(working layer: traffic isolation, plug&play, optimal routing: hubs (physical, no, y, n) switch (link, y, y, n) bridge (link, y, y, n) router (network, y, n, y)

yes)

3. **DDos attacks are much harder to detect**
①hard to be monitored or tracked, attackers hide themselves well ②based on legal packets that can't be monitored effectively. Firewall spends high-intensive check to prevent attacks, so massive amount of data in DDoS attack leading to its performance sliding down ③systems optimization and increasing bandwidth cost lot, but escalation of the DDoS attack costs much less.

4. **The status quo of FTTx deployment**
By May 2016, the coverage rate of FTTH in China is nearly 90%. Some provinces (Tianjin, Jiangsu) almost cover 100% of homes. FTTH users weighs 66.4% of all users connecting to the Internet.

5. **Not keep the same VC number on each of the links**
①replacing the number from link to link reduces the length of VC field in the packet header ②VC setup is considerably simplified by permitting a different number at each link along the path of the VC, because each link can choose a VC number independently and common VC number costs a lot.

6. **benefits of IPv6 when compared with IPv4**
①more addresses ②improved Security, IPv4: not designed with security, IPv6: IPSEC is built into the IPv6 protocol, usable with a suitable key infrastructure ③easier and cheaper to mange, IPv4: must be configured manually or with DHCP, demand increasing maintenance efforts, IPv6: provide auto-configuration capabilities ④end-to-end transparency, IPv4: NAT devices make end-to-end integrity unachievable, IPv6: the need for NAT devices is effectively eliminated, making direct addressing possible

7. **Private addresses in IPv6**
①Site-local address: Unique in a site, like private address of IPv4, begin with "1111 1110 11" ["FEC", "FED", "FEE" or "FEF"]
②Link-local address: Unique in a link, specify an interface to reduce ambiguity in a node, used only for special purpose, e.g. exchanging msg among nodes within a network segment, begin with "1111 1110 10" ["FE8", "FE9", "FEA" or "FEB"]

8. **Where does queuing occur in a router**
Router = Input ports + Switch fabric + Output ports + Routing processor
Location: input ports (switch fabric < input line) and output ports (switch fabric > output line).
Cause: the relative speed of the switching fabric and the line speed.

9. **MPLS (multiprotocol label switching) Operation**
①MPLS works by prefixing packets with an MPLS header, containing one or more labels. This is called a label stack. These MPLS-labelled packets are switched after a label lookup/switch instead of a lookup into the IP table. ②When an LSR (label switch router) receives a packet, it uses the label included in the packet header as an index to determine the next hop on the LSP (label switched path) and a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is routed forward. ③When forwarding an IP datagram into the MPLS domain, an LER (label edge router) uses routing information to determine the appropriate label to be affixed, labels the packet accordingly, and then forwards the labelled packet into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using normal IP forwarding rules.

10. **Describe the status quo of MPLS applications**
MPLS is currently in use in IP-only networks. It is deployed to connect as few as two facilities to very large deployments. In practice, MPLS is mainly used to forward IP protocol data units (PDUs) and Virtual Private LAN Service (VPLS) Ethernet traffic. Major applications of MPLS are telecommunications traffic engineering, and MPLS VPN.

11. **Brief description about current Internet Architecture**
①IP over ATM (Asynchronous Transfer Mode): multi-service telecommunication environment, high QoS (Quality of Service), need complex management, not suitable for large IP network.
②IP over SDH (Synchronous Optical Network): high bandwidth utilization, high degree of standardization, the routing information occupies a large amount of bandwidth.
③IP over WDM (Wavelength Division Multiplexing): directly optical transmission, high capacity IP service, large-scale backbone network.

12. **Find present routers for access networks, regional networks and WAN**
Two key router functions: ①run routing algorithms/protocol (RIP, OSPF, BGP) ②forwarding datagrams from incoming to outgoing link

13. **Working process of a load balancer in data center**
①load balancer receives a request for a particular application and forwards it to one of the hosts that handles the application (a host may then invoke the services of other hosts that handles the application) ②host finishes processing the request and sends its response back to the load balancer ③load balancer sends its response back to the external client.

