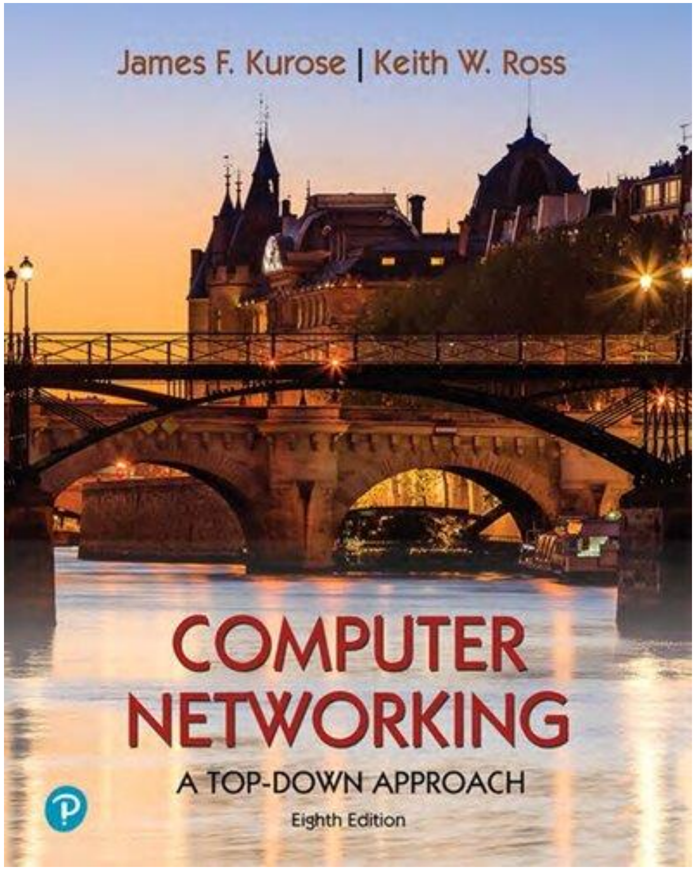
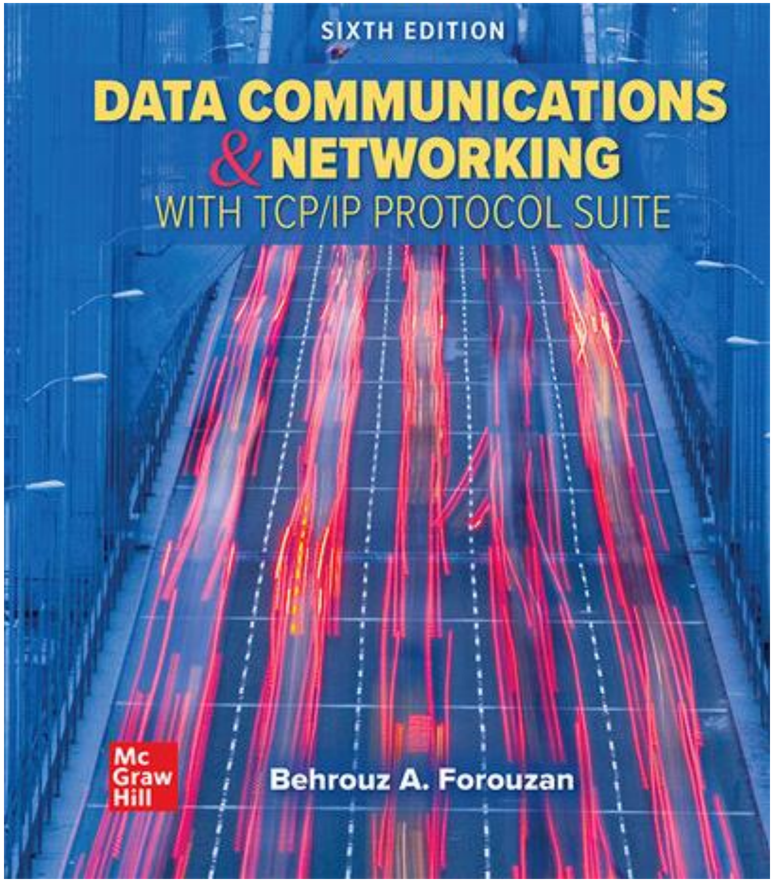
UNIVERSITE LIBANAISE

I3304
Network administration and security

Ahmad Fadlallah

Reference Textbooks





Outline

- Introduction
  - Introduction to the course
  - Recall Network Basics (I2208)
- Network Layer
  - Static Routing
  - Dynamic Routing
    - Dynamic Routing Algorithm
    - Dynamic Routing Protocols
  - NAT (Network Address Translation)
- Transport Layer
  - Function of the transport layer
  - UDP Protocol
  - TCP Protocol
    - Connection management
    - Flow control
    - Congestion control
- Application Layer
  - HTTP protocol
  - FTP protocol
  - Mail protocols
  - DNS
- Introduction to Security
  - Security services
  - Cryptography
  - Digital Signature
  - Principle of network security protocols

References

- The slides are based on the:
  - Cisco Networking Academy Program, Routing and Switching Essentials v6.0, Chapter 1: Routing Concepts
  - Jim Kurose, Keith Ross Slides for the Computer Networking: A Top-Down Approach, 8th edition, Pearson, 2020

Dynamic Routing Protocols

Making routing scalable

Our routing study thus far - idealized

- All routers identical/ executing the same routing algorithm
- Network "flat"

… not true in practice

Scale: billions of destinations:

- Can't store all destinations in routing tables!
- Routing table exchange would swamp links!

Administrative Autonomy:

- Internet: a network of networks
- Each network admin may want to control routing in its own network
  - Different Routing Algorithms
  - Hiding aspects of network's internal organization

Internet approach to scalable routing

- Aggregate routers into regions known as "Autonomous Systems" (AS) (a.k.a. "domains")
- Each AS consisting of a group of routers that are under the same administrative control.
- One ISP network ➔ one or more AS
- An autonomous system is identified by its globally unique Autonomous System Number (ASN) [RFC 1930].
- AS numbers, like IP addresses, are assigned by ICANN regional registries

