

## Part 2: Design Principles

### Goals:

- identify, study common architectural principles, protocol mechanisms
- *synthesis*: big picture

### Overview:

- Separation of data and control: signaling
- state management: hard vs. soft-state
- randomization
- indirection
- multiplexing
- virtualization
- design for scale

Part 2 2-1

## 6. Virtualization of networks

Virtualization of resources: a powerful abstraction in systems engineering:

- computing examples: virtual memory, virtual devices
  - Virtual machines: e.g., java
  - IBM VM OS from 1960's/70's
- layering of abstractions: expose only the abstraction exported by the lower layer, but not its implementation details

Part 2 2-2

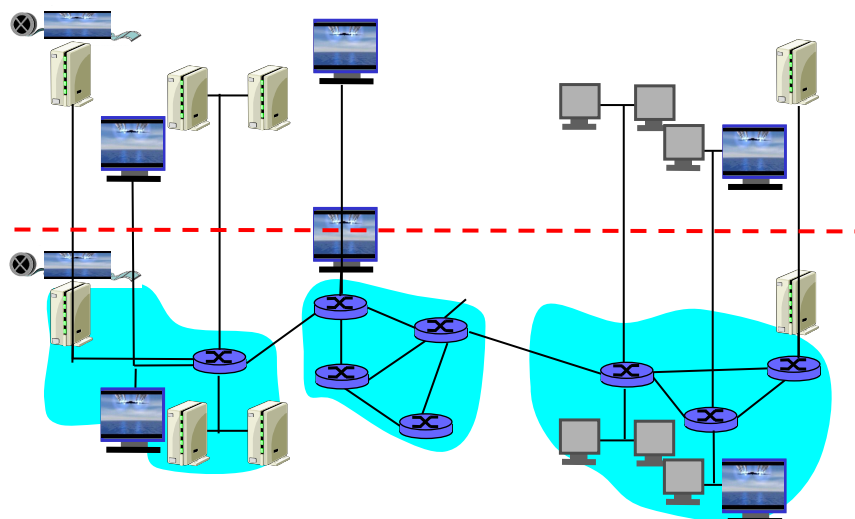
## Overlay Networks

### Overlay network:

- applications, running at various sites as "nodes" on an application-level network
- create "logical" links (e.g., TCP or UDP connections) pair-wise between each other
- each logical link: multiple physical links, routing defined by native Internet routing

Part 2 2-3

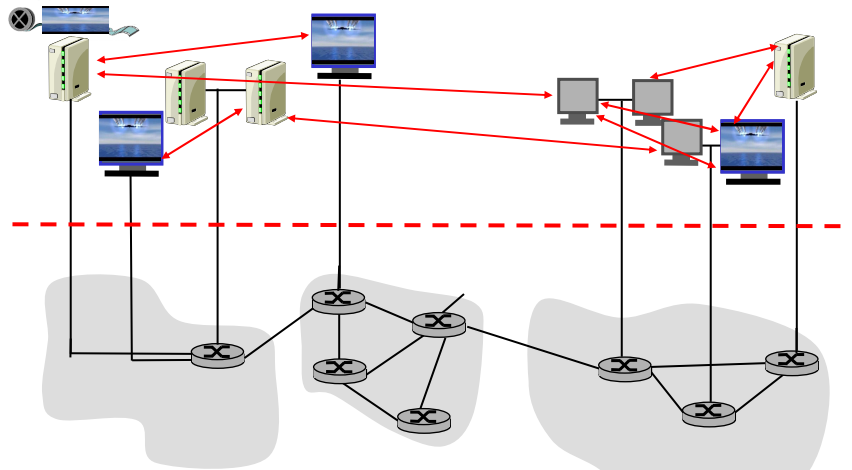
## Overlay network



Part 2 2-4

## Overlay network

Focus at the application level



Part 2 2-5

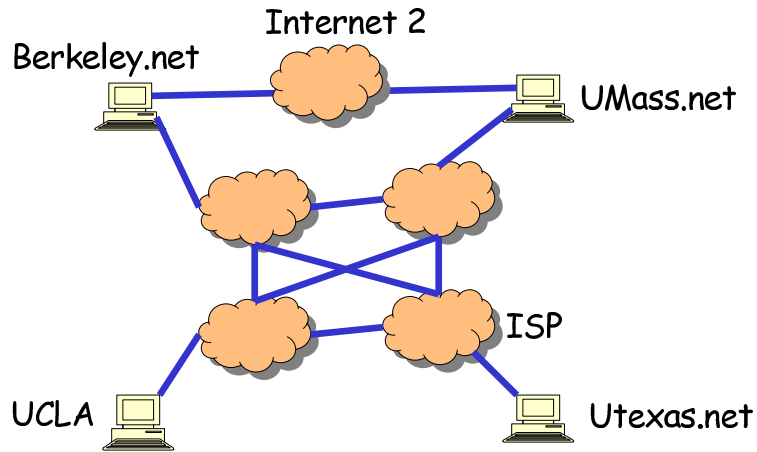
## What's new/what's old here?

