

Notes n Hindi

SUBJECT

Advance Computer Network

PREPARED BY

TEAM NOTESINHINDI

Notesinhindi.com

2026 Edition

Unit 1: Advanced IP Networking and Transport Layer Concepts	1.1	Networking Basics – Quick Review: OSI and TCP/IP Models — Layers, functions, common protocols
	1.2	IP Addressing (IPv4) — Classes, static/dynamic, private/public
	1.3	Routing vs Switching — Overview
	2.1	Advanced IPv4 Concepts: Subnetting — CIDR notation, subnet masks, Designing Subnet
	2.2	Multicasting — Concepts of unicast, broadcast, multicast, Applications
	3.1	Advanced TCP Mechanisms: Brief overview of TCP Header
	3.2	Flow Control — Sliding window, acknowledgments
	3.3	Congestion Control — Slow start, congestion avoidance, fast retransmit/recovery
	3.4	Protocol Spoofing — Purpose (WAN optimization), types, security concerns
	4.1	Introduction to IPv6: Need for IPv6 — IPv4 limitations, address exhaustion
	4.2	IPv6 Addressing and Features

Table of Contents

1. Networking Basics — Quick Review

1. 1.1 OSI aur TCP/IP Models
2. 1.2 IP Addressing (IPv4)
3. 1.3 Routing बनाम Switching

2. Advanced IPv4 Concepts

1. 2.1 Subnetting
2. 2.2 Multicasting

3. Advanced TCP Mechanisms

1. 3.1 TCP Header
2. 3.2 Flow Control
3. 3.3 Congestion Control
4. 3.4 Protocol Spoofing

4. Introduction to IPv6

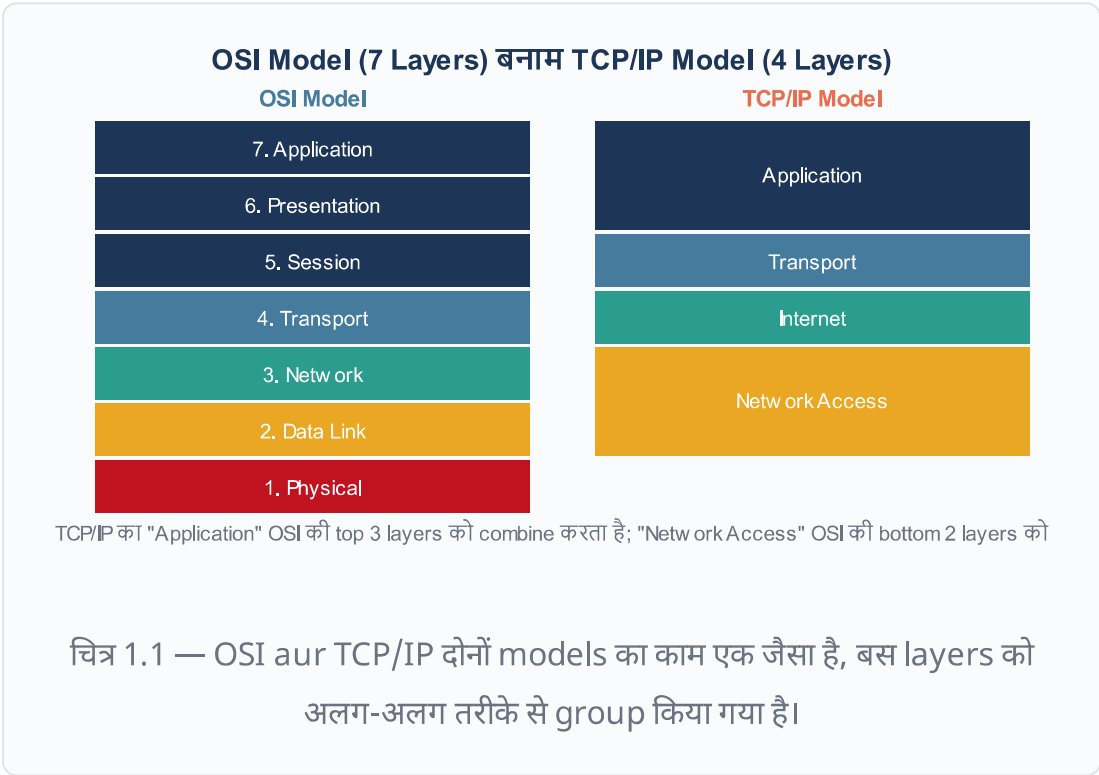
1. 4.1 Need for IPv6
2. 4.2 IPv6 Addressing aur Features

