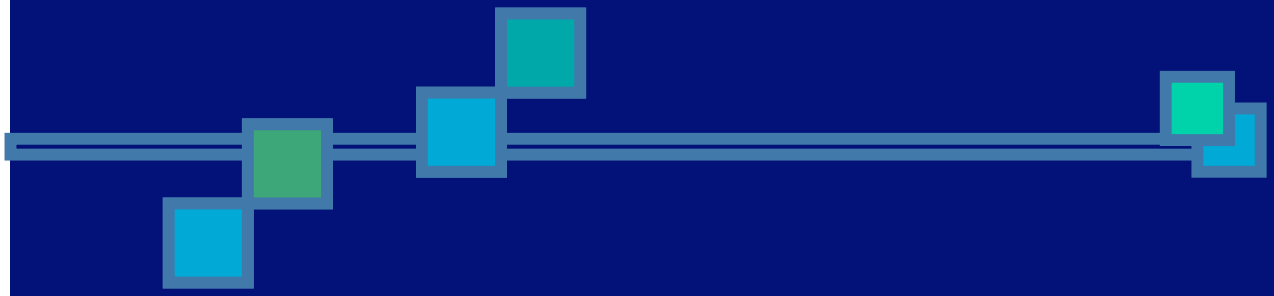
Peer to Peer Infrastructure : QoS enabled traffic prioritization

Mary Barnes (mary.barnes@nortel.com)
Bill McCormick (billmcc@nortel.com)



