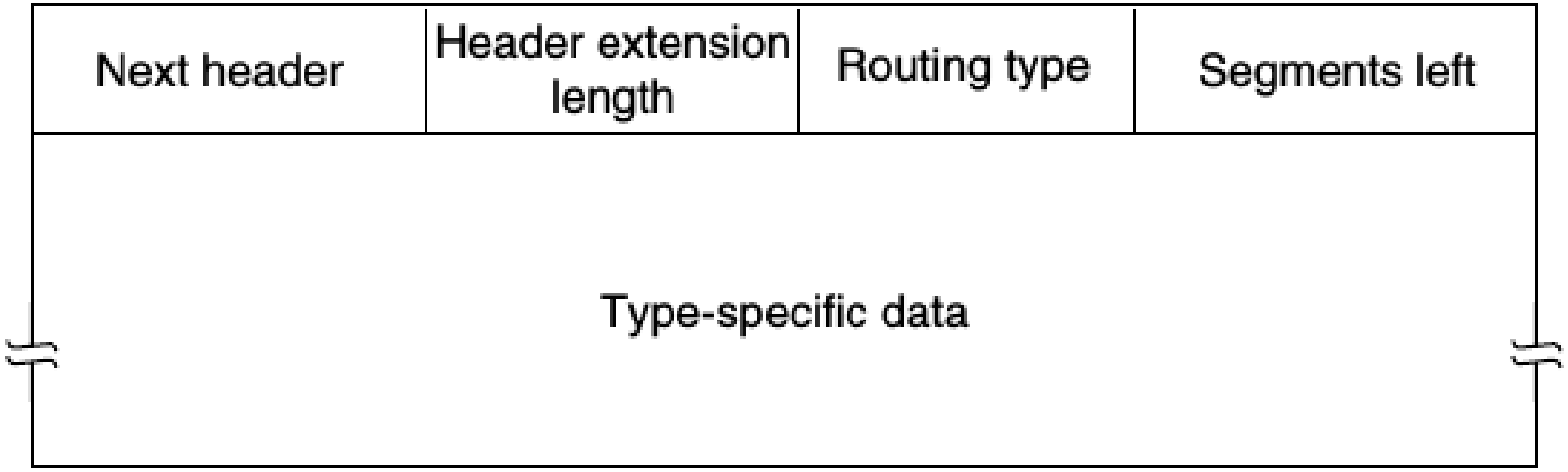


Figure 5-59. The extension header for routing.

Kontraversiškumas

Kadangi IPv6 svarbus protokolas nekeista, kad dizaino sprendimai jame kelia dideles aistras. Čia išvardiname kelis atvejus.

- Manoma, kad gali neužtekti maksimalaus **hop count** kuris dabar yra 255 peršokimų.
- Kai kas mano, kad 64 KB maksimalus paketo dydis yra per mažas (pvz. superkompiuterininkai).
- Atsisakyta IPv4 kontrolinės sumos. Skaičiuoti ją užtrukdavo daug brangaus maršrutizatoriaus laiko.
- Kai kurios šalys (Prancūzija, Irakas) įvedusios apribojimus duomenų šifravimui.

ICMP - The Internet Control Message Protocol (I)

Naudojamas pranešimams kuriuos maršrutizatoriai perduoda siuntėjui. Pranešimai supakuojami į IP paketus. Pranešimų tipai žemiau:

- DESTINATION UNREACHABLE - maršrutizatorius negali pristatyti paketo.
- TIME EXCEEDED - Time to live skaitliukas pasiekė nulį. Šiuo pranešimu gudriai pasinaudoja traceroute programa siųsdama paketus su TtL $= 1$, TtL $= 2$ ir t.t. ir taip sekdama paketo kelią tinklu.
- PARAMETER PROBLEM - antraštėje aptikta negalima reikšmė.
- SOURCE QUENCH - buvo naudojama tinklo užkimšimui reguliuoti.

