



SCION: Architecture Overview

Adrian Perrig

Network Security Group, ETH Zürich

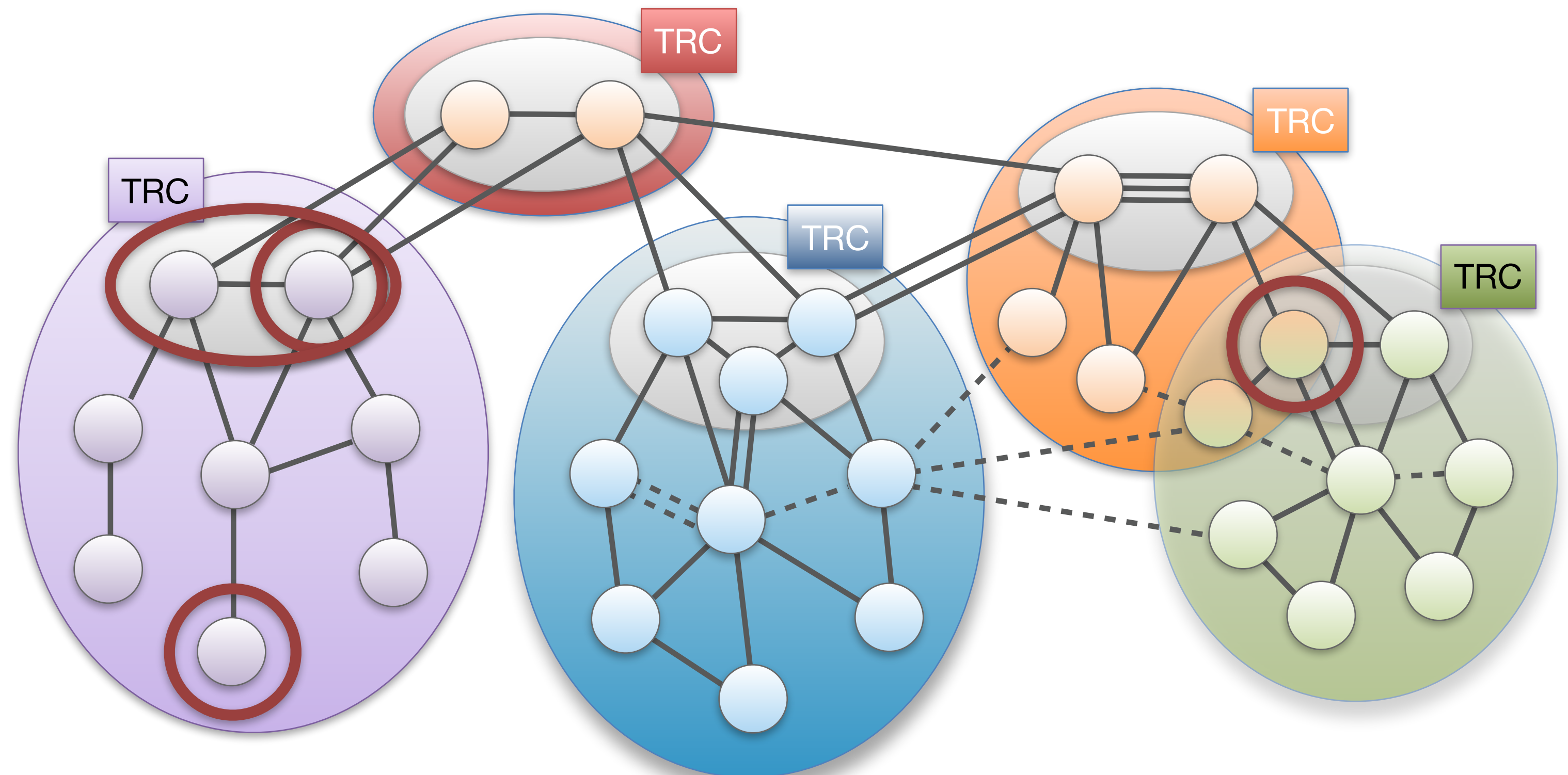
SCION Architectural Design Goals

- **High availability**, even for networks with malicious parties
 - Adversary: access to management plane of router
 - Communication should be available if adversary-free path exists
- **Secure entity authentication**
that scales to global heterogeneous (dis)trusted environment
- **Flexible trust**: operate in heterogeneous trust environment
- **Transparent operation**: clear what is happening to packets and whom needs to be relied upon for operation
- **Balanced control** among ISPs, senders, and receivers
- **Scalability, efficiency, flexibility**



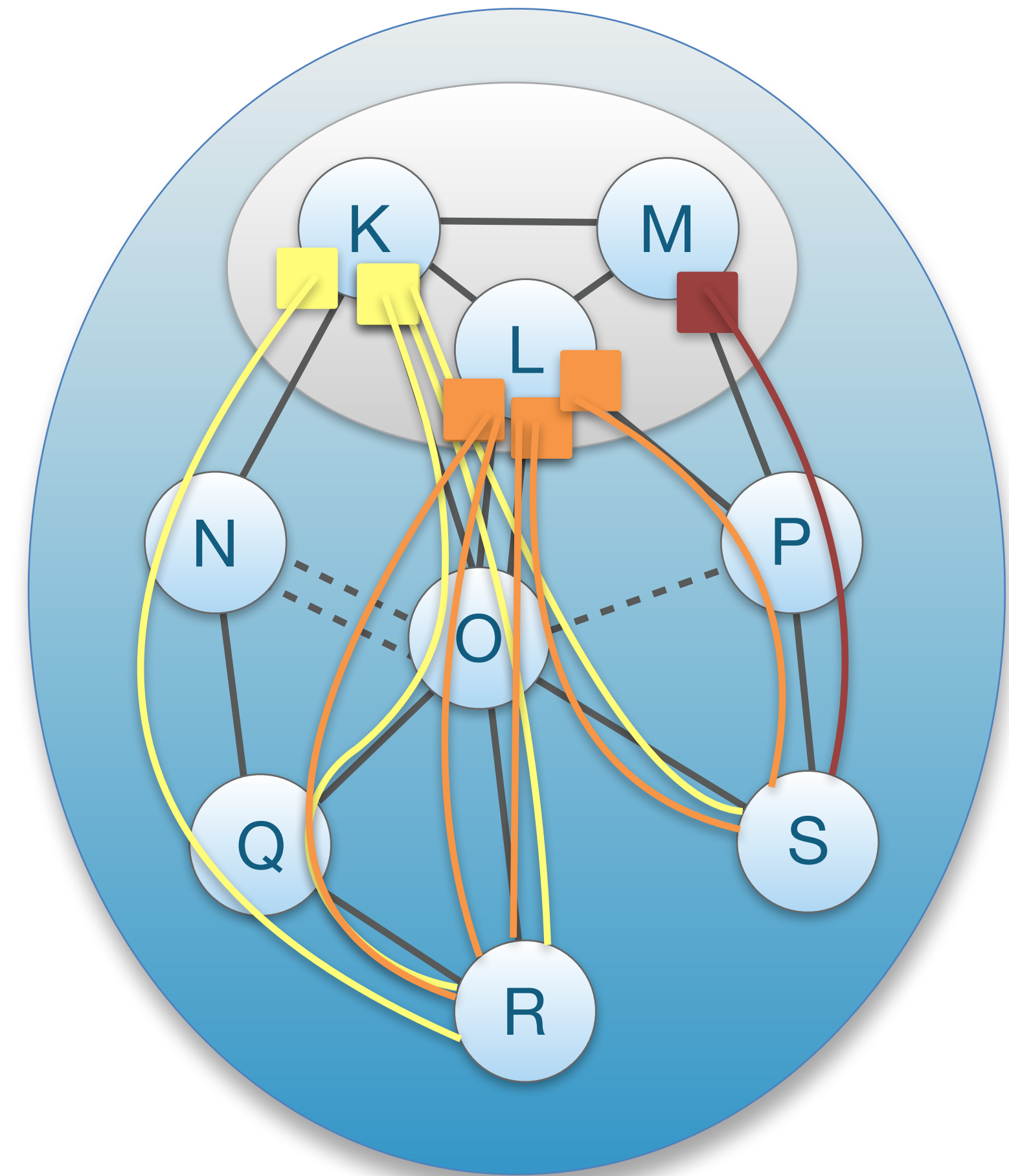
Approach for Scalability: Isolation Domain (ISD)