Internet approach to scalable routing

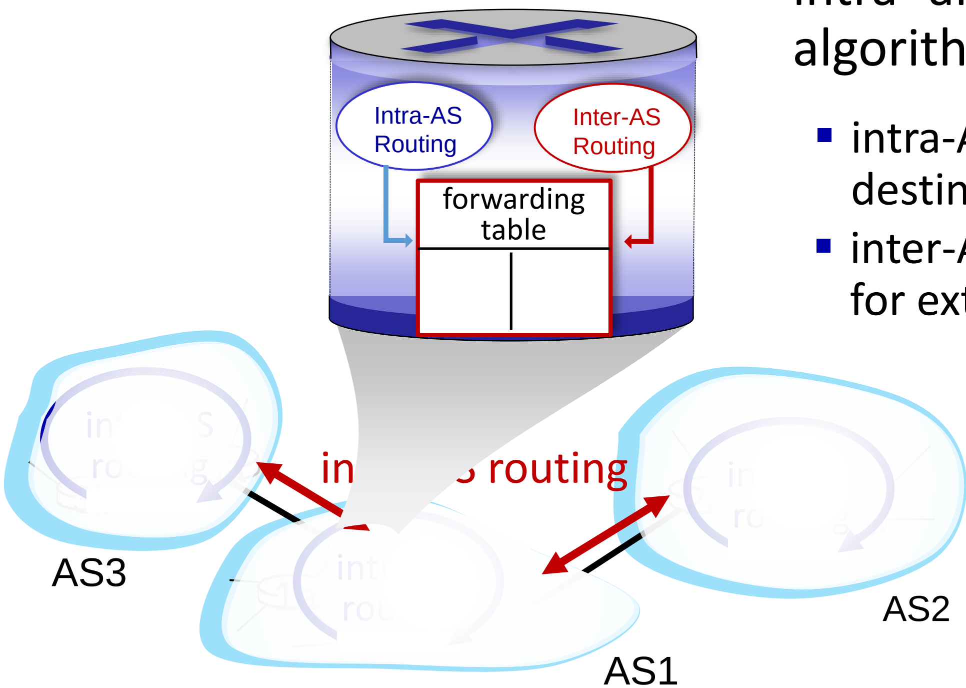
Intra-AS

- Routing *within same AS ("network")*
- All routers in AS must run <u>same intra-domain protocol</u>
- Routers in different AS can run different intra-domain routing protocols
- Gateway router: at "edge" of its own AS, has link(s) to router(s) in other AS'es

Inter-AS

- Routing *among* AS'es
- Gateways perform <u>inter-domain routing</u> (as well as intra-domain routing)

Interconnected ASes



Forwarding table configured by intra- and inter-AS routing algorithms

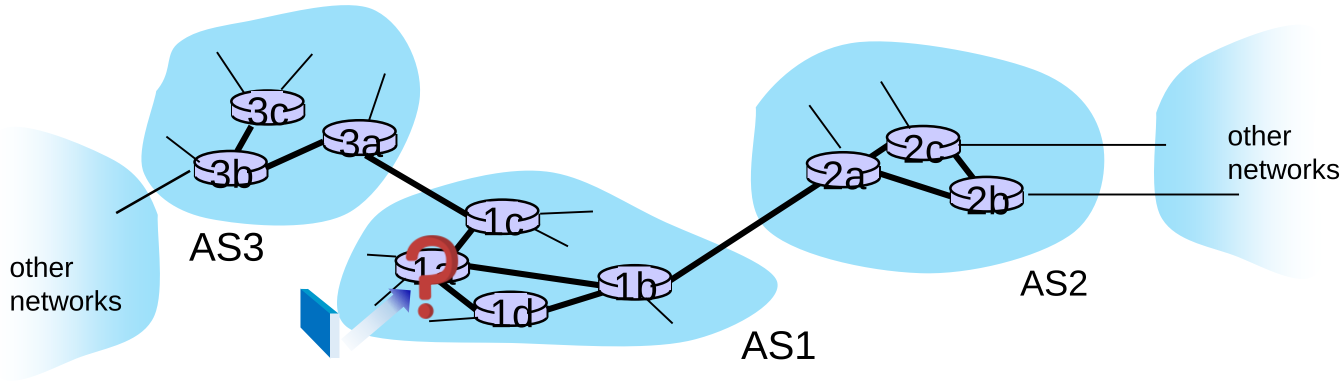
- intra-AS routing determine entries for destinations within AS
- inter-AS & intra-AS determine entries for external destinations

Intra-AS routing: a role in intra-domain forwarding

- Suppose router in AS1 receives datagram destined outside of AS1:
  - Router should forward packet to gateway router in AS1, but which one?

AS1 inter-domain routing must:

1. Learn which destinations reachable through AS2, which through AS3
2. Propagate this reachability info to all routers in AS1

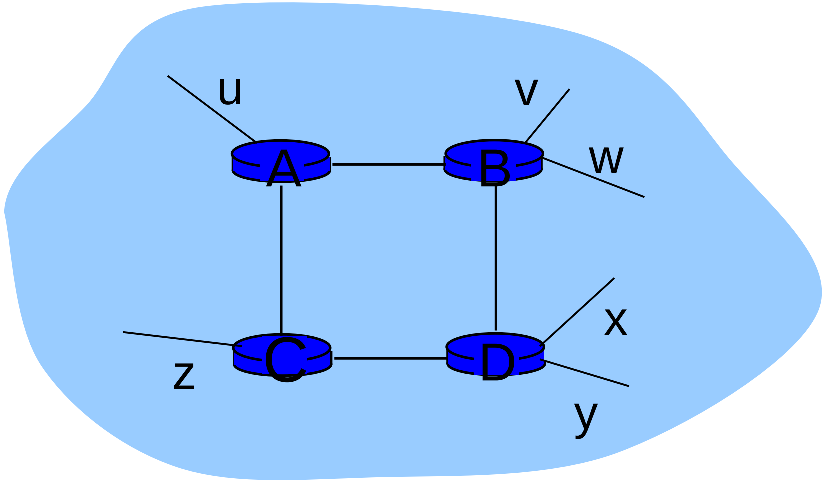


Intra-AS routing: routing within an AS

- Most common intra-AS routing protocols:
- RIP: Routing Information Protocol [RFC 1723]
    - classic DV: DVs exchanged every 30 secs
    - no longer widely used
- EIGRP: Enhanced Interior Gateway Routing Protocol
    - DV based
    - formerly Cisco-proprietary for decades (became open in 2013 [RFC 7868])
- OSPF: Open Shortest Path First [RFC 2328]
    - link-state routing
    - IS-IS protocol (ISO standard, not RFC standard) essentially same as OSPF

RIP (Routing Information Protocol)

