



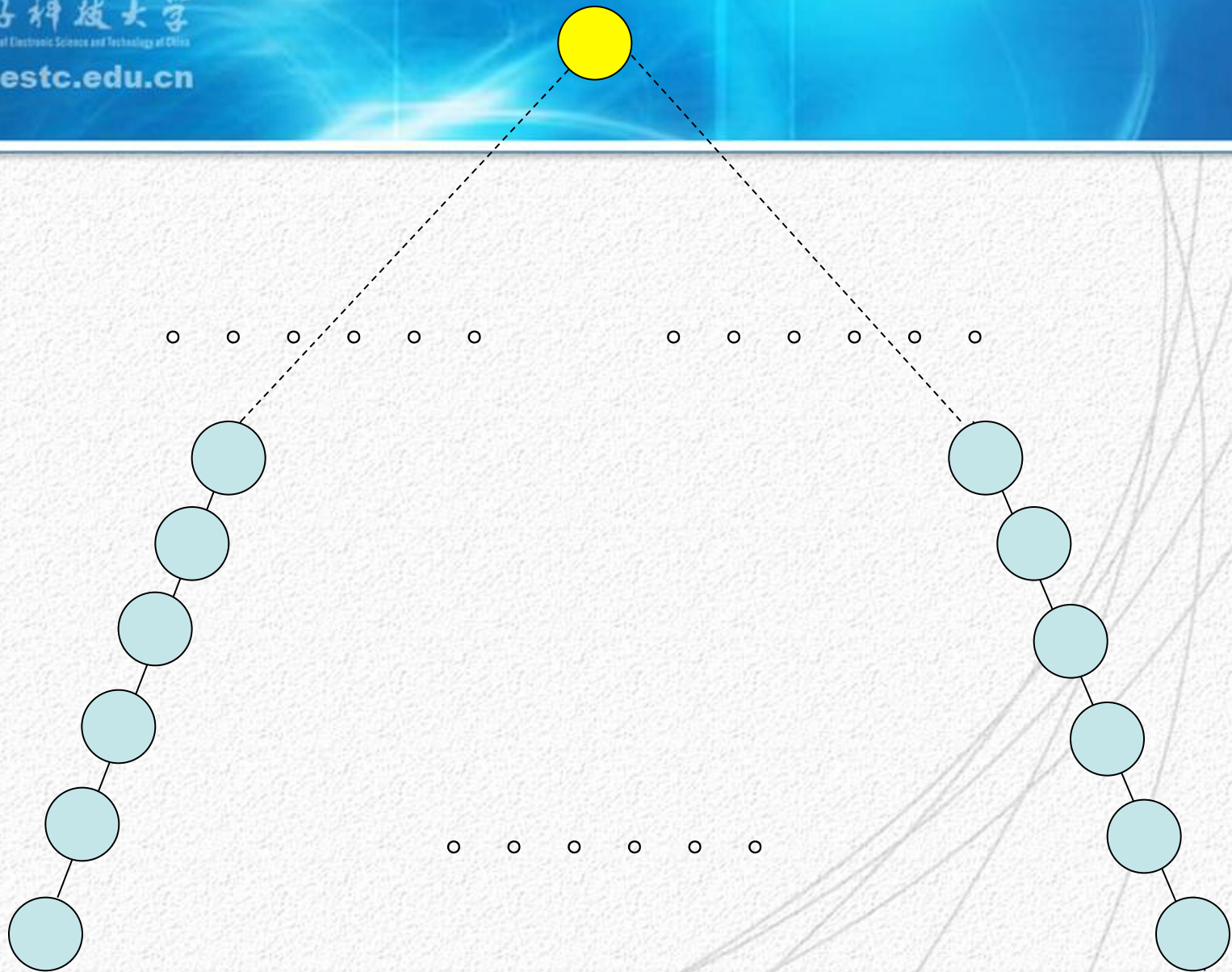
电子科技大学  
University of Electronic Science and Technology of China

