Exam2 Review

CS 326E Elements of Networking

Mikyung Han

mhan@cs.utexas.edu

Exam format

- Exam will be cumulative by nature
- 3 hours
- Similar format as Exam 1
  - Probably shorter tho ☺
- 2 double-sided 8.5x11in cheat sheets allowed
  - Either handwritten or typed ok
- No electronic devices allowed including the calculator
- Review all EXs, in-class EXs, Hands-on Assignments
- Panopto videos and async lecture videos

Everything in Exam 1

Refer to the Exam 1 Review Slides in the Course Calendar

Transport Layer

- RDT
- UDP
- TCP
- TCP Congestion Control

Network Layer

- Router, subnet, IPv4
- NAT
- IPv6
- SDN & GF
- OSPF and BGP
- ICMP: ping and traceroute
- Specific routing algorithms will NOT be on the exam

Link Layer

- MAC
- ARP
- Ethernet Switch

Network Security

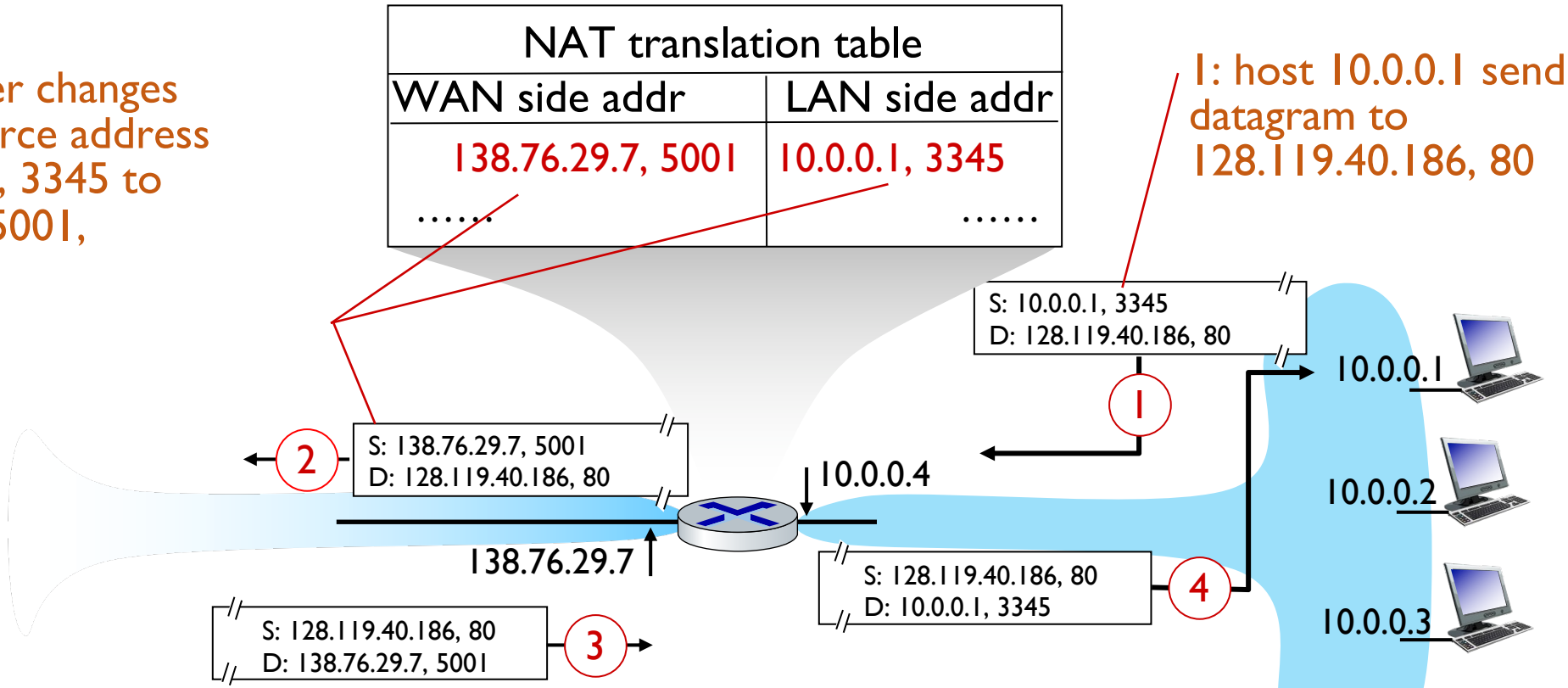
- All about Tor
- Encryption
  - Symmetric encryption
  - Asymmetric encryption (PKI)
- Diffie Hellman Key exchange
- Digital signature
- Digital certificate
- Authentication
- Message Integrity
- TLS handshake

Network Security

- All about Tor
  - Ho
- Encryption
  - Symmetric encryption
  - Asymmetric encryption (PKI)
- Diffie Hellman Key exchange
- Digital signature
- Digital certificate
- Authentication
- Message Integrity
- TLS handshake

NAT: network address translation

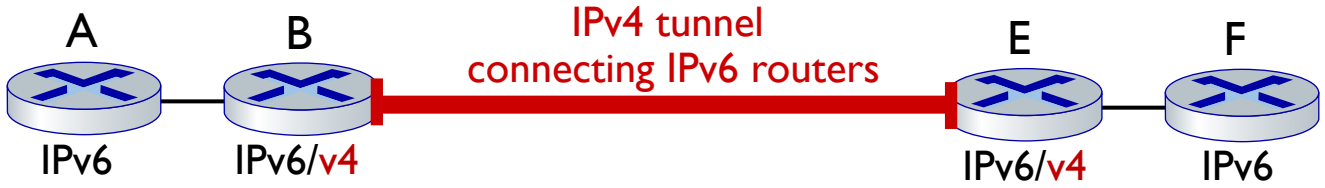
2: NAT router changes datagram source address from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table



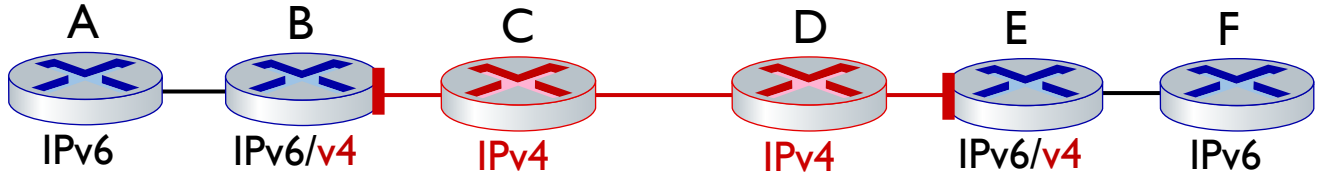
3: reply arrives, destination address: 138.76.29.7, 5001