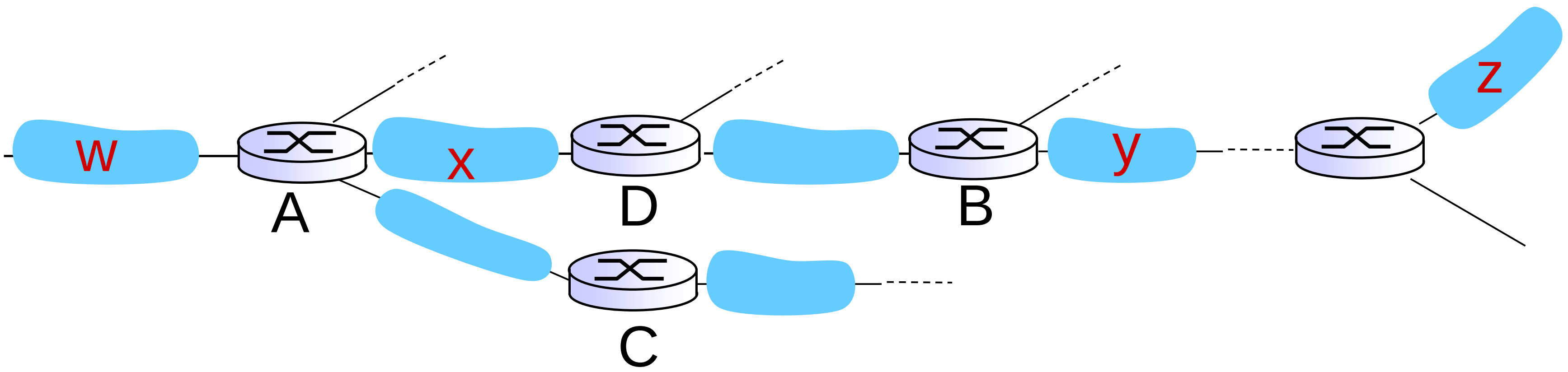
- Included in BSD-UNIX distribution in 1982
- Distance vector algorithm
  - distance metric: # hops (max = 15 hops), each link has cost 1
  - DVs exchanged with neighbors every 30 sec in response message (aka advertisement)
  - Each advertisement: list of up to 25 destination *subnets (in IP addressing sense)*



from router A to destination *subnets:*

subnet	hops
u	1
v	2
w	2
x	3
y	3
z	2

RIP: example



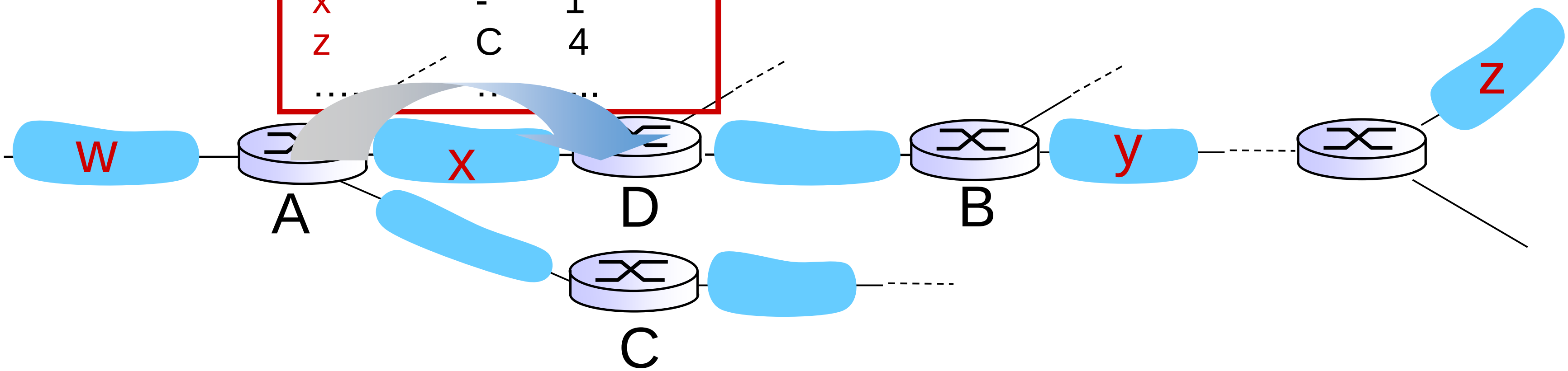
routing table in router D

destination subnet	next router	# hops to dest
w	A	2
y	B	2
z	B	7
x	--	1
….	….	….

RIP: example

A-to-D advertisement

dest	next	hops
w	-	1
x	-	1
z	C	4
….	…	…



routing table in router D

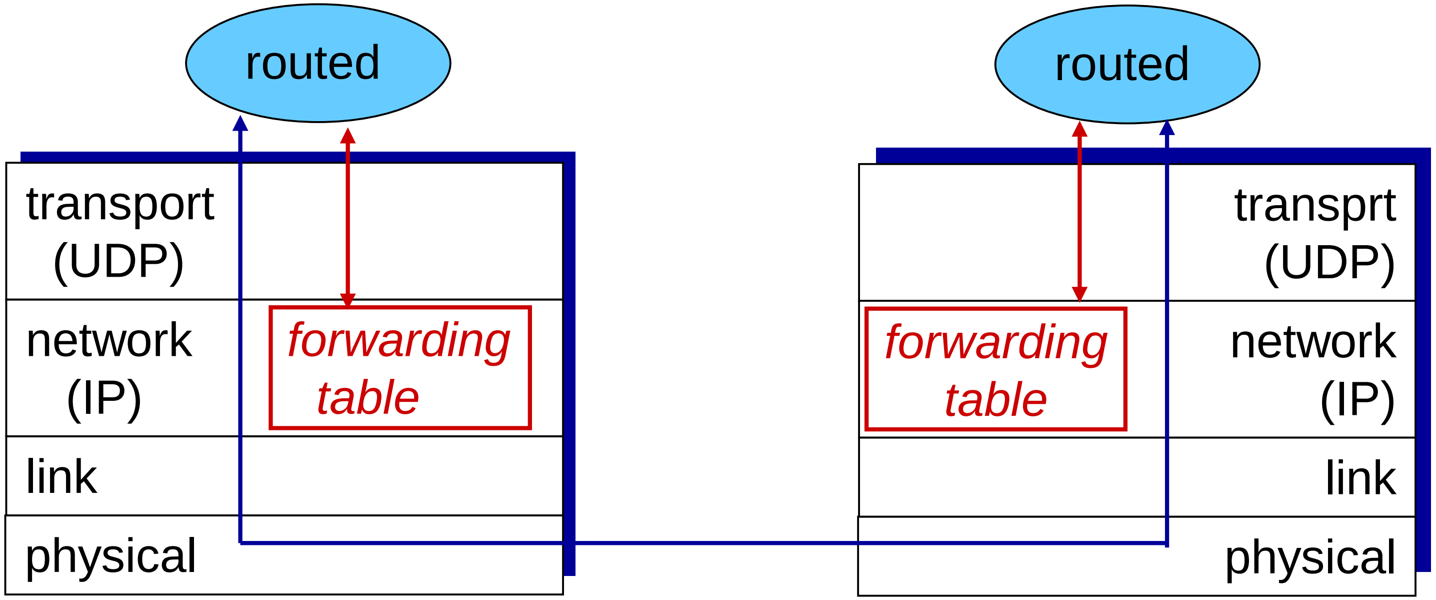
destination subnet	next router	# hops to dest
w	A	2
y	B	2
z	~~B~~ A	~~7~~ 5
x	--	1
….	….	….

