1. [ch1]**Protocols define format**, order of msgs sent and received among network entities, and actions taken on msg transmission & receipt
2. **Circuit switching**: end-end resources reserved for 'call', dedicated resources: no sharing, in the exchange of the constant speed, call setup required
3. **Packet switching**: each end-end data stream divided into packets, share network resources, each packet uses full link bandwidth; no link setup; Resource contention: aggregate resource demand can exceed amount available, no admission control, congestion, store and forward -- ex. STDM(bandwidth shared on demand)
4. **PSvsCS**: PS allows mores users, great for burst data. How to provide circuit-like behavior? Virtual circuit
5. **Four sources of packet delay**: nodal processing (check bit errors), queuing, transmission delay (store-and-forward delay, packet length/link bandwidth), propagation delay

1. **[ch2]Two main network-layer function: forwarding: move packets from router's input to appropriate router output (IP protocol), routing: determine route taken by packets from source to dest (routing alg.)**
2. **Internet**: only elastic, connectionless, try best datagram service is supported (no call setup)
3. 32bit IP (network layer and above) → Address Resolution Protocol (ARP) → 48bit MAC (physical, link layer)
4. **ARP: broadcast APR query packet first, target-host replies to src-host with its MAC address, src-host caches/saves IP-to-MAC address pair in its ARP table until info. becomes old (times out) (ARP is p&p)**
5. **Subnetting**: every part has equal capacity, CIDR: every part may have diff. capacity
6. **How does a host get IP address?** static configuration: hard-coded by system admin in a file; dynamic: DHCP
7. **ICMP**: Internet Control Message Protocol – used by hosts & routers to communicate network-level information; network-layer above IP
8. **Technologies & efforts to slow the consumption rate**: Dail-access / PPP /DHCP, strict allocation policies, CIDR, NAT
9. **Summary of main IPv6 benefits**: larger addresses (128bit), extended address hierarchy, flexible header format, improved options, provision for protocol extension, support for auto-configuration and renumbering, support for resource allocation (extension headers are generally processed only by the final destination, and neglected by the intermediate routers, fragmentation is end-to-end)
10. **Transition from IPv4 to IPv6**: dual-stack techniques (to allow IPv4 and IPv6 to co-exist in the same devices and networks), tunneling techniques (IPv6 carries as payload in IPv4 datagram among IPv4 routers) , translation techniques (to allow IPv6-only devices to communicate with IPv4-only devices)

1. [ch3]**Two key router functions**: run routing algorithms/protocol (RIP\OSPF\BGP), forwarding datagrams from incoming to outgoing link; Two core parts: switching fabric (is a network inside a router, connecting input ports to output ports), routing processor (executes routing protocols, maintains routing tables, and performs network management functions)
2. **switch**: link-layer device; store, forward Ethernet frames, uses CSMA/CD to get segment, transparent (hosts are unaware of presence of switches), p&p, self-learning(switch do not need to be configured); allows multiple simultaneous transmissions.
3. **switch & routers:** both store-and-forward devices, both maintain tables, network topologies (switch: only spanning tree in order to prevent the cycling of broadcast storm, switch do not offer any protection against broadcast storm, router: support firewall, rich topology)
4. **bridges**: switch is a multi-port bridge; can only connect two LAN segments, perform forwarding in software, traffic isolation(filter packets & separate collision domains)
5. **Multiprotocol Label Switching (MPLS)**: control-driven model, run over any link-layer technology, QoS of connection-oriented, traffic engineering, support VPN. Advantages: **lower cost (allow share network resources), QoS, Scalability (allow auto-configuration), traffic routing**