IPv6 Tunneling

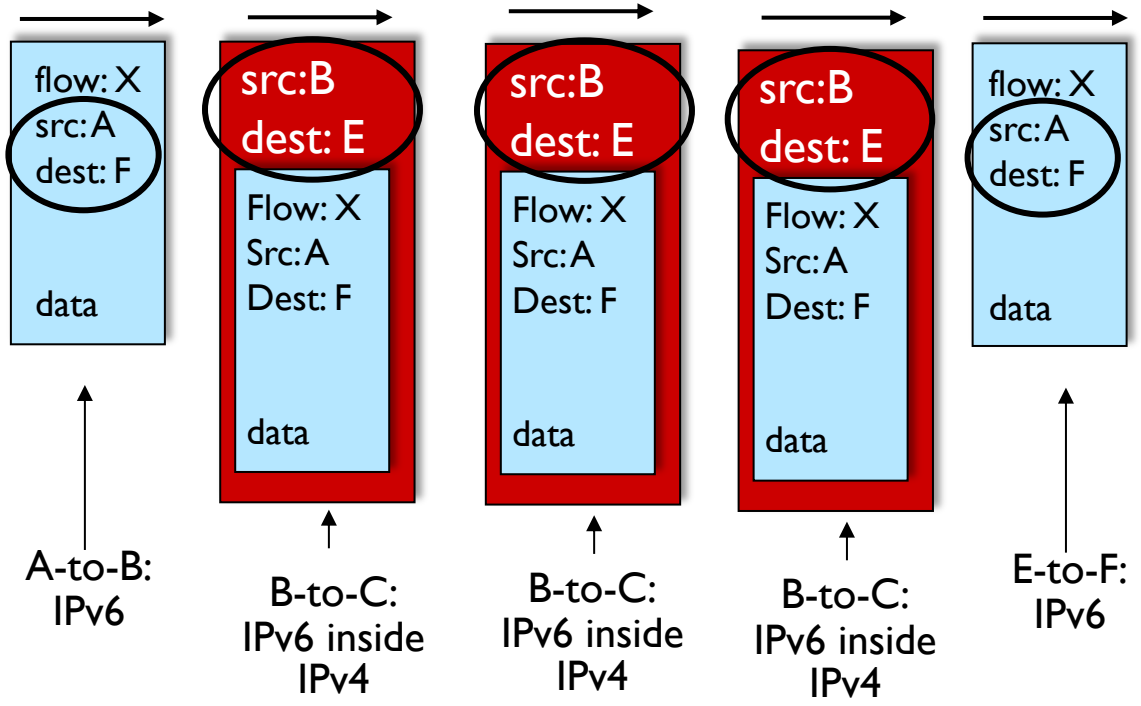
logical view:



physical view:



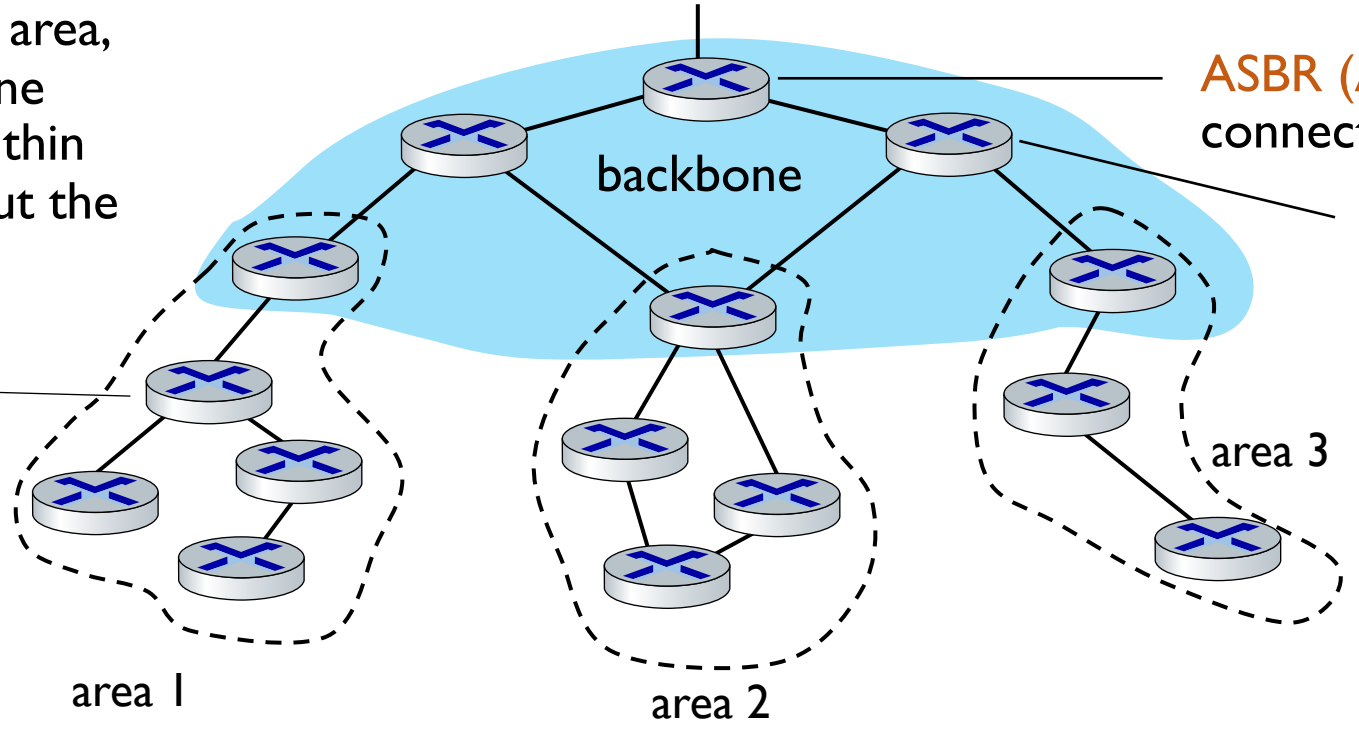
Note source and destination addresses!