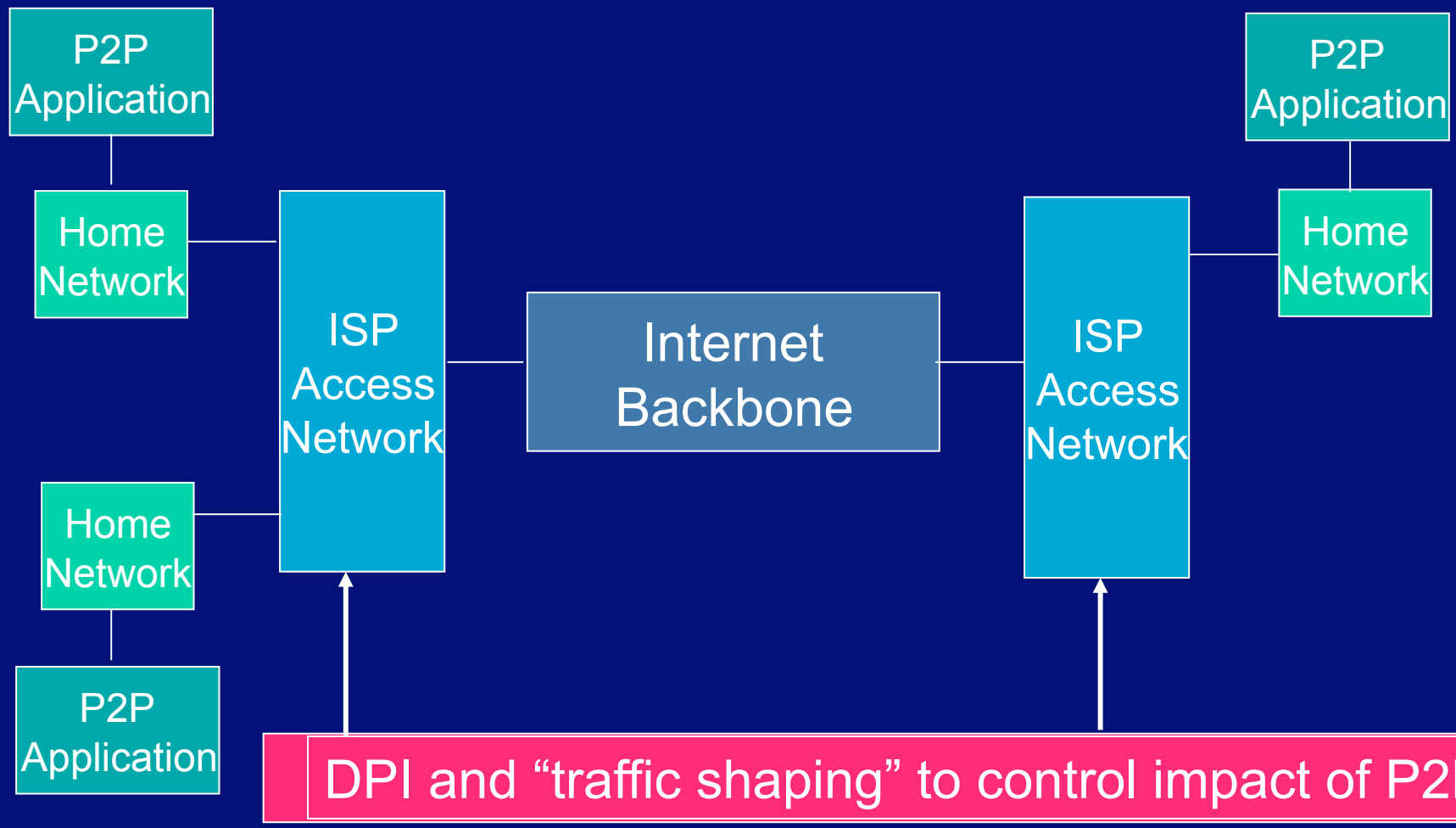
Overview

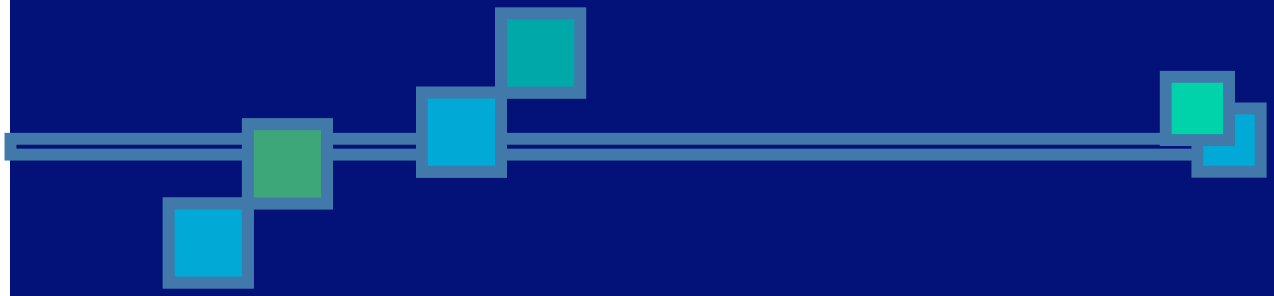
- Discuss the mechanisms and implications of deploying QoS enabled equipment to support traffic prioritization

Current Traffic Prioritization Approaches:

- Many service providers are implementing deep packet inspection as a means of prioritizing traffic on their networks.
  - This approach is not viable for the long term due to the limitations in being able to determine types of traffic.
- Other alternatives include traffic analysis in an attempt to detect user networks engaged in peer to peer applications.
  - Processing overhead for this approach limits the feasibility.