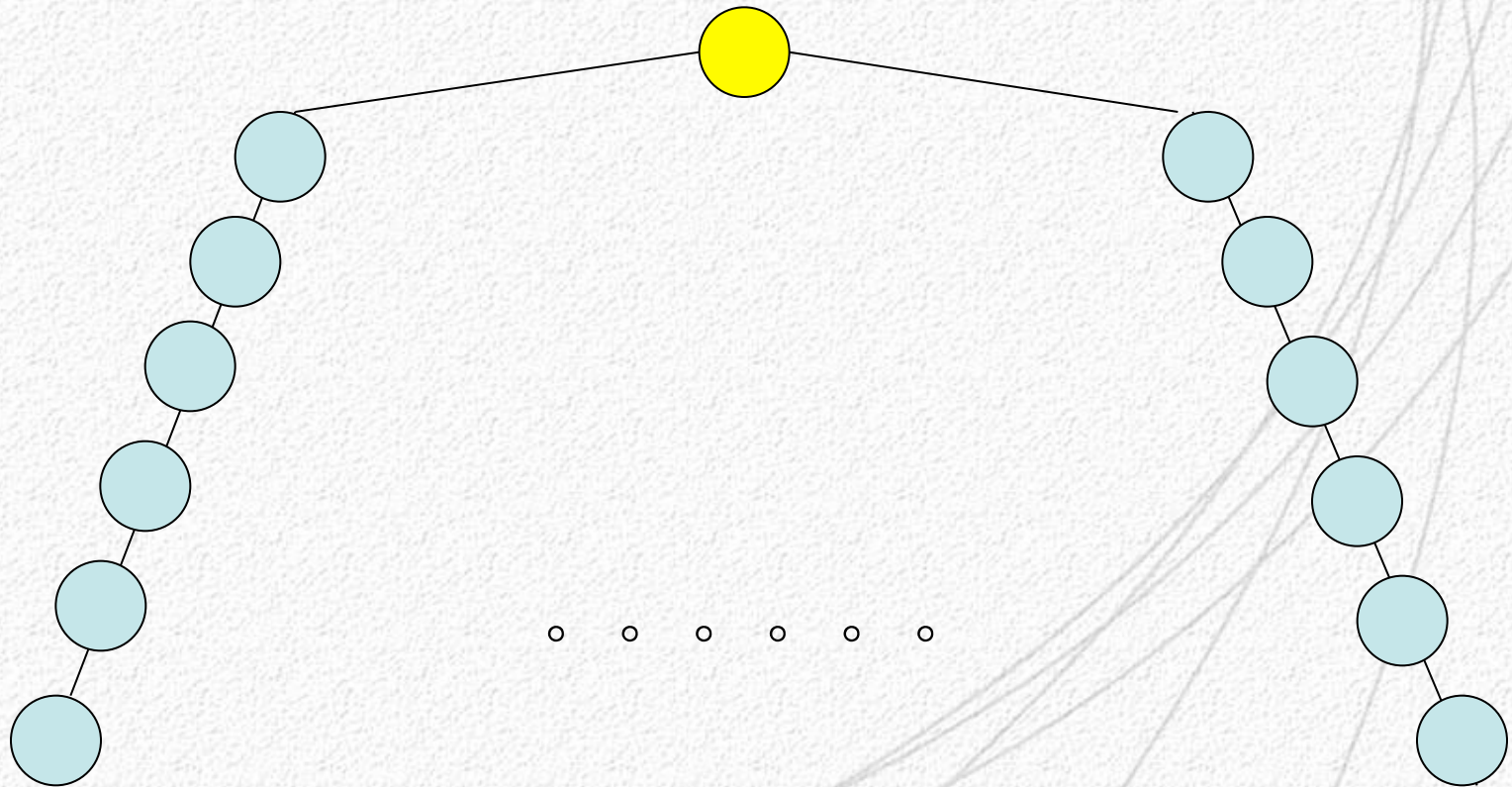
# Fault diagnostics of IP network based on passive measurement

August 9, 2011  
Kunming, China

[www.uestc.edu.cn](http://www.uestc.edu.cn)