RIP: link failure, recovery

- If no advertisement heard after 180 sec → neighbor/link declared dead
  - Routes via neighbor invalidated
  - New advertisements sent to neighbors
  - Neighbors in turn send out new advertisements (if tables changed)
  - Link failure info quickly (?) propagates to entire net
  - Poison reverse used to prevent ping-pong loops (infinite distance = 16 hops)

RIP table processing

- RIP routing tables managed by application-level process called *route-d* (daemon)
- Advertisements sent in UDP packets, periodically repeated

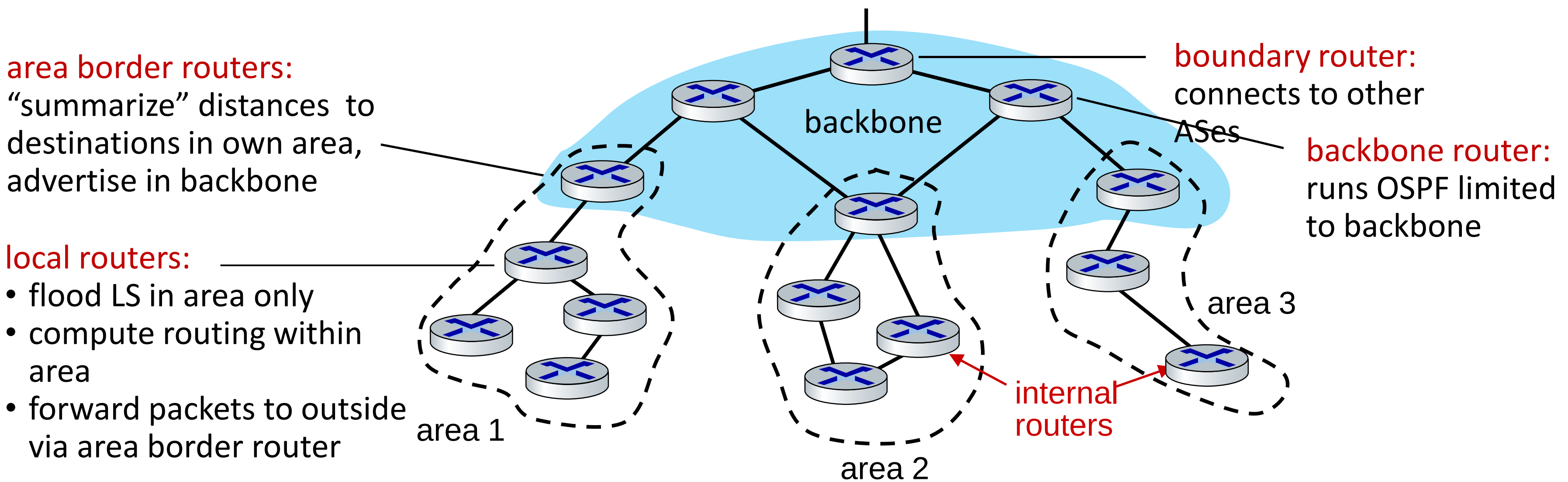


OSPF (Open Shortest Path First) routing

- "open": publicly available
  - OSPFv2, defined in RFC2328
- OSPF is a **link-state protocol** that uses flooding of link-state information and a Dijkstra's least-cost path algorithm.
  - Each router floods OSPF link-state advertisements (**directly over IP rather than using TCP/UDP**) to all other routers in entire AS
  - Multiple link costs metrics possible: bandwidth, delay
  - Each router has full topology, uses Dijkstra's algorithm to compute forwarding table
- **Security**: all OSPF messages authenticated (to prevent malicious intrusion)

Hierarchical OSPF

- **two-level hierarchy:** local area, backbone.
  - Link-state advertisements flooded only in area, or backbone
  - Each node has detailed area topology; only knows direction to reach other destinations



Dynamic Routing Protocols routing among ISPs: BGP

Introduction

- Building the forwarding table for a router (within an AS)
  - For destinations that are within the same AS, the entries in the router's forwarding table are determined by the AS's intra-AS routing protocol
  - What about destinations that are outside of the AS?

This is precisely where the Border Gateway Protocol (BGP) comes to the rescue.

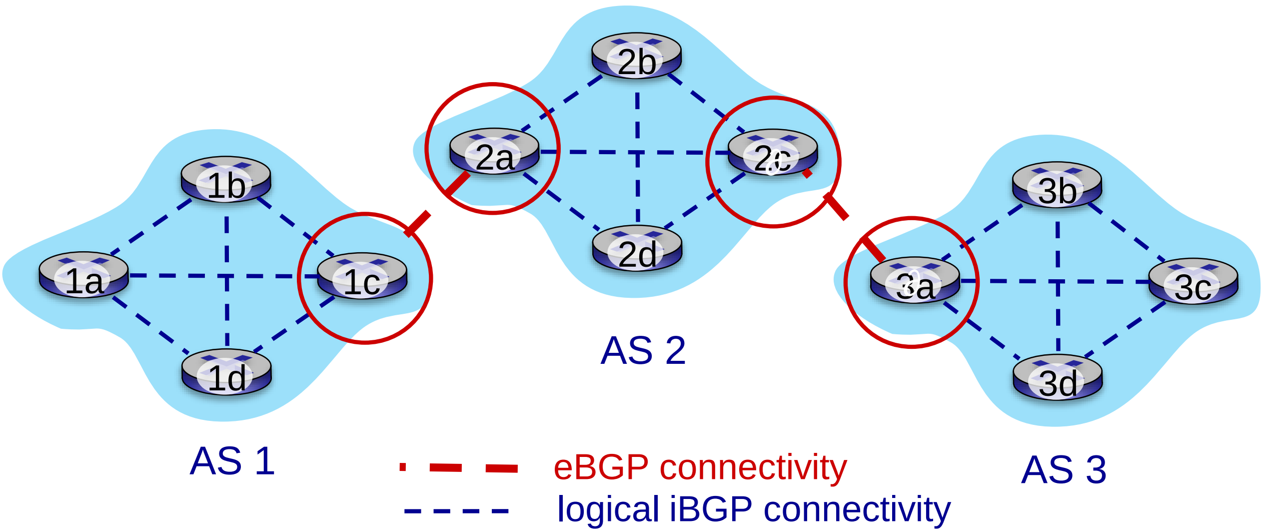
Internet inter-AS routing: BGP

- BGP (Border Gateway Protocol): the *de facto* inter-domain routing protocol
  - The most important of all Internet protocol (in contest with IP)
  - "**glue** that holds the Internet together"
- Allows subnet to advertise its existence, and the destinations it can reach, to rest of Internet: "I am here, here is who I can reach, and how"
- In BGP, packets are not routed to a specific destination address, but instead to **CIDRized prefixes**, with each prefix representing a subnet or a collection of subnets.
  - Example: a destination may take the form 138.16.68/22, which for this example includes 1,024 IP addresses.
  - A router's forwarding table will have entries of the form (*x*, *I*), where *x* is a prefix (such as 138.16.68/22) and *I* is an interface number for one of the router's interfaces.