Current Network Infrastructure Mechanisms

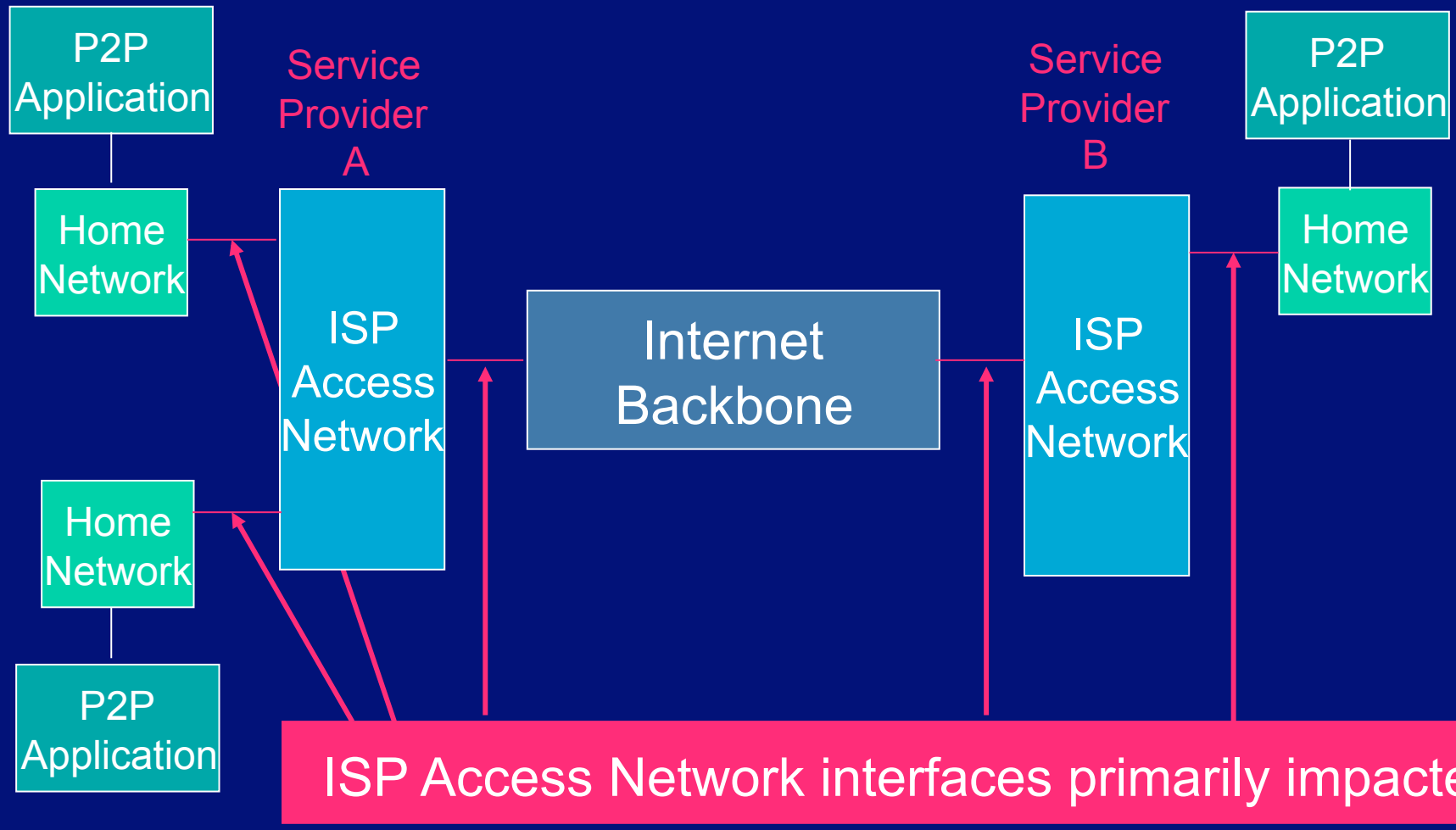




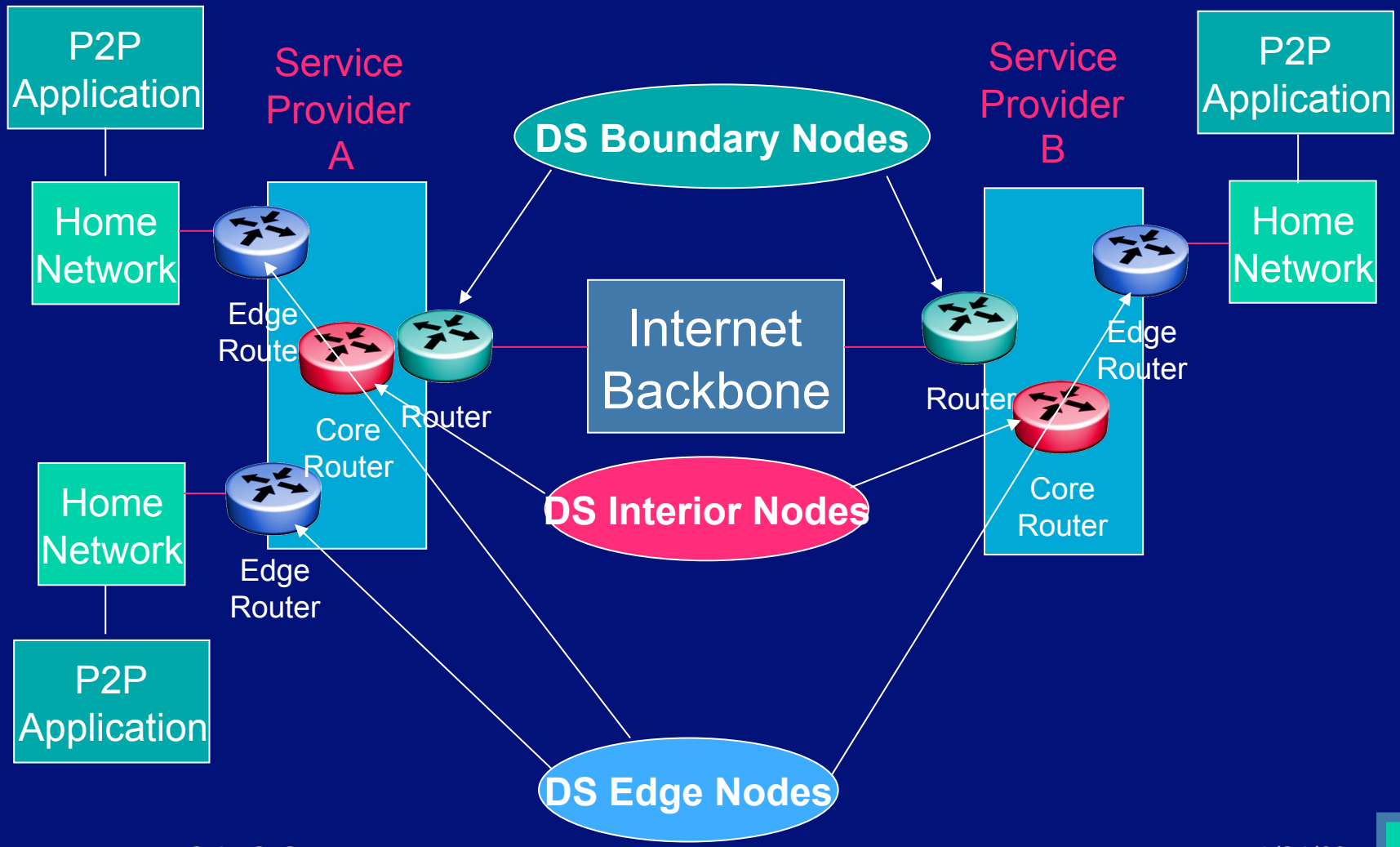
Traffic Prioritization Approach:

- Rather than rely on ad hoc methods of traffic control, consider the use of designed in traffic prioritization such as DiffServ Code Points (DSCP).
- This approach allows service providers and network operators to charge for use in a straightforward manner.
- DSCP is a simple, reliable approach.

Network Infrastructure Implications



DiffServ Network Example

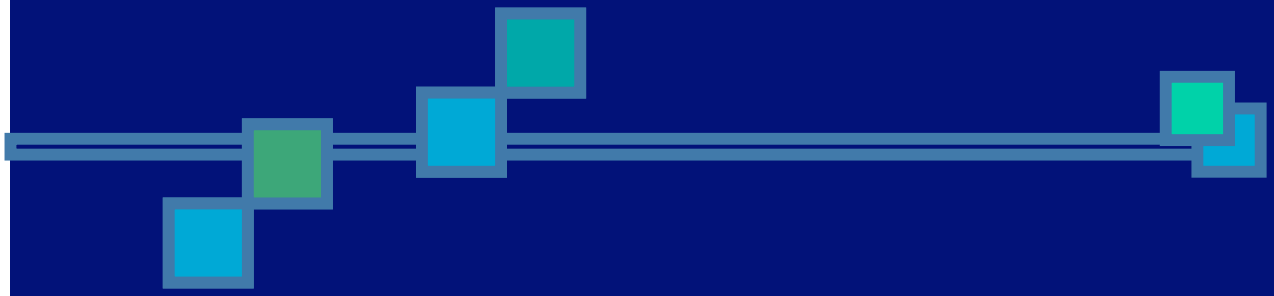


DiffServ Advantages:

- DiffServ devices at the edge mark the packets in a manner to describe the service level they should receive.
  - Appropriate class to support inelastic traffic is already in place.
- Stateless approach of DiffServ minimizes the need for nodes in the network to remember anything about flows.
  - Applications don't need to request a particular service level or provide advance notice about where traffic is going
- Practical to implement:
  - Equipment to support DSCP is already available.

Additional Considerations:

- Provisioning and managing the network to ensure adequate resources for high priority traffic is still required:
  - Charging based on usage could help to minimize the impact of “always on” high bandwidth applications
  - Alternatively or in addition, consider engineering the network to support max usage by top tier customers (still in effect “paying per use”).
  - Additional modeling is likely required to fully understand the impacts.
- Provisioning and managing must still consider events causing peak usage.



