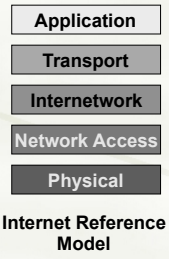
# *Routes & Routing*

Info 341 Networking and Distributed Applications

## *Context*

- Layer 3
  - Addresses, fragmentation, reassembly
- Layer 4
  - end-to-end communication
  - UDP, TCP
- Routing
  - At layer 3
  - Often relies on layer 4



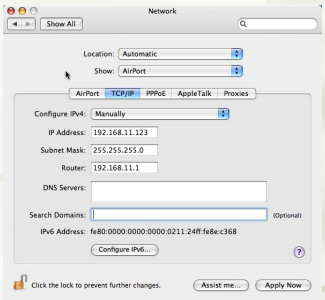

Internet Reference Model

# *Two Types of Routes*

- Static Routes
  - Set at boot, don't change
- Dynamic Routes
  - Set at boot
  - Re-calculated as the network changes

# *Static Routing*

- Most hosts (machines) use a static route
  - What does the netmask do?
  - What happens when the the destination machine is not on the same network?



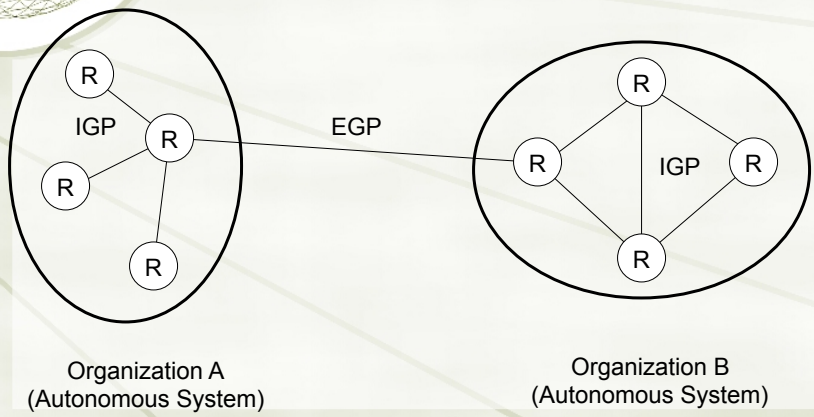
## *Dynamic Routes*

- Routing Protocols
  - Solve the routing problem by allowing routers to communicate with each other
  - They facilitate the discovery of additional routing connections

## *Two Routing Domains*

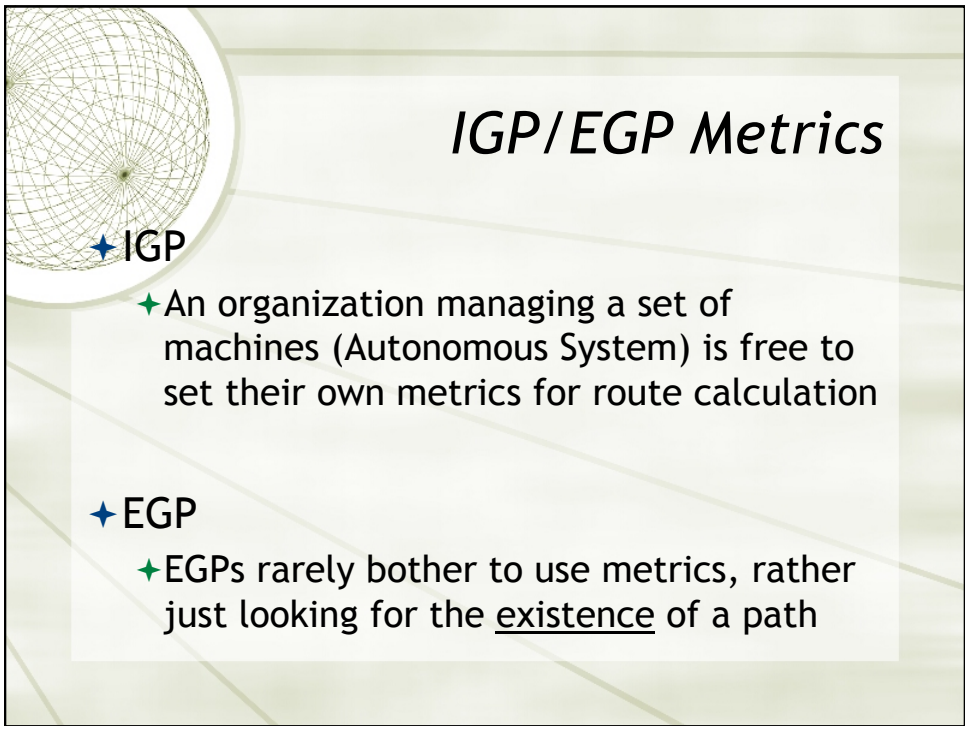
- Interior & Exterior Routing
  - Logically separate
  - Interior routing is for routes among routers that you control
    - IGP - Interior Gateway Protocols
  - Exterior routing is for the larger global networks
    - EGP - Exterior Gateway Protocols