1. Networking Basics — Quick Review

1.1 OSI aur TCP/IP Models

OSI (Open Systems Interconnection) Model एक conceptual framework है जो network communication को 7 अलग-अलग layers में बाँटता है। **TCP/IP Model** इसी concept का एक practical, widely-used रूप है, जो सिर्फ 4 layers में काम को बाँटता है।

- OSI Model network operations को साफ़ तौर पर 7 layers में divide करता है, ताकि हर layer अपना specific काम independently कर सके।
- TCP/IP Model इसी concept को simplify करके सिर्फ 4 layers में present करता है, aur यही model actual internet में सबसे ज़्यादा इस्तेमाल होता है।
- हर layer अपने से ऊपर/नीचे वाली layer को specific services देती है, बिना उसके internal working में दखल दिए।
- Networking devices सिर्फ कुछ specific layers पर ही काम करते हैं — जैसे switch Layer 2 पर, router Layer 3 पर।
- इन models की वजह से अलग-अलग vendors के hardware/software भी आपस में compatible बने रहते हैं, क्योंकि सब same standard follow करते हैं।
- Troubleshooting करते समय problem को layer-by-layer isolate करना आसान हो जाता है।



Layers, Functions aur Common Protocols

OSI Layer	Function	Common Protocols
Application	User को सीधे network services देता है, जैसे browsing, email	HTTP, FTP, SMTP, DNS
Presentation	Data को encode/decode, encrypt/decrypt aur compress करता है	SSL/TLS, JPEG, ASCII
Session	दो devices के बीच एक session (बातचीत) शुरू, manage, aur खत्म करता है	NetBIOS, RPC

Transport	Data को reliably (या fast) end-to-end भेजने की ज़िम्मेदारी लेता है	TCP, UDP
Network	Data को सही destination तक पहुँचाने के लिए routing/addressing करता है	IP, ICMP
Data Link	Physical link पर data frames को error-free तरीके से भेजता है	Ethernet, ARP, PPP
Physical	Raw bits को actual signal (electrical, light, radio) में बदलकर भेजता है	Ethernet cables, Wi-Fi

Advantages of Layered Models

- हर layer independently design aur troubleshoot की जा सकती है, बिना बाकी layers को छुए।
- अलग-अलग vendors के devices भी एक जैसे standard follow करके आपस में compatible बने रहते हैं।
- Network problems को debug करना आसान हो जाता है, क्योंकि layer-by-layer check किया जा सकता है।

Disadvantages

- हर layer पर अपना header जुड़ने से थोड़ा extra overhead (data size बढ़ना) होता है।
- Real implementations में layers के बीच strict separation हमेशा possible नहीं होती।

1.2 IP Addressing (IPv4)

IP Address एक unique numerical पहचान है, जो network से जुड़े हर device को दी जाती है। **IPv4** address 32-bit का होता है, जिसे चार numbers (0-255) के रूप में, dot से अलग करके लिखा जाता है — जैसे 192.168.1.1 ।

- हर device को network पर पहचानने के लिए एक unique IP address चाहिए होता है, जैसे घर का address post office को device पहचनवाता है।
- IPv4 addresses को उनके पहले octet के आधार पर 5 classes (A से E) में divide किया गया है, हर class अलग size के network के लिए design है।
- Addresses static (fix, manually set) या dynamic (DHCP से automatically assign) हो सकते हैं, use-case के हिसाब से दोनों का अपना फ़ायदा है।
- Private IP addresses सिर्फ local network के अंदर valid होते हैं, जबकि Public IP पूरे internet पर unique होता है।
- Router NAT (Network Address Translation) का उपयोग करके कई private-IP devices को एक ही public IP के पीछे छुपा देता है।
- IPv4 addressing आज भी अधिकतर networks की foundation है, चाहे IPv6 धीरे-धीरे इसे replace कर रहा हो।

Classes of IPv4

Class	Range (पहला Octet)	इस्तेमाल
Class A	1 – 126	बहुत बड़े networks के लिए (कम networks, बहुत सारे hosts)
Class B	128 – 191	Medium size networks (जैसे universities) के लिए