- ❑ routing all over again (except at application layer)
- ❑ more security (as in VPNs). Can do more "heavyweight" security/authentication since application-level-router is a potentially "powerful" computer rather than a packet router
- ❑ can choose next hop on basis of (i) IP address (ii) congestion status of outgoing links; performance oriented routing
- ❑ anonymity on TCP connection (a-la SoS routing)
- ❑ Routing based on content - look at what is inside packet and determine who downstream "wants" the content

Part 2 2-6

## Internet Routing

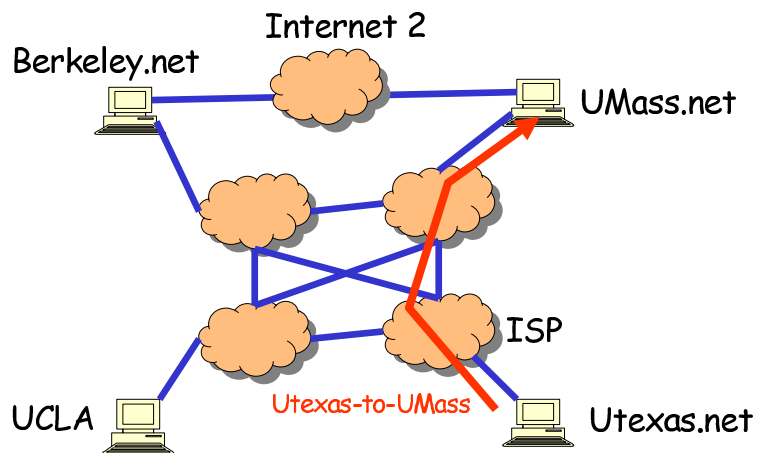
- BGP defines routes between stub networks



Part 2 2-7

## Internet Routing

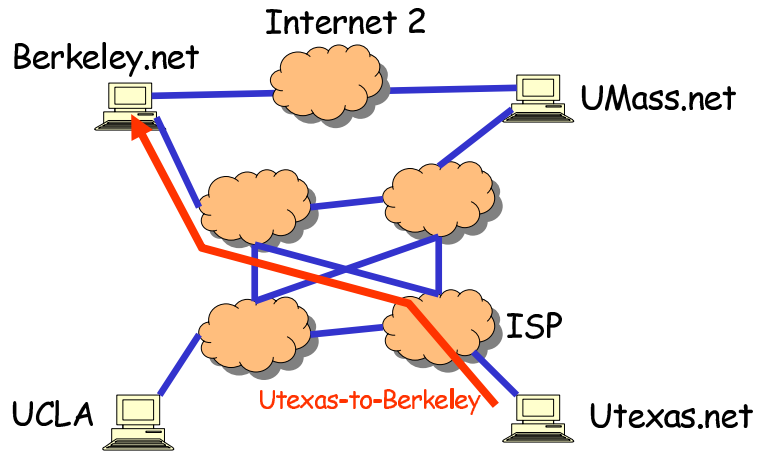
- BGP defines routes between stub networks