ICMP - The Internet Control Message Protocol (II)

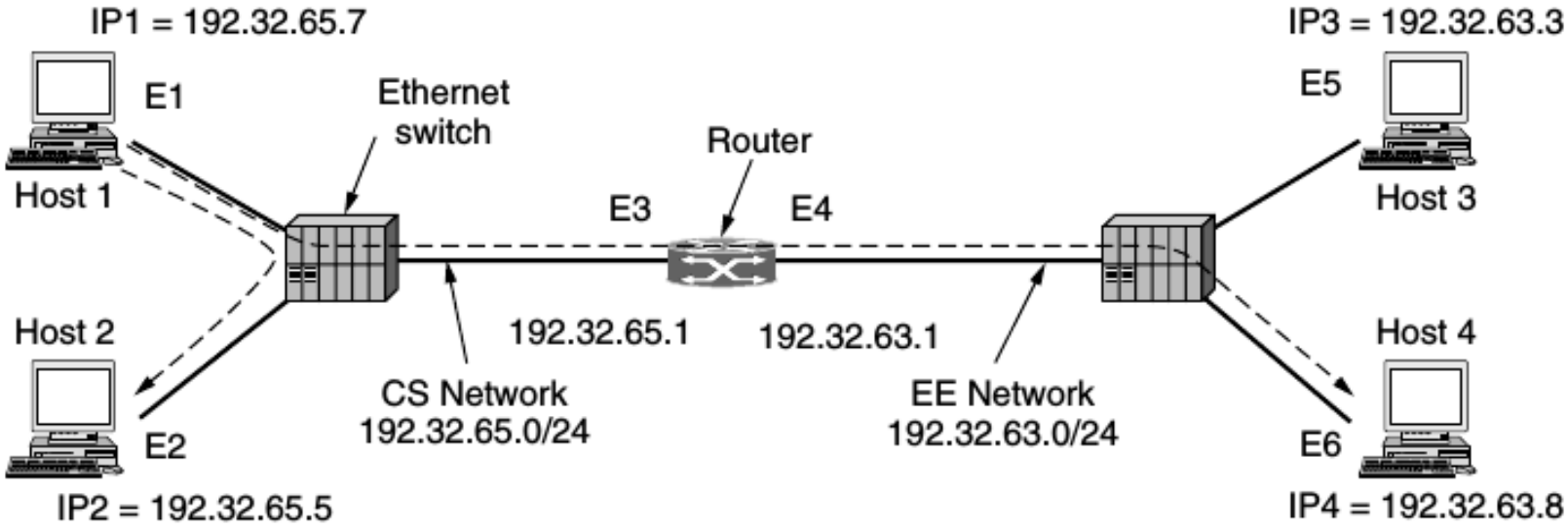
- ECHO ir ECHO REPLY - naudojama nustatyti ar adresatas pasiekiamas. Siuntėjas siunčia ECHO ir laukia ECHO REPLY žinutės.
- TIMESTAMP REQUEST ir TIMESTAMP REPLY - naudojama matuoti tinklo efektyvumui, įrašomas žinutės atvykimo ar išvykimo laikas.
- ROUTER ADVERTISEMENT ir ROUTER SOLICITATION - naudojamas kompiuterių atrasti greta esantiems maršrutizatoriams.
- Visus galimus variantus galima rasti čia: `www.iana.org/assignments/icmp-parameters`.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

Figure 5-60. The principal ICMP message types.

ARP - The Address Resolution Protocol

- Duomenų kanalų sluoksnis (pvz. Ethernet) nieko nežino apie IP adresus. Jis naudoja savo adresavimo sistemą (pvz. MAC adresus). Kaip IP adresai konvertuojami į atitinkamus duomenų kanalo sluoksnio adresus?
- Vienas variantas yra turėti konfiguracinį failą kuriame būtų surašyta, koks IP adresas atitinka kokį duomenų kanalo sluoksnio adresą.
- Paprastesnis būdas būtų panaudoti Ethernet broadcast paketą su klausimu - "kieno yra šitas IP adresas"? Būtent tokiu principu ir veikia **ARP** protokolas.
- Kad nereiktų to daryti kiekvieną kartą užklausų rezultatai kurį laiką saugomi.



Frame	Source IP	Source Eth.	Destination IP	Destination Eth.
Host 1 to 2, on CS net	IP1	E1	IP2	E2
Host 1 to 4, on CS net	IP1	E1	IP4	E3
Host 1 to 4, on EE net	IP1	E4	IP4	E6

Figure 5-61. Two switched Ethernet LANs joined by a router.

DHCP - The Dynamic Host Configuration Protocol

- Tinklo duomenis, tokius kaip kompiuterio IP adresas galima įvesti ranka, tačiau yra geresnis būdas.
- Naudojant DHCP kiekvienas tinklas turi DHCP serverį.
- Norėdamas susižinoti savo IP adresą kompiuteris siunčia DHCP DISCOVER paketą.
- Gavęs tokį paketą serveris kompiuteriui priskiria laisvą IP adresą ir išsiunčia jį kompiuteriui su DHCP OFFER paketu, naudodamas kompiuterio Ethernet adresą.
- DHCP aprašytas RFC 2131 ir 2132.