Class C	192 – 223	छोटे networks के लिए (ज़्यादा networks, कम hosts) — सबसे common
Class D	224 – 239	Multicasting के लिए reserved
Class E	240 – 255	Research/experimental इस्तेमाल के लिए reserved

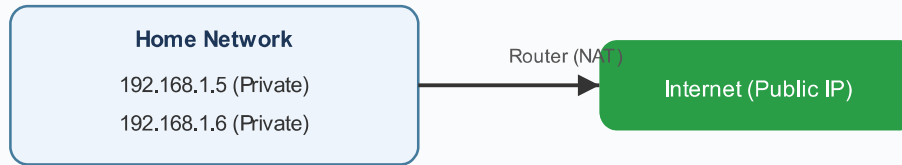
Static बनाम Dynamic Addressing

बिंदु	Static IP	Dynamic IP
Assignment	Manually, एक बार fix करके दिया जाता है	Automatically, DHCP server द्वारा दिया जाता है
बदलता है?	नहीं, हमेशा same रहता है	हाँ, हर बार अलग हो सकता है
कहाँ इस्तेमाल होता है	Servers, printers जैसे fixed devices में	घर/office के normal computers, mobiles में

Private बनाम Public IP

- **Private IP:** सिर्फ किसी particular local network (जैसे घर या office) के अंदर इस्तेमाल होता है, Internet पर सीधे visible नहीं होता (जैसे 192.168.x.x , 10.x.x.x)।
- **Public IP:** पूरे Internet पर unique होता है, aur इसी से कोई device Internet पर सीधे पहचाना जाता है।

Private IP बनाम Public IP



चित्र 1.2 — घर के अंदर सभी devices private IPs इस्तेमाल करते हैं; router NAT के through सबको एक public IP के पीछे छिपा देता है।

1.3 Routing बनाम Switching — Overview

Switching data को एक local network (LAN) के अंदर, device से device तक भेजने का काम करता है (MAC address के आधार पर), जबकि **Routing** data को अलग-अलग networks के बीच (IP address के आधार पर) सही रास्ते से भेजने का काम करता है।

- Switch Data Link Layer (Layer 2) पर काम करता है aur MAC addresses देखकर decide करता है कि frame किस port पर भेजनी है।
- Router Network Layer (Layer 3) पर काम करता है aur IP addresses के आधार पर best path चुनता है।
- Switching सिर्फ एक ही broadcast domain के अंदर होती है, जबकि Routing अलग-अलग broadcast domains/networks को आपस में जोड़ती है।
- एक typical office network में switch computers को आपस में जोड़ता है, aur router उस पूरे network को internet से जोड़ता है।
- Modern networks में दोनों devices साथ मिलकर काम करते हैं — पहले switching (local), फिर routing (external) होती है।

बिंदु	Switching	Routing
-------	-----------	---------

Device	Switch	Router
काम करता है	Same network (LAN) के अंदर	अलग-अलग networks के बीच
किसके आधार पर decision	MAC Address	IP Address
Layer (OSI)	Data Link Layer (Layer 2)	Network Layer (Layer 3)

Example: किसी office के अंदर सभी computers को आपस में जोड़ने के लिए switch इस्तेमाल होता है, जबकि उस office के network को Internet से जोड़ने के लिए router इस्तेमाल होता है।

2. Advanced IPv4 Concepts

2.1 Subnetting

Subnetting एक process है जिसमें किसी बड़े network को कई छोटे-छोटे sub-networks (subnets) में बाँटा जाता है।

- इससे IP addresses का इस्तेमाल ज़्यादा efficient तरीके से होता है, क्योंकि हर department/location को सिर्फ उतने ही addresses मिलते हैं जितनी ज़रूरत है।
- Network administrator CIDR notation (जैसे /24) या subnet mask (जैसे 255.255.255.0) का इस्तेमाल करके यह define करता है कि address का कौन सा हिस्सा network है aur कौन सा host।
- हर subnet अपना अलग broadcast domain बनाता है, जिससे unnecessary traffic पूरे बड़े network में नहीं फैलता।
- Subnetting से security भी improve होती है क्योंकि अलग-अलग departments को अलग subnets में रखकर उनके बीच access control किया जा सकता है।
- बड़े organizations में subnetting एक standard practice है, ताकि network को logically aur manageable तरीके से organize किया जा सके।