- Isolation Domain (ISD): grouping of ASes
- ISD core: ASes that manage the ISD
- Core AS: AS that is part of ISD core
- Control plane is organized hierarchically
 - Inter-ISD control plane
 - Intra-ISD control plane



Intra-ISD Path Exploration: Beaconing

- Core ASes K, L, M initiate Path-segment Construction Beacons (PCBs), or “beacons”
- PCBs traverse ISD as a flood to reach downstream ASes
- Each AS receives multiple PCBs representing path segments to a core AS

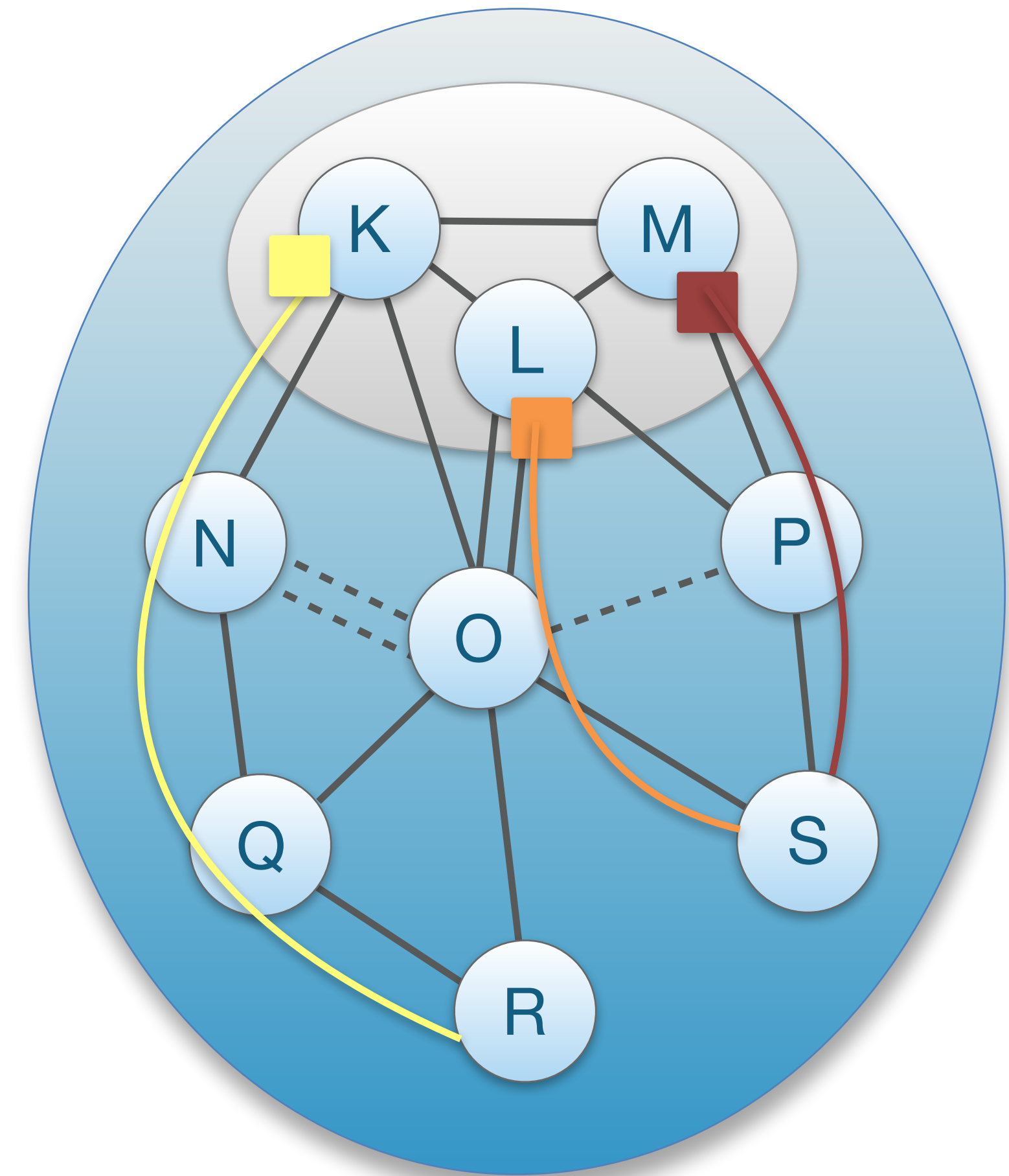


Path Property Dissemination

- Beacon binds properties to paths
- Per-AS information included
 - MTU
 - Available bandwidth
 - Path policy
 - Services supported
 - Cryptographic algorithms supported