Hierarchical OSPF to solve scalability

ABR (Area Border router):
- "summarize" distances to destinations in own area, advertise in backbone
- Also lets routers within one area know about the other area

Local router:
- flood LS in area only
- compute routing within area
- forward packets to outside via area border router

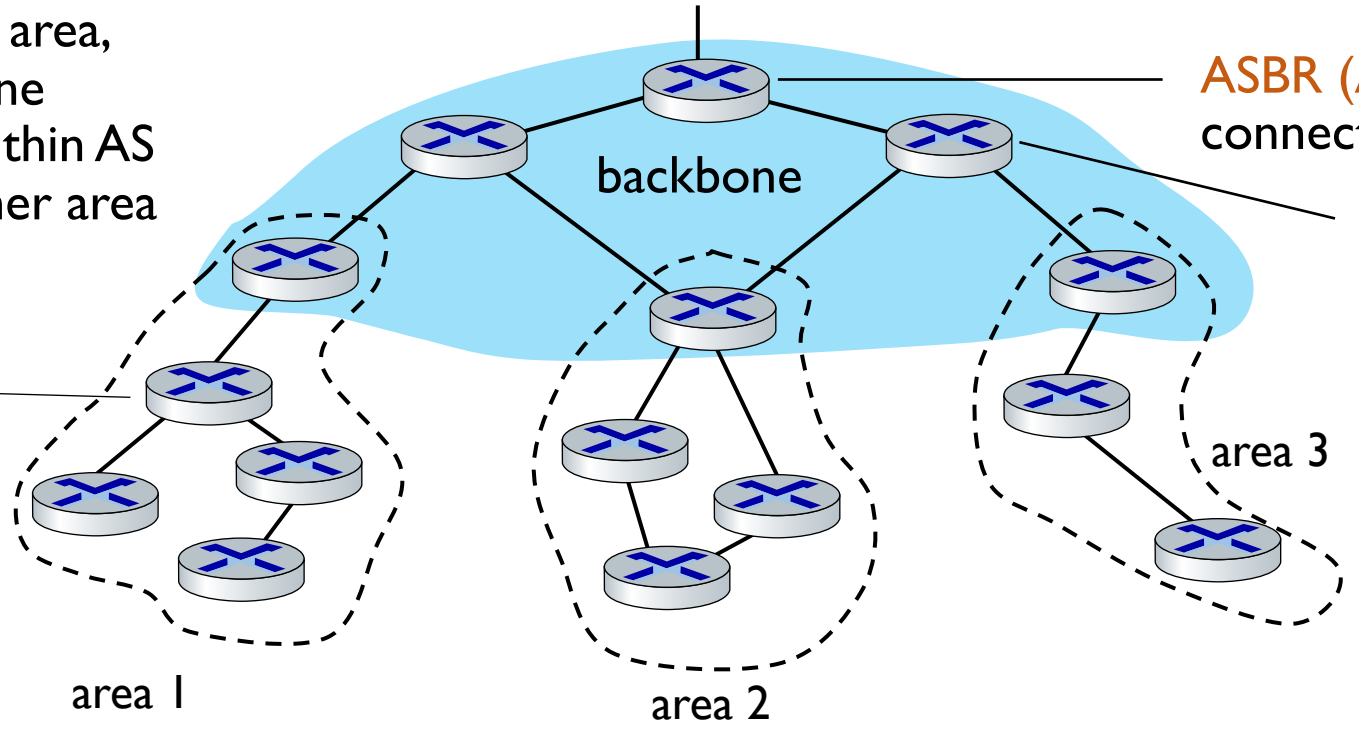


ASBR (AS Border Router):
connects to other ASes

Backbone router:
runs OSPF limited to backbone

- Link-state advertisements are NOT flooded across multiple areas/backbone
- Each node has detailed topology for its own area but just next hop for outside
- ASBR must run both BGP as well as IGP (such as OSPF)

ABR (Area Border router):
- "summarize" distances to destinations in own area, advertise in backbone
- Also lets routers within AS know about the other area



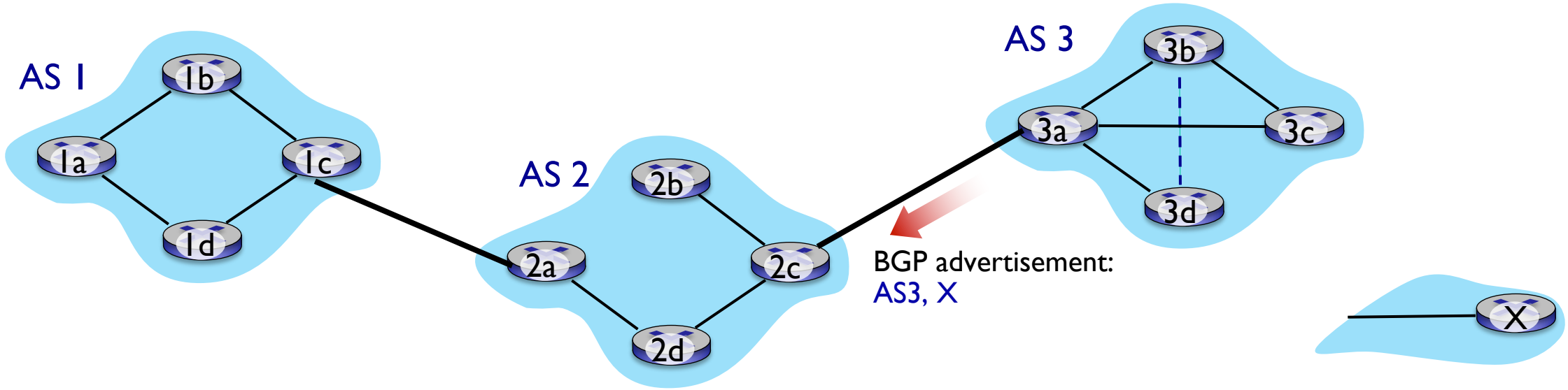
ASBR (AS Border Router): connects to other ASes