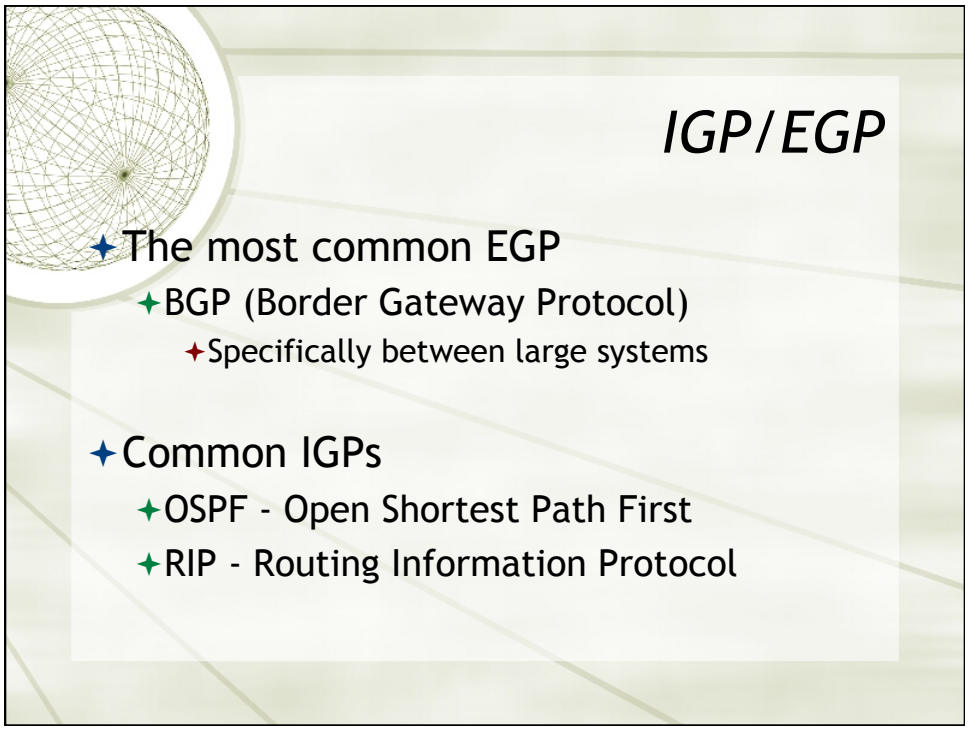
# Interior/Exterior Routing




# Routing Metrics

- How can we get an "optimal" route?
  - Routing Metric is the measure (weight) of a path used when choosing a route
  - Hop count
    - The number of hops to a destination
    - Number of intermediate routers (hops) to get to the destination
  - Administrative cost
    - Manually set "weight" on the link
    - Used to specifically control quantity of traffic over a link


IGP/EGP Metrics
IGP
An organization managing a set of machines (Autonomous System) is free to set their own metrics for route calculation
EGP
EGPs rarely bother to use metrics, rather just looking for the existence of a path


IGP/EGP
The most common EGP
BGP (Border Gateway Protocol)
Specifically between large systems
Common IGPs
OSPF - Open Shortest Path First
RIP - Routing Information Protocol

# *Border Gateway Protocol (BGP) Characteristics*

- Routing among Autonomous Systems
- *Policy Enforcement* - either sender or receiver can enforce policy. A manager could set BGP to restrict route advertisements to limited other networks
- *Transit Routing* - BGP allows networks to specify if they will (or won't) pass traffic to other networks
- *Reliable Transport* - BGP uses TCP for communication of route information

# *OSPF*

- OSPF is a standard
  - Open Shortest Path First
  - IETF (Internet Engineering Task Force)
    - RFCs (Request For Comment) 1131, 1247, 1583, 2328

# OSPF Characteristcs

- *Full CIDR and Subnet Support* - OSPF supports 32 bit addresses and masks
- *Authenticated Exchanges* - Routers can be set to authenticate to each other before exchanging route information
- *Imported Routes* - OSPF can allow routes learned from other protocols
- *Link-State algorithm*
- *Admin assigned metrics*

# OSPF Mechanics

- Hierarchical Assignment
  - Each router is assigned a level in a hierarchy
    - The number of levels in an organization define the administrative area (responsibility) for each router
  - There must be at least 2 levels in the hierarchy
    - Logically this corresponds to the Internet (outside the organization) and LAN (inside the organization)
  - Only routers at the same level in the hierarchy exchange data

