The benefits of IPv6 when compared with IPv4: Larger Addresses +Extended Address Hierarchy + Flexible Header Format + Improved Options + Support for Autoconfiguration and Renumbering + Support for Resource Allocation

Compare and contrast the IPv4 and the IPv6 header fields

Streamlined: fragmentation fields moved out of base header + IP options moved out of base header, indicated by "Next Header" field + Header Checksum eliminated to reduce processing time at each hop + Header Length field eliminated + Length field excludes IPv6 base header / Revised: Time to Live -> Hop Limit + Protocol -> Next Header + Service Type -> Traffic Class + Addresses increased 32 bits -> 128 bits / Extended: Flow Label field added, identify datagrams in same "flow."

Give more detailed information about the plane of network layer:

Forwarding(in Data plane):
move packets from router's input to appropriate router output
- IP protocol
- involves a single router
- forwarding takes place typically in a few nanoseconds, and thus is typically implemented in hardware.

forwarding: process of getting through single interchange

Routing(in Control plane):
determine route taken by packets from source to dest. (network-wide process)
- routing algorithms
- involves all of a network's routers
- routing takes place on much longer timescale (typically seconds) and often is implemented in software.

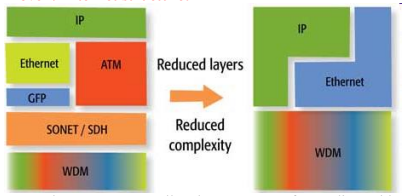
routing: process of planning trip from source to dest.

Queue: Output port: buffering when arrival rate via switch exceeds output line speed + queuing (delay) and loss due to output port buffer overflow! + Consequence: a packet scheduler at the output port must choose one packet, e.g., selection can be based on first-come-first-served (FCFS) scheduling / Input port: Fabric slower than input ports combined -> queuing may occur at input queues + Head-of-the-Line (HOL) blocking: queued datagram at front of queue prevents others in queue from moving forward + queuing delay and loss due to input buffer overflow!

Switching Interconnection: Overcome bus bandwidth limitations + A crossbar switch is an interconnection network consisting of 2n buses that connect n input ports to n output ports. + Advanced design: fragmenting datagram into fixed length cells, switch cells through the fabric. + Cisco 12000: switches 60 Gbps through the interconnection network + The fastest switching type

Present router: run routing algorithms/protocol (RIP, OSPF, BGP) + forwarding datagrams from incoming to outgoing link

IP-over / Internet structure:



SDN: The remote controller that computes forwarding tables and interacts with routers is implemented in software + providing many of these network-layer functions and certain link-layer functions as well, in a modern, elegant, and grated manner

Load balancer: Inside the data center, the external requests are first directed to a load balancer whose job is distributing requests to the hosts, balancing the load across the hosts as a function of their current load + a large data center will often have several load balancers, each one devoted to a set of specific cloud applications + Such a load balancer is sometimes referred to as a "layer-4 switch" + since it makes decisions based on the destination port number (layer 4) as well as destination IP address in the packet. + the load balancer not only balances the workload across hosts, but also provides a NAT-like function.

limited host-to-host capacity: Problem: suppose each host connects to its TOR switch with 1Gbps link rate, but the links between switches are 10 Gbps rate. If there are many flows between different racks at the same time, the max rate for two hosts may be less than 1Gbps because sharing 10 Gbps link. + Solution: deploy higher-rate switches and routers and deploy new interconnection architectures and network protocols, e.g., a fully connected topology.

Trends in data center: deploy new interconnection architectures and network protocols + employ shipping container-base modular data centers (MDCs)

MPLS applications: Traffic Engineering (use QoS to control the rate of traffic on each path) + Class of Service (Support for differentiated services), VPN (MPLS allows ISPs to offer VPN services by providing a simple, flexible, and powerful tunneling mechanism)

Compare flow control and congestion control: Flow control: end-to-end + control and handle the traffic between a sender and a receiver + slide window congestion control / Congestion control: entire network + control congestion in the network and prevent loss of packets and delay + make sure the entire work can handle the traffic that is coming to the network + slow start + congestion avoidance + fast retransmit + fast recovery

TCP = GBN / SR: hybrid of GBN and SR protocols / GBN-like: TCP sender need only maintain the smallest sequence number of a transmitted but unacknowledged byte (SendBase) and the sequence number of the new byte to be sent (NextSeqNum) / SR-like: Many TCP implementations will buffer correctly receive but out-of-order segments. TCP, on the other hand, would retransmit at most one segment, namely, segment n. Moreover, TCP would not even retransmit segment n if the acknowledge for segment n+1 arrived before the timeout for segment n. A proposed modification to TCP, the so-called selective acknowledgement, allows TCP receivers the acknowledge out-of-order segments selectively rather than just cumulatively acknowledge the last correctly received, in order segment.