Wenyong Wang



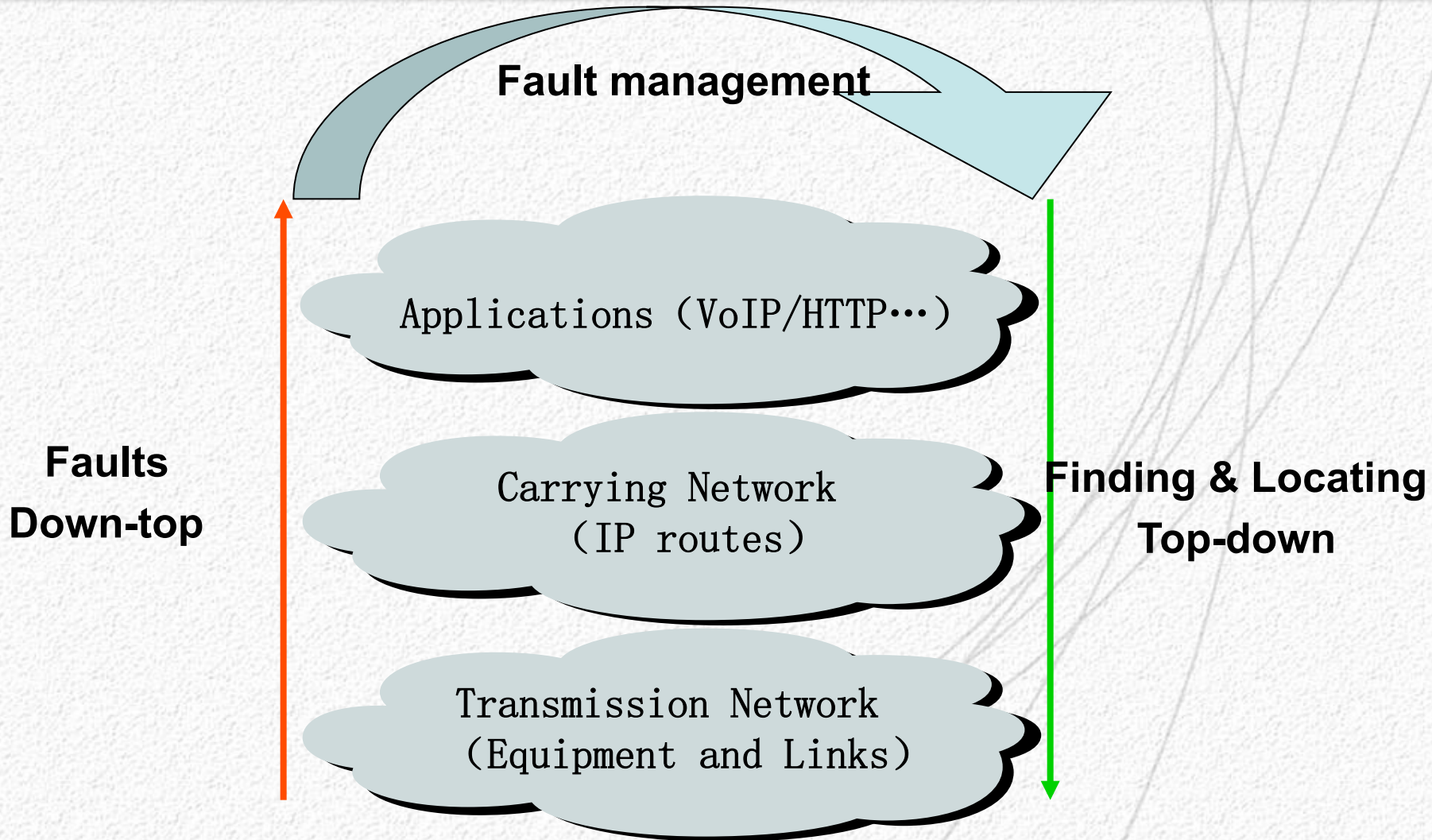


- Background and problem description
- Key points
- Our solution
- Demos

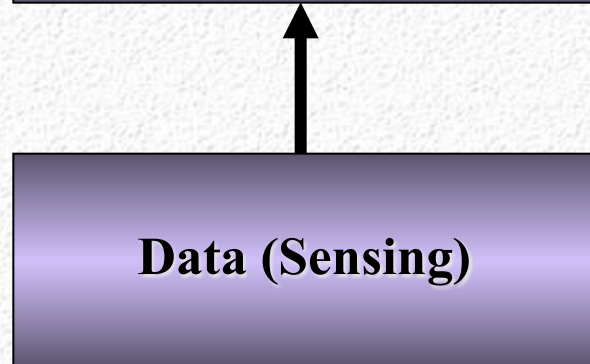
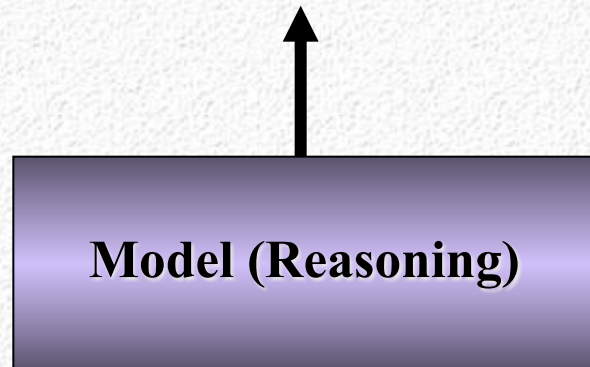
- Difficulties of fault diagnostics on carrier IP networks
  - Complicated structure: heterogeneous, triple-play
  - Complicated resources: multiple suppliers
  - Complicated services: new applications and computing models
  - Complicated behaviors: sharply increasing users

- Fault management
  - Fault finding, diagnosis and locationg
  - Especially when the three management planes are independent