Part 2 2-8

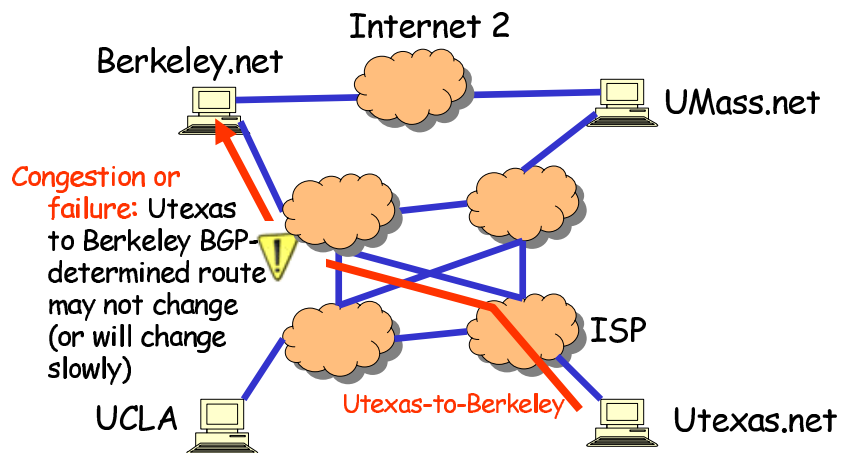
## Internet Routing

- BGP defines routes between stub networks



Part 2 2-9

## Internet Routing

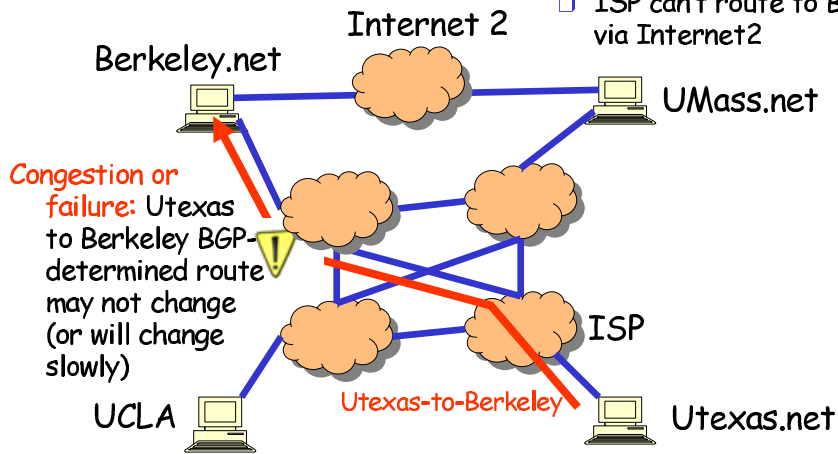


Part 2 2-10

# Internet Routing

Utexas → UMass → Berkeley

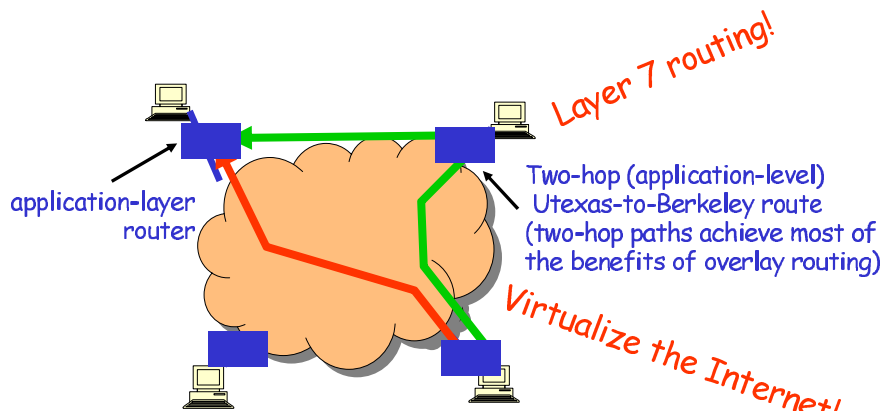
- route not visible or available via BGP!
- ISP can't route to Berkeley via Internet2



Part 2 2-11

# RON: Resilient Overlay Networks

**Premise:** by building application overlay network, can increase performance, reliability of routing



Part 2 2-12

## RON Research Issues

- How to design overlay networks?
  - Measurement and self-configuration
  - Understanding performance of underlying net.
  - Fast fail-over.
  - Sophisticated metrics.
  - application-sensitive (e.g., delay versus throughput) path selection.
- Effect of RON on underlying network
  - If everyone does RON, are we better off?
  - Interacting levels of control (network- and application-layer routing)