Compare UDP and TCP: point-to-point + reliable, in-order byte stream + pipelined + send & receive buffers + full duplex data + connection-oriented + flow controlled / UDP: no frills + best effort service + connectionless + no congestion control + loss tolerant + rate sensitive

Compare three service models: Best effort service model: single model is a single service model try its best to send message but does not provide guarantee for the performance like time delay, reliability + no QoS, simple, all packets are equal at the router, no special treatment for any delay-sensitive multimedia applications / Intserv (Integrated Services): Reserved Resources + Call Setup / call admission + architecture for providing QoS guarantees in IP networks for individual application sessions / Diffserv (Differentiated Services): aims to handle different "classes" of traffic in a scalable and flexible manner + scalability: simple functions in network core, relatively complex functions at edge routers (or hosts) + flexibility: don't define specific service classes, but provide functional components to build service classes

VoIP: a methodology and group of technologies for the delivery of voice communications and multimedia sessions over IP networks: Receiver -> analogy-digital converter -> compression encoder -> IP encapsulation -> digital-analog converter ->player

CDN: replicate stored content and put the replicated content at the edges of the Internet. CDNs provide a differentiated service to content providers + replicate content at hundreds of servers throughout Internet + placing content "close" to user + CDN server typically in edge/access network + Servers nearest to the website visitor respond to the request. The content delivery network copies the pages of a website to a network of servers that are dispersed at geographically different locations, caching the contents of the page. When a user requests a webpage that is part of a content delivery network, the CDN will redirect the request from the originating site's server to a server in the CDN that is closest to the user and deliver the cached content. CDNs will also communicate with the originating server to deliver any content that has not been previously cached

Token bucket / leaky bucket: Token Bucket: limit input to specified Burst Size and Average Rate and can allow a certain degree of burst transmission/ Leaky bucket: limit the transmission rate

Peering and transit: Peering: peering is a business relationship whereby two companies interconnect directly without charging, RECIPROCALLY exchange access to each other's customers + Peering is open only to traffic coming from a peer's end-users or from networks that have bought transit. / Transit Provider sells metered access to the Global Internet + A transit provider will not announce its peering and transit

Compare LS and DV: LS: Dijkstra's algorithm+ all routers have complete topology, link cost info + net topology, link costs known to all nodes + computes least cost paths from one node ("source") to all other nodes / DV: Bellman-Ford Equation + router knows physically-connected neighbors, link costs to neighbors + iterative process of computation, exchange of info with neighbors + a node gradually calculates the least-cost path to a destination or set of destinations + From time-to-time, each node sends its own distance vector estimate to neighbors + Asynchronous

Compare RIP, OSPF and IS-IS: Routing Information Protocol (RIP): Routing Information Protocol (RIP): distance vector algorithm + distance metric: # of hops (max = 15 hops) + distance vectors: exchanged among neighbors every 30 sec via Response Message (also called advertisement) + UDP + slow response to change + no security + no hierarchy / Open Shortest Path First (OSPF): link state algorithm, criterion of routing: bandwidth & delay, advertisements disseminated to entire AS (via flooding), use flooding to send msgs, use IP (not UDP) directly to transmit IP datagrams + security + hierarchy / Intermediate System to Intermediate System is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. It accomplishes this by determining the best route for data through a Packet switching network.

Link-state algorithm (oscillations): Oscillations possible (with congestion-sensitive routing): link A and B is empty first, sender choose link A send first, then link A will become busy and if sender would send data immediately, it would choose link B + e.g., link cost = amount of carried traffic + => link cost is asymmetric + i.e., c(u,v) = c(v,u) only if the load carried on both directions on the link (u,v) is the same

Count-to-infinity: Slow convergence problem + good news travels fast + bad news travels slowly: It occurs when one router feeds another old information, which continues to propagate through the network toward infinity. This occurs when a link is removed.

Poisoned reverse: If Z routes through Y to get to X: Z tells Y its (Z's) distance to X is infinite (so Y won't route to X via Z) + This ensures all routers in the domain receive the poisoned router update. + used to prevent ping-pong loops (infinite distance = 16 hops)

BGP incidents: illegitimate takeover of groups of IP addresses by corrupting Internet routing tables maintained using the Border Gateway Protocol (BGP) + Like the TCP reset attack, session hijacking involves intrusion into an ongoing BGP session, i.e., the attacker successfully masquerades as one of the peers in a BGP session, and requires the same information needed to accomplish the reset attack

