Resource Management for Multipoint Communication Applications and Services

GRADUATE INSTITUTE OF INFORMATION MANAGEMENT
NATIONAL TAIWAN UNIVERSITY

Outline
- An Introduction to VPN
- VPN Service Models
  - The pipe model
  - The hose model
- Implementation Alternatives of the Hose Model
- MPLS Traffic Engineering Applications
- Temporal Sharing
- Future Research Directions

Private Network
- A Private Network (PN) is established by dedicated leased lines connecting several geographically dispersed sites (endpoints).
  - Each site is a campus or a branch office of an enterprise.
  - Since the lines are dedicated, security and Quality of Service (QoS) are ensured.
  - But connecting a large number PN sites with dedicated lines is expensive.

Virtual Private Network
- Virtual Private Network (VPN) is a replacement for Private Network.
  - A VPN establishes connectivity between a set of endpoints over a shared network infrastructure (e.g., The Internet).
  - The goal of VPN is to provide endpoints with a service comparable to Private Network.
  - Thus providers of VPN services need to address QoS and security issues.

VPN Three Types
- In terms of commercial applications, VPN can be classified into three types:
  - Access VPN (a.k.a Remote Access VPN)
  - Intranet VPN (a.k.a Enterprise VPN)
  - Extranet VPN (a.k.a E-commerce VPN)

VPN Three Types (con’t)
Technologies for Providing VPN Service

- In order to provide VPN service over shared network, VPN adopts three technologies:
  - Tunneling
  - Encryption, decryption and key management
  - Authentication

Outline

- An Introduction to VPN
- VPN Service Models
  - The pipe model
  - The hose model
- Implementation Alternatives of the Hose Model
- MPLS Traffic Engineering Applications
- Temporal Sharing
- Future Research Directions

VPN Service Models

- VPN Service Providers need a flexible and resource efficient model to be able to support a variety of customer needs.
- Two common VPN service Models are
  - The Customer-pipe model
  - The Hose model

The Customer-Pipe Model

- This Model emulate the private line.
  - VPN customers need to buy a set of customer-pipes.
  - VPN service provider uses a path between source-destination pairs of endpoints to implement a customer-pipe.
  - VPN service provider also need to provision adequate bandwidth along the path to ensure Service Level Agreement (SLA) is satisfied.

The Pro and Cons of the Customer Pipe Model

- Pro
  - The task of resource management becomes more simple.
- Con
  - It requires the customer to have precise knowledge of the traffic matrix between all the VPN sites.
  - Resource made available to a customer pipe cannot be allocated to other traffic.
  - An endpoint must maintain a logical interface for each of its customer-pipes.
The Hose Model

- In this model, the connectivity of each endpoint to the network is specified by:
  - The capacity for aggregate outgoing traffic from the endpoint into the network (gress bandwidth requirement).
  - The capacity for aggregate incoming traffic out of the network to the endpoint (egress bandwidth requirement).

Advantages of the Hose Model

- Ease of specification
- Flexibility
- Multiplexing Gain
- Characterization

Challenge of Provision the Hose Model

- From a VPN service provider’s perspective, it is more challenging to support the hose model
  - The need to meet the SLA with a very weak specification of the traffic matrix.
  - This complicate the VPN’s resource management issue.

Outline

- An Introduction to VPN
- VPN Service Models
  - The pipe model
  - The hose model
- Implementation Alternatives of the Hose Model
- MPLS Traffic Engineering Applications
- Temporal Sharing
- Future Research Directions

Implementation Alternatives of the Hose Model

- The most important implementation alternatives for the hose model VPN’s are
  - Provider-pipe scheme
  - Hose-specific state scheme
  - VPN-specific state scheme
  - Tree routing scheme
Example Networks

Provider-Pipe scheme

Hose-specific state scheme

VPN-specific state scheme

Tree Routing Scheme

Outline
- An Introduction to VPN
- VPN Service Models
  - The pipe model
  - The hose model
- Implementation Alternatives of the Hose Model
- MPLS Traffic Engineering Applications
- Temporal Sharing
- Future Research Directions
In MPLS technology, packets are encapsulated at network ingress router with label that are then used to forward the packets along label switched paths (LSPs).

One of the main advantages of MPLS technology is that LSPs can be explicitly routed along specific paths (explicit routing).

- Specify all intermediate routers between the ingress router and the egress router.

One of the key purposes of network traffic engineering is for efficient network resource usage.

According to RFC 2702, the most significant application of MPLS will be traffic engineering.

This means that available network resources are not being used well and there is potential for providing better QoS with the same network infrastructure.

- Link congestion caused by shortest path routing can be avoided by using different routing scheme.
- Routing schemes that can make better use of network infrastructure are needed.

VPN service provider can use bandwidth guaranteed tunnels as component of an VPN service.

- The bandwidth guaranteed can be used to satisfy customer service level agreement (SLA).
- Other QoS requirements are assumed to be translated into an effective bandwidth requirement.
Routing Algorithms for Setting up Bandwidth Guaranteed Tunnels

- In recent traffic engineering literature, there are five well-known routing algorithms for setting up bandwidth guaranteed tunnels:
  - MHA (Minimum Hop Algorithm)
  - WSP (Widest Shortest Path Algorithm)
  - SWP (Shortest Widest Path Algorithm)
  - MIRA (Minimum Interference Routing Algorithm)
  - PBR (Profile-Based Routing Algorithm)

MIRA

- The MIRA exploits the knowledge of ingress-egress pairs in finding a path for tunnel.
  - The idea is that a newly routed tunnel should follow a path that does not interfere too much with a future tunnel setup requests.
  - Critical link: if a path is routed through it, the maxflow value of one or more ingress-egress pairs decreases.
  - The algorithm aims to avoid these critical links.

PBR

- Profile-Based Routing was proposed to deal with the dynamic routing problem of bandwidth-guaranteed flows.
  - PBR use a “traffic profile” of the network, obtained by measurement or SLA as a rough predictor of the future traffic distribution.
  - The “profile” is used to solve a multi-commodity network flow problem, whose output is used to guide online path-selection as well as impose admission control.

Outline

- An Introduction to VPN
- VPN Service Models
  - The pipe model
  - The hose model
- Implementation Alternatives of the Hose Model
- MPLS Traffic Engineering Applications
- Temporal Sharing
- Future Research Directions
Temporal Sharing

- Traditional approaches to resource allocation in the Internet use signaling protocols (e.g., RSVP) that allocate resources for each flow independently.
- This approach is called independent per-flow allocation.


However, “related” flows in most applications can share the same set of resources over time.
- We call this type of behavior temporal sharing.
- ISP can exploit temporal sharing technique to save network resources.

Examples of Exploiting Temporal Sharing

Hose Model VPN:

Examples of Exploiting Temporal Sharing

Broadcast TV with Picture-in-Picture:

Outline

- An Introduction to VPN
- VPN Service Models
  - The pipe model
  - The hose model
- Implementation Alternatives of the Hose Model
- MPLS Traffic Engineering Applications
- Temporal Sharing
- Future Research Directions

Future Research Directions

- In the previous literature of MPLS traffic engineering, they focus on how to establish point-to-point tunnels for constructing VPNs.
  - These literature handle setup requests in unit of a tunnel.
Future Research Directions

- However, a VPN comprises several tunnels.
  - It is more reasonable for customers to establish a whole VPN at a time.
  - In MPLS traffic Engineering context, if an ISP handle setup requests in unit of a VPN, what’s the impact on resource efficiency and setup requests blocking ratio?