1. [ch4]Process-to-Process (Transport layer) is supported by **multiplexing** (send host: gathering data from multiple sockets, enveloping data with header) **/demultiplxing**(rcv host: delivering received segments to correct socket)
2. **TCP**: 'handshake' before starts to send app data; reliable, in-order delivery, congestion control, flow control (sender will not overwhelm receiver), connection setup, integrity checking, point-to-point, pipelined (TCP congestion and flow control set window size), send & receive buffers (SMTP:25, HTTP:80, FTP:21, Telnet:23)
3. **UDP**: unreliable, no-handshake, unordered delivery, process-to-process data delivery and error checking, 'best effort' service, no connection establishment, simple, small segment header, no congestion control, often used for streaming multimedia apps (DNS, SNMP)
4. **Reliable data transfer (rdt)**: ack, retransmission timeout, sliding window; stop-and-wait →pipelined protocols(go-back-n, selective repeat)
5. **TCP [flow control]: sender won't overflow receiver's buffer by transmitting too much, too fast, point to point communication; [Congestion control]: focus on the whole network, preventing the source from sending data that will end up getting dropped by a router, complicated(causes: retransmissions of packets still in flight, undelivered packets, fragments, control traffic, unwanted packets) global solution: additive increase, multiplicative decrease**
6. **Tcp can buffer out-of-order segments(like SR), tcp sender need only maintain smallest seq# of a transmitted but unacknowledged byte and the seq# of next byte to be sent(like GBN), it's hybrid between GBN&SR**

1. [ch5]**Multimedia**: (delay sensitive, loss tolerant) use UDP, client-side adaptive playout delay to compensate for delay, server side matches stream bandwidth to available client-to-server path bandwidth; error recovery, CDN.
2. **Principles of QoS**: packet marking/classification; isolation for one class from others; improve the efficiency of resource; call admission (declare its need, network may block call if it cannot meet needs)
3. **Best-effort-serv: no QoS, simple, all packets are equal at the router, no special treatment for any delay-sensitive multimedia applications**
4. **Differentiated Services (Diff-Serv): aims to handle different classes of traffic in a scalable and flexible manner, simple functions in network core, relatively complex functions at edge routers; Per-Hop Behavior (PHB) result in a different observable forwarding performance behavior**
5. **Integrated Services (Int-Serv): provide individualize QoS guarantees to individual app; reserved resources; call setup/call admission**

1.Hitstory: 1961-1972: Early packet-switching principle 1980-1990: new protocols (smtp, dns, tcp/ip, ftp, tcp, congestion control), a proliferation of network 1990-2000 commercialization, the web, new apps (html, http)
2.Transition from IPv4 to IPv6: dual-stack techniques (to allow IPv4 and IPv 6 to co-exist in the same devices and networks), tunneling techniques (IPv6 carries as payload in IPv4 datagram among IPv4 routers), translation techniques (to allow IPv6-only devices to communicate with IPv4-only device)
3.A: 1.0.0.0. to 127.0.0.0 B: 128.0.0.0 to 191.255.0.0 C: 192.0.0.0 to 233.255.255.0 D: 244.0.0.0 to 239.255.255.255 E:240.0.0.0 to 255.255.255.254

1. **[ch6]Link-state alg: use Dijkstra's alg. to find shortest path (one to all), each node broadcast its info (only the cost between its neighbors) to all, link costs known to all nodes, all gateways have the same LS map, global routing alg.**
2. **Distance-Vector alg: Bellman-Ford, each node only exchange info (shortest paths to all) with its neighbors, good news traverse fast, bad news travels slowly.**
3. **Routing Information Protocol (RIP): distance vector algorithm, criterion of routing: # of hops, exchanged among neighbors every 30 sec via Response Message (also called advertisement), max-distance: 15 hops (16 == infinite), RIP is not very secure, only suitable for small networks, slow to adjust for link failure.**
4. **Open Shortest Path First (OSPF): use link state algorithm, criterion of routing: bandwidth & delay, dvertisements disseminated to entire AS (via flooding), use flooding to send msgs, use IP (not UDP) directly to transmit IP datagrams**

1. [ch7]**AS**: a network under a single-administrative control with a single routing protocol
2. **Border Gateway Protocol (BGP):** a fairly simple protocol, but not easy to configure
3. **Reasons of Pakistan Youtube incident: misconfigurations of iBGP, Pakistan Telecome routed the address block of youtube's servers into a "black hole", packets would flow towards Pakistan telecom because of longest match first rule.**

1. [ch8]With a VPN, institution's inter-office traffic is sent over public Internet instead; IPv4: 10.0.0.0 / 172.16.0.0 – 172.31.255.255 / 192.168.0.0; IPv6: FEC0::0/10; access the network from remote locations, secured networks, Internet is used as the backbone for VPNs, save costs, scalability.
2. **VPN protocols**: 2 tunneling layer: PPTP, L2F, L2TP; 3TL: GRE, IPsec, MPLS; 3 most common: pptp, l2tp, ipsec (here tunneling refers to: the encapsulation of packets inside packets of a diff. protocol to create and maintain the virtual circuit)
3. **Future: MPLS VPN will be the main stream, and the combination of IPsec VPN and MPLS VPN will be preferred by most ISPs; The powerful transmission capacity of public backbone network can be fully used by MPLS, also it can save cost for companies, and improve the efficiency of network management.**