Internet inter-AS routing: BGP

- BGP provides each AS a means to:
  - ⊙Obtain subnet reachability information from neighboring Ases
    - The role of **eBGP (external BGP)**
    - BGP allows each subnet to advertise its existence to the rest of the Internet
    - *A subnet screams, “I exist and I am here,” and BGP makes sure that all the routers in the Internet know about this subnet.*
  - ⊙Propagate reachability information to all AS-internal routers
    - The role of **iBGP (internal BGP)**
  - ⊙Determine the “best” routes to the prefixes.
    - The router will locally run a BGP route-selection procedure
    - determine “good” routes to other networks based on reachability information and policy

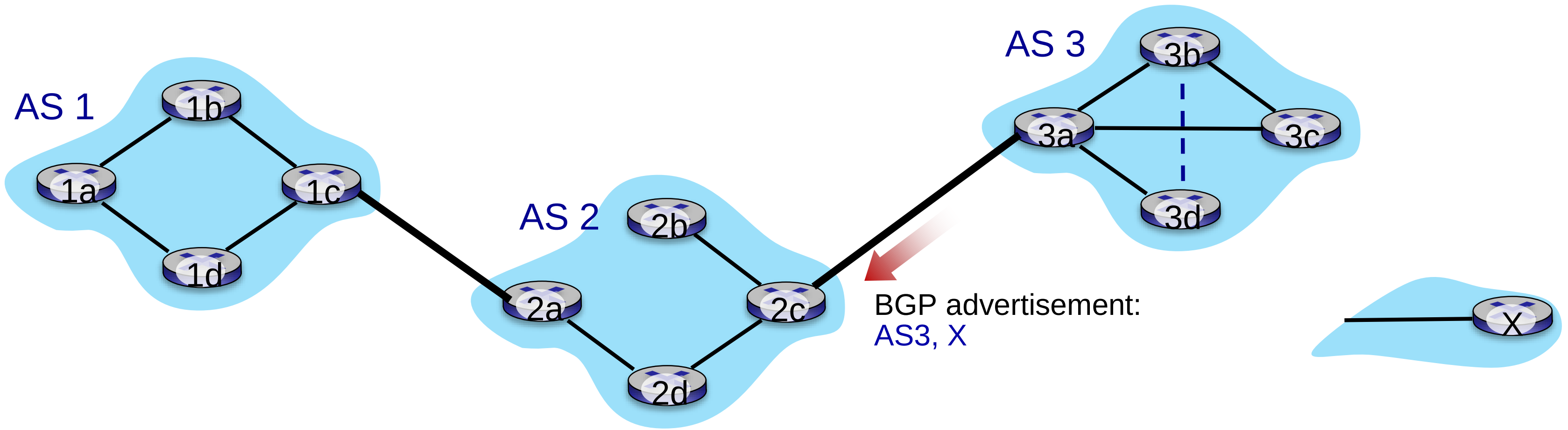
eBGP, iBGP connections



gateway routers run both eBGP and iBGP protocols

BGP basics

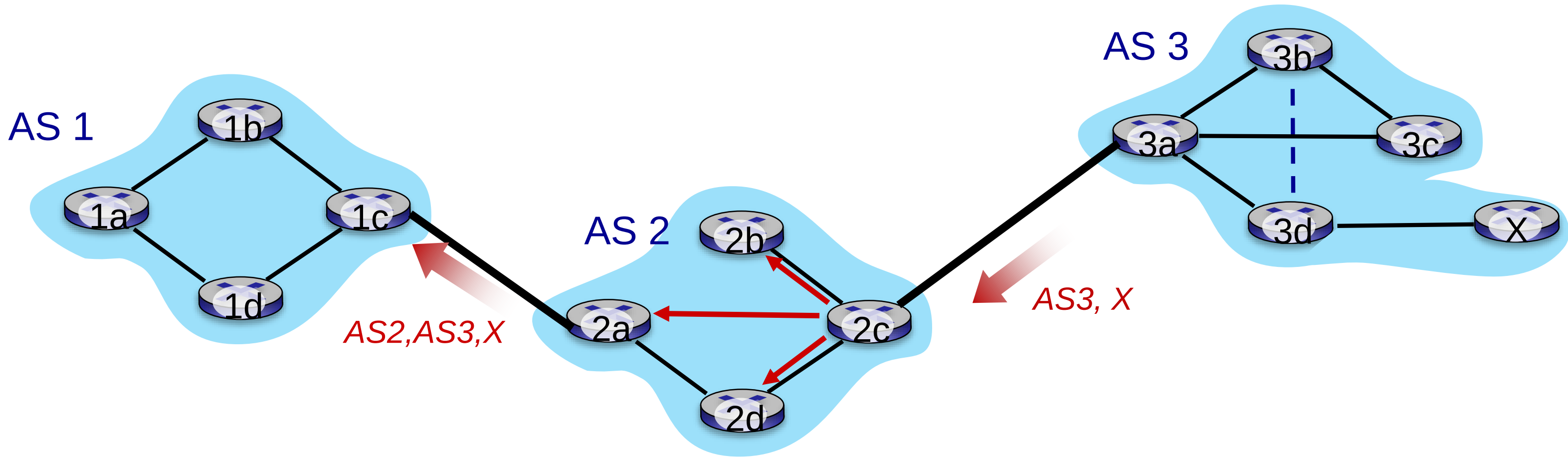
- BGP session: two BGP routers ("peers") exchange BGP messages over semi-permanent TCP connection (port 179):
  - ⊙Advertising paths to different destination network prefixes (BGP is a **"path vector" protocol)**
- When AS3 gateway 3a advertises path AS3,X to AS2 gateway 2c:
  - ⊙AS3 promises to AS2 it will forward datagrams towards X



