A TINA-based solution for Dynamic VPN Provisioning on heterogeneous networks

Patricia Lago
Riccardo Scandariato

Politecnico di Torino, Italy
Contents

Motivation
- Premises and objectives

The starting point
- TINA concepts
- IETF Policy Control Architecture

The design solution
- VPN representation
- VPN control architecture
Premises

Current technologies
- Manual configuration
- Low level interfaces
- Static VPN definition

New generation of network devices
- Policy enabled (e.g. IETF PIB)
- Active elements (triggering event notifications)

New management protocols (e.g. IETF COPS)
Objectives

VPN provisioning as a semi-automated added-value service

- High level VPN interfaces
- Dynamic VPN service
  - Policy-enabled
  - Off-the-shelf
- Transparent to Hybrid networks
Starting point

A Provider Architecture for dynamic VPN provisioning

- Network Architecture
  - A modified Virtual Private Routed Network model
  - A high level description of VPNs (as an information model)
- Control Architecture
  - A set of software components to maintain the VPN description and to enforce policies into the physical devices
Starting point -
TINA Approach-level concepts

Connections as VPN links
Abstraction layering / connection graph

- Connectivity layer
- Layer network

as

- Provider Connectivity View (ConnView)
- Provider Topology
Applied Approach-level concepts

Customer
Edge
Device (CED)

Area Topology

ATM Area
IP Area

Provider Topology

Provider
ConnView

NN1
TT1
NN2
NN3

Politecnico di Torino – TINA’2000
Starting point -
TINA Model-level concepts

Customer
Edge
Device (CED)

Area
ConnView

Area
Topology

ATM Area
IP Area

Provider
ConnView

Provider
Topology

Tunnel
Switch

Politecnico di Torino – TINA’2000
Applied TINA Model-level concepts

Provider A ConnView

Provider B Foreign ConnView

Provider Topology
Starting point – IETF

The VPRN (VPN description)
- IETF Network WG model
- Extensions
- VPRN operations

The Control Architecture (VPN administration)
- The IETF RAP WG model
- The proposed architecture
The VPRN model according to IETF

- ISP as an opaque IP cloud edged by Border Nodes
- Customer Edge Device
- Stub link
- Mesh of tunnels among the border nodes
Extensions to the VPRN model

Cybernetic Entities and Domains (CEDs) are connected through Physical Links to the Core Nodes, which are part of the Provider Network. The Provider Network supports Client Initiated Tunnels, allowing Ignorant Providers to establish secure connections. The diagram illustrates the integration of these components within the VPRN model.
Extensions to the VPRN model

The ISP network is not an opaque cloud
- Core node are integral part of the VPN description
- The network is structured in areas

We consider also the dial-in customers
- CED as a single host

A more flexible definition of the Stub Link concept
- Dedicated, PPP connection, virtual (tunnel)
The 4 operations

- VPRN membership determination
- Tunnel establishment
- Stub link reachability configuration
- Intra-VPRN reachability info propagation

ISP Net

VPN #1 ("orange")
Site A (Headquarter)

VPN #1 ("orange")
Site B (Branch Office)

Politecnico di Torino – TINA’2000
The 4 operations

- VPRN membership determination
- Tunnel establishment
- Stub link reachability configuration
- Intra-VPRN reachability info propagation

ISP Net

I got an “Orange” client too!

Site A (Headquarter)

Site B (Branch Office)
The 4 operations

- VPRN membership determination
- Tunnel establishment
- Stub link reachability configuration
- Intra-VPRN reachability info propagation

ISP Net

Site A (Headquarter)

Site B (Branch Office)
The 4 operations

- VPRN membership determination
- Tunnel establishment
- Stub link reachability configuration
- Intra-VPRN reachability info propagation

These are the addresses that belong to the VPN

Site A (Headquarter)

Site B (Branch Office)
The 4 operations

- VPRN membership determination
- Tunnel establishment
- Stub link reachability configuration
- Intra-VPRN reachability info propagation

You can reach these addresses through me
The 4 operations

- VPRN membership determination
- Tunnel establishment
- Stub link reachability configuration
- Intra-VPRN reachability info propagation
The policy model according to IETF

- Policy enforcement coordinated by a central controller (CPC)
- Storing policies and user info
- Policies pushed by the Policy Decision Points
- Policy decisions coded in COPS messages
Current status

- VPN graph (information model)
  - To be optimized
- Test lab implementation of a simplified VPN scenario