14. **Limited host-to-host capacity problem and solutions in data center**
Problem: Suppose each host connects to its TOR switch with 1 Gbps link rate, but the links between switches are 10 Gbps rate. If there are many flows between different racks at the same time, the maximum rate for two hosts may be less than 1 Gbps because sharing 10 Gbps link. Solution: ①Deploy higher-rate switches and routers ②Deploy new interconnection architectures and network protocols, e.g., a fully connected topology.

15. **Trends in data center networking.**
①deploy new interconnection architectures and network protocols ②employ shipping container–based modular data centers (MDCs)

16. **Is TCP a GBN or an SR protocol?**
[U4_Pipelining Protocols (GBN+SR)]+[U4_TCP_Fast retransmit]
GBN-style: TCP sender need only maintain SendBase and NextSeqNum, SR-style: receiver will buffer correctly received but out-of-order segments, the retransmission mechanism of TCP is probably best categorized as a hybrid of GBN and SR protocols.

17. **Compare flow control and congestion control**
(Application Scope, Function, Mechanisms, Algorithm) **flow control:** ①end to end ②control the traffic between a sender and a receiver ③handle the transmission between a sender and a receiver ④slide window **congestion control:** ①entire network ②control congestion in the network; prevent loss of packets and delay ③make sure the entire work can handle the traffic that is coming to the network ④slow start, congestion avoidance, fast retransmit, fast recovery

18. **Discuss the fairness problem of TCP**
[U4_TCP congestion control fairness]

19. **Describe the details of TCP congestion control**
[U4_TCP congestion control]

20. **TCP Global Synchronization [+U4_TCP congestion control]**
phenomenon: the network traffic suddenly dropped a lot, and in the network back to normal after the sudden increase in its traffic a lot
reason ①tail drop ②limited sources

resources of routers -> many TCP connections go into slow-start at the same time
solution: ①starts randomly dropping packets before actual congestion occurs (random early detection (RED)).

21. **Compare best-effort service, DiffServ and IntServ**
①Best Effort service model is a single service model and the simplest service model. It can be realized through the FIFO queue. The network under this model try its best to send the message. But it does not provide any guarantee for the performance like time delay, reliability, performance, and etc. ②IntServ is an integrated service model which can satisfy various QoS requirements, using the resource reservation protocol (RSVP). RSVP runs on devices from source to the destination so that it can monitor each flow to prevent the excessive resources consumption. This system can make a clear distinction of the service quality among traffic flows, and provide the most fine granular for network service quality. However, IntServ model has a high requirement on the equipment. When a high number of data flow transferred on the network, equipment storage and processing power will encounter a lot of pressure. IntServ model has a poor extensibility and it difficult for IntServ to be implemented in the core network. ③DiffServ is a multiple service model that can meet different QoS requirements. Unlike IntServ, it does not need to notify the network to reserve resources for each business. It is easy for DiffServ model to distinguish service with a good expansibility.

22. **VoIP (Voice over Internet protocol)**
a methodology and group of technologies for the delivery of voice communications and multimedia sessions over IP networks
receiver->analog-digital converter->compression encoder->IP encapsulation->IP packet-switched network->IP decapsulation->compression decoder->digital-analog converter->player

23. **CDN (Content Distribution Networks)**
Definition: a globally distributed network of proxy servers deployed in multiple data centers
Goal: manages servers in multiple geographically distributed locations, stores copies of Web content in its servers, and attempts to direct each user request to a CDN location that will provide the best user experience.
Operation: Most CDNs take advantage of DNS to intercept and redirect requests.
Cluster selection strategies: Geographically/Real-time measurements/IP anycast

24. **RSVP (Resource Reservation Protocol)**
Role: ①rides on top of unicast/multicast routing protocols ②must be present at senders, receivers, and routers ③carries resource requests all the way through the network ④at each hop consults admission control and sets up reservation, informs requester if failure **Design goal:** ①accommodate heterogeneous receivers (different bandwidth along paths) ②accommodate different applications with different resource requirements ③make multicast a first class service, with adaptation to multicast group membership ④ leverage existing multicast/unicast routing, with adaptation to changes in underlying unicast, multicast routes ⑤control protocol overhead to grow (at worst) linear in # receivers ⑥modular design for heterogeneous underlying technologies.