Path attributes and BGP routes

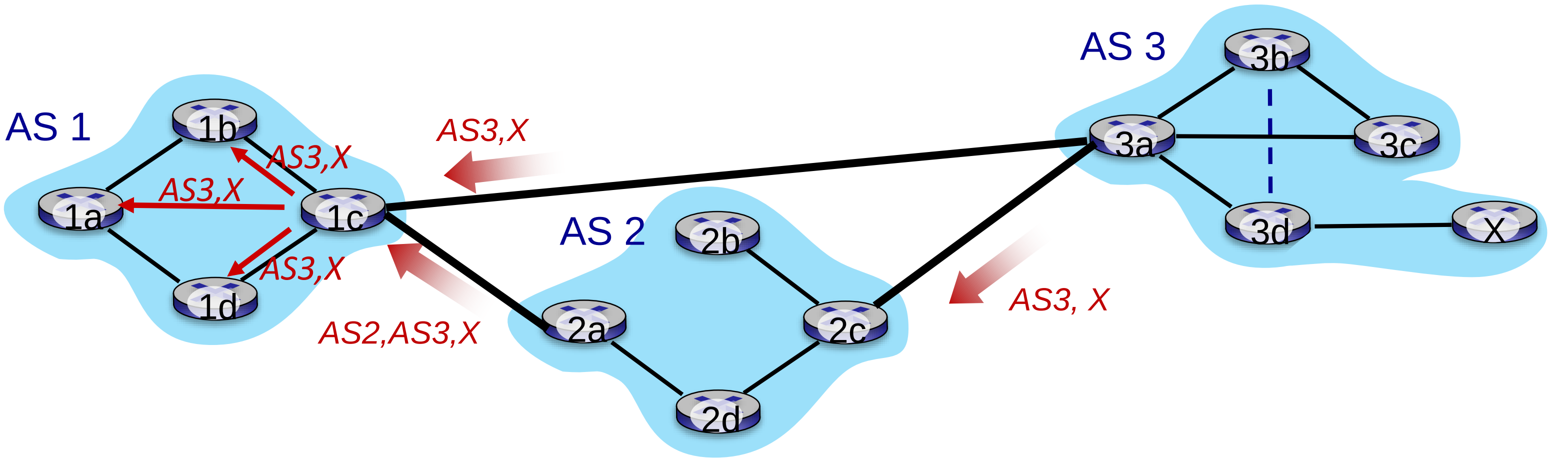
- BGP advertised route: prefix + attributes
  - ⊙prefix: destination being advertised
  - ⊙two important attributes:
    - ⊙AS-PATH: list of ASes through which prefix advertisement has passed
    - ⊙NEXT-HOP: indicates specific internal-AS router to next-hop AS
      - the IP address of the router interface that begins the AS-PATH.
- Policy-based routing:
  - ⊙Gateway receiving route advertisement uses *import policy* to accept/decline path (e.g., never route through AS Y).
  - ⊙AS policy also determines whether to *advertise* path to other neighboring ASes

BGP path advertisement



- AS2 router 2c receives path advertisement AS3,X (via eBGP) from AS3 router 3a
- based on AS2 policy, AS2 router 2c accepts path AS3,X, propagates (via iBGP) to all AS2 routers
- based on AS2 policy, AS2 router 2a advertises (via eBGP) path AS2, AS3, X to AS1 router 1c

BGP path advertisement (more)



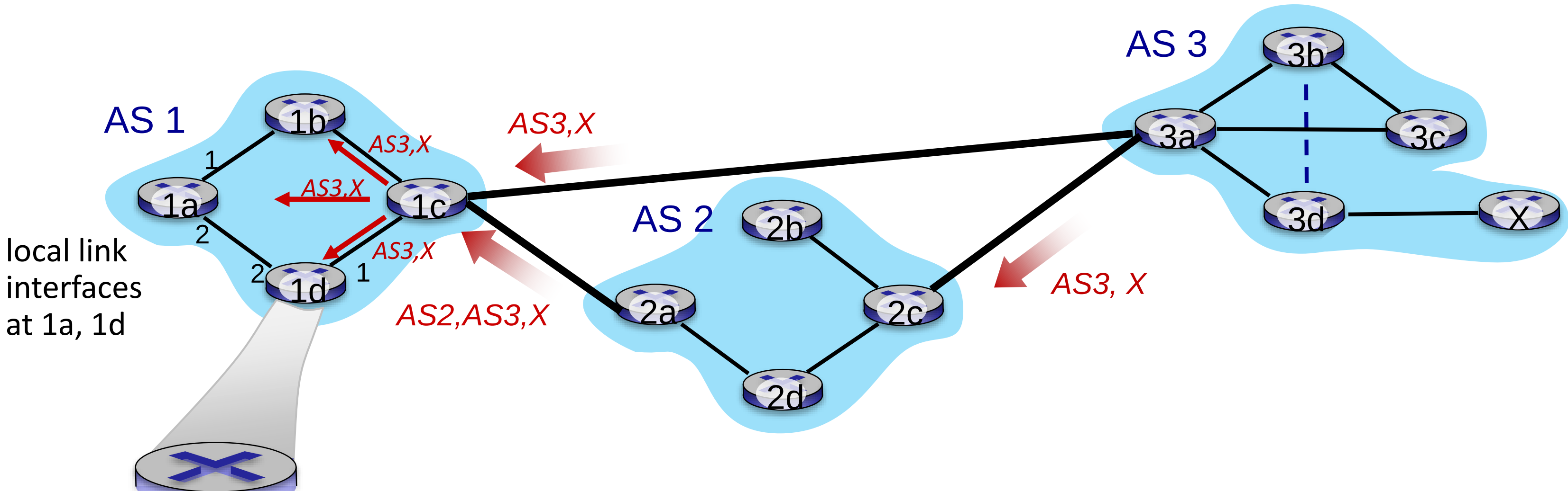
gateway router may learn about multiple paths to destination:

- AS1 gateway router 1c learns path *AS2,AS3,X* from 2a
- AS1 gateway router 1c learns path *AS3,X* from 3a
- based on *policy,* AS1 gateway router 1c chooses path *AS3,X* and advertises path within AS1 via iBGP

BGP messages

- BGP messages exchanged between peers over TCP connection
- BGP messages:
  - OPEN: opens TCP connection to remote BGP peer and authenticates sending BGP peer
  - UPDATE: advertises new path (or withdraws old)
  - KEEPALIVE: keeps connection alive in absence of UPDATES; also ACKs OPEN request
  - NOTIFICATION: reports errors in previous msg; also used to close connection