Backbone router: runs OSPF limited to backbone

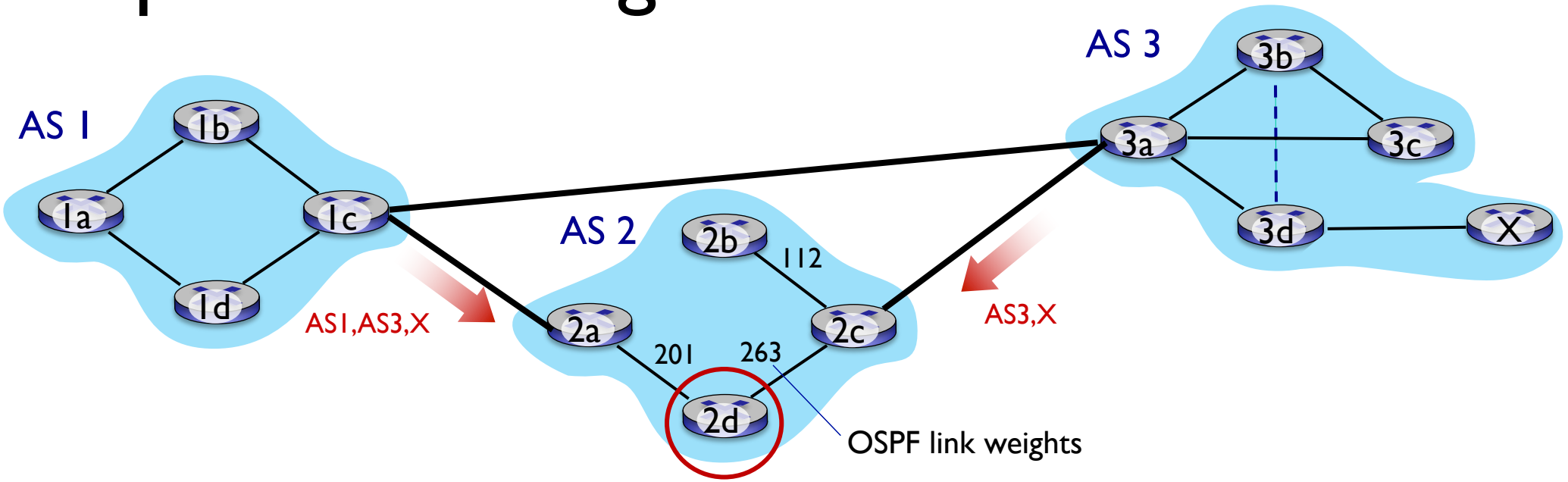
Local router:
- flood LS in area only
- compute routing within area
- forward packets to outside via area border router

BGP basics

- BGP session: two BGP routers ("peers, speakers") exchange BGP messages over semi-permanent TCP connection:
  - advertising paths to different destination network prefixes (e.g., to a destination /16 network)
  - BGP is a "path vector" protocol
- when AS3 gateway 3a advertises path AS3,X to AS2 gateway 2c:
  - AS3 promises to AS2 it will forward datagrams towards X



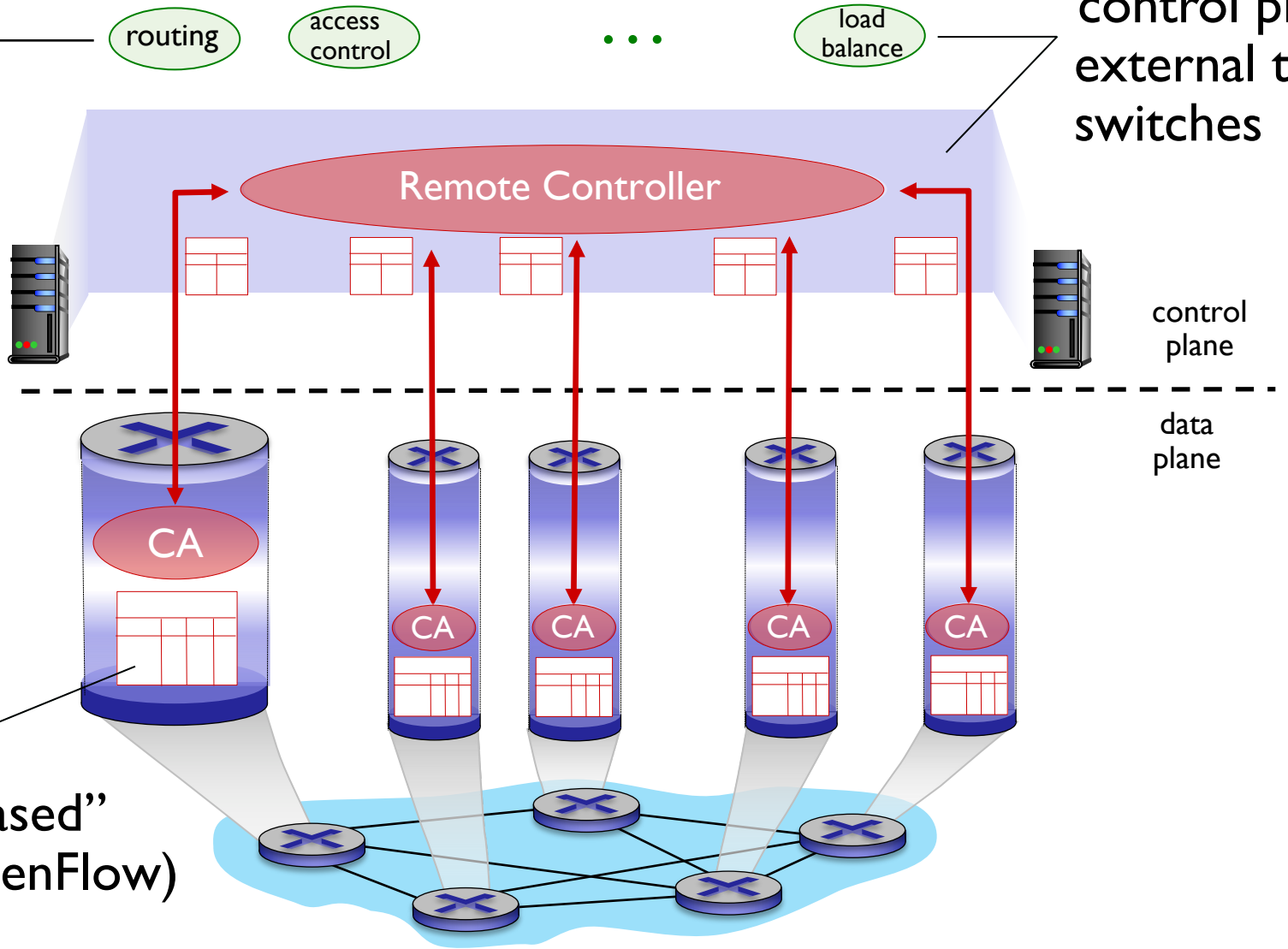
Hot potato routing



- 2d learns (via iBGP) it can route to X via 2a or 2c
- hot potato routing: choose local gateway that has least intra-domain cost (e.g., 2d chooses 2a, even though more AS hops to X): don't worry about inter-domain cost!