25. **Token bucket / leaky bucket**
Leaky bucket: limit the transmission rate
Token bucket: limit the average transmission rate, it can allow a certain degree of burst transmission. For token bucket algorithm, if there is any token in the bucket, user can send data.

26. **Comparison DV & LS**
(Based on, input, requirement, advantages) **DV:** ①The Bellman–Ford algorithm ②Its immediate neighbors, and the direct cost involved in reaching them ③A router knows from which neighbor a route was learned ④Requires less overhead **LS:** ①A standard shortest paths algorithm such as Dijkstra's algorithm ②A graphical map of the network ③All routers know about the paths reachable by all other routers in the network ④Provide more robust operation and scalability

27. **Comparison RIP & OSPF**
(Core algorithm, link state exchange, hop limitation, broadcast time, message layer, response to change, hierarchy, security) **RIP:** DV, between neighbors, 15, every 30s, TCP/UDP, slow, no, no **OSPF:** LS, among area, infinite, when link change, IP, fast, yes, yes

28. **LS algorithm oscillations**
with congestion-sensitive routing, link cost equal to amount of carried traffic, link A and Link 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.

29. **Count-to-infinity 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 can definitely occur when a link is removed.

30. **Poisoned reverse**
If router B receives a route poisoning of network 4 from router C, then router B will send an update back to router C with the same poisoned hop count of 16. This ensures all the routers in the domain receive the poisoned route update.

31. **RIP disadvantages**
①The hop count cannot exceed 15 ②Increased network traffic ③Converges slowly ④Closest may not be fastest, e.g., a path with hop count 3 crossing three Ethernets may be much faster than a path with hop count 2 crossing two satellite connections ⑤Not very secure, because only support generic notion of authentication and only "password" is defined ⑥Prone to routing loops ⑦Variable Length Subnet Masks are not supported (for RIP version1)

32. **BGP incidents**
BGP hijacks where an attacker cleverly misused the Bitcoin stratum protocol. By hijacking IP addresses of the pool server IP addresses, the attacker stole 83,000 dollars worth of Bitcoins. BGP hijacks happen on an almost daily basis, some are targeted while many are operational errors. Many of the incidents affect one or a few prefixes at a time.

33. **Why are there different Intra- and Inter-AS routing?**
Inter-AS: ①admin wants control over how its traffic routed, who routes through its net ②can focus on performance **Intra-AS:** ①single admin, so no policy decisions needed ②policy may dominate over performance hierarchical routing saves table size, reduced update traffic

34. **Describe your understanding about peering and transit.**
Peering: ①the business relationship that two companies (ISPs) provide access to each others` customers in win-win situation ②provides connectivity to a provider's customer destinations ③settlement-free, cost efficient ④Traffic optimization and low latency ⑤Improved end-user experience ⑥Scalability and redundancy ⑦Community and marking **Transit:** ①no network connect directly ②transit providers receive a "transit fee " ③the business relationship whereby an ISP provides (usually sells) access to the global Internet
④ Predictable usage experience

global internet ④Predictable usage experience ⑤Contracts have a specific term

35. **Hot potato routing**
①hand over traffic at the earliest convenience ②minimize the amount of work ③the closest egress point ④for service provider (prefer to keep traffic)

36. **Cold potato routing**
①hold onto traffic as long as you can before handing it over to another network ②maximize the control on the end-to-end quality of service ③the closest actual destination point ④for content delivery network

37. **SSL / TLS**
SSL/TLS and eg-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 Transport Layer protocols. Sometimes referred to as web VPNs or clientless VPNs because no special client software is required other than a web browser. Functionality can be added by installing SSL VPN client software on remote access client devices! Can help internet application software to enhance integrity of data communication and security (SSL web site).