Subnetting को actually implement करने के लिए दो चीज़ों को समझना ज़रूरी है — **CIDR Notation** aur **Subnet Mask**। यह दोनों subnetting के अलग topics नहीं, बल्कि वह दो तरीके हैं जिनसे किसी IP address में network aur host part बताया जाता है।

CIDR Notation — Network aur Host Part को दिखाने का तरीका

CIDR (Classless Inter-Domain Routing) notation यह बताने का एक तरीका है कि किसी IP address में से कितने bits **network** को represent करते हैं — इसे IP address के बाद / लगाकर एक number से दिखाया जाता है, जैसे 192.168.1.0/24 , जहाँ /24 का मतलब है कि पहले 24 bits network के लिए हैं।

Subnet Mask — CIDR को ही एक दूसरे रूप में लिखना

Subnet Mask एक 32-bit number होता है, जो यह बताता है कि IP address के किस हिस्से को **network part** aur किस हिस्से को **host part** माना जाए — जैसे

255.255.255.0 एक common subnet mask है, जो /24 के बराबर होता है।

IP Address — Network Part बनाम Host Part (/24)

192.168.1 (Network Part)	.5 (Host)
--------------------------	-----------

/24 का मतलब पहले 24 bits (यानी पहले 3 octets) network को identify करते हैं, बाकी 8 bits host को

चित्र 2.1 — /24 subnet में पहले तीन numbers network बताते हैं, आखिरी number उस network के अंदर particular device (host) बताता है।

Designing a Subnet — Steps

1. यह तय करें कि कितने subnets (छोटे networks) चाहिए, aur हर subnet में कितने hosts (devices) होंगे।
2. ज़रूरी hosts की संख्या के according यह calculate करें कि कितने bits **host bits** के लिए चाहिए।
3. बाकी बचे bits को **subnet bits** के तौर पर, original network address से उधार (borrow) लें।
4. नया subnet mask aur हर subnet की range (शुरुआत, आखिर, broadcast address) calculate करें।
5. हर subnet को अलग-अलग departments/locations को assign कर दें।

Example: मान लीजिए किसी company को 192.168.1.0/24 network मिला है, aur उसे 4 अलग departments (Sales, HR, IT, Finance) के लिए अलग subnets चाहिए — तो इसे 4 बराबर subnets में बाँटा जा सकता है (जैसे 192.168.1.0/26 , 192.168.1.64/26 आदि), हर एक subnet में 62 usable hosts के साथ।

Advantages of Subnetting

- IP addresses का इस्तेमाल ज़्यादा efficient (कम waste) तरीके से होता है।
- Network traffic कम होता है, क्योंकि broadcast सिर्फ उसी subnet तक सीमित रहता है।
- Security बेहतर होती है, क्योंकि अलग-अलग departments को अलग subnets में रखकर access control किया जा सकता है।

Disadvantages

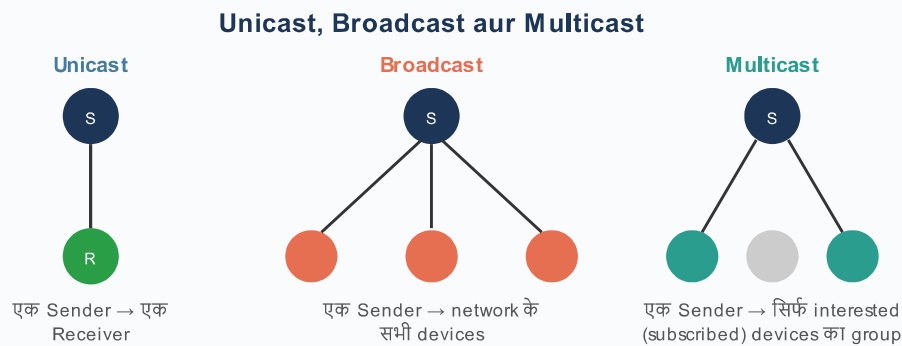
- Subnet design aur calculation करना शुरूआत में थोड़ा technical aur confusing लग सकता है।
- ज़्यादा subnets बनाने से network administration का काम बढ़ जाता है।

