A tunnel discovery and monitoring overview

Ryszard Jurga

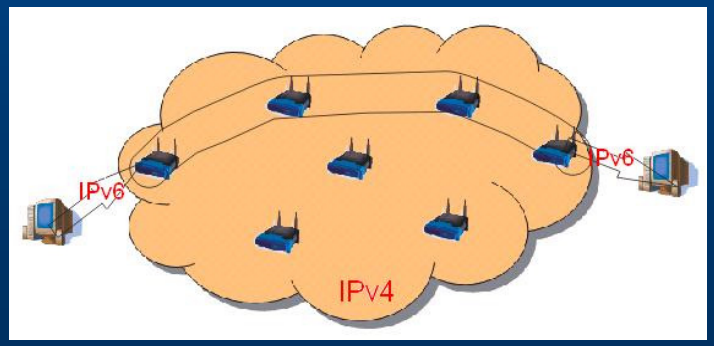
CERN openlab

Agenda

- What is the tunnel?
- The tunnel discovery
- The tunnel monitoring
- Conclusions

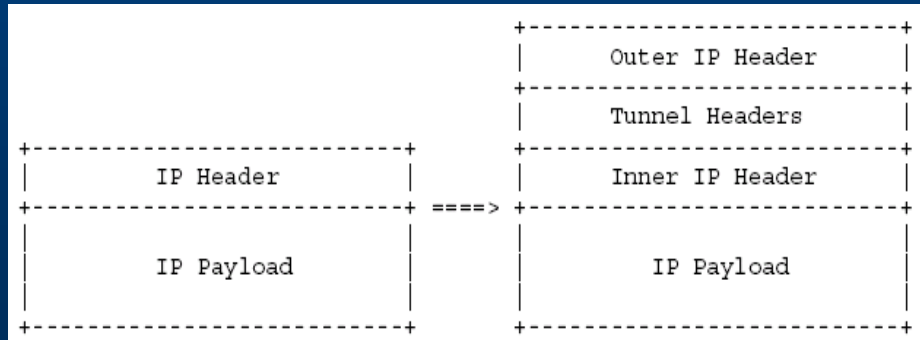
What is the tunnel?

- A connection where the packets of the network protocol are encapsulated within another protocol,
- Possibility to expand networks without having to deploy native infrastructure,
- They are very common (L2TP, GRE, IPV6-in-IPv4)



How it works

- The real and virtual interface and the address of endpoint,
- The route table,
  - The virtual addresses are used
- TTL,
- Encapsulation,
  - The real addresses of the endpoints of the tunnel are used,
- MTU
  - The extra IP header
  - increased overhead



The tunnel discovery

The tunnel discovery is the process of detecting tunnel and determining their end points and the set of all intermediate nodes involved in the tunnel.

The tunnel discovery - methods

- **Passive methods,**
  - **IP Spoofing**
  - **SNMP-based**
    - ***IF-MIB, RFC1213-MIB***
    - ***IP Tunnel MIB***
- **Active methods**
  - ***traceroute***
  - **Path MTU discovery algorithm**

The SNMP-based method

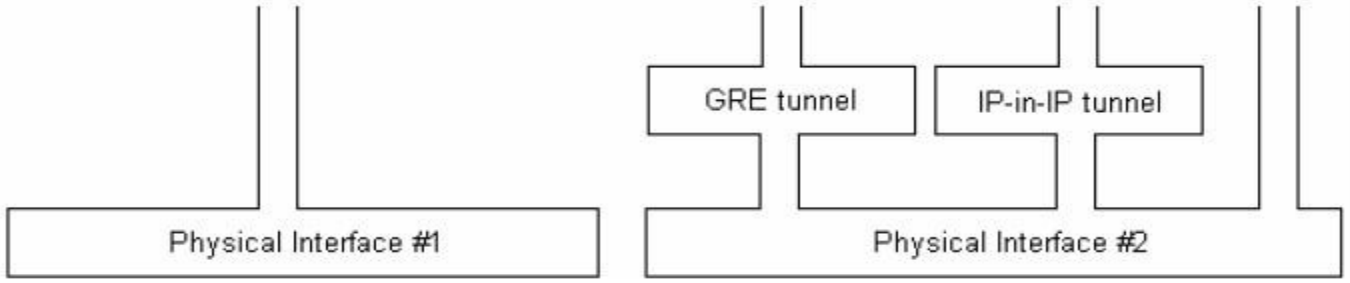
- **IF-MIB**
  - ***ifTable***

    - an individual row to represent each logical (physical or virtual) interface

    - the type of the interface is identified by the value of the *ifTable.ifType*
  - ***ifStackTable***

    map which identifies the superior and subordinate sub-layers through pointers to the appropriate entry in the *ifTable*

The SNMP-based method – cont.



ifTable

ifIndex	*ifType*
1	ethernetCsmacd (6)
2	ethernetCsmacd (6)
3	Tunnel(131)
4	Tunnel(131)

ifStackTable

HigherLayer	*LowerLayer*
0	1
0	3
0	4
1	0
2	0
3	2
4	2

The SNMP-based method – cont.