SDN architecture

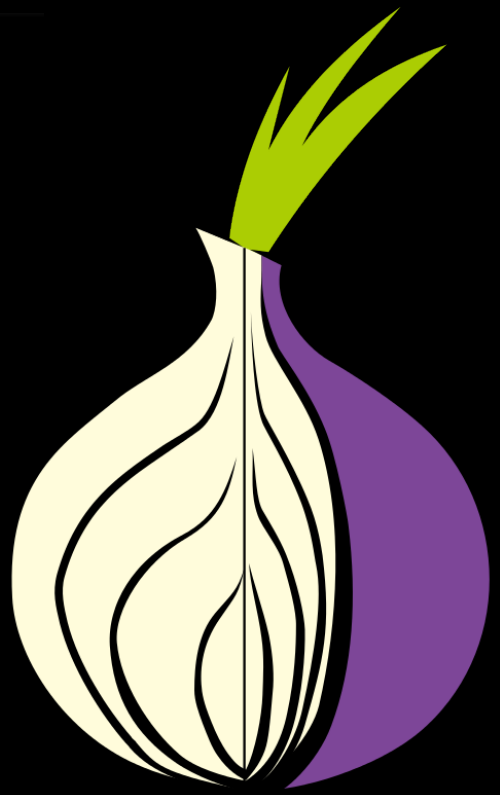
programmable network-control applications



Internet Reference Model

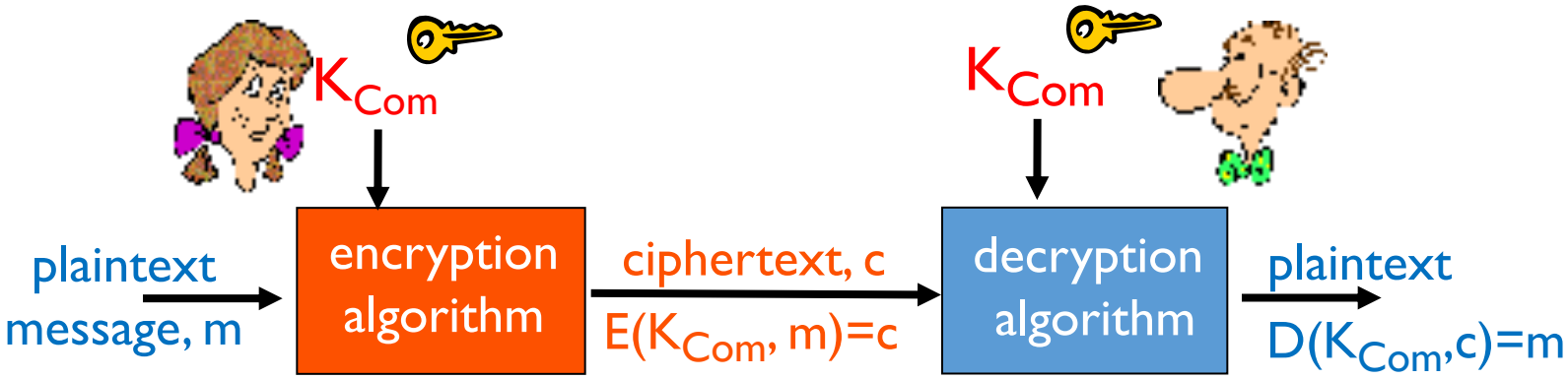
Example Protocols		Responsible for
FTP, HTTP, SMTP	Application	application specific needs
TCP, UDP	Transport	process to process data transfer
IP	Network	host to host data transfer across different network
Ethernet, WiFi	Link	data transfer between physically adjacent nodes
802.3 PHY	Physical	bit-by-bit or symbol-by-symbol delivery

16



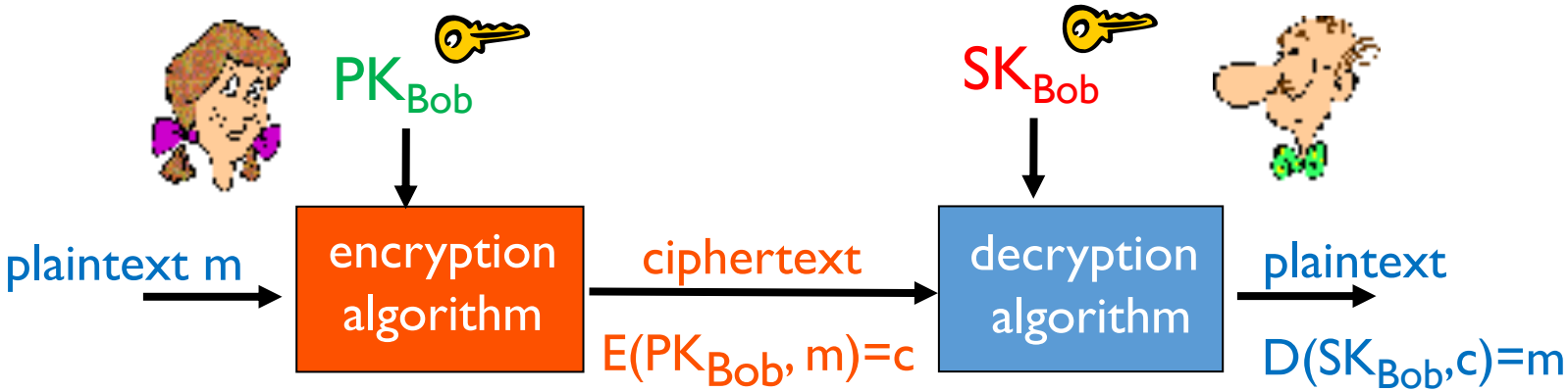
WE ARE
ANONYMOUS

TLS uses symmetric encryption



How do Alice and Bob establish the shared key?