# Problem description



**Output (Finding & Locating)**

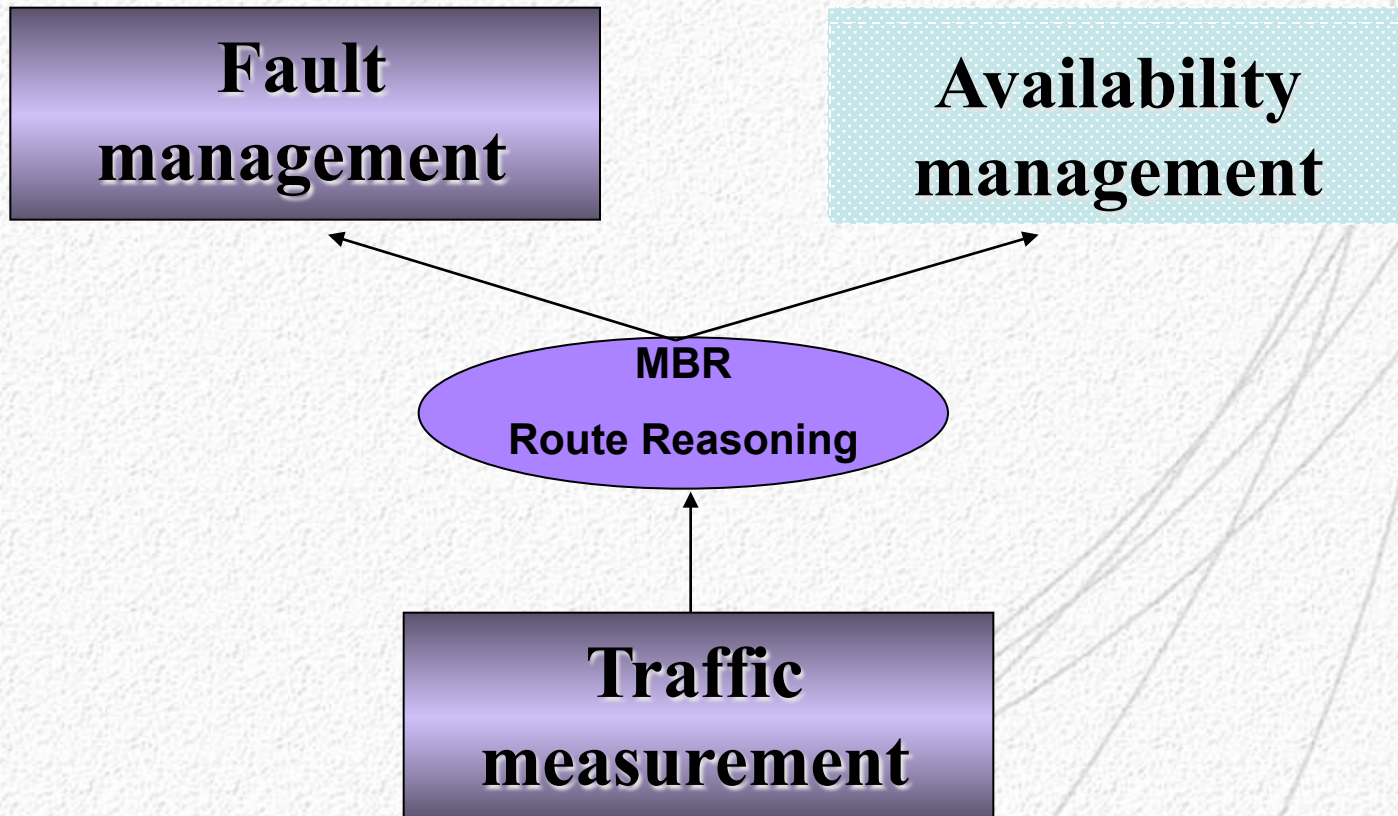


- **Data acquirement**
  - **SNMP/RMON**
  - **System log**
  - **Customer complaints**
  - **Active measuring**