Part 2 2-13

## Virtual Private Networks (VPN)

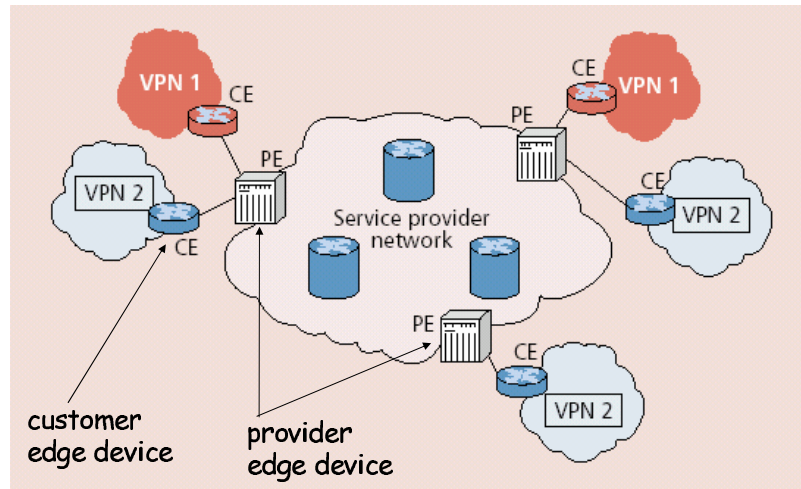
### VPNs

Networks perceived as being private networks by customers using them, but built over shared infrastructure owned by service provider (SP)

- SP infrastructure:
  - backbone
  - provider edge (PE) devices
- Customer:
  - customer edge (CE) devices (communicating over shared backbone)