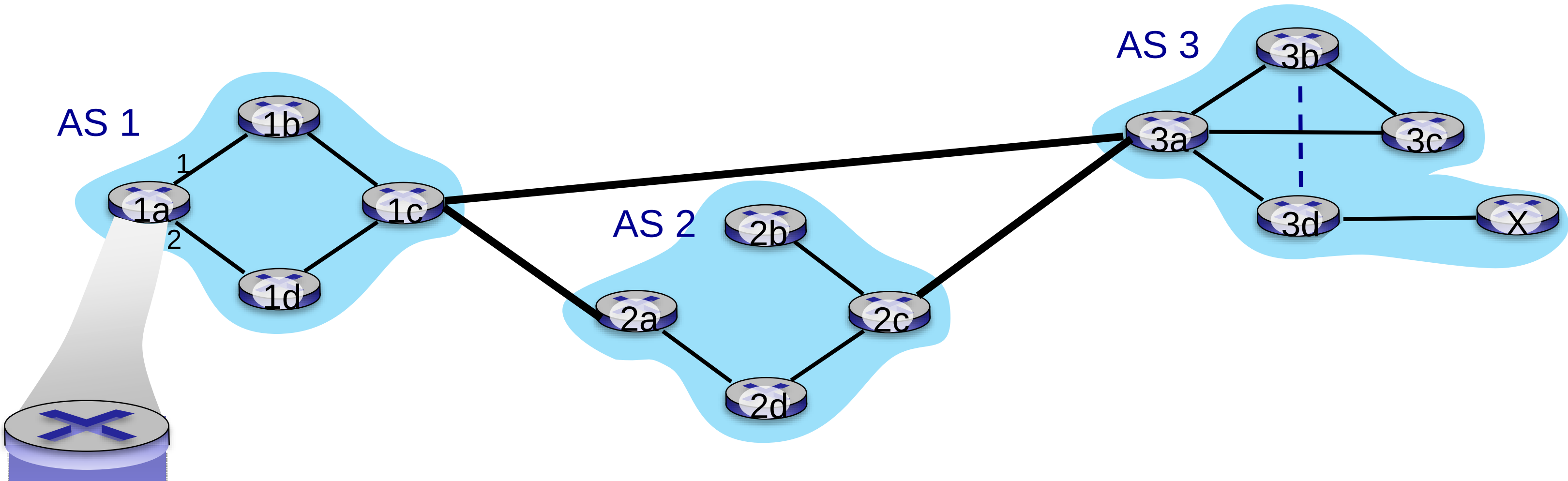
BGP path advertisement



dest	interface
…	…
1c	1
X	1
…	…

- recall: 1a, 1b, 1d learn via iBGP from 1c: “path to X goes through 1c”
- at 1d: OSPF intra-domain routing: to get to 1c, use interface 1
- at 1d: to get to X, use interface 1

BGP path advertisement



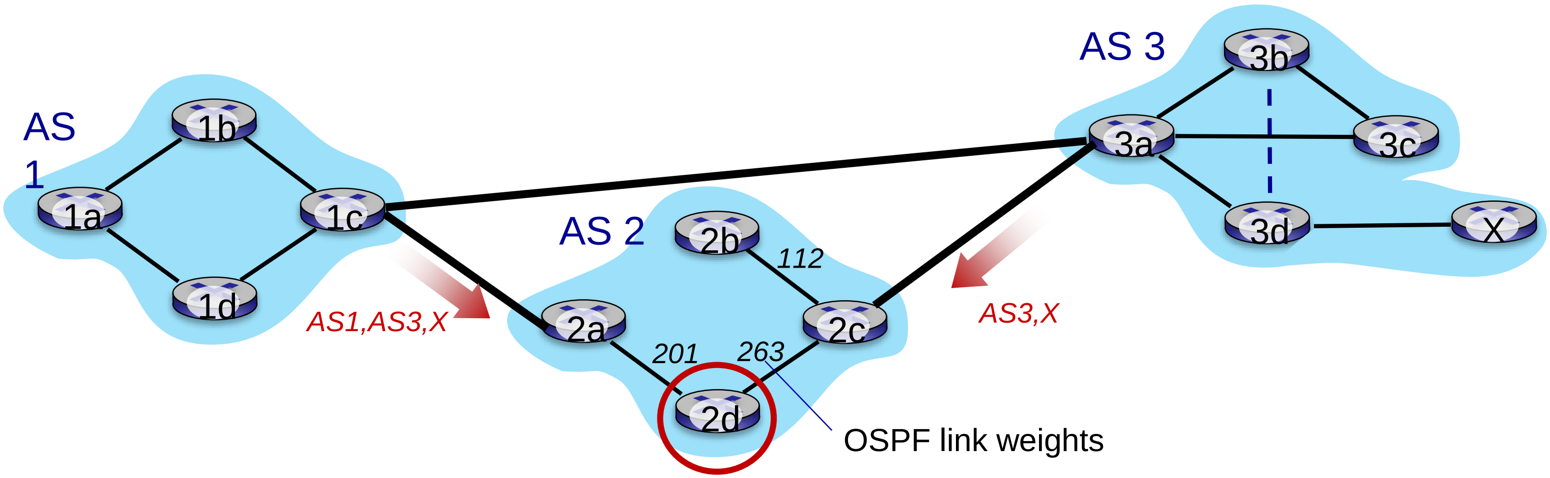
dest	interface
…	…
1c	2
X	2
…	…

- recall: 1a, 1b, 1d learn via iBGP from 1c: "path to X goes through 1c"
- at 1d: OSPF intra-domain routing: to get to 1c, use interface 1
- at 1d: to get to X, use interface 1
- at 1a: OSPF intra-domain routing: to get to 1c, use interface 2
- at 1a: to get to X, use interface 2

Why different Intra-, Inter-AS routing ?

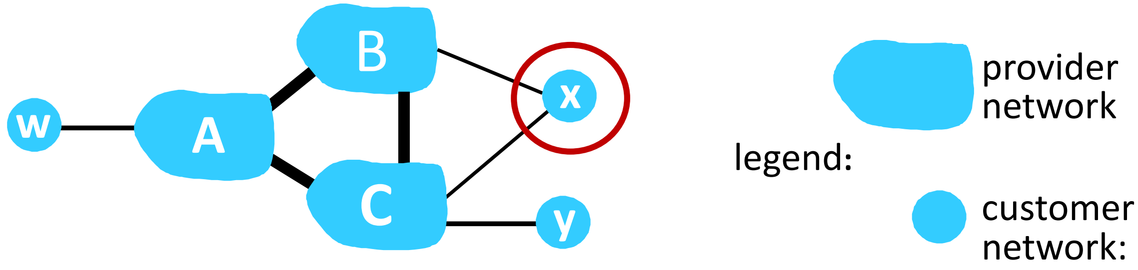
- Policy:
  - ⊙Inter-AS: admin wants control over how its traffic routed, who routes through its network
  - ⊙Intra-AS: single admin, so policy less of an issue
- Scale:
  - ⊙Hierarchical routing saves table size, reduced update traffic
- Performance:
  - ⊙Intra-AS: can focus on performance
  - ⊙Inter-AS: policy dominates over performance

Hot potato routing



- Router 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!