Compare Intra- and Inter-AS routing: Inter-AS: Policy based + The Routing Domain of BGP is the entire Internet Used to convey routing information between ASes / Intra-AS: no policy decisions needed focus on performance + Metric based + Automatic discovery + Generally trust your IGP routers + Routes go to all IGP routers

Hot/cold potato routing: With hot potato routing, you want the traffic going to a particular destination off your network ASAP + the practice of handing over traffic at the earliest convenience + Go for the Closest Egress Point + minimize the amount of works thus resulting in lower QoS / Cold potato routing is the opposite. You want to keep that traffic on your network as long as possible transport it to a point as close as possible to the final destination before handing it over to a peer/provider (if necessary) + where you hold onto traffic as long as you can before handing it over to another network + more expensive to do and requires a level of trust between two networks that either side will not attempt to "cheat" the other

SSL / TLS: Secure Sockets Layer (SSL) — a security protocol that was originally developed by Netscape Communications, later developed into Transport Layer Security (TLS), an IETF standard, is similar to SSLv3. + usually implemented on top of any of the Transport Layer protocols + sometimes referred to as web VPNs or clientless VPNs because no special client software is required other than a web browser + More functionality can be added by installing SSL VPN client software on remote access client devices

VPN disadvantages: VPNs require an in-depth understanding of public network security issues and proper deployment of precautions + Availability and performance depends on factors largely outside of their control + Immature standards + VPNs need to accommodate protocols other than IP and existing internal network technology

Symmetric encryption: Alice's , Bob's keys are identical and are secret

Public key: A pair of keys is used + One of the keys is known to both Bob and Alice (indeed, it is known to the whole world) + The other key is known only by either Bob or Alice (but not both).

RSVP: Resource Reservation Protocol + known as a soft-state protocol, i.e., can expire + used to install state (bandwidth reservations) in routers + To implement RSVP, RSVP software must be present in the receivers, senders, and routers along the end-end path

MPLS (Operation): works by prefixing packets with MPLS header, containing one or more labels, called label stack. MPLS-labeled packets are switched after label lookup (switch instead of lookup into IP table + LSR receives a packet, it uses label included as an index to determine the next hop on the LSP and a corresponding label for packet from lookup table. The old label is removed from the header and replaced with new label before the packet routed + When forwarding IP datagram into MPLS domain, an LER uses routing information to determine label to be affixed and forwards the labelled packet into the MPLS domain. Upon receiving a labelled packet destined to exit MPLS domain, LER strips off the label and forwards the IP packet using IP forwarding rules / MPLS allows most packets to be forwarded at Layer 2 (the switching level) rather than having to be passed up 17. to Layer 3 (the routing level). Each packet gets labeled on entry into the service provider's network by the ingress router. All the subsequent routing switches perform packet forwarding based only on those labels—they never look as far as the IP header. Finally, the egress router removes the label(s) and forwards the original IP packet toward its final destination. The label determines which pre-determined path the packet will follow. The paths, which are called label-switched paths (LSPs), allow service providers to decide ahead of time what will be the best way for certain types of traffic to flow within a private or public network.

Ipsec: Symmetric Key Encryption + for securing the network-layer transport + designed to protect IP traffic between security gateways or hosts as it transits an intervening network + As well as enabling site-to-site VPNs, IPsec can also be used to securely tunnel data traffic between remote access or mobile users and a VPN gateway/concentrator

L2TPv3: Layer Two Tunneling Protocol version 3 (L2TPv3) — allows the point-to-point transport of protocols over an IP or other backbone + L2TP has limited intrinsic security, and so L2TP tunnels are often protected using IPsec + allows the point-to-point transport of protocols over an IP or other backbone

GRE: construct tunnels and transport multiprotocol traffic between CE devices in a VPN. GRE has little or no inherent security, but GRE tunnels can be protected using Ipsec + tunning protocol that encapsulates network layer inside virtual p2p links + support multiprotocol and multicast + support multipoint tunnel + provide QoS

PPTP: Point-to-Point Tunneling Protocol + layer 2 protocol hat encapsulates PPP frames in IP datagrams for transmission over an IP internetwork + lower transmission cost + lower hardware cost + lower administrative overhead + security

AIMD: The approach taken is to increase the transmission rate (window size), probing for usable bandwidth, until loss occurs. The policy of additive increase may, for instance, increase the congestion window by a fixed amount every round trip time. When congestion is detected, the transmitter decreases the transmission rate by a multiplicative factor; for example, cut the congestion window in half after loss. The result is a saw-tooth behavior that represents the probe for bandwidth

Delay Jitter: In computer networking, packet delay variation (PDV) is the difference in end-to-end one-way delay between selected packets in a flow with any lost packets being ignored. The effect is sometimes referred to as jitter

UDP socket: identified by two-tuple + (dressIP address, dest port number)