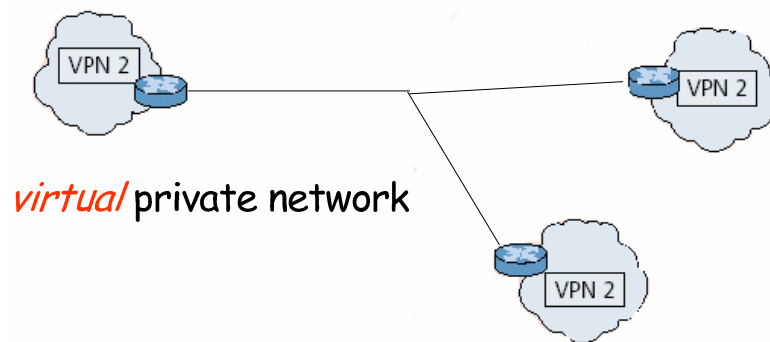
Part 2 2-14

## VPN reference architecture



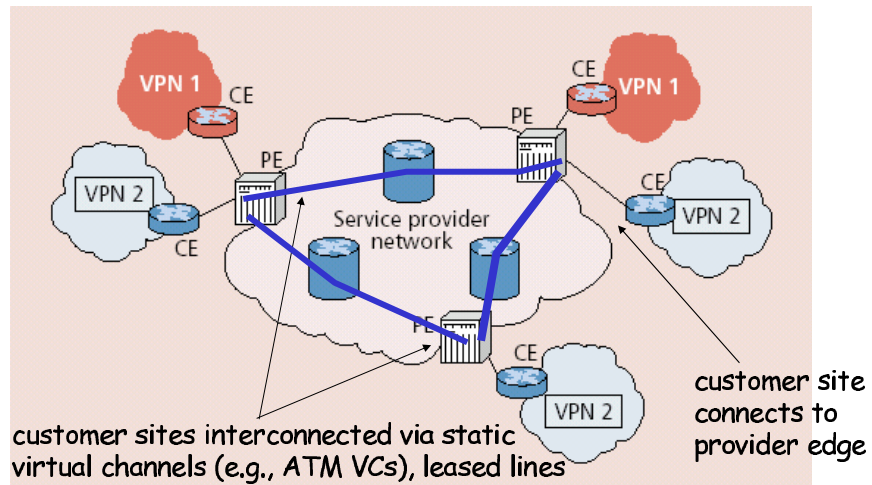
Part 2 2-15

## VPN: logical view



Part 2 2-16

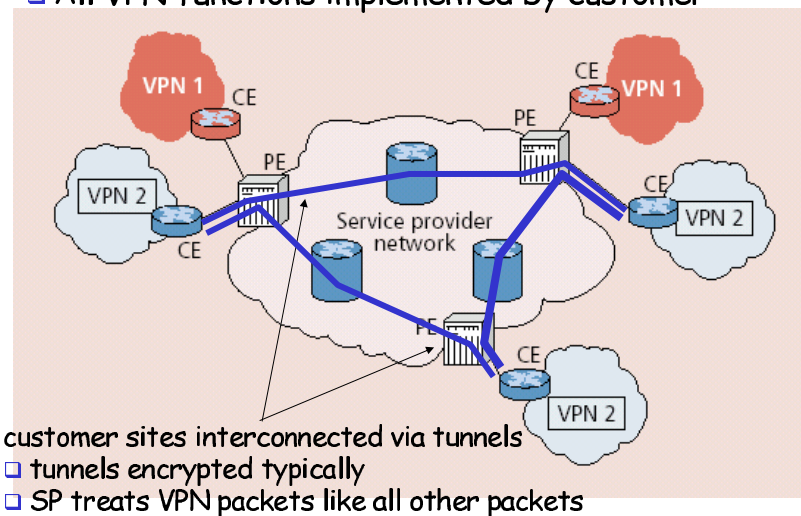
## Leased-line VPN



Part 2 2-17

## Customer premise VPN

- All VPN functions implemented by customer



Part 2 2-18

## Drawbacks

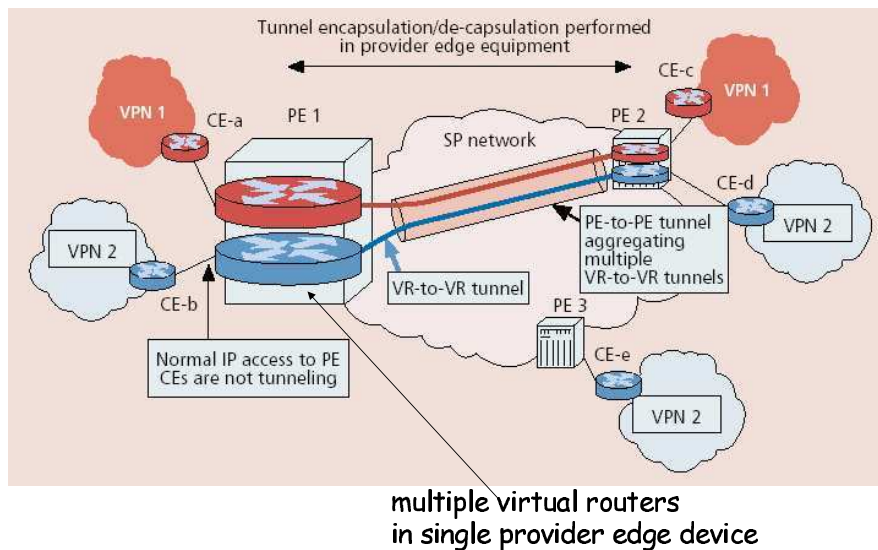
- ❑ Leased-line VPN: configuration costs, maintenance by SP: long time, much manpower
- ❑ CPE-based VPN: expertise by customer to acquire, configure, manage VPN

## Network-based VPN

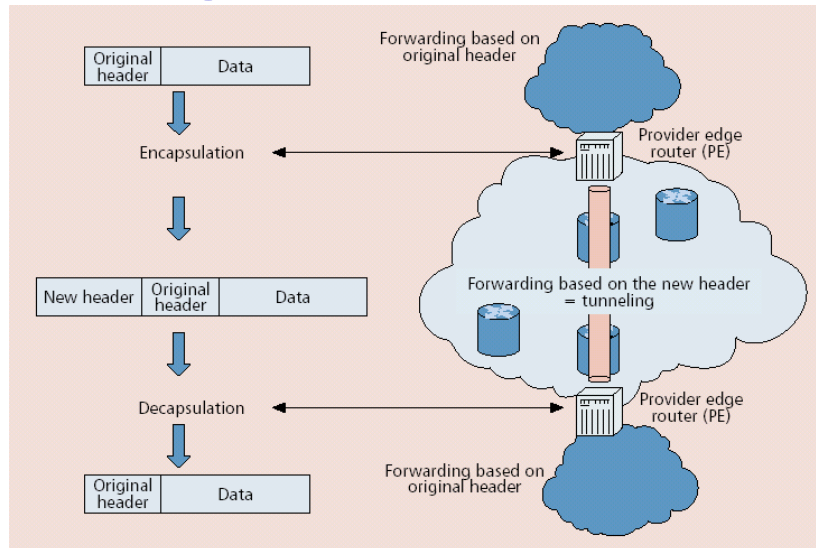
- ❑ customer's routers connect to SP routers
- ❑ SP routers maintain separate (independent) IP contexts for each VPN
  - sites can use private addressing
  - traffic from one VPN can't be injected into another

Part 2 2-19

## Network-based Layer 3 VPNs



## Tunneling



Part 2 2-21

## VPNs: why?

- ❑ privacy
- ❑ security
- ❑ works well with mobility (looks like you are always at home)
- ❑ cost: Newer VPNs are cheaper than leased line VPNs
  - ability to share at lower layers → lower cost
  - Exploit multiple paths, redundancy, fault-recovery in lower layers
  - Need isolation mechanisms to ensure resources are shared appropriately
- ❑ abstraction and manageability: all machines with addresses that are "in" are trusted no matter where they are

Part 2 2-22