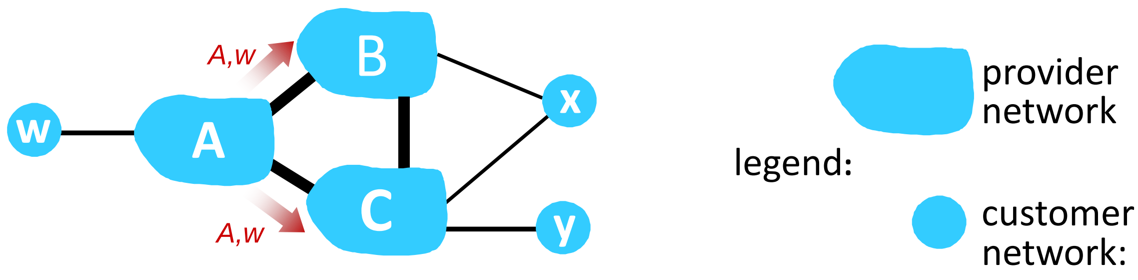
BGP: achieving policy via advertisements



ISP only wants to route traffic to/from its customer networks (does not want to carry transit traffic between other ISPs – a typical “real world” policy)

- A,B,C are provider networks
- x,w,y are customer (of provider networks)
- x is dual-homed: attached to two networks
- *policy to enforce:* x does not want to route from B to C via x
  - .. so x will not advertise to B a route to C

BGP: achieving policy via advertisements



ISP only wants to route traffic to/from its customer networks (does not want to carry transit traffic between other ISPs – a typical "real world" policy)

- A advertises path Aw to B and to C
- B *chooses not to advertise* BAw to C!
  - B gets no "revenue" for routing CBAw, since none of C, A, w are B's customers
  - C does *not* learn about CBAw path
- C will route CAw (not using B) to get to w

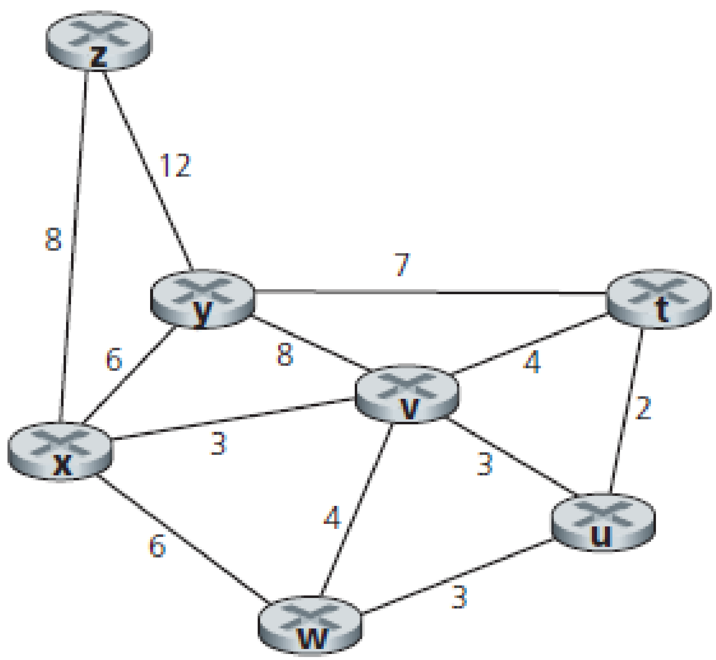
BGP route selection

- Router may learn about more than one route to destination AS, selects route based on:
  - Local preference value attribute: policy decision
  - Shortest AS-PATH
  - Closest NEXT-HOP router: hot potato routing
  - Additional criteria

Problems and Exercises

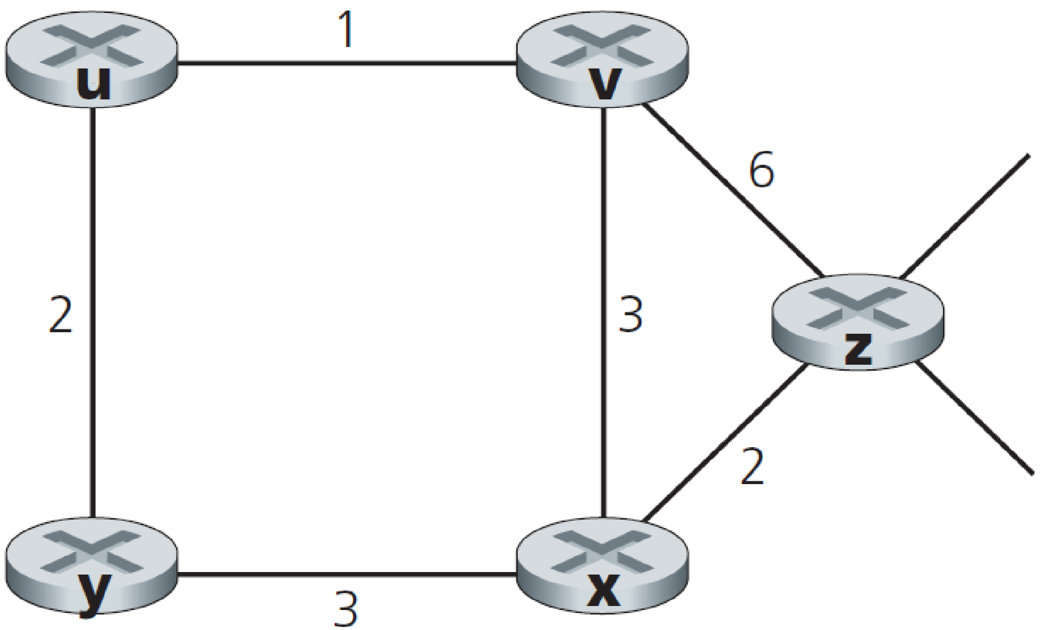
Problem – Dijkstra Algorithm

- Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to compute the shortest path from x to all network nodes.



Problem DV-Algorithm

- Consider the network shown below, and assume that each node initially knows the costs to each of its neighbors. Consider the distance-vector algorithm and show the distance table entries at node *z*.



Problem - BGP

- Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is *no* physical link between AS2 and AS4.
  a) Router 3c learns about prefix *x* from which routing protocol: OSPF, RIP, eBGP, or iBGP?
  b) Router 3a learns about *x* from which routing protocol?
  c) Router 1c learns about *x* from which routing protocol?
  d) Router 1d learns about *x* from which routing protocol?