1. [ch9]application: bulk data transfer, streaming continuous, shared data applications, data feeds, web cache updating, interactive gaming; Group address: unique class D address. Host uses Internet Group Management Protocol(IGMP) to announce participation in multicast.
2. 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.
3. 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)
4. Techniques to control multicast scope: IP's TTL field, Administrative scoping.

问答题： **1.PoPs, multi-homing, peering, IXPs**. Pops: point-of-presence is the physical location where two or more different networks or communication devices establish a connection with each other. Multi-homing: It means that an organization (include ISP) has multiple points of connection to the internet. Peering: It is the arrangement of traffic exchange between ip. IXPs: An internet exchange point(IXP) is a physical infrastructure where different IP networks meet to exchange local traffic with each other via switches.
2.Why doesn't a packet just keep the same VC number on each of the links along its route? Replacing the number from link to link to reduce the length of the VC field. Permitting different VC number for each link along the path of the VC to simplified a network management function.
3.Comparison between RIP and OSPF? RIP: A distance vector protocol which advertises network updates periodically. The advertisements are sent every 30 seconds, and it too late to update when a change in network happens. RIP, the 16th hop is considered unreachable. So, RIP can be used efficiently in small networks only. OSPF maintains routing table, neighbor table, database table. To select best path, it uses Dijkstra's Shortest Path First algorithm. OSPF select a DR and BDR for a network. Similarity: RIP and OSPF are routing protocols used to advertise about routes in a network. They are both used as Interior Gateway Protocols(IGP), which are configure inside an autonomous system. Both RIP and OSPF are open standard industry protocols which can also be used with non-Cisco devices like Juniper. RIP and OSPF use Hello message to find about routes and establish neighbor.
4.Brief introduction about VPN? VPN extends a private network across a public network, encryption the data when transmitting. Virtual point-to-point connection.
5.Is TCP a GBN or an SR protocol? TCP sender need only maintain the smallest sequence number of a transmitted but unacknowledged byte and the sequence number of the new byte to be sent. So, TCP looks like GBN-style protocol. But there are some striking differences between TCP and GBN. 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. When combined with selective recovery mechanism is probably best categorized as a hybrid of GBN and SR protocols.
6.Flow control and congestion control. Flow control: Eliminating the possibility that the sender overflows receiver's buffer by transmitting too much and too fast. A point-to-point control. Congestion control: Preventing too much data from being injected into the network, causing switch or links to become overloaded. Involves every router and host. Both adjust senders' sending rate. But-flow control: point-to-point control. Congestion control: global control.
7.Why are there different intra- and inter-AS routing? Intra-AS Routing: refers to routing within the Autonomous Systems, where live RIP and OSPF, no policy decisions needed focus on performance. Inter-AS routing: ISPs are divided into hierarchical levels. Admin wants control over how its traffic is routed, and who routes through its net, policy may dominate over performance.
8.Where does queuing occur in a router? Output port: Buffering required when datagrams arrive from fabric faster than the transmission rate. Scheduling discipline choose among queued datagrams for transmission Input port: queuing: if datagrams arrive faster than forwarding rate into switch fabric. Given datagram dest, lookup output port using local copies of the forwarding table in input port memory(decision made locally at each input port)
9.IGMP-Joining a group two-step process. Example: 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

10.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.