CSMA/CD: Carrier Sense Multiple Access / Collision Detection

IGMP : (Internet Group Management Protocol) announce participation in multicast. 2. Phases: When it joins a group, host sends message declaring membership; Multicast router periodically polls a host to determine if any host on the network is still a member of a group (no explicit when leaving) + R joins to group 224.2.0.1--R sends IGMP Membership-report to 224.2.0.1;DR receives it. DR will start forwarding packets for224.2.0.1 to network A; DR periodically sends IGMP Membership-Query to 224.0.0.1(all systems mcast); R answers IGMP Membership-report to 224.2.0.1

Advantages and Disadvantages of the Original Classful IP Addressing scheme: Advantage: a router can keep one routing entry per network instead of per destination host + Use classful addressing to determine the boundary between prefix and suffix, e.g., Class A partitioned an address into 8-bit network portion and a 24-bit host portion / Weakness: requiring a unique prefix for each physical network would exhaust the address space quickly as the Internet proliferates.

Mobility comparison between GSM and Mobile IP: both have high mobility and mobile user can maintain connections through multiple access point, both use indirect routing to communicate with users; Diff: mobile IP prefers user who move infrequently and can stay for a relatively long period of time because of the considerable overhead during the transmission of data; In GSM, Mobile Switching Center work instead of routers in IP network. HLR(Home Location Register), VLR(Visitor Location Register)are used to store phone num, like the IP address in IP network.

The same VC number: Replacing the number from link to link to reduce the length of the VC field in header + Permitting a different VC number for each link along the path of the VC to simplified a network management function and VC setup because each link chooses VC num independently and common VC num costs a lot

DDOS: hard to monitored or tracked, attackers hide themselves well + based on legal packets So firewall spends high-intensive check to prevent + systems optimization and increasing bandwidth cost lot, but escalation of DDoS attack costs les

Reliable data transfer (rdt): ack + retransmission + timeout + sliding window + stop-and-wait + pipelined protocols(buffering at sender and/or receiver; error recovery protocols like go-back-n, selective repeat)s

Most common VPN protocols: PPTP (point to point tunneling protocol) + L2TP + IPSES

The disadvantages of RIP: Increased network traffic: RIP checks with its neighboring routers every 30 seconds, which increases network traffic. Maximum hop count: RIP has a maximum hop count of 15, which means that on large networks, other remote routers may not be able to be reached. Closest may not be shortest: Choosing the closest path by hop count does not necessarily mean that the fastest route was selected. RIP does not consider other factors when calculating best path. RIP only updates neighbors so the updates for non-neighboring routers are not first-hand information

Overlay VPNs a VC or tunnel connects CE devices, no routing information is exchanged with the service provider (PE devices) Examples: those built using Frame Relay or ATM virtual circuits, as well as those built using GRE or IPsec tunnels

Peer VPNs PE devices are aware of customer network addressing and route customer data traffic according to customer network addressing Example: BGP/MPLS (RFC4364/2547bis) VPNs

Three basic IPv6 address types: unicast (destination address specifies a single computer, delivery to single), anycast, multicast (destination is a set of computers, possibly at multiple locations. Delivery to each member in the set using hardware multicast or broadcast if viable)

Three types of switching fabrics: twisted pair, memory, bus, crossbar

RFC: request for comments + never change once published + not all RFCs are standards

SLA: Service Level Agreement; An SLA is a formal negotiated agreement

Switch: link-layer device: smarter than hubs, take active role; transparent: hosts are unaware of presence of switches; self-learning: switches do not need to be configured

Compare switch and bridge: number of network segments, bridge 1-1 + switch 1-N + switches perform in hardware, bridges perform in software + Both store-and-forward devices; Both maintain tables topology: switch--> a spanning tree, routers--> a rich topology

MTU: maximum transmission unit + a link's maximum transmission unit transmitted over the link

Protocols: protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission & receipt

Compare Transport and network layer network layer: logical communication between hosts; transport: between processes

VC implementation: VC consists of path, VC numbers, entries in forwarding table + Replacing the number from link to link reduces the length of the VC field in the packet header. 2. VC setup is considerably simplified by permitting a different number at each link along the path of the VC. Each link can choose a VC number independently and common VC number costs a lot

Core-based trees (CBT): better for sparse network; Protocol Independent Multicast (PIM), no dependent on any specific underlying unicast routing alg. PIM-SM (like CBT), PIM-DM (use flooding to forward data)

Joining a mcast group: two-step process: local: host informs local mcast router of desire to join group (IGMP); wide area: local router interacts with other routers to receive mcast datagram flow.

QoS for networked applications: packet classification + isolation scheduling and Policing + high resource utilization + call admission + queuing delay + loss due to input buffer overflow