OSPF - An Interior Gateway Routing Protocol

- Naudojamas maršrutizavimui autonominėse sistemose.
- OSPF veikia abstrahuodamas tinklo maršrutizatorius, jungtis ir t.t. į grafą kurio lankams suteikiami svoriai.
- Grafe randami trumpiausi keliai ir paketai siunčiami jais.
- Jeigu keli keliai turi vienodą kainą, paketai paskirstomi tarp jų.
- OSPF leidžia suskirstyti tinklą zonomis. Zonos negali persidengti bet maršrutizatorius gali nepriklausyti nei vienai zonai.

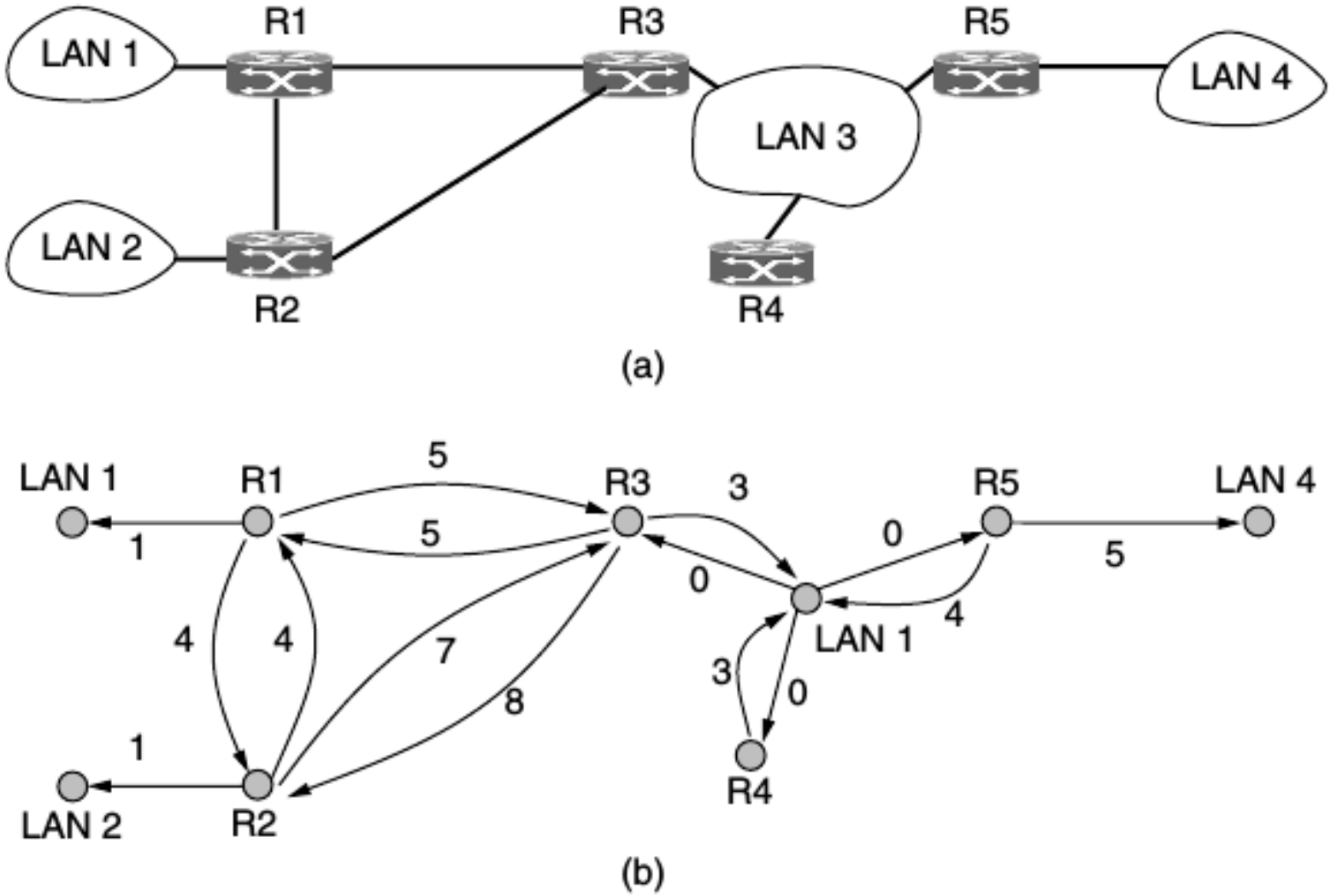


Figure 5-64. (a) An autonomous system. (b) A graph representation of (a).