PhiloSophia2017

1. 冷土豆热土豆: In commercial network routing between autonomous systems which are interconnected in multiple locations, hot-potato routing is the practice of passing traffic off to another autonomous system as quickly as possible, thus using their network for wide-area transit. Hot potato is to get rid of traffic as soon as possible and to minimize the amount of works thus resulting in lower QoS. Cold-potato routing is the opposite, where the originating autonomous system holds onto the packet until it is as near to the destination as possible. Cold-potato routing is more expensive to do and requires a level of trust between two networks that either side will not attempt to "cheat" the other.
2. Most common VPN protocols:1.PPTP(point to point tunneling protocol)2. L2TP 3. IPSES
3. MPLS-based application: 1. Traffic engineering 2.COS 3.VPNS
4. In computer networking, the maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction. Fixed MTU parameters usually appear in association with a communications interface or standard. Some systems may decide MTU at connect time. The MTU relates to, but is not identical with the maximum frame size that can be transported on the data link layer, e.g. Ethernet frame.
5. Jitter：Jitter is defined as a variation in the delay of received packets. The sending side transmits packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant, as shown in the figure.
6. LS和DV比较(1)distance vector routing protocol to send routing information to neighbors (2) distance vector routing protocol regularly updated routing information (3) distance vector routing protocol will be all local routing information as update information (4) link state routing protocol to the entire network Diffusion link state information (5) link state routing protocol changes immediately when the network structure to send updated information (6) link state routing protocol to send only the need to update the information.
7. 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.
8. 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.
9. 流量控制拥塞控制区别：Congestion control is to allow the network to withstand the existing network load, it is a global process, involving all the hosts and routers, and to reduce network transmission of all the factors. On the contrary, flow control often refers to the point-to-point traffic control, that is, the receiving side controls the sending side. All it has to do is to restrain the sending rate of sending side to make the receiving side can receive the data.
10. 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.
11. 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.
12. SLA: A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.
13. CDNS: CDN is short for content delivery network. A content delivery network (CDN) is a system of distributed servers (network) that deliver pages and other Web content to a user, based on the geographic locations of the user, the origin of the webpage and the content delivery server. How CDN works? 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.
14. VC number: 1. 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.
15. Advantages of IPv6 over IPv4:1 No more NAT (Network Address Translation) 2Auto-configuration 3No more private address collisions 4Better multicast routing 5Simpler header format 6Simplified, more efficient routing 7True quality of service (QoS), also called "flow labeling" 8Built-in authentication and privacy support Flexible 9options and extensions 10Easier administration (say good-bye to DHCP)
16. MPLS: 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.
18. Multicast(act of sending datagram to multiple receivers with single “transmit” operation) 3-layer ->routers 5-layers ->end systems. Multicast Scope: 1.IP’s TTL field (TTL>1: multicast routers attached to the local network forward IP Multicast datagrams; TTL=1 local only; TTL=0 only inter process locally) 2.Administrative scoping
19. IGMP (Internet Group Management Protocol) to 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)

AIMD Additive Increase, Multiplicative Decrease ; approach: increase transmission rate (window size), probing for usable bandwidth, until loss occurs
Anycast Destination is a set of computers, possibly at different location, that all share a single address. Delivery to exactly one member in the set (often the closest member
ARP Address Resolution Protocol
AS autonomous systems
ATM asynchronous transfer mode
BGP Policy based Gateway Protocol
Cable modems cable TV infrastructure
CDNs content distribution networks; placing content “close” to user avoids impairments (loss, delay) of sending content over long paths
CIDR Classless Inter-Domain Routing
circuit switching end-end resources reserved for "call"
Congestion too many sources sending too much data too fast for network to handle
CSMA/CD Carrier Sense Multiple Access / Collision Detection
cwnd congestion window
Demultiplexing at rcv host delivering received segments to correct socket
Dial-up modem telephony infrastructure
Dijkstra-->a Dutch computer scientist
DSL Digital subscriber line, using telephone infrastructure
DSLAM DSL access modem
dual-stack to allow IPv4 and IPv6 to co-exist in the same devices and networks
eBGP external BGP
EGP Exterior Gateway Protocol
fast retransmit resend segment before timer expires
FDM Frequency-Division Multiplexing
flow control sender won’t overflow receiver’s buffer by transmitting too much, too fast
FTTH fiber to the home
Go-Back-N sliding window protocol
GRE Generic Routing Encapsulation
HFC hybrid fiber coax
HOL blocking Head-of-the-line
iBGP internal BGP
ICANN Internet Corporation for Assigned Names and Numbers
ICMP Internet Control Message Protocol
IETF internet engineering task force
IGMP Internet Group Management Protocol
IGMP Internet Group Management Protocol
IGP Interior Gateway Protocols
IGP Interior Gateway Protocol
IGRP Interior Gateway Routing Protocol
Internet 10000km +
Internet Draft (ID) not finalized not stable
Internet protocol stack application,transport,network,link,physical
IP internet protocol
IXP Internet eXchange Point
IXPs internet exchange points
LAN local area network 10 - 1km
Layers each layer implements a service