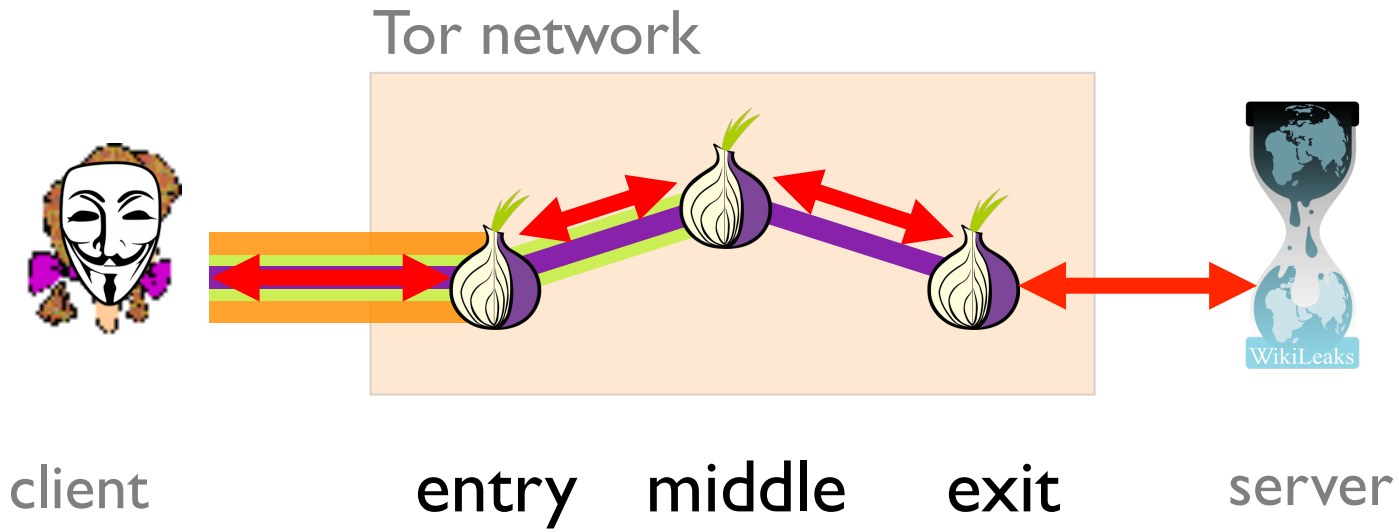
Public Key (aka asymmetric) Encryption



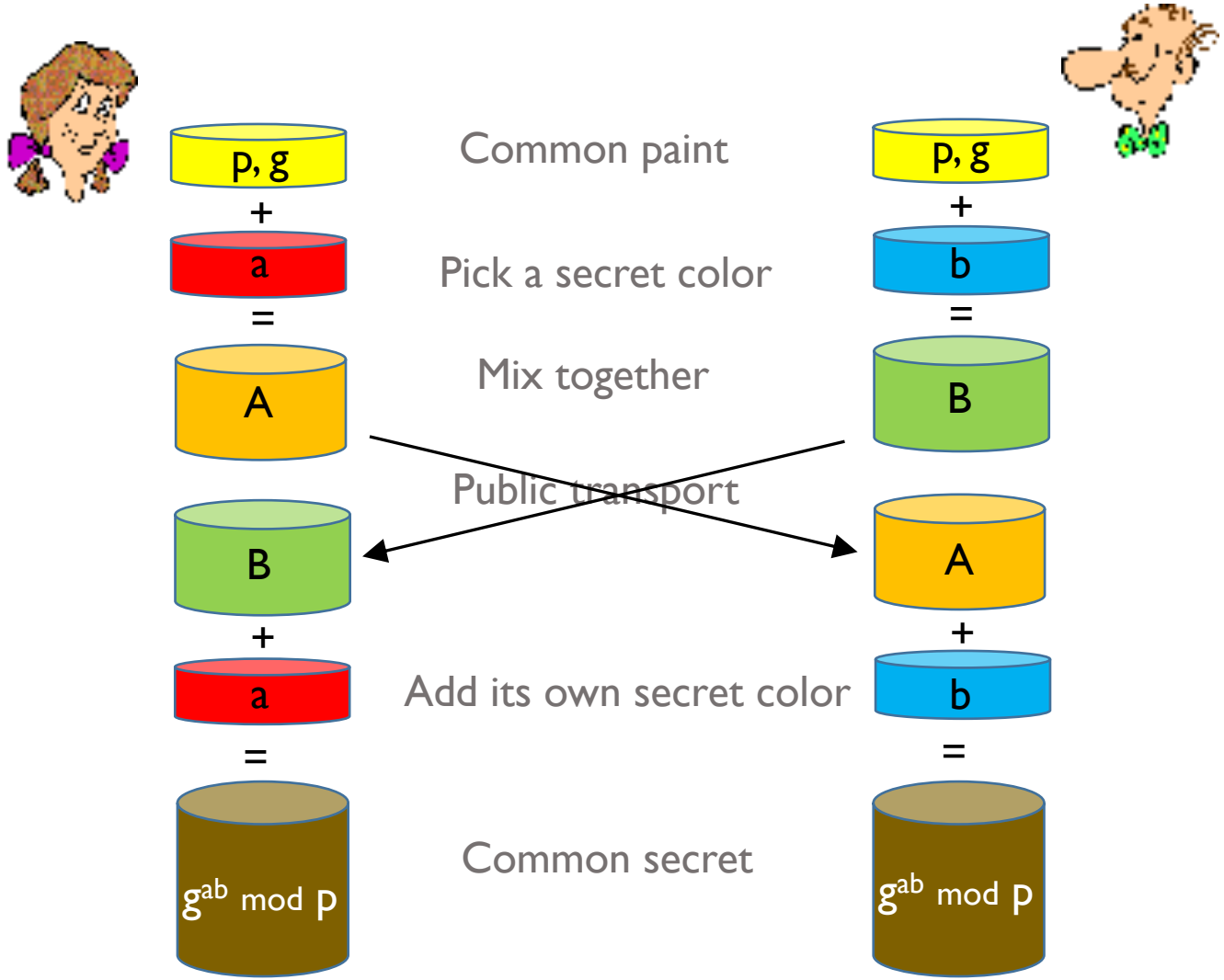
ex) RSA, Elliptic Curve, etc.