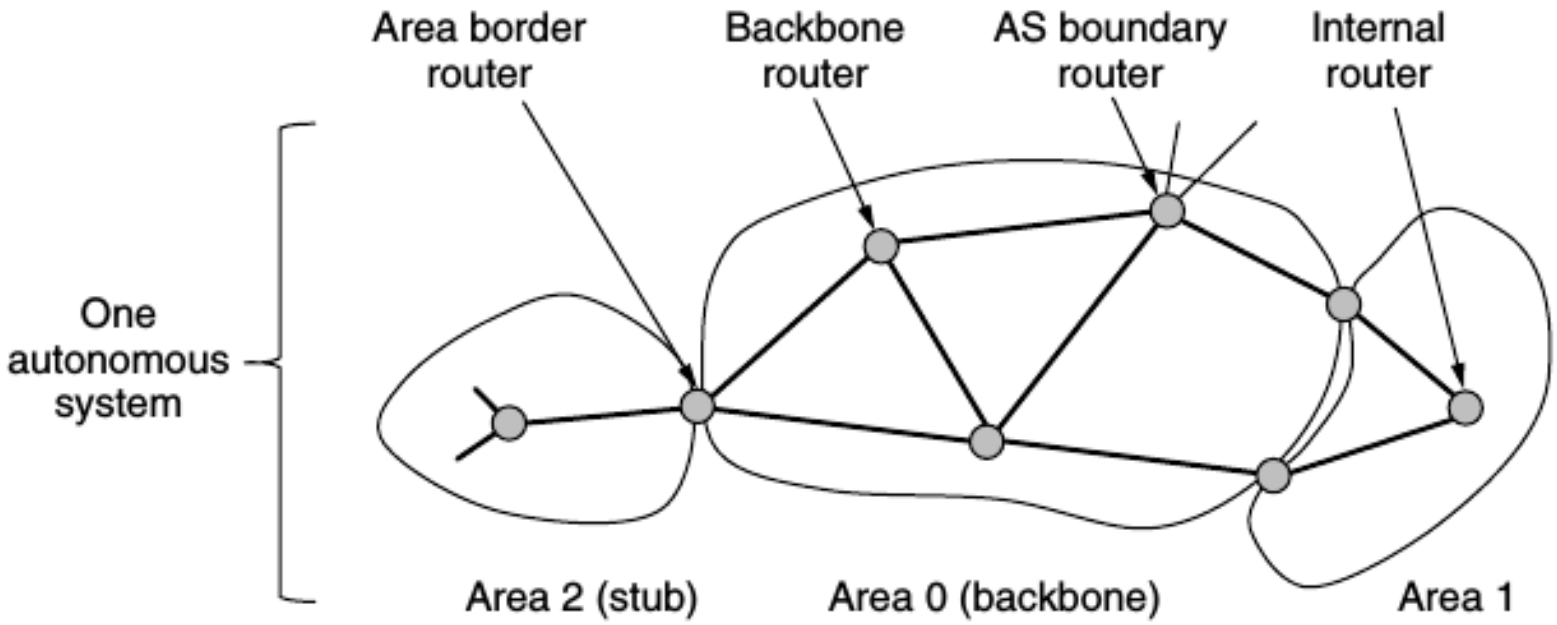


Figure 5-65. The relation between ASes, backbones, and areas in OSPF.

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

Figure 5-66. The five types of OSPF messages.

BGP - The Exterior Gateway Routing Protocol

- Autonominėse sistemose naudojami OSPF ar IS-IS protokolai.
- Tarp AS naudojamas **BGP (Border Gateway Protocol)**.
- AS viduje kompanijos tvarkosi kaip nori, **BGP** leidžia apibrėžti taisykles duomenų srautams tarp AS.
- Taisyklių pavyzdžiai:
  1. Neperdavinėti komercinių duomenų mokslo institucijų tinklais.
  2. Neperdavinėti duomenų iš Pentagono per Iraką.
  3. Naudoti vieną ISP o ne kitą nes taip pigiau.
  4. Nenaudoti AT&T Australijoje dėl prastos paslaugų kokybės.
  5. Duomenys iš ar į Apple neturėtų būti perduodami per Google tinklus.