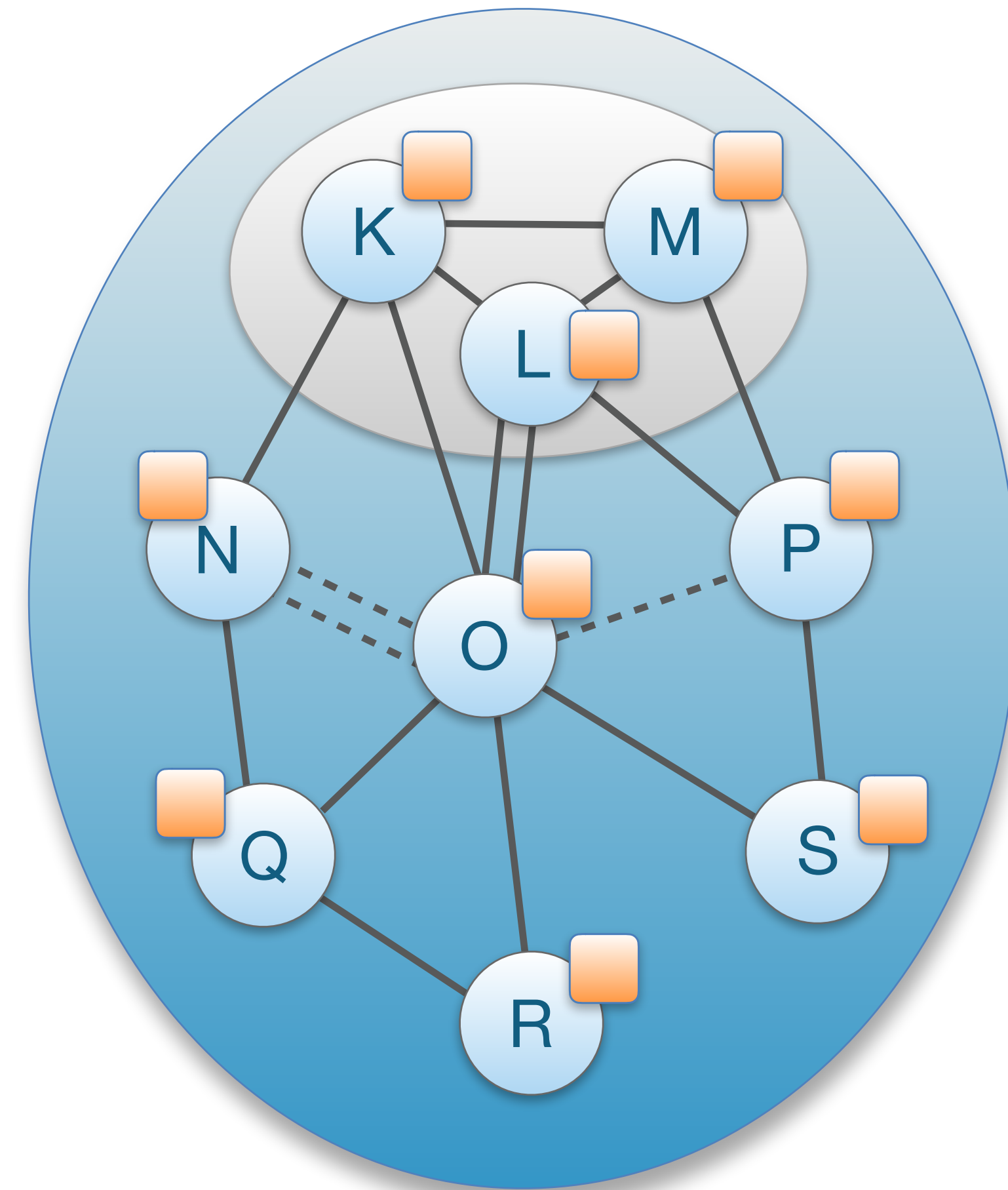
Up-Path and Down-Path Segments

- Intra-ISD beaconing process sends PCBs to ASes
- PCBs contain **path segments** that can be used as communication paths to communicate with the core AS that initiated it
- **Up-path segment**: PCB is used from AS to core AS
 - Example: $R \rightarrow K$
- **Down-path segment**: PCB is used from core AS to AS
 - Example: $M \rightarrow S$



Path Server Infrastructure

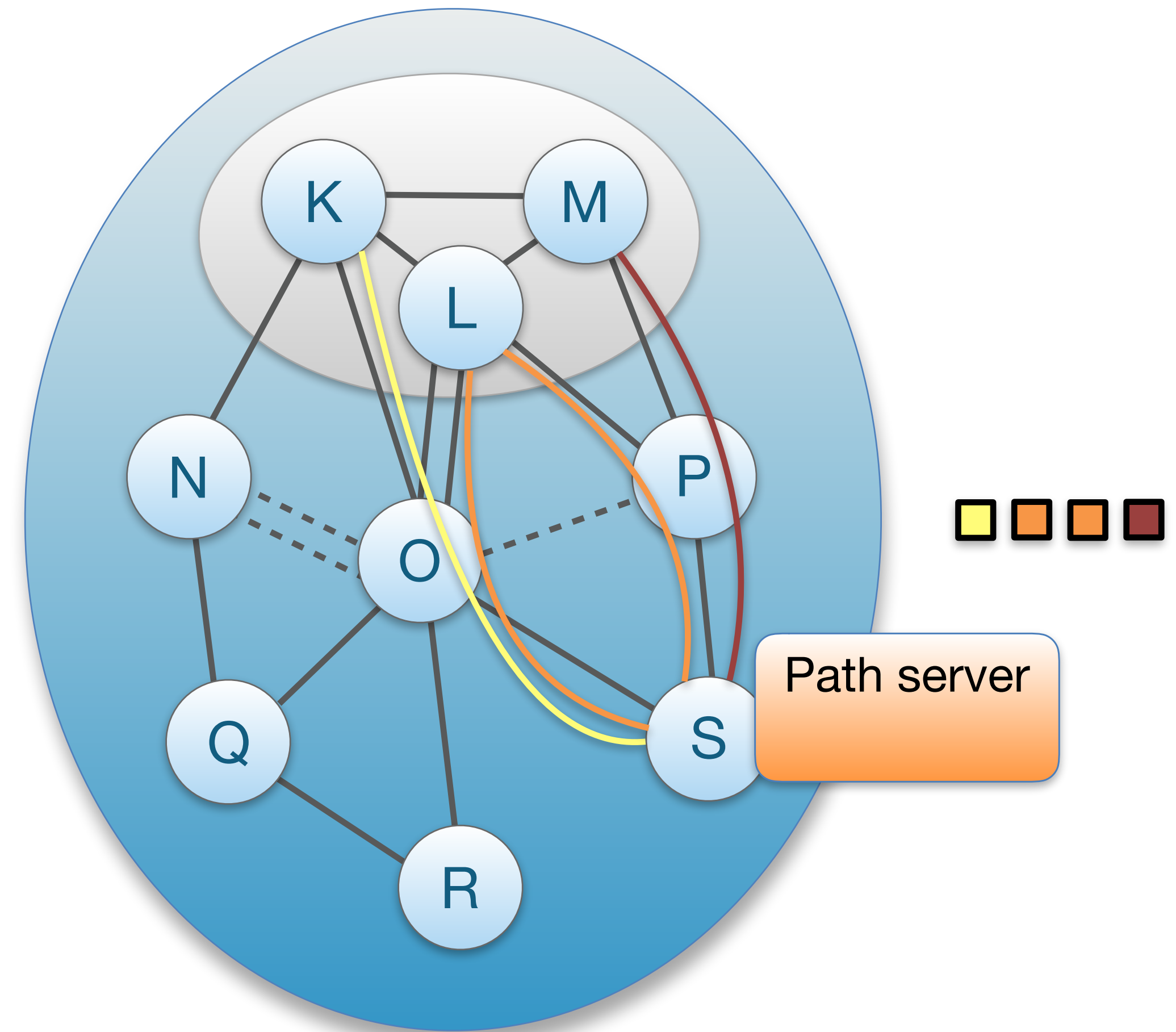
- Each AS operates path server(s)
- Path servers offer lookup service:
 - ISD, AS → down-path segments, core-path segments
 - Local up-path segment request → up-path segments to core ASes
- Core ASes operate core path server infrastructure
- Each non-core AS runs local path servers
 - Serves up-path segments to local clients
 - Resolves and caches response of remote AS lookups