QoS for networked applications packet classification; isolation scheduling and policing; high resource utilization; call admission
queuing delay and loss due to input buffer overflow
RARP Reverse Address Resolution Protocol
RED Random early detection
RFC request for comments; never change once published (not all RFCs are standards)
RIP Routing Information Protocol
routing algorithm algorithm that finds least-cost path
RPM Reverse Path Multicasting
RSVP ReSource reserVation Protocol
SDH Synchronous Digital Hierarchy
SLA Service Level Agreement; An SLA is a formal negotiated agreement
SPT Shortest Path Tree
SR Selective Repeat
SSL Secure Sockets Layer
subnet "device interfaces with same subnet part of IP address can physically reach each other without intervening router"
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
switches vs bridges main difference: number of network segments, bridge 1-1, switch 1-N; switches perform in hardware, bridges perform in software
switches vs routers Both store-and-forward devices; Both maintain tables; topology: switch--> a spanning tree, routers--> a rich topology
TCP (20 bytes fixed length header) Transmission Control Protocol, reliable, in-order delivery
TCP Congestion Control AIMD; slow start; conservative after timeout events

link MTU a link’s maximum transmission unit, i.e., the max IP packet size that can be transmitted over the link
LTE long term evolution
MAC Media Access Control -->get frame from one interface to another physically-connected interface (same network)
MAN metropolitan area network 1km - 100km
MPLS Multiprotocol Label Switching
MPLS Applications Traffic Engineering, Class of Service (CoS), Virtual Private Networks (VPNs)
MTU maximum transmission unit
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
multi-homed hosts A conventional computer that has two or more physical network connections
Multiplexing at send host gathering data from multiple sockets, enveloping data with header
NAS Network Access Servers
NAT Network Address Translation
NAT network address translator
network core interconnected routers network of networks
network edge applications and hosts
network-layer two key function forwarding, routing
OSI reference model presentation(interpret meaning of data), session(synchronization, checkpointing, recovery of data exchange)
OSPF Open Shortest Path First
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
packet switch categorized into datagram networks and virtual circuit networks
packet switching each end-end data stream divided into packets
PAN personal area network 1-10m
path MTU the minimum MTU of all the links in a path between a source and a destination
PD packetization delay
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
PIM Protocol Independent Multicast
Pipelining buffering at sender and/or receiver; error recovery protocols: go-Back-N, selective repeat
PoPs points of presence
protocols protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission & receipt
QoS quality of service
TCP Connection Management "Three way handshake: Step 1: client host sends TCP SYN segment to server; Step 2: server host receives SYN, replies with SYNACK segment
Step 3: client receives SYNACK, replies with ACK segment, which may contain data"
TCP socket identified by 4-tuple source IP address, src port number, dest IP address, dest port number
TDM Time-Division Multiplexing
TDM channels are called time slots
Three approaches to supporting MM appbest-effort service; differential QoS; guaranteed QoS
Three basic IPv6 address tyoes unicast, anycast, multicast
Three types of switching fabrics memory, bus, crossbar
throughput rate (bits/time unit) at which bits transferred between sender/receiver
TP twisted pair
translation to allow IPv6-only devices to communicate with IPv4-only devices
transport layer send side= messages -> segments; receive side= segments -> messages
transport vs network layer network layer: logical communication between hosts; transport :between processes
tunneling IPv6 carried as payload in IPv4 datagram among IPv4 routers
two fundamental approaches to transfer data circuit switching, packet-swirching
UDP (8 bytes segment header) User Datagram Protocol, unreliable, unordered delivery, data delivery, error checking
UDP socket identified by two-tuple dest IP address, dest port number
unicast destination address specifies a single computer, delivery to single interface
VC virtual circuit
VC implementation a vc consists of path, VC numbers, entries in forwarding tables
VPN Virtual Private Networks
WAN wide area network 100km - 1000km
WDM channels are called wavelengths
wider-area wireless access WIMAX
WIFI wireless lans
WiMAX Wireless Interoperability for Microwave Access

PhilSophia2017