# OSPF Mechanics

- Route Determination
  - Routers at the same level in the hierarchy exchange Link-State Advertisements (LSAs)
    - Sometimes you can see these in Wireshark!
  - The LSA indicates a link is 'live' – after some time without an LSA the link is assumed to be 'dead'
  - Routers use the LSAs to build a graph representation of the known 'networks'
  - The Shortest-Paths algorithm is used to determine the best route to a known location

# Why use OSPF?

- Hierarchical strategy
  - Good for scalability, can handle many routers in an organization
  - Limits scope of LSAs
  - High administrative overhead and complex to implement, only high end devices typically support OSPF
- Because of the overhead, smaller organizations often pick RIP

# RIP

- The most simple Interior Gateway Protocol (IGP)
- One of the first TCP/IP routing protocols
- Originated in BSD Unix
  - routed
- Has become a standard over time
  - two different versions, RIP1 and RIP2

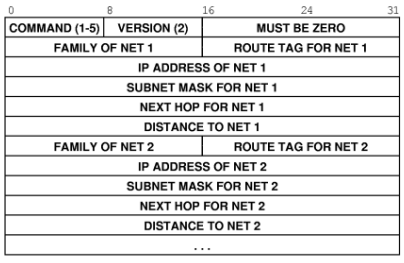
# RIP Characteristics

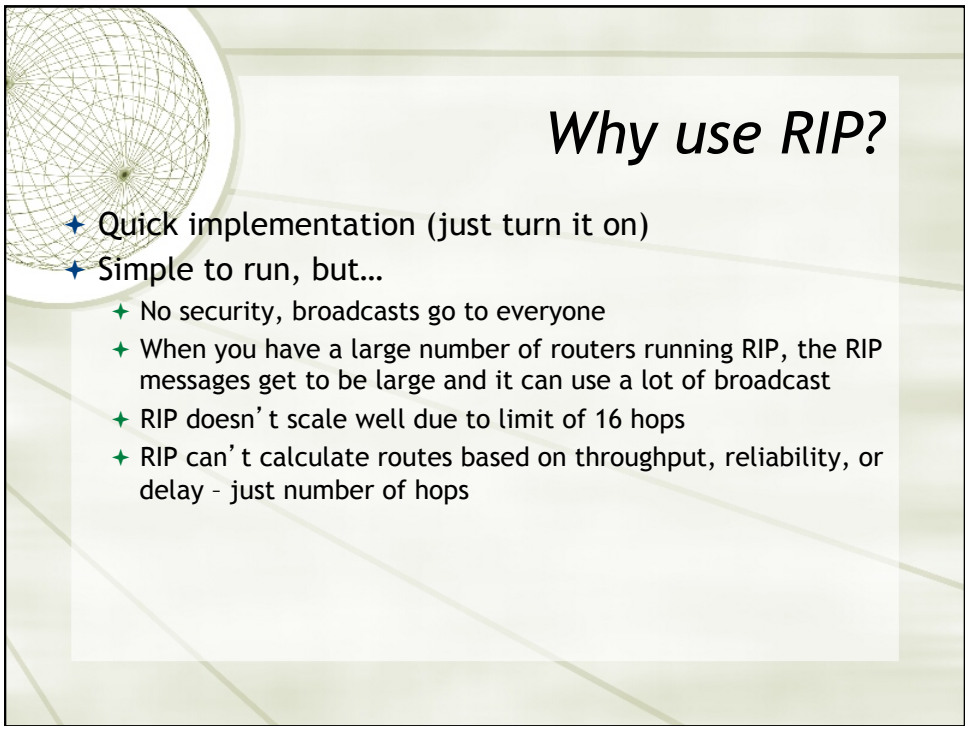
- *Hop Count Metric* - distance in hops
- *Unreliable delivery* through UDP
- *Broadcast or Multicast* delivery
- *Support for default route propagation*
- *Passive route detection* - by listening to route information

# RIP Mechanics

- Each RIP router periodically broadcasts its whole route table
  - Sometimes you can see these in Wireshark!
- When a RIP message is received, the router compares its internal table with the route table it received
- If the router that sent the RIP message knows a shorter path to a network, accounting for the cost of sending to that router, then the new route replaces the old route
- Any route longer than 16 hops on the network is considered unreachable

# RIP Packet Format




Why use RIP?
Quick implementation (just turn it on)
Simple to run, but…
No security, broadcasts go to everyone
When you have a large number of routers running RIP, the RIP messages get to be large and it can use a lot of broadcast
RIP doesn't scale well due to limit of 16 hops
RIP can't calculate routes based on throughput, reliability, or delay – just number of hops