 Path server

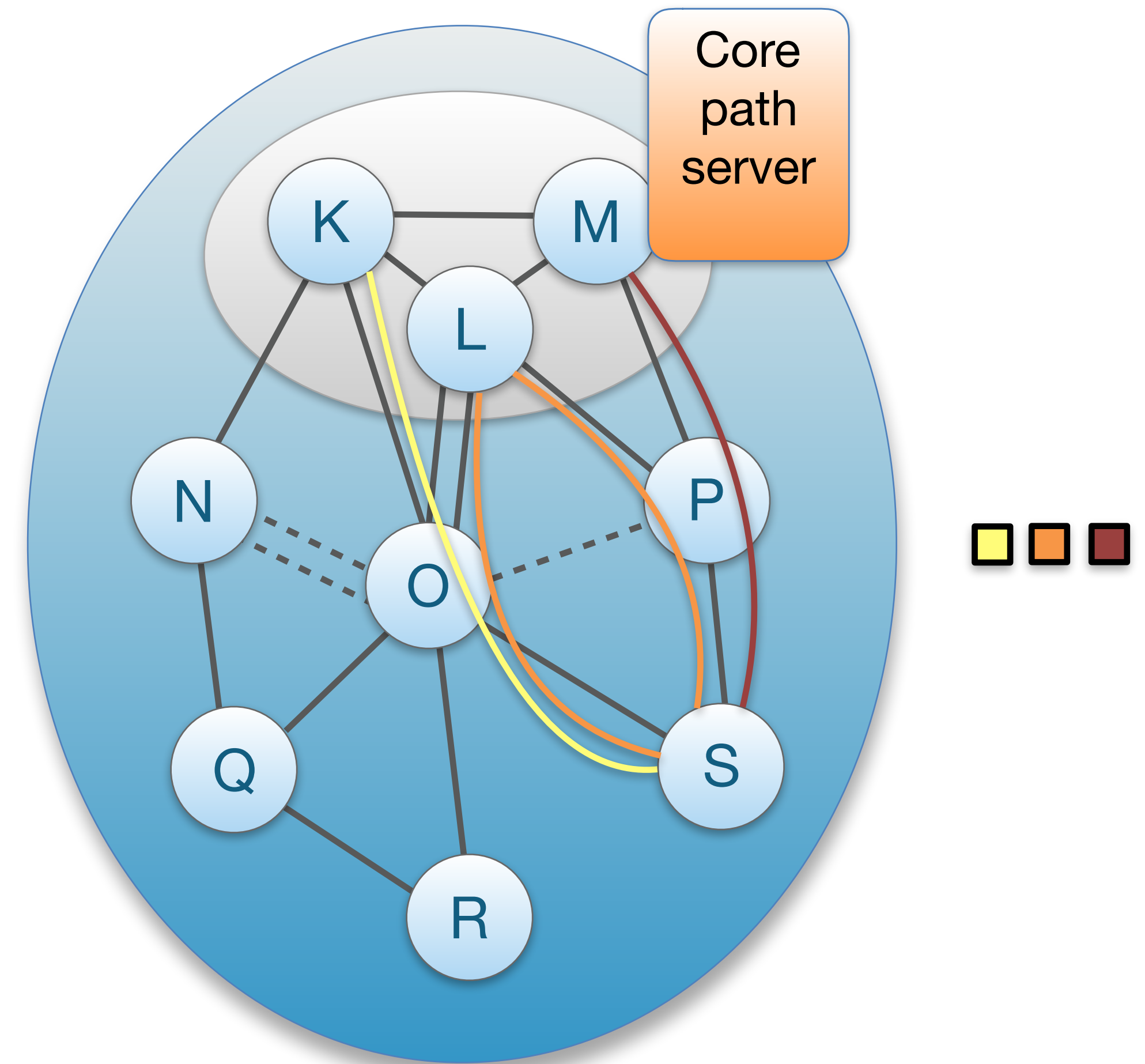
Up-Path Segment Registration

- AS selects path segments to announce as **up-path segments** for local hosts
- Up-path segments are registered at local path servers

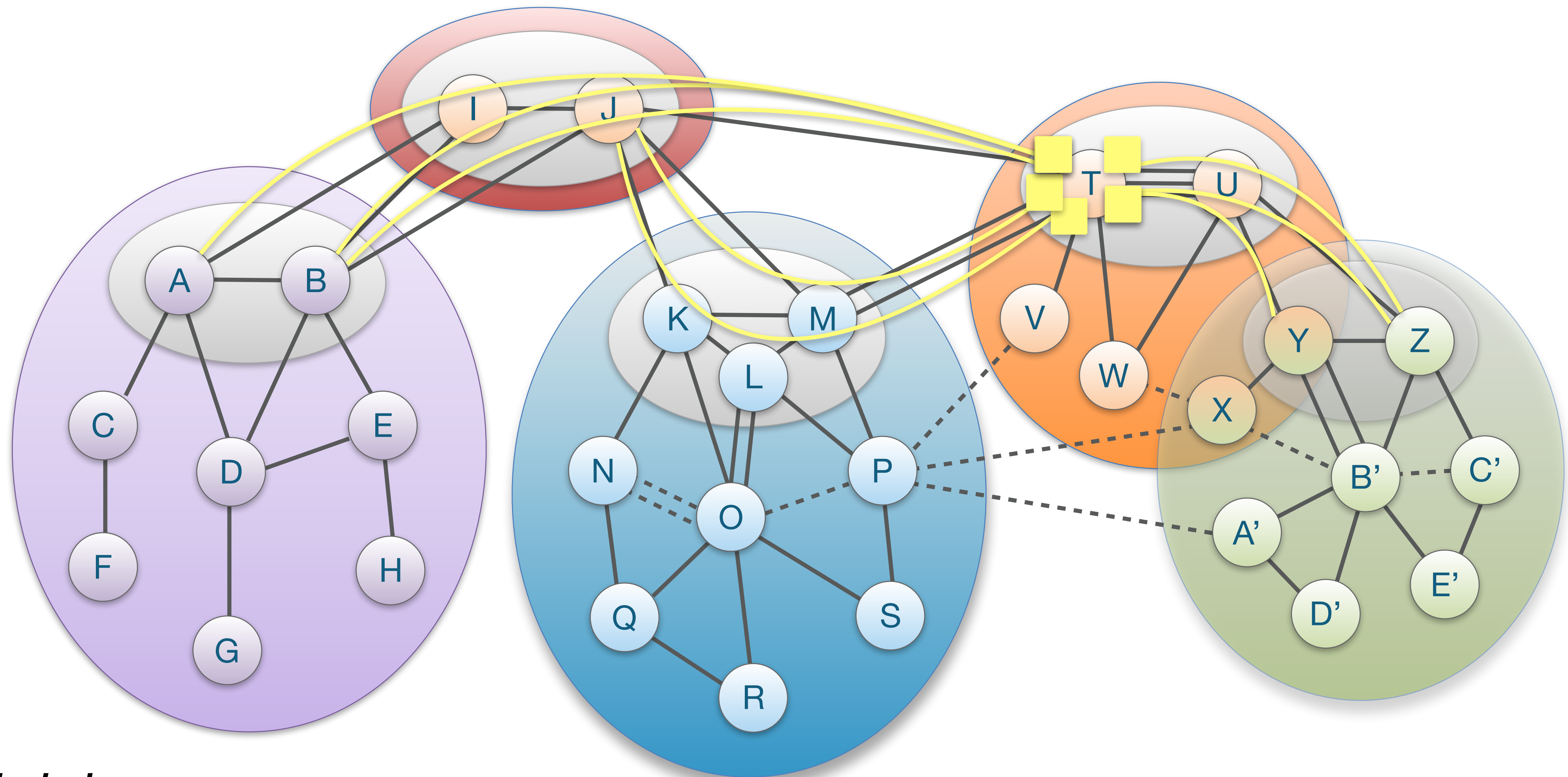


Down-Path Segment Registration

- AS selects path segments to announce as **down-path segments** for others to use to communicate with AS
- Down-path segments are uploaded to core path server in core AS