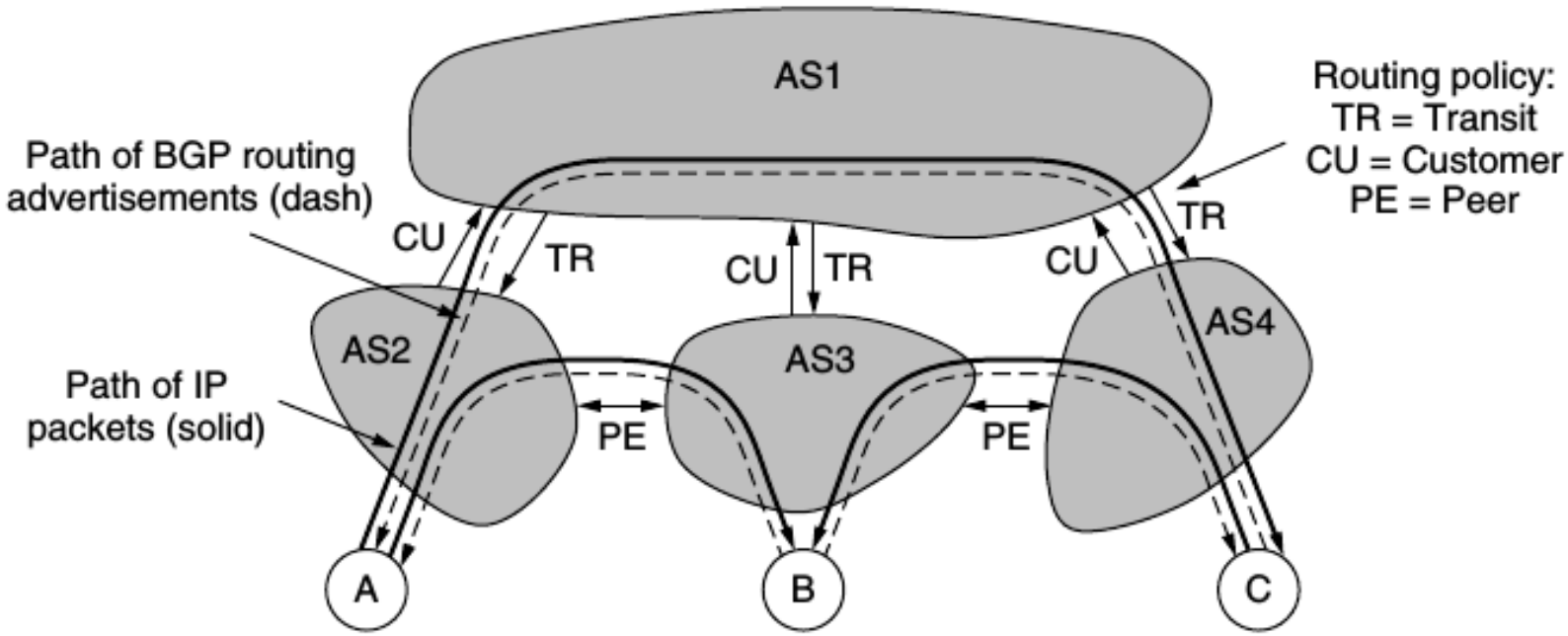


Figure 5-67. Routing policies between four autonomous systems.