2.2 Multicasting

Multicasting एक तरीका है जिसमें एक sender अपना data एक साथ, सिर्फ उन specific devices के group को भेजता है जिन्होंने उस data में interest दिखाया हो (subscribe किया हो)।

- यह Unicast (एक-को-एक) aur Broadcast (एक-से-सबको) के बीच का रास्ता है, जो सिर्फ interested devices तक data पहुँचाता है।
- Multicast के लिए एक special IP address range (Class D: 224-239) reserved है, जिसे multicast group address कहते हैं।
- Network devices (routers) को multicast traffic handle करने के लिए special protocols (जैसे IGMP) support करने पड़ते हैं।
- इससे bandwidth की बहुत बचत होती है, क्योंकि sender को हर receiver के लिए अलग से data नहीं भेजना पड़ता।
- यह widely video streaming, online gaming, aur stock market updates जैसे real-time applications में इस्तेमाल होता है।

Unicast, Broadcast aur Multicast — Data भेजने के तीन तरीके



चित्र 2.2 — Unicast में एक-को-एक, Broadcast में एक-से-सबको, aur Multicast में एक-से-चुनिंदा group को data भेजा जाता है।

Applications of Multicasting

- **Video/Audio Streaming:** Live TV या video conferencing में एक साथ कई viewers को data भेजने के लिए।
- **Online Gaming:** Multiplayer games में सभी connected players को updates भेजने के लिए।
- **Stock Market Updates:** Real-time price updates को एक साथ कई subscribers तक भेजने के लिए।
- **Routing Protocol Updates:** Routers के बीच routing information share करने के लिए (जैसे OSPF)।

Advantages of Multicasting

- Broadcast के मुकाबले network bandwidth की काफी बचत होती है, क्योंकि data सिर्फ interested devices को जाता है।
- Sender को हर receiver को अलग-अलग (unicast की तरह) data भेजने की ज़रूरत नहीं पड़ती, जिससे efficiency बढ़ती है।

Disadvantages

- Multicast को सही तरीके से implement करने के लिए network devices (routers) का special support चाहिए होता है।
- Security aur reliability manage करना unicast के मुकाबले ज़्यादा complex होता है।

3. Advanced TCP Mechanisms

3.1 Brief Overview of TCP Header

TCP Header वह extra जानकारी है जो हर TCP segment के आगे जोड़ी जाती है, ताकि receiver को यह पता चल सके कि data कहाँ से आया, कहाँ जाना है, aur उसे सही क्रम में कैसे जोड़ना है।

- यह header data को reliable aur ordered तरीके से भेजने के लिए ज़रूरी सारी जानकारी carry करता है।
- इसके fields (Sequence Number, Acknowledgment Number) यह ensure करते हैं कि data सही क्रम में, बिना duplicate या loss के पहुँचे।
- Flags (SYN, ACK, FIN) connection को शुरू करने, maintain करने, aur बंद करने के लिए control signals देते हैं।
- Window Size field flow control के लिए इस्तेमाल होता है, जो बताता है कि receiver एक बार में कितना data accept कर सकता है।
- TCP header, IP header के साथ मिलकर पूरी packet बनाता है जो network पर भेजी जाती है।

Field	Purpose
Source/Destination Port	यह बताता है कि data किस application से आया aur किस application के लिए जा रहा है
Sequence Number	Data के हर byte को एक क्रम (order) देता है, ताकि receiver उसे सही तरतीब में जोड़ सके

Acknowledgment Number	यह बताता है कि अगला कौन सा byte receiver को चाहिए, यानी अब तक क्या-क्या सही मिल चुका है
Flags (SYN, ACK, FIN आदि)	Connection को शुरू करना, acknowledge करना, या बंद करना जैसे control signals देते हैं
Window Size	Receiver बताता है कि वह एक बार में कितना data बिना acknowledgment के accept कर सकता है