PK public key
SK private key

Anonymous communication takes place by forwarding traffic across consecutive tunnels



Key Exchange: Diffie-Hellman's Nifty Idea



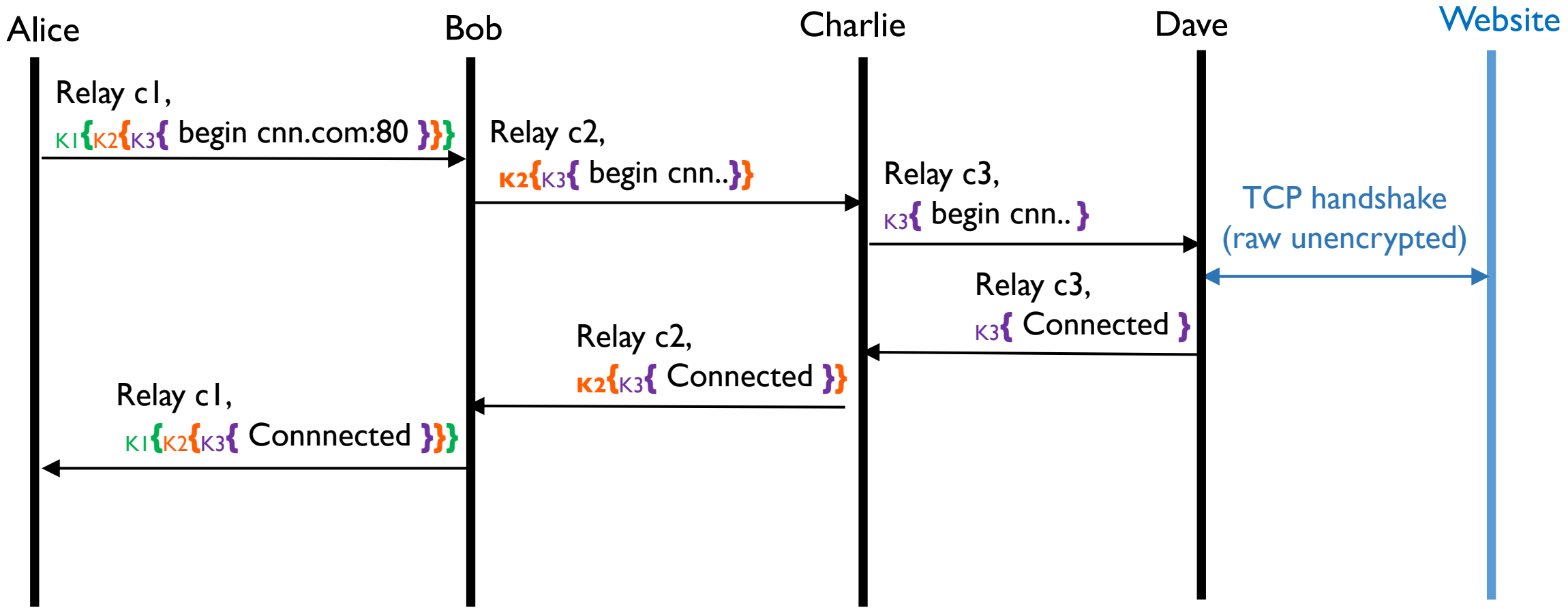
- p = a large prime
  g = a number [1.. p]
- a, b = random num [1..p-1]
- $A = g^a \bmod p$
  $B = g^b \bmod p$

- Alice computes $B^a \bmod p$
- Bob computes $A^b \bmod p$
- $g^{ab} \bmod p$ is the shared key!

21

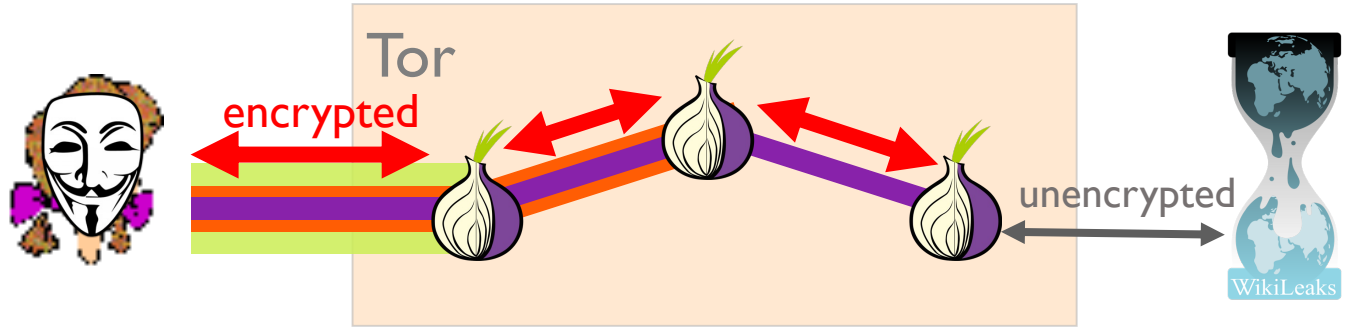
Tor Packet Forwarding via 3 hop Circuit

- Alice – Bob, Alice – Charlie, Alice – Dave has shared session key K_1, K_2 and K_3



22

VPN vs Tor (vs Proxy)