Inter-ISD Path Exploration: Sample Core-Path Segments from AS T

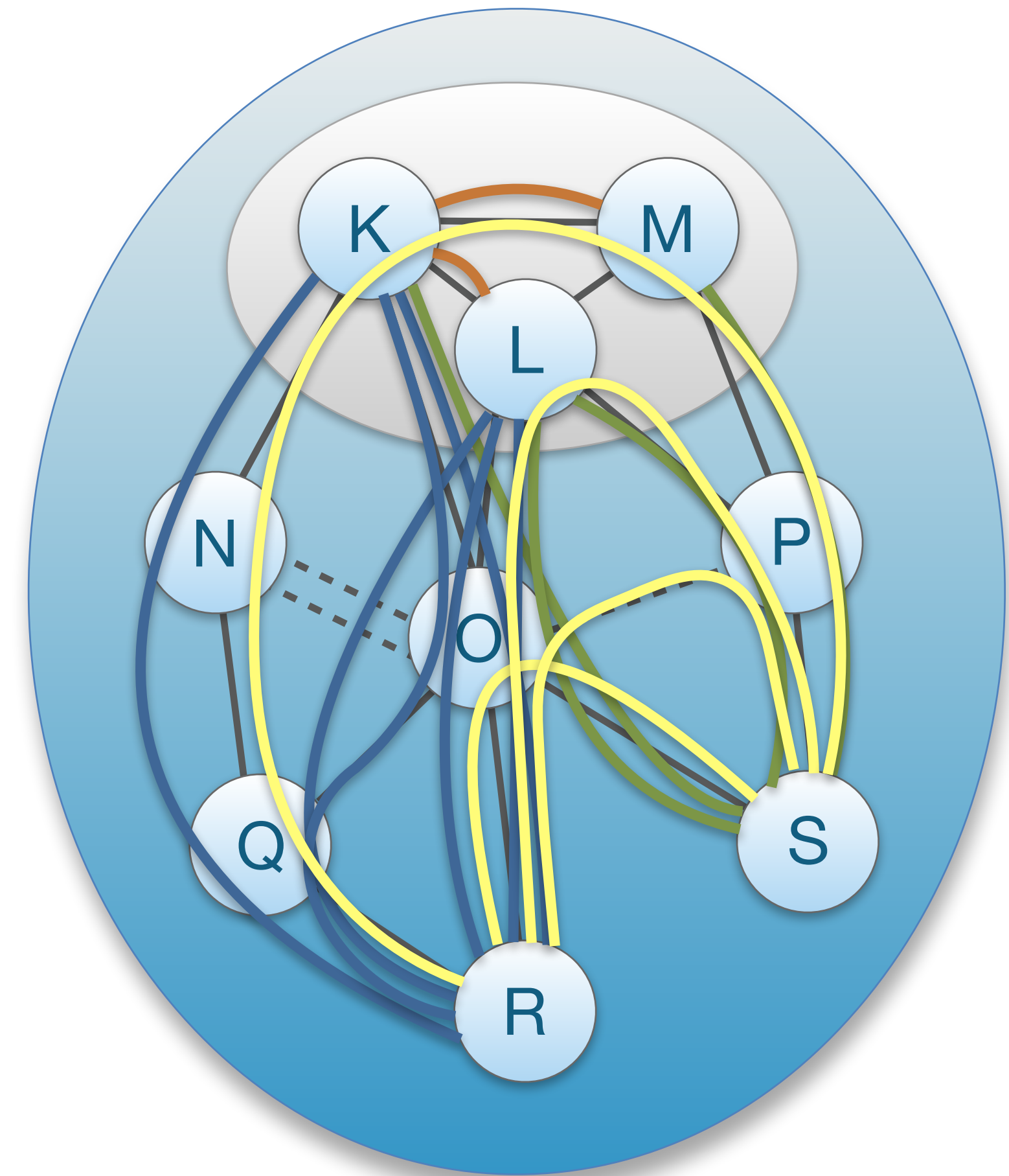


Path Lookup

- Steps of a host to obtain path segments
 - Host contacts RAINS server with a name
H → RAINS: www.scion-architecture.net
RAINS → H: ISD X, AS Y, local address Z
 - Host contacts local path server to query path segments
H → PS: ISD X, AS Y
PS → H: up-path, core-path, down-path segments
 - Host combines path segments to obtain end-to-end paths, which are added to packets