3.2 Flow Control

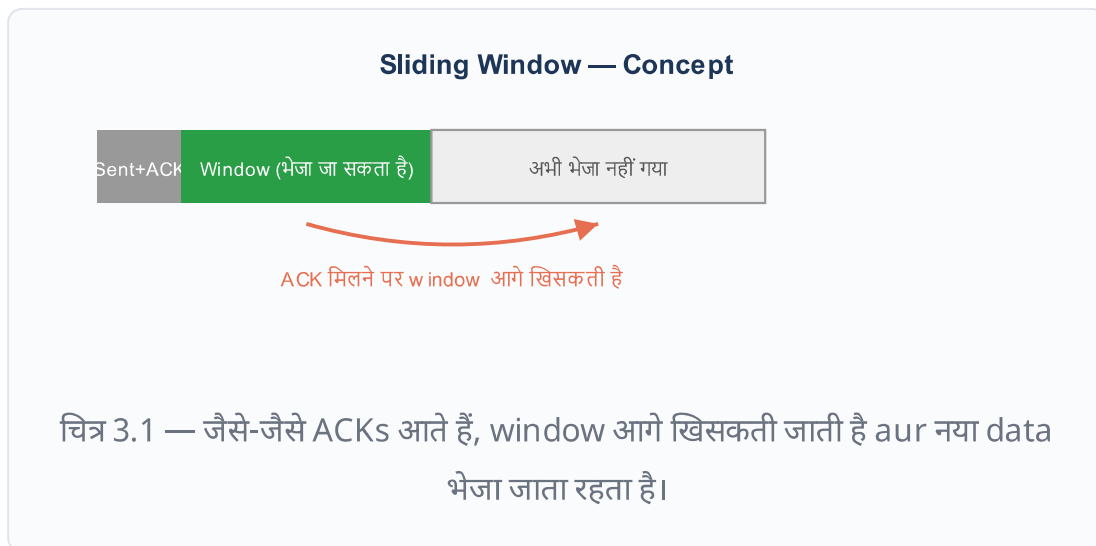
Flow Control एक mechanism है जो यह सुनिश्चित करता है कि sender, receiver की क्षमता (capacity) से ज़्यादा तेज़ data ना भेजे।

- इसका main goal receiver के buffer को overflow होने से बचाना है, जिससे data loss ना हो।
- यह Sliding Window technique इस्तेमाल करता है, जिसमें sender-receiver एक "window" (एक साथ भेजी जा सकने वाली data की मात्रा) पर सहमत होते हैं।
- Acknowledgments (ACKs) receiver द्वारा भेजे जाते हैं, जो confirm करते हैं कि data safaltapoorvak मिल गया।
- जैसे-जैसे ACKs आते जाते हैं, window आगे खिसकती जाती है, जिससे sender continuous data भेज सकता है।
- अगर किसी data का ACK ना मिले, तो sender उसे lost मानकर दोबारा भेज देता है।

Sliding Window — कितना Data एक साथ भेजा जाए

Sliding Window एक technique है जिसमें sender aur receiver एक "window" (यानी एक साथ भेजे जा सकने वाले data की मात्रा) पर सहमत होते हैं। जैसे-जैसे acknowledgments (ACKs) मिलते जाते हैं, यह window आगे "खिसकती (slide)" जाती

है, जिससे sender बिना हर byte के लिए रुके, लगातार data भेज सकता है।



Acknowledgments — Sliding Window को आगे बढ़ाने वाला Signal

Acknowledgment (ACK) receiver द्वारा sender को भेजा गया एक confirmation message है, जो बताता है कि data सही तरीके से मिल गया है। यही ACKs Sliding Window को आगे खिसकाते हैं — जब तक ACK ना आए, window आगे नहीं बढ़ती।

3.3 Congestion Control

Congestion Control उन mechanisms को कहते हैं जो network में भीड़-भाड़ (congestion) को रोकने या कम करने के लिए इस्तेमाल होते हैं।

- जब network में बहुत ज़्यादा data भेजा जाता है, तो routers पर load बढ़ जाता है aur packets delay या drop होने लगते हैं — इसी को congestion कहते हैं।
- TCP इस समस्या को manage करने के लिए अलग-अलग phases से गुज़रता है — Slow Start, Congestion Avoidance, aur Fast Retransmit/Recovery।
- Slow Start में sender कम data से शुरुआत करके, हर successful ACK के बाद window को exponentially बढ़ाता है।
- Congestion Avoidance में window को धीरे-धीरे (linearly) बढ़ाया जाता है, ताकि network पर अचानक load ना पड़े।
- Packet loss होने पर window तुरंत छोटा कर दिया जाता है, aur process दोबारा शुरू होती है।