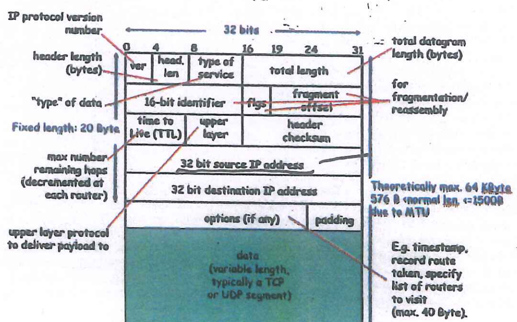
38. **Ipsec.**
Protect IP traffic between security gateways or hosts as it transits an intervening network. Has two different packet forms: tunnel mode (being more appropriate for VPNs) & transport mode (widely deployed).

39. **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.

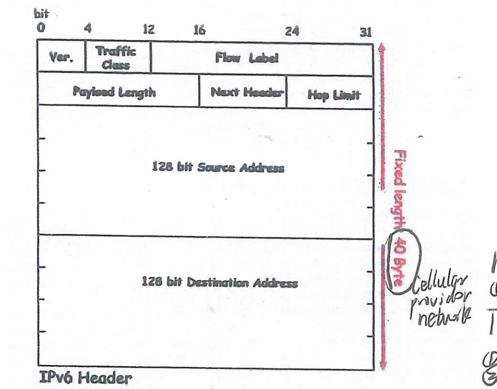
40. **GRE.**
Definition: a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network
Features: ①It is a standard protocol ②support multiprotocol and multicast ③support multipoint tunnel ④provide quality of service
Disadvantages: ①Lack of encryption ②no standard control protocol to keep tunnel (usually use keep alive) ③tunnel consumes many CPU resources ④hard to debug when problem occurs

41. **PPTP.**
Definition: PPTP is a layer 2 protocol that encapsulates PPP frames in IP datagrams for transmission over an IP internetwork.
Advantages: ①lower transmission cost ②lower hardware cost ③lower administrative overhead ④enhanced security

- **IPv4 structure**



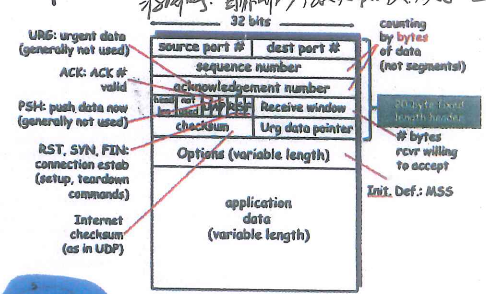
- **IPv6 structure**

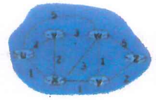


IPv6 Header
40 octets, 8 fields
+ Unlimited Chained Extension (options) Header

TCP

UDP 4个16位(2字节)
源端口, 目标端口, 数据报长度, 校验值

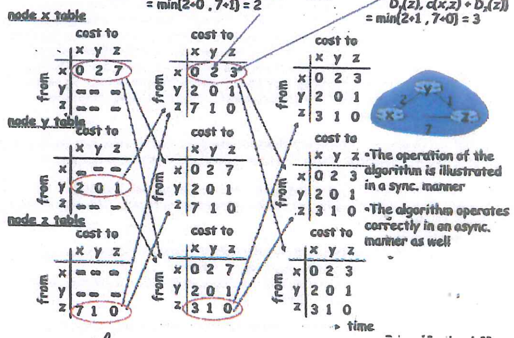




Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\} = \min\{2+0, 7+1\} = 2$

$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\} = \min\{2+1, 7+0\} = 3$



- The operation of the algorithm is illustrated in a sync. manner
- The algorithm operates correctly in an async. manner as well

msdf

- application layer—message
- transport layer—segment

link-layer: Stop-and-wait

handling mobility in cellular networks
cellular provider network
① home network (Home location Register HLR) ② visited network (VLR)
mobile currently reside

Characteristics of Mobile IP
① Transparent to applications and transport protocols
② Interoperates with standard IPv4 ③ secure
④ Scales to large Internet ⑤ Macro mobility

- GSM (Global system for mobile communication)
combined FDMA/TDMA
- IS-95 CDMA: code division multiple access

mobility: ① ~~routing~~ handle it ② end system handle it
② ① indirect routing ② ② direct routing