- **Algorithm for obtaining all logical interfaces and dependencies between them**
  Let's assume that *X* is the set included all logical interfaces.

  1. Read all interfaces from *X* which have no other interfaces stacked on top of them.
  2. From the interfaces read in the step 1, select those which have no other interfaces below them. Those are the interfaces without any others stacked on top or below them. All of them form the single interface tree.
  3. For all interfaces not selected in the step 2, form the set *Y* of interfaces. Start to build the interface tree for all of them.
  4. For each interface in the set *Y*, find its immediate successors in the lower layer.
  5. Exclude from the set found in the step 4, those interfaces which do not have other interfaces below them. For these interfaces the tree is complete. Form the new set *Y* included the other interfaces found in step 4.
  6. Go to the step 4 until the set *Y* is empty.

The SNMP-based method – cont.

- RFC1213-MIB
  - *ifAddrTable*

    The IP address and the network mask of each logical interface (the network mask 255.255.255.255 for tunnel)
    - the real addresses
    - the virtual addresses
  - *ifRouteTable (ipRouteNextHop)*

IF INDEX	IP	MASK
1	192.168.1.10	255.255.255.0
2	192.168.2.10	255.255.255.252
3	172.19.20.20	*
4	172.19.21.21	*

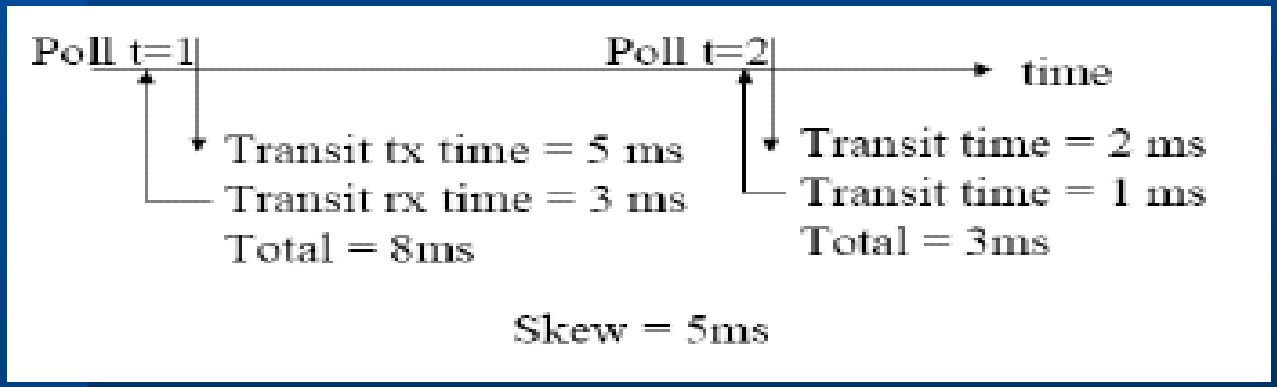
ADDRESS	MASK	IF INDEX	NEXT HOP
…	…	…	…
192.168.1.0	255.255.255.0	1	192.168.1.10
192.168.2.8	255.255.255.252	2	192.168.2.9
172.19.20.21	255.255.255.255	2	192.168.2.9
172.19.21.22	255.255.255.255	2	192.168.2.9
…	…	…	…

The SNMP-based method – cont.

- IP Tunnel MIB
  - Proposed on August 1999, updated on June 2005,
  - Consists all necessary information about the tunnel, can save a lot of calculations
  - Only few vendors have supported the first version of this MIB
    - **Jupiter with its E-series routers,**
    - **Alcatel with its Omni Switch 7700 and 8800,**
    - **Nokia with its geteways**

The tunnel monitoring

- **32-bit *(ifTable)* and 64-bit *(ifXTable)* counters**
  - **On the 10Gb interface at 50% load, the 32-bit counter wraps around every 6 seconds**
- **The time estimation**
  - **The high speed of the network (10Gb)**
  - **The long distance (RTT to Taiwan ~300ms)**
  - ***sysUpTime***



from C.Elliott, M. R. MacFaden „SNMP Counters Tutorial"

The tunnel monitoring –cont.

- **Data collection**
  - **Grouping counters in one request**
- **Counter discountinuity**
  - ***sysUpTime (wraps every 1.36 years)***
  - ***IF-MIB::ifCounterDiscountinuityTime***

Conclusions

- The process of the tunnel discovery is similar to the process of the IP network discovery,
- The prior knowledge of the IP network topology can speed up the discovery process considerably,
- IP Tunnel MIB might save a lot of computations and the network trafic, so if it is implemented by the routers it should be used,
- The proposed methodology has to be verified in the real environment (do all vendors really implement the mentioned MIB?), and its impact on the network and the router performance must be discused,
- We have to check if our proposed method of the tunnel discovery can be adapted to different network connections,
- We do not know any publications about the tunnel discovery and monitoring by means of the SNMP.