  - **Passive measuring**

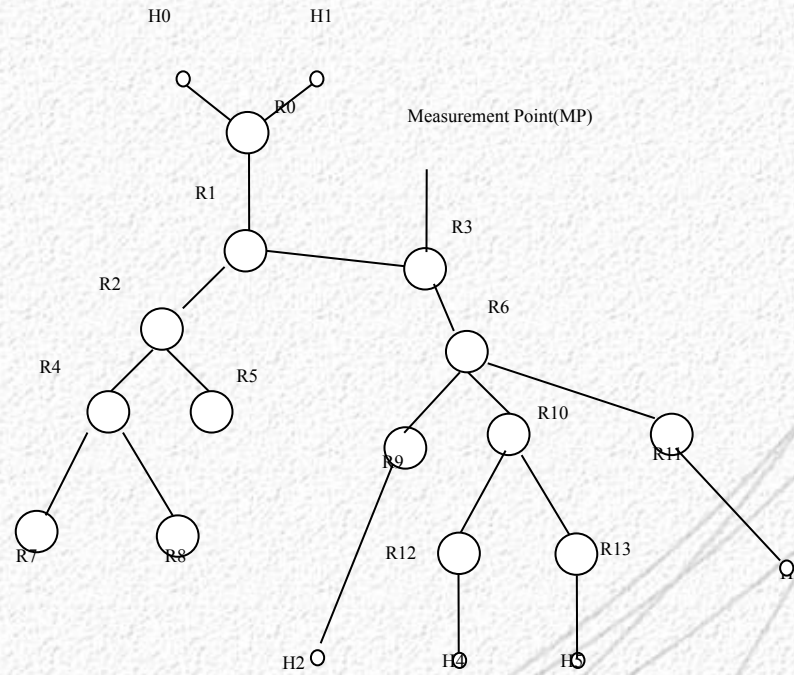
## – Fault management methods

- CBR
- RBR
- **MBR: Model Based Reasoning**
- Codebooks
- CGM / DGM
- Neural Network
- .....