Phase 1 — Slow Start

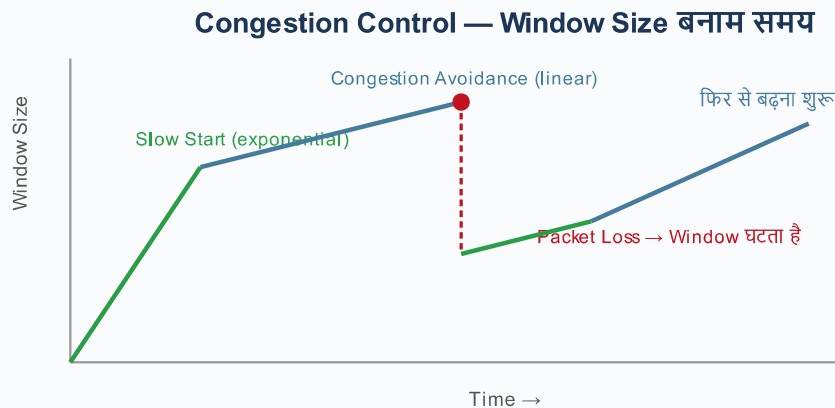
शुरुआत में sender बहुत कम data भेजना शुरू करता है, aur हर बार सफलतापूर्वक ACK मिलने पर भेजे जाने वाले data की मात्रा (congestion window) को तेज़ी से (exponentially) बढ़ाता जाता है, जब तक कि कोई loss ना हो जाए या एक threshold ना पहुँच जाए।

Phase 2 — Congestion Avoidance

एक बार threshold पहुँचने के बाद, sender अब window को बहुत धीरे-धीरे (linearly) बढ़ाता है, ताकि network पर अचानक ज़्यादा load ना पड़े।

Phase 3 — Fast Retransmit / Fast Recovery (Loss होने पर)

अगर sender को एक ही ACK number बार-बार (duplicate ACKs) मिलता है, तो वह समझ जाता है कि कोई particular packet खो गया है, aur उसे बिना timeout का इंतज़ार किए, तुरंत दोबारा भेज (retransmit) देता है।



चित्र 3.2 — Slow Start में window तेज़ी से बढ़ता है, फिर Congestion Avoidance में धीरे; loss होने पर window फिर से छोटा होकर प्रक्रिया दोहराता है।

3.4 Protocol Spoofing

Protocol Spoofing एक technique है जिसमें किसी slow या high-latency WAN link पर, एक local device खुद असली destination की तरह act करता है aur locally ही acknowledgments भेज देता है।

- इसका main purpose **WAN optimization** है — यानी slow links पर भी applications को fast feel करवाना।
- Satellite links जैसे high-latency connections में यह technique बहुत useful होती है, जहाँ real acknowledgment का wait करना बहुत slow होता।
- यह TCP Spoofing aur DNS Spoofing (caching context में) जैसे रूपों में implement किया जाता है।
- इससे end-to-end verification थोड़ी कमज़ोर हो सकती है, जिसका फायदा attackers उठा सकते हैं अगर सही से secure ना किया जाए।
- Encrypted traffic (HTTPS) के साथ इसे implement करना मुश्किल होता है, क्योंकि content locally inspect नहीं किया जा सकता।

Purpose — यह Technique क्यों इस्तेमाल होती है

WAN links (जैसे satellite links) में delay (latency) बहुत ज़्यादा हो सकती है। अगर हर acknowledgment के लिए असली, दूर के destination तक wait करना पड़े, तो पूरा communication बहुत धीमा हो जाएगा। Protocol Spoofing इस delay को छिपा देता है, जिससे local applications को लगता है कि response जल्दी मिल रहा है।

Types

- **TCP Spoofing:** Local device TCP acknowledgments को locally ही generate कर देता है, बिना असली remote receiver के जवाब का इंतज़ार किए।
- **DNS Spoofing (WAN optimization context में):** बार-बार होने वाली DNS queries को locally cache करके तुरंत जवाब देना।

Security Concerns

- चूंकि local device असली destination की तरह behave करता है, इससे end-to-end verification कमज़ोर हो सकती है।
- अगर सही तरीके से secure ना किया जाए, तो यह technique man-in-the-middle जैसे attacks के लिए एक रास्ता बन सकती है।