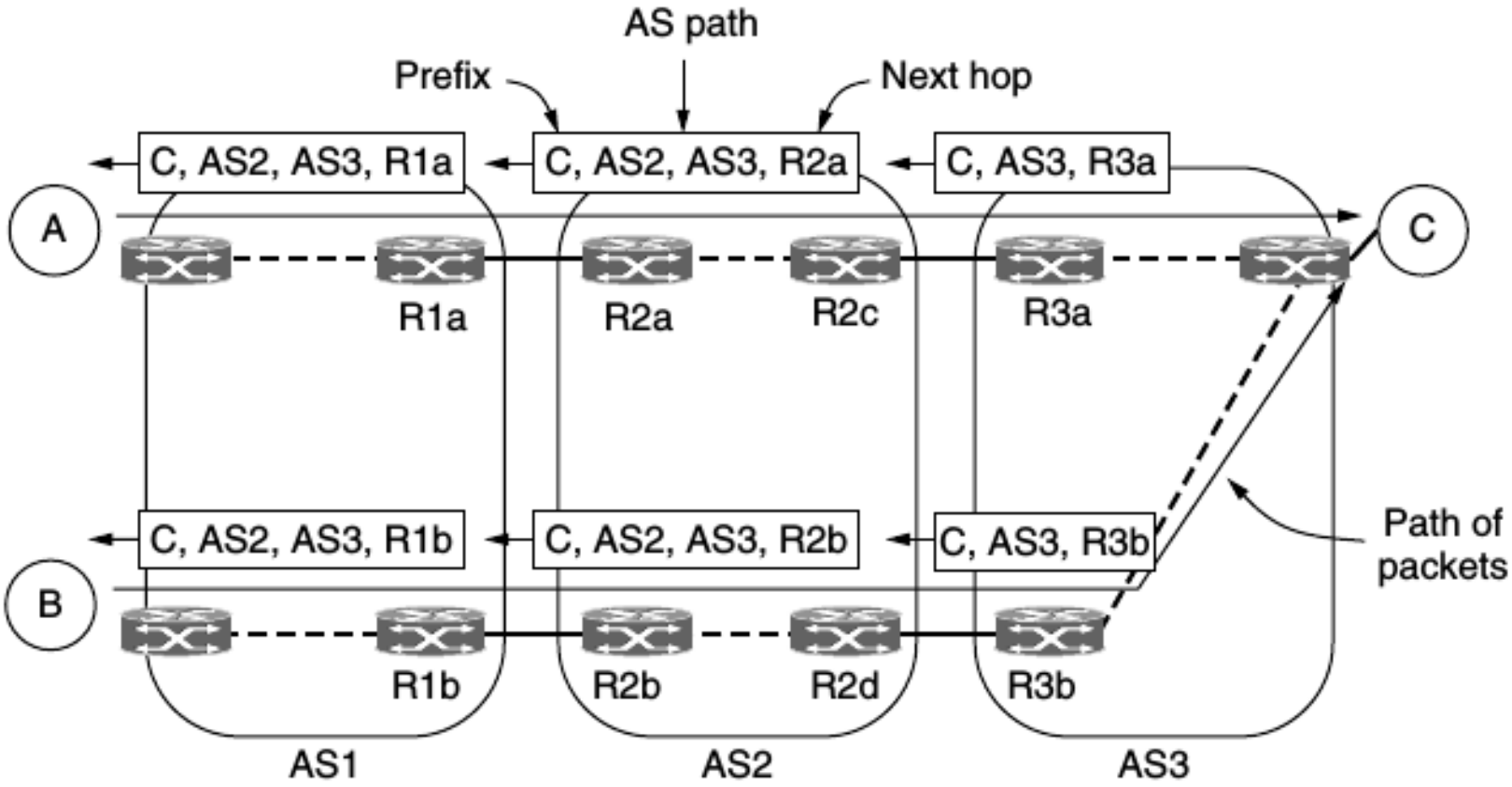


Figure 5-68. Propagation of BGP route advertisements.

Uždaviniai

Uždaviniai (I)

54. Tarkime, kad vietoje 16 bitų tinklo dalyje, B klasės adresai naudotų 20 bitų. Kiek klasės B tinklų galėtų būti?
55. Tarkime tinklas Internete turi potinklio kaukę 255.255.240.0. Kiek daugiausiai hostų gali būti tokiame tinkle?
56. Tarkime iš eilės einantys IP adresai prasideda nuo 198.16.0.0 ir turi būti paskirstyti kompanijoms A, B, C ir D, kurioms reikia 4000, 2000, 4000 ir 8000 adresų atitinkamai. Kiekvienai duokite pirmą ir paskutinį skirto intervalo IP adresą ir kaukę w.x.y.z/s formatu.
57. Maršrutizatorius gavo tokius naujus IP prefiksus: 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21 ir 57.6.120.0/21. Jei visi naudoja tą patį kanalą išeinantiems duomenims ar jie gali būti agreguojami? Jei taip į kokį prefiksą? Jei ne, kodėl?

Uždaviniai (II)

58. Aprašykite IPv4 antraštės formatą.
59. Aprašykite IPv6 antraštės formatą.
60. Aprašykite savais žodžiais kam skirtas ir kaip veikia **ARP** protokolas.
61. Kas yra **NAT**, kaip jis veikia ir kokie jo privalumai ir trūkumai?
62. Aprašykite kaip įgyvendinti traceroute programos funkcionalumą naudojant **ICMP** žinutes.
63. Kodėl IPv4 paketo antraštės kontrolinę sumą reikia perskaičiuoti po kiekvieno šuolio?