- **Measurement based fault finding and locating**



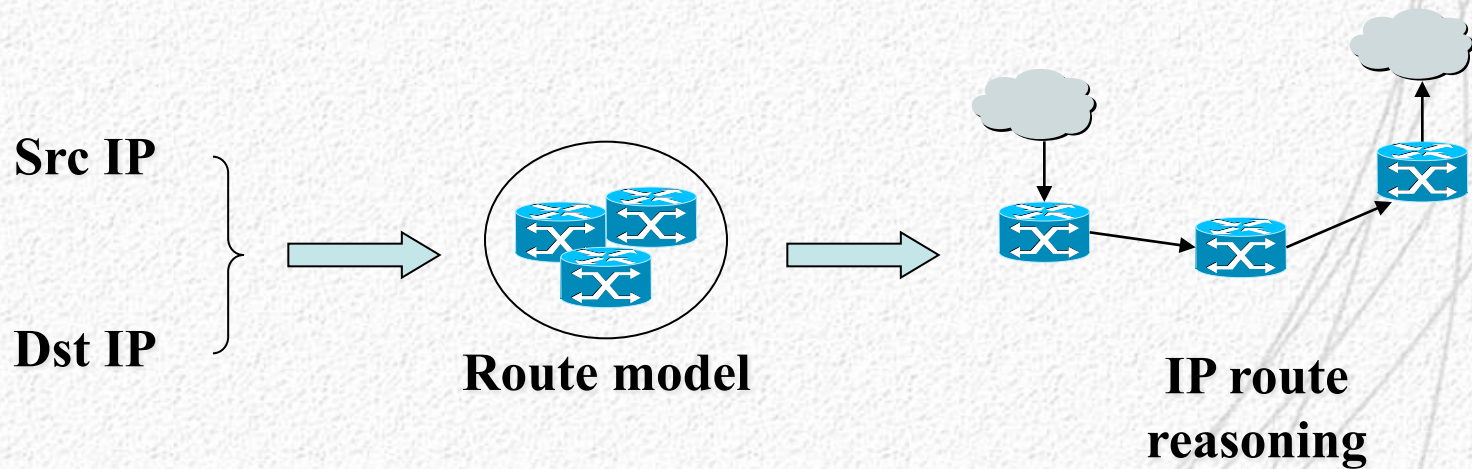
- Step1-Measuring Point(s) (MP) deployment on critical path(s)



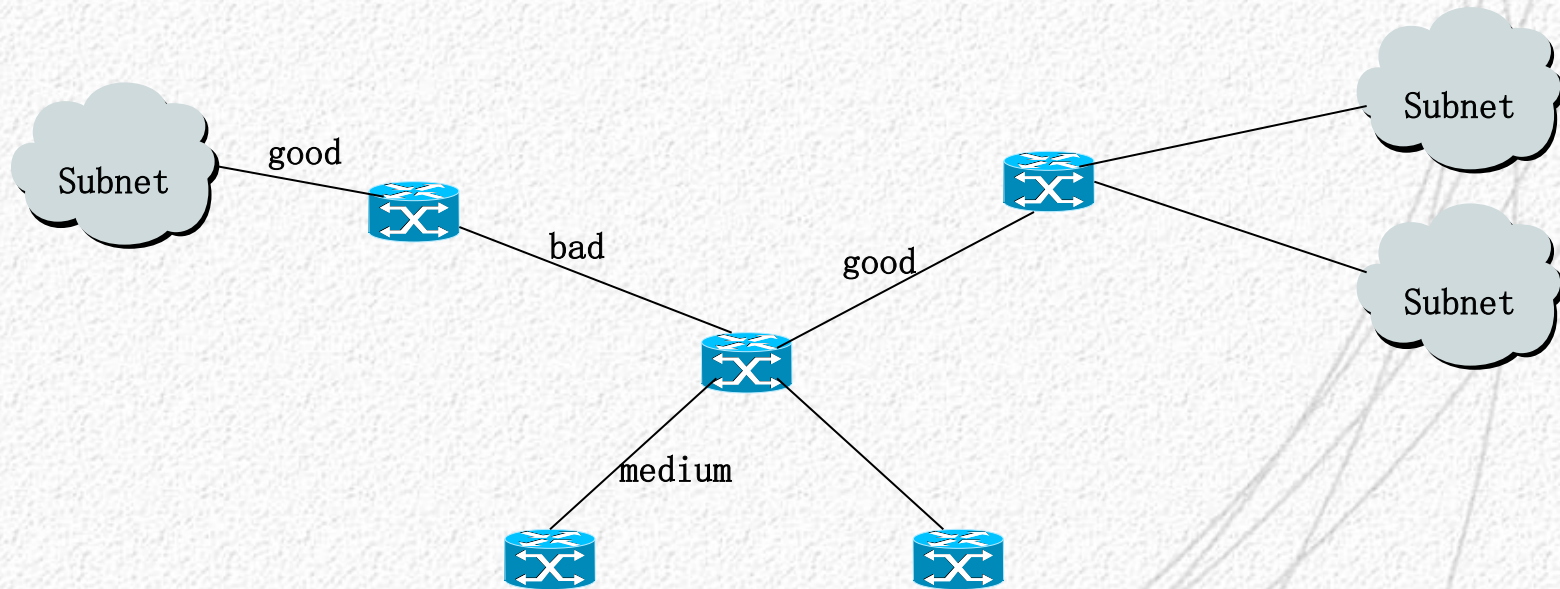
- **Step2-Obtaining e2e(IP pair) quality of service**