client entry middle exit server

23

Internet Reference Model

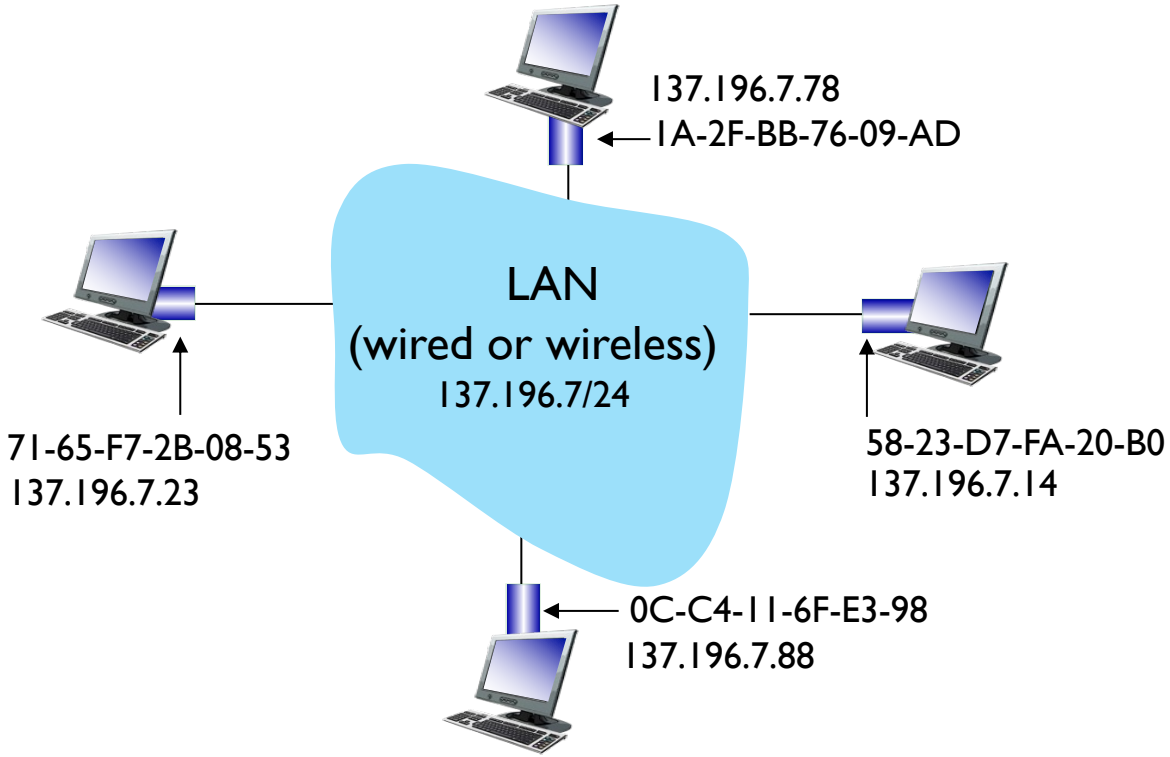
Example Protocols		Responsible for
FTP, HTTP, SMTP	Application	application specific needs
TCP, UDP	Transport	process to process data transfer
IP	Network	host to host data transfer across different network
Ethernet, WiFi	Link	data transfer between physically adjacent nodes
802.3 PHY	Physical	bit-by-bit or symbol-by-symbol delivery

24

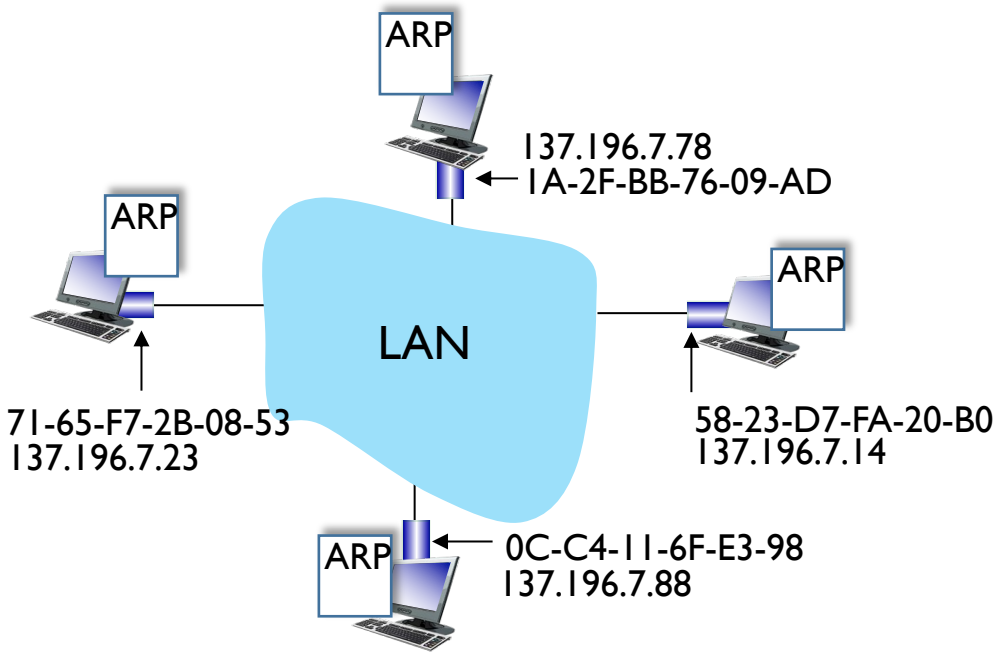
MAC addresses

each interface on LAN

- has unique 48-bit MAC address
- has a locally unique 32-bit IP address (as we've seen)



ARP: address resolution protocol



ARP table: each IP node (host, router) on LAN has table

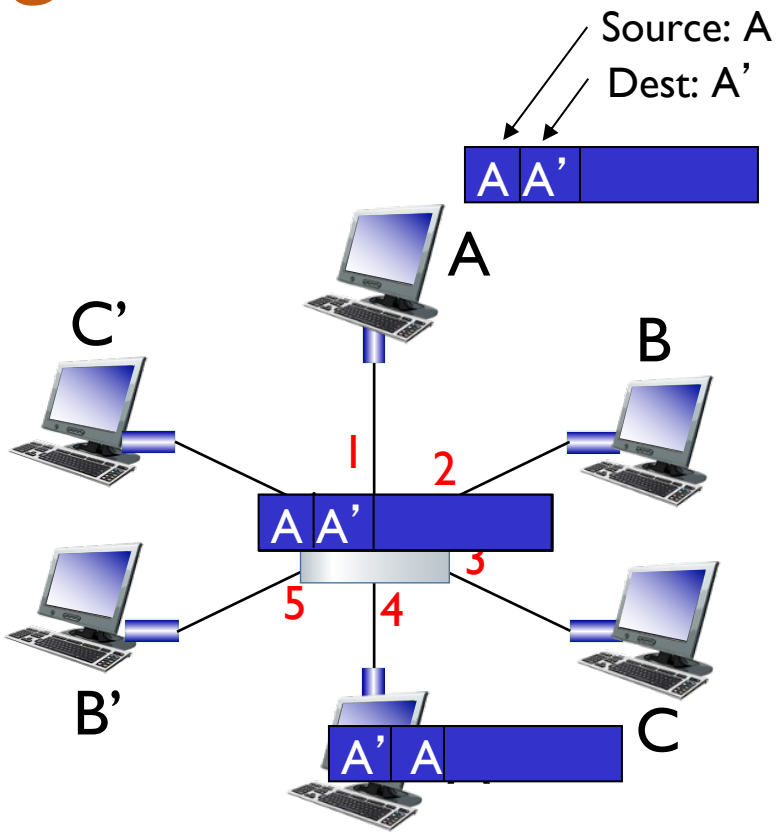
- IP/MAC address mappings for some LAN nodes:

  < IP address; MAC address; TTL>

- TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

Self-learning switch example

- frame destination, A', location unknown: flood
- destination A location known: selectively send on just one link



MAC addr	interface	TTL
A	1	60
A'	4	60

switch table (initially empty)