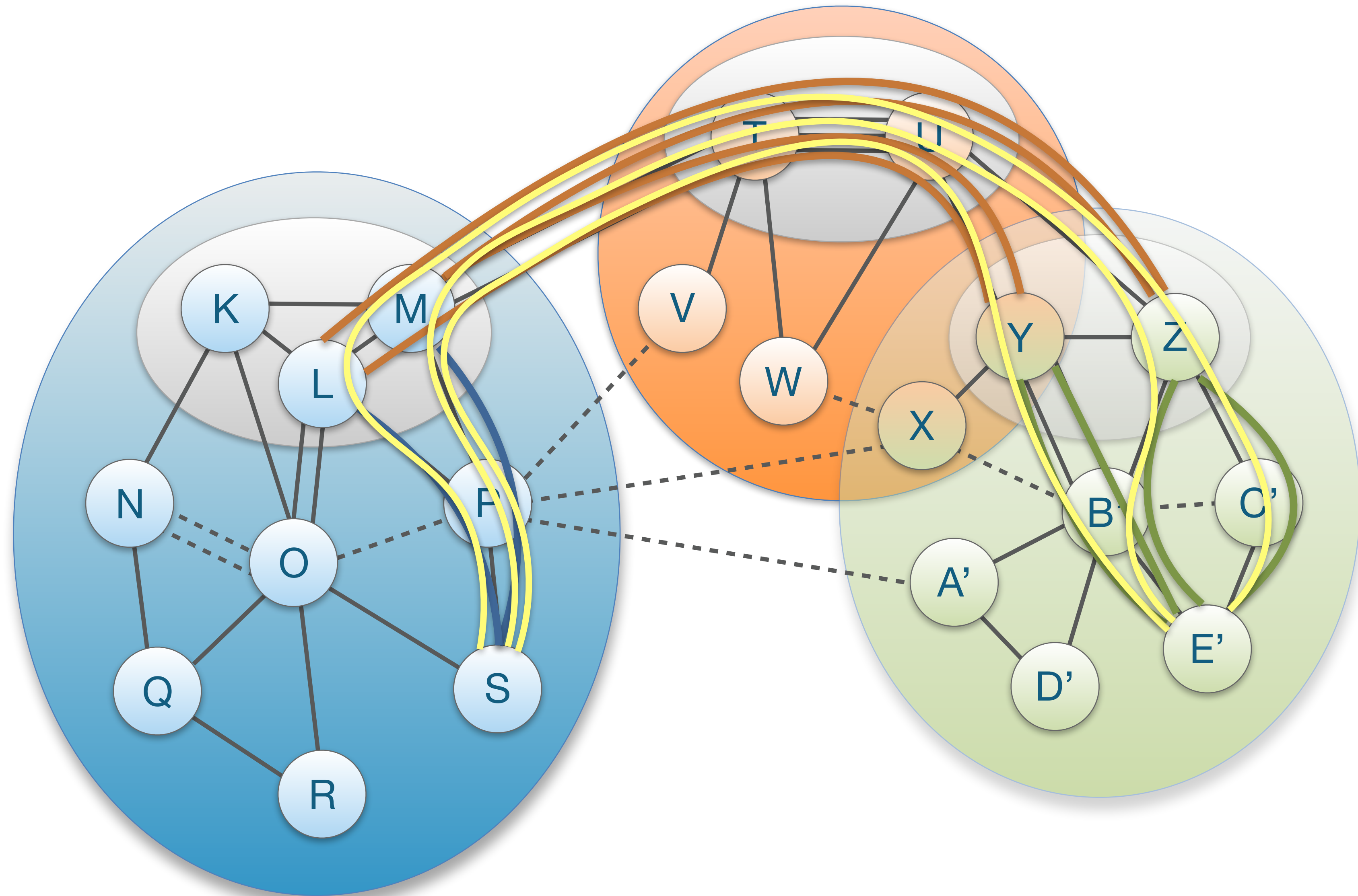
Path Lookup and Combination: Local ISD

- Client requests path segments to $\langle \text{ISD}, \text{AS} \rangle$ from local path server
- If down-path segments are not locally cached, local path server send request to core path server
- Local path server replies
 - Up-path segments to local ISD core ASes
 - Down-path segments to $\langle \text{ISD}, \text{AS} \rangle$
 - Core-path segments as needed to connect up-path and down-path segments



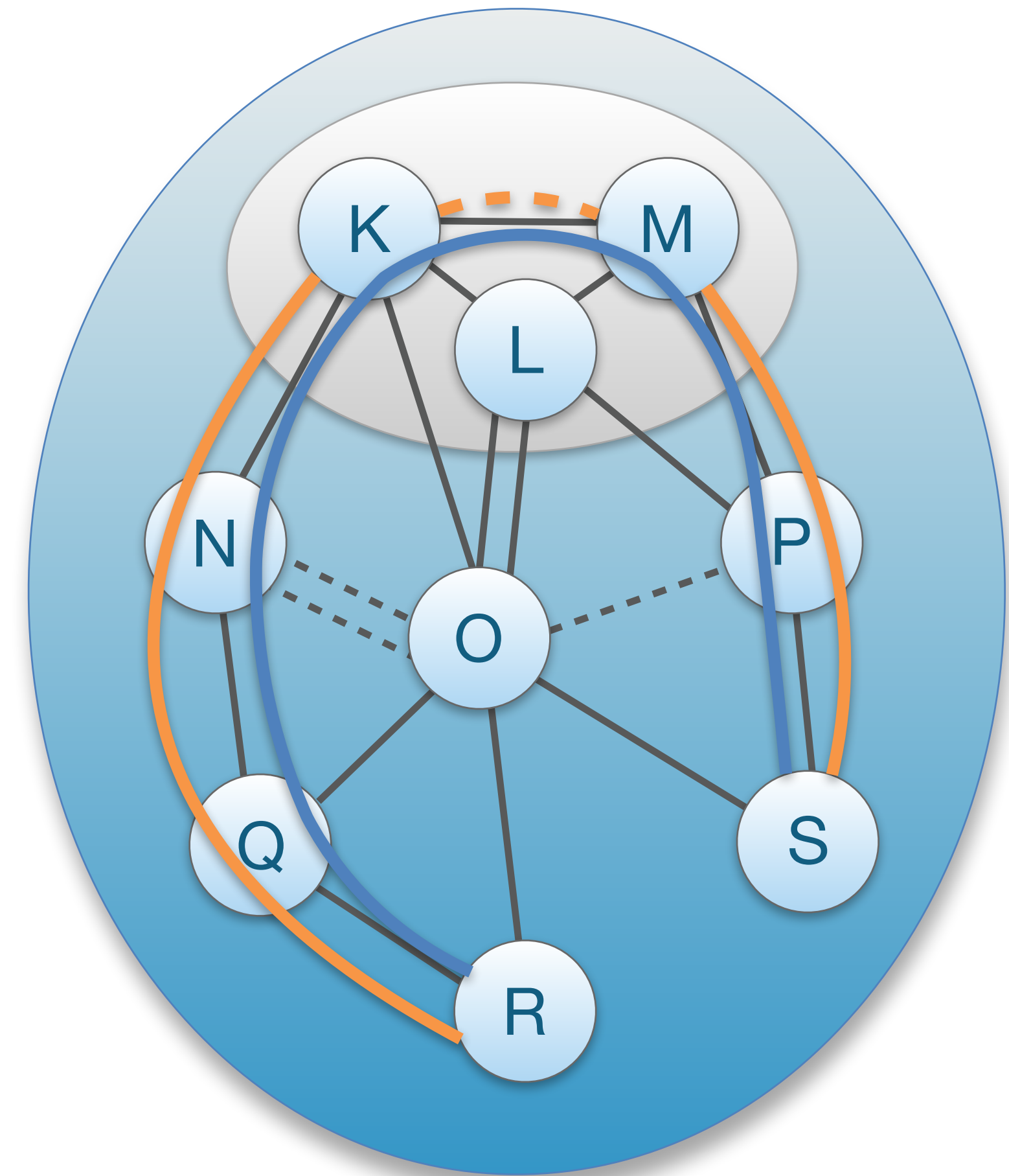
Path Lookup and Combination: Remote ISD

- Host contacts local path server requesting $\langle \text{ISD}, \text{AS} \rangle$
- If path segments are not cached, local path server will contact core path server
- If core path server does not have path segments cached, it will contact remote core path server
- Finally, host receives up-, core-, and down-segments