Example: Satellite internet connections में, जहाँ delay बहुत ज़्यादा होती है, router-level TCP spoofing का इस्तेमाल करके उपयोगकर्ता को websites तेज़ी से load होती हुई महसूस होती हैं, जबकि असल में data अभी भी satellite के through ही जा रहा होता है।

4. Introduction to IPv6

4.1 Need for IPv6

IPv6 (Internet Protocol version 6) IPv4 का अगला version है, जिसे इसलिए बनाया गया क्योंकि IPv4 की address capacity Internet के तेज़ी से बढ़ते इस्तेमाल के सामने बहुत कम पड़ गई।

- IPv4 सिर्फ 32-bit addresses इस्तेमाल करता है, जिससे कुल लगभग 4.3 अरब unique addresses ही बन सकते हैं।
- Smartphones, IoT devices, smart-home gadgets — हर चीज़ को अब एक IP address चाहिए, जिससे existing IPv4 addresses कम पड़ गए।
- इस समस्या को **IPv4 Address Exhaustion** कहा जाता है।
- NAT जैसी techniques से इसे temporarily manage किया गया, लेकिन यह एक permanent solution नहीं था।
- IPv6, 128-bit addressing के साथ इस समस्या को लगभग हमेशा के लिए खत्म कर देता है।

IPv4 Address Space बनाम IPv6 Address Space

IPv4 ≈ 4.3 अरब

IPv6 ≈ 340 undecillion
(यानी लगभग असीमित)

IPv6, IPv4 के मुकाबले इतना बड़ा address space देता है कि आने वाले दशकों तक कमी की चिंता नहीं

चित्र 4.1 — IPv6 का address space IPv4 से खरबों गुना बड़ा है, इसलिए address exhaustion जैसी समस्या लगभग खत्म हो जाती है।

4.2 IPv6 Addressing aur Features

IPv6 Address एक 128-bit address होता है (IPv4 के 32-bit के मुकाबले), जिसे 8 groups में, colon (:) से अलग करके, hexadecimal (0-9, a-f) में लिखा जाता है — जैसे 2001:0db8:85a3:0000:0000:8a2e:0370:7334 ।

- इसका address space इतना बड़ा है (340 undecillion) कि आने वाले दशकों तक address की कमी की चिंता नहीं रहेगी।
- IPv6 header IPv4 से simpler है, जिससे routers packets को तेज़ी से process कर पाते हैं।
- हर device को directly एक unique public address मिल सकता है, इसलिए NAT की ज़रूरत नहीं रहती।
- IPv6 में IPSec (encryption aur authentication) शुरू से ही built-in support के साथ आता है।
- Devices बिना DHCP server के भी खुद-ब-खुद एक valid IPv6 address generate कर सकते हैं (auto-configuration)।

IPv6 Address Format — 8 Groups (128 bits)

2001 : 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334

हर group 16 bits का है (hexadecimal में) — कुल 8 groups × 16 bits = 128 bits

चित्र 4.2 — IPv6 address 8 hexadecimal groups से मिलकर बनता है, colon (:) से अलग किए गए।

बिंदु	IPv4	IPv6
Address Length	32-bit	128-bit
Format	Decimal (जैसे 192.168.1.1)	Hexadecimal (जैसे 2001:0db8::1)

Total Addresses	~4.3 अरब	लगभग असीमित (340 undecillion)
NAT की ज़रूरत	ज़्यादातर हाँ	आमतौर पर नहीं

Advantages of IPv6

- Address की कमी की समस्या लगभग पूरी तरह खत्म हो जाती है।
- Header simple होने की वजह से routing तेज़ aur efficient होती है।
- Built-in security features से network ज़्यादा सुरक्षित बनता है।

Disadvantages of IPv6

- IPv4 से IPv6 में migrate करना एक लंबी aur complex process है, क्योंकि पूरी दुनिया की infrastructure अभी भी काफी हद तक IPv4 पर आधारित है।
- कुछ पुराने devices/software IPv6 को पूरी तरह support नहीं करते।

Example: आजकल mobile network operators (जैसे Jio) अपने mobile data network में IPv6 का व्यापक इस्तेमाल करते हैं, ताकि करोड़ों नए mobile users को बिना address की कमी की चिंता किए, आसानी से जोड़ा जा सके।