Backup

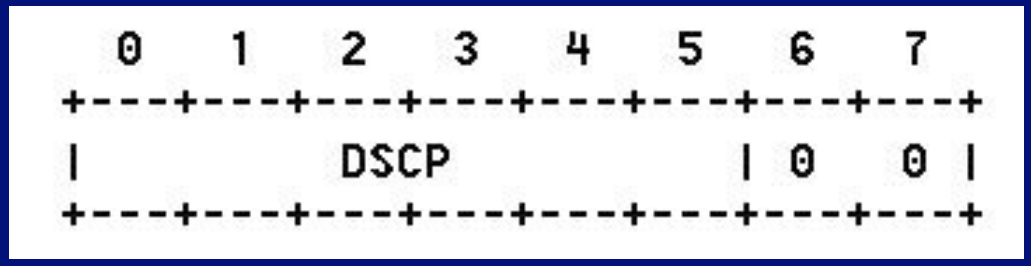
- Diffserv overview

IP Differentiated Services (DiffServ)

- Defines DiffServ Code Point (DSCP) tag in IP packet header
  - to indicate QoS level packet is to receive
- Defines network elements into 3 types based on functionality:
  - Edge, Boundary, Interior
- Defines how packets are treated hop-by-hop throughout network
  - Referred to as Per Hop Behavior (PHB) treatment
- Basic behaviors (with multiple levels within each behavior type)
  - Expedited Forwarding - Used for Voice services
  - Assured Forwarding - Used for Real-time and Non-real-time services
  - Class Selector - Used to support legacy routers
  - Default Forwarding (Best Effort) - Used for everything else