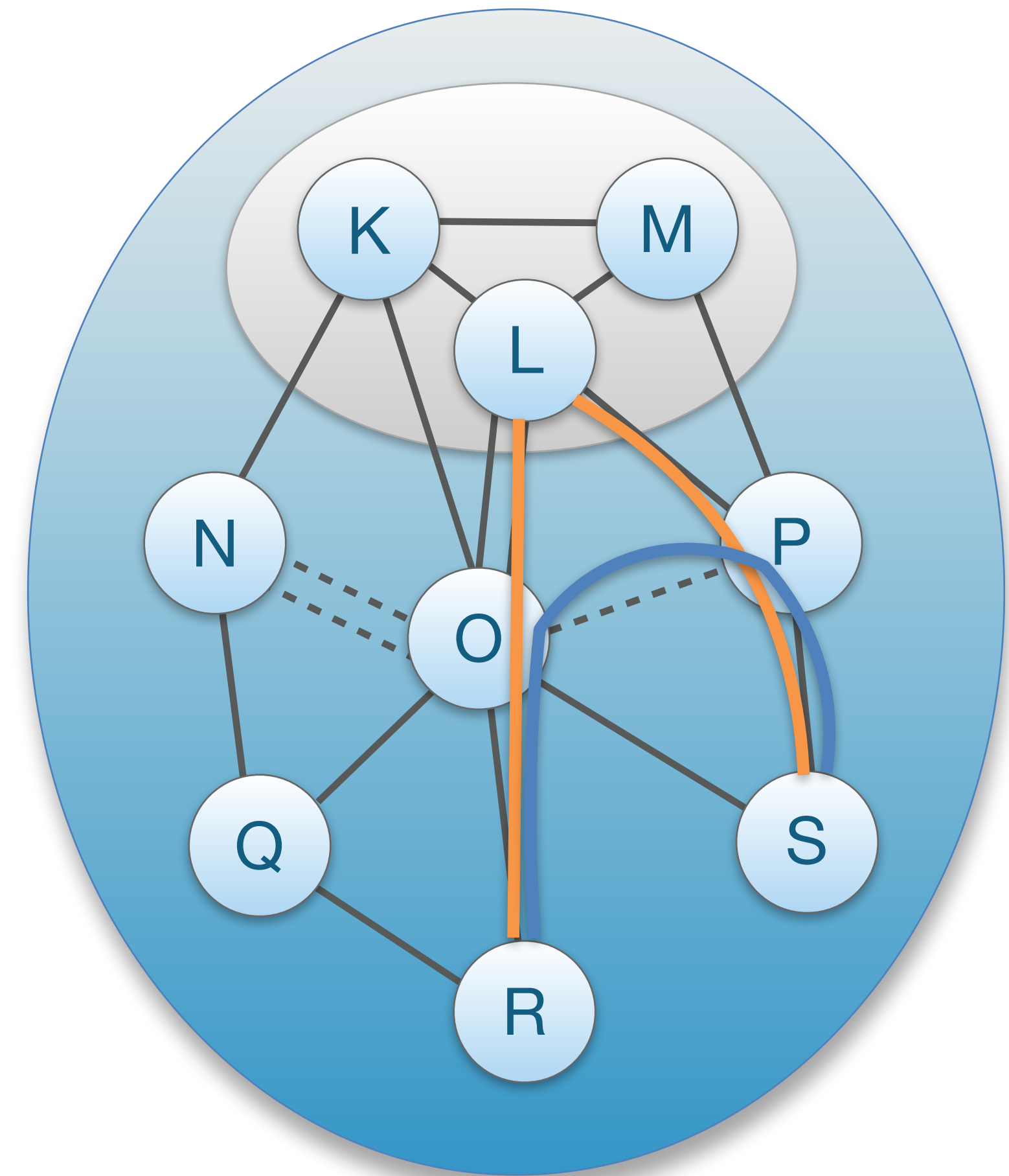
Path Combination Example (1)

- Core-segment combination:
Up-path segment +
core-path segment +
down-path segment



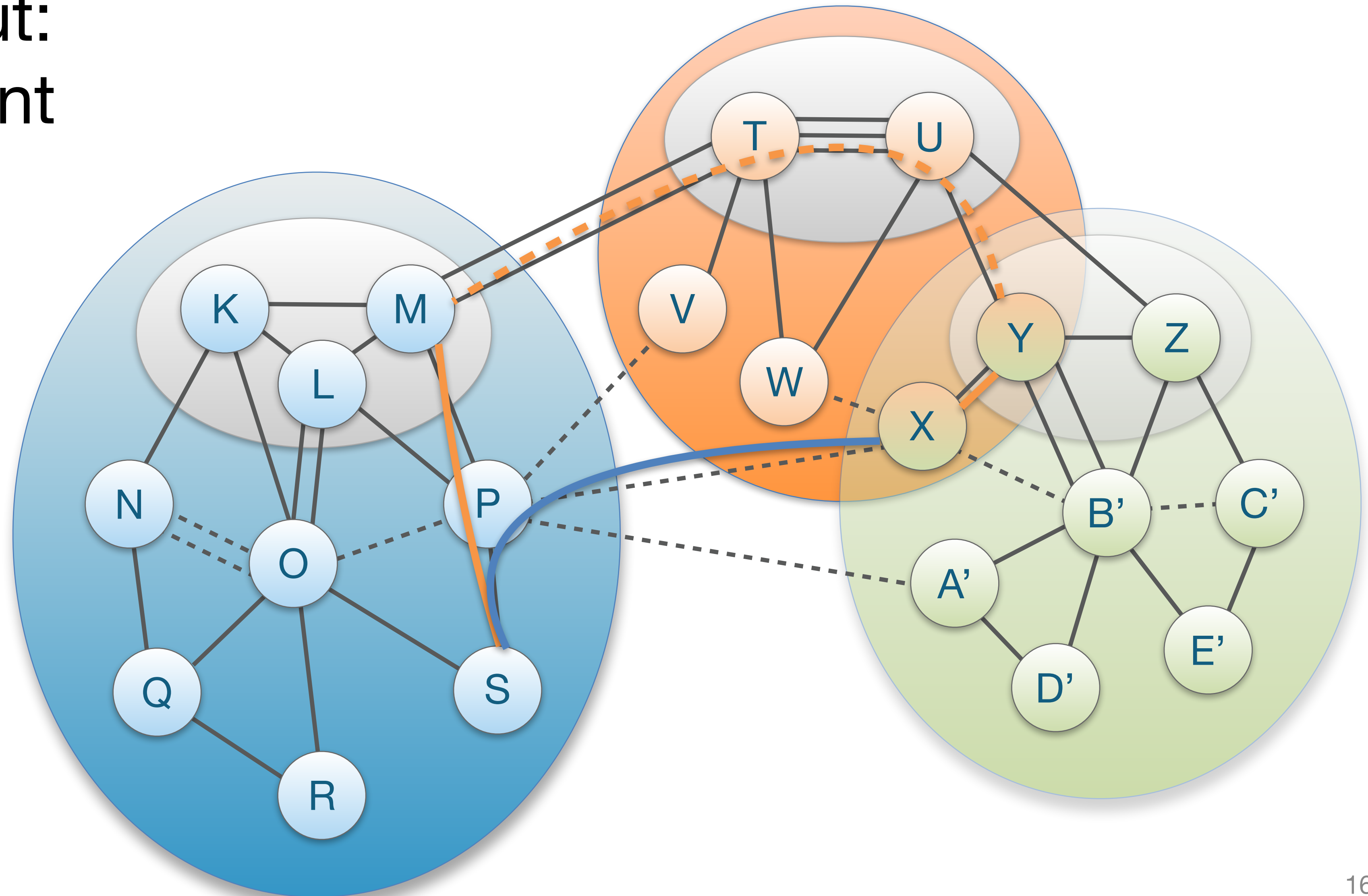
Path Combination Example (2)

- Peering shortcut: up-path segment and down-path segment offer same peering link