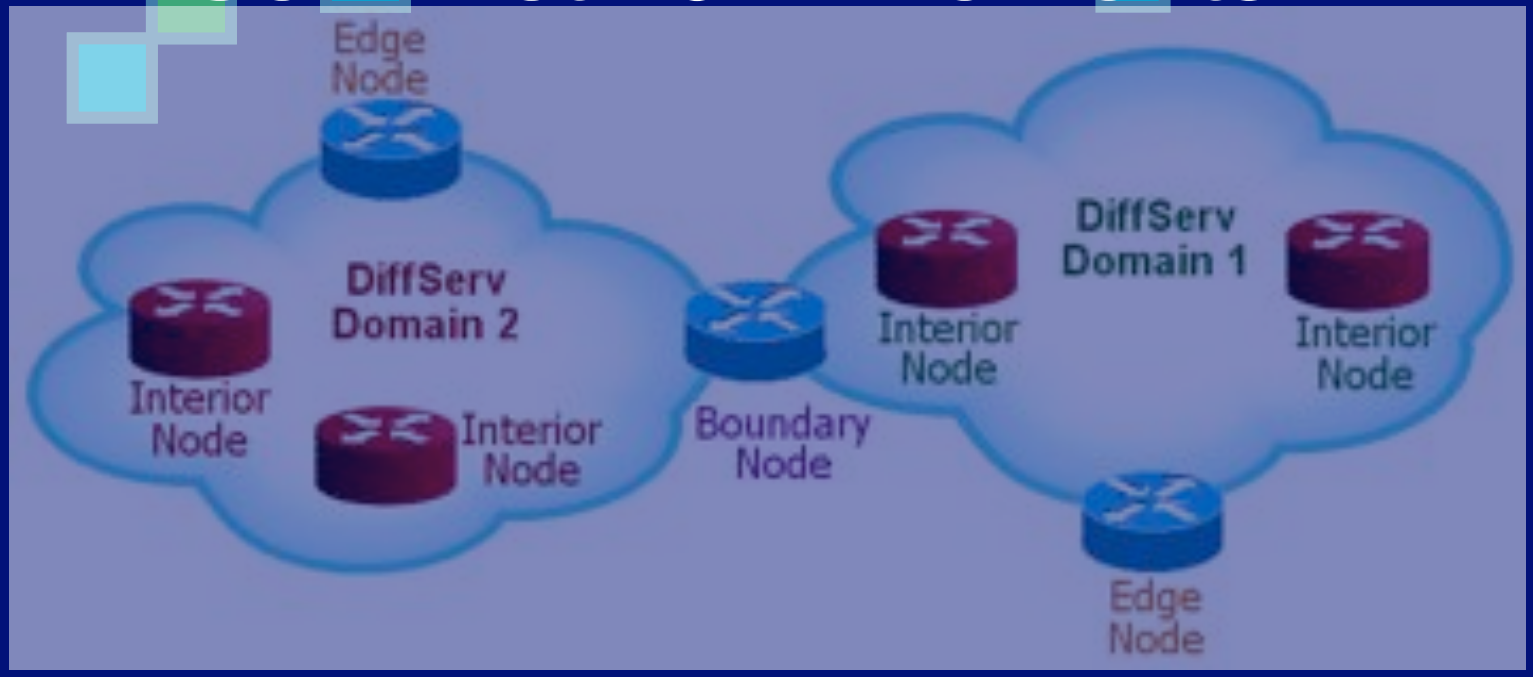
DiffServ (DS) Field vs. ToS Field

- 8-bit field in IP Header defined in RFC 2474
- The DS Field contains the DS Code Point (DSCP)