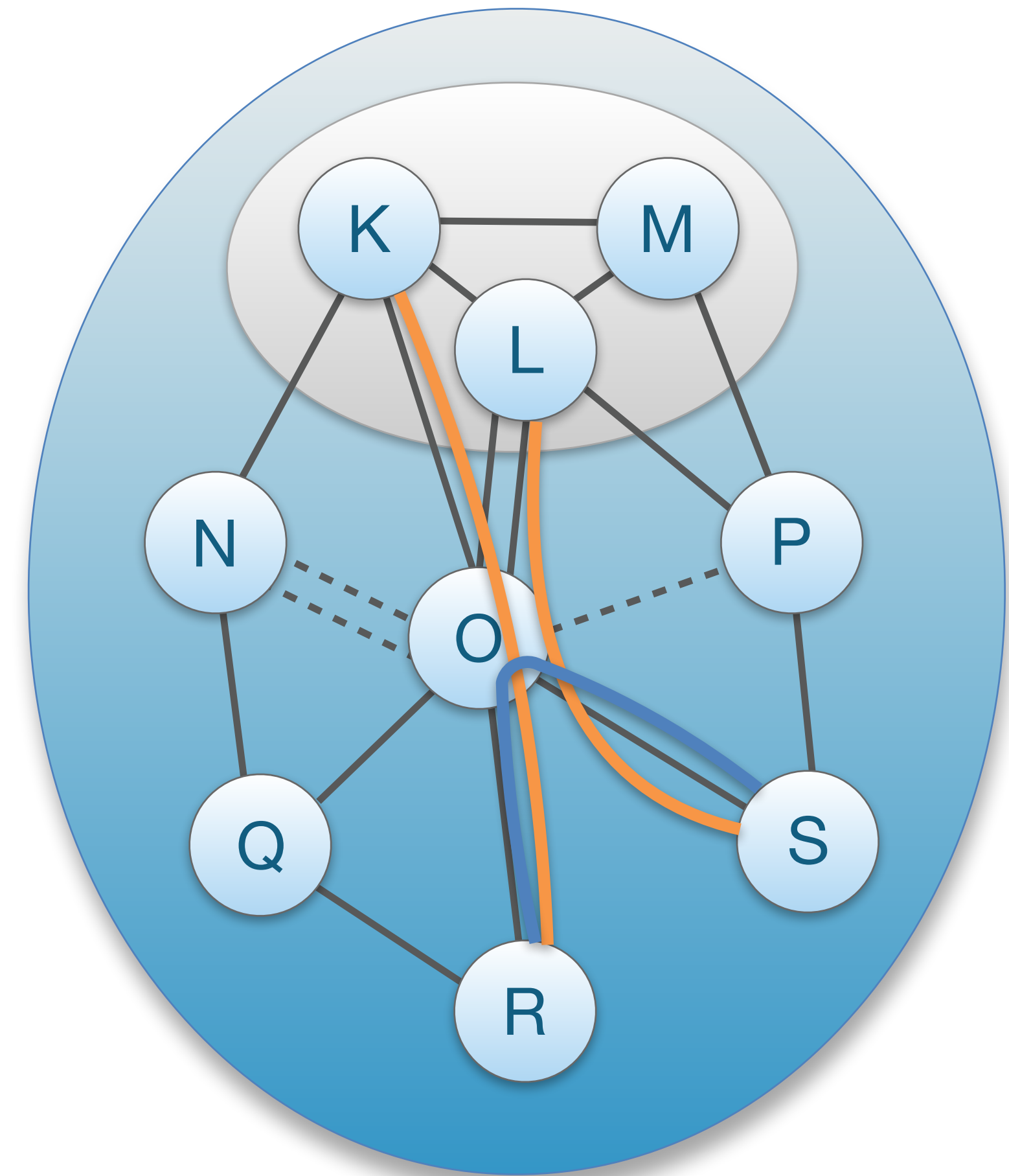
Path Combination Example (3)

- Peering shortcut: up-path segment and down-path segment offer same peering link



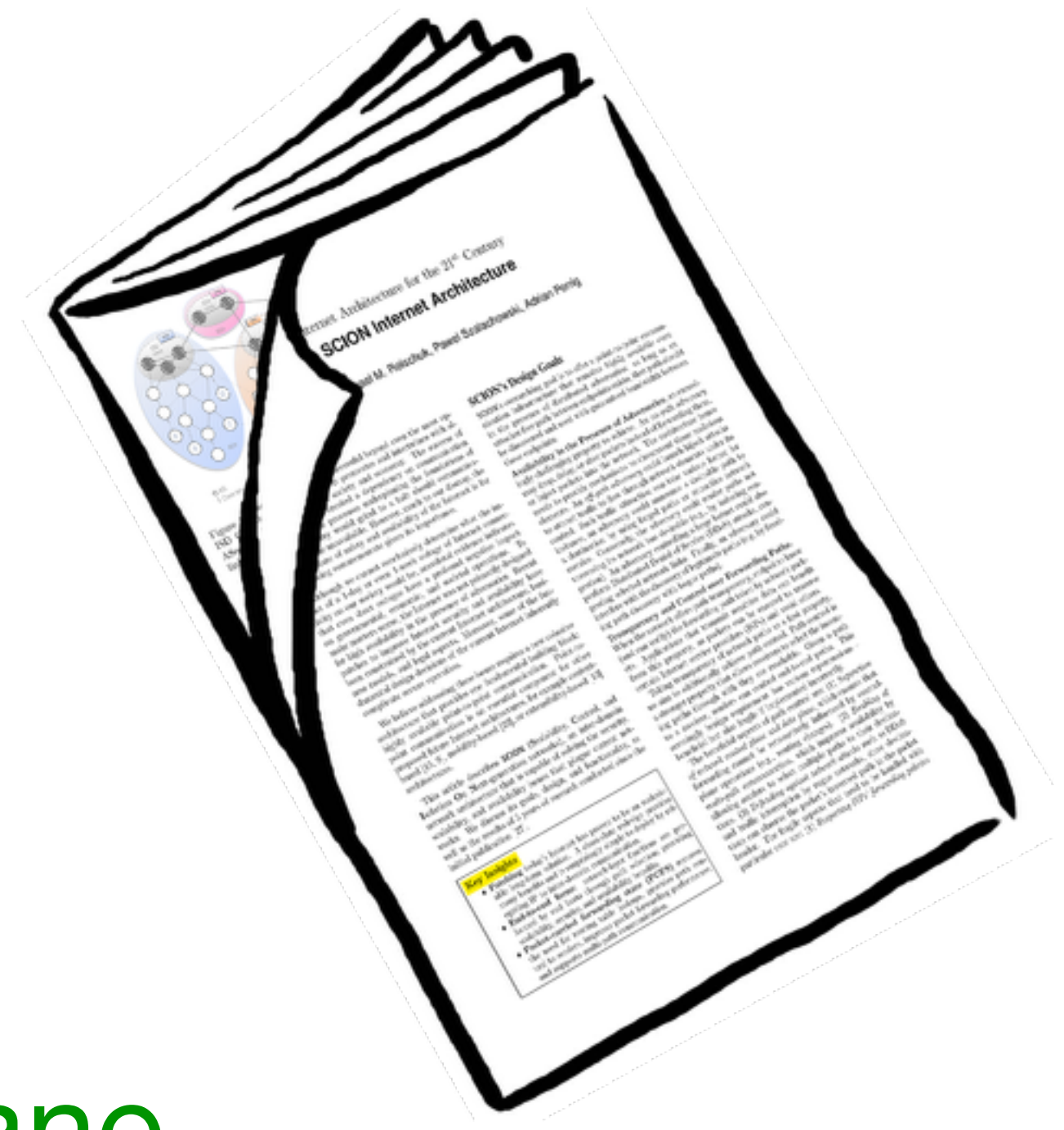
Path Combination Example (4)

- AS shortcut path through common AS on up-path and down-path segment



SCION Summary

- Complete re-design of network architecture resolves numerous fundamental problems
 - Path control by senders and receivers
 - Rich path property discovery through beaconing
 - Root of trust selectable by each ISD
 - Meaningful multipath with end point control
 - Receiver control of announced paths
- An **isolation architecture** for the **control plane**, but a **transparency architecture** for the **data plane**.



For More Information ...

- ... please see our web page:
www.scion-architecture.net
- Chapter 2 of our book “SCION: A secure Internet Architecture”
 - Available from Springer this Summer 2017
 - PDF available on our web site