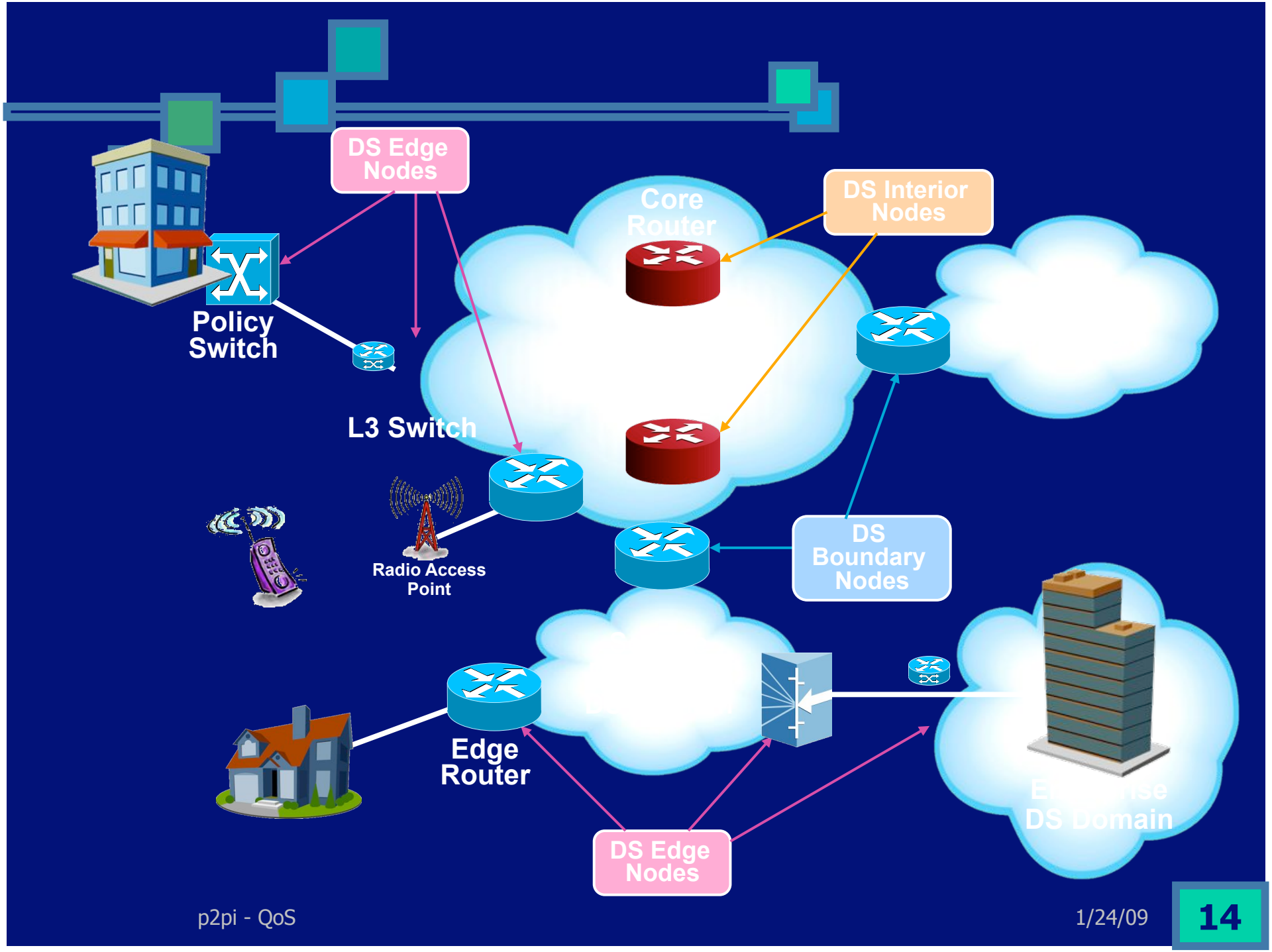


DS Field

DiffServ Network Elements

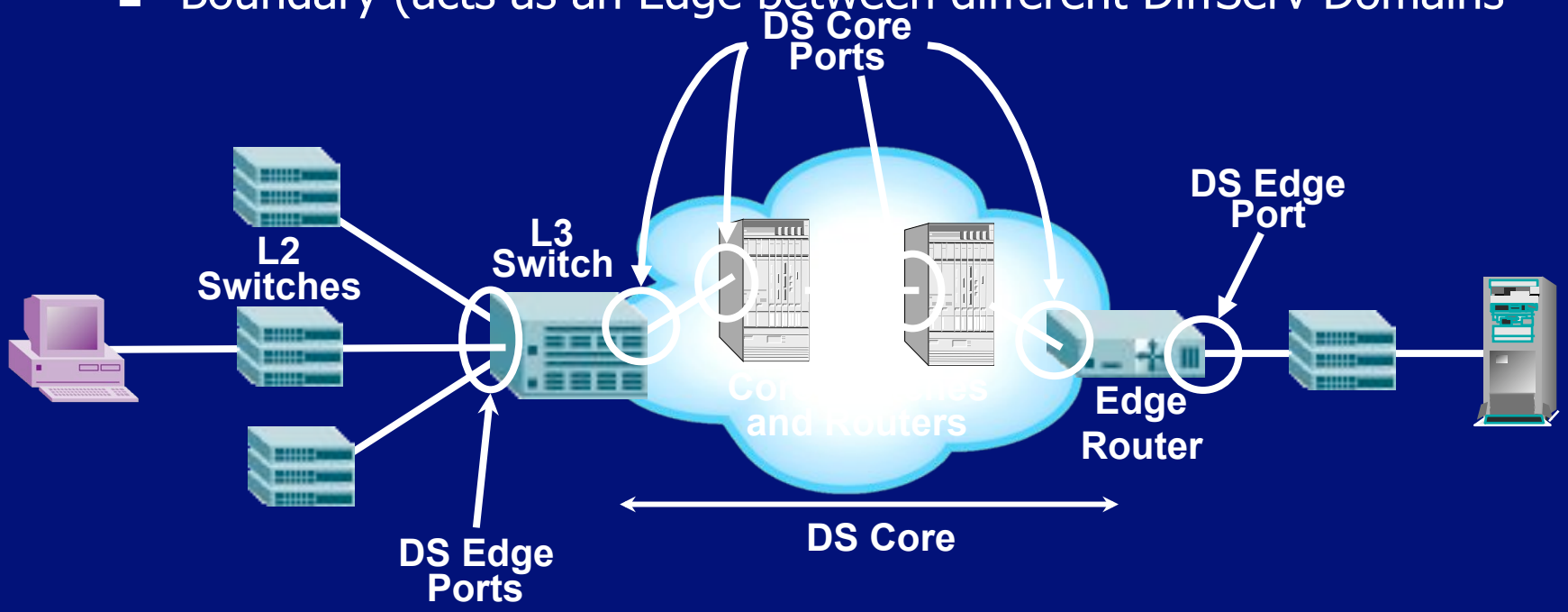


- A DiffServ Domain has a set of common QoS Policies or rules
- DiffServ Edge Nodes interconnect untrusted and trusted sources
  - The DS Edge Node is typically the first "IP-aware" device in the network
- DiffServ Interior Nodes interconnect trusted sources
  - in the same DiffServ Domain
- DiffServ Boundary Nodes interconnect DiffServ Domains
  - Each DS Domain may have different network resources and QoS policies implemented


DS Edge Nodes
Core Router
DS Interior Nodes
Policy Switch
L3 Switch
Radio Access Point
DS Boundary Nodes
Edge Router
DS Edge Nodes
DS Domain

DiffServ Interface Types

- DiffServ Nodes with different DiffServ I/F Types
  - Core (Interior)
  - Edge
  - Boundary (acts as an Edge between different DiffServ Domains



DiffServ Packet Treatment

- After packets are classified they may be:
  - Metered
  - Policed
  - Marked
  - Shaped
  - Dropped