- **Step3-Establishing route model, reasoning route between IP pairs**



- **Step4-Link quality evaluation**



- **Step5-Fault locating**

- Fault link locating: Screening bad link from the link set and locating the fault link**

- Fault equipment locating: locating fault equipment by bad links aggregation**

- **Network model**

- Weighted graph  $G=(V,E)$ : IP network
- Constraint function  $F(B(e),D(e),L(e))$ : QoS for  $e \in E$
- Route:  $P=(V_1,V_2,\dots,V_k)$

- **Path QoS metrics**

- Bandwidth(concave model)

$$B(P) = \mathbf{Min}_{i=1,2,\dots,k-1} B(e_i)$$

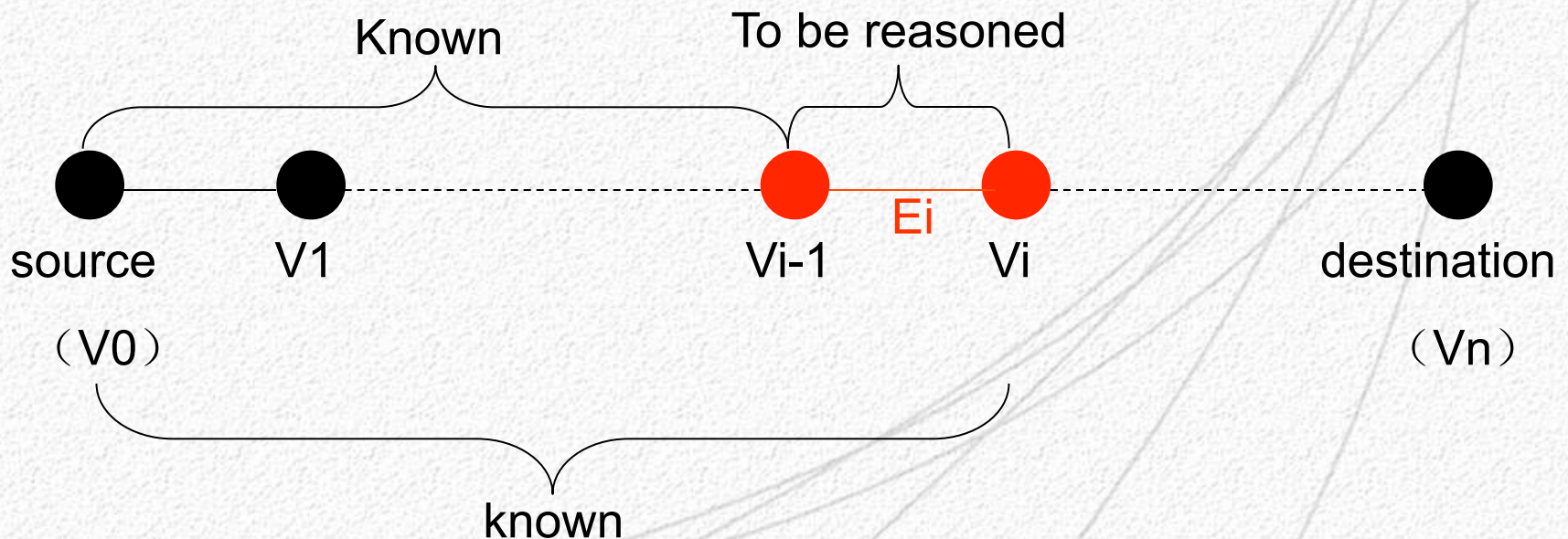
- Delay and package loss(convex model)

$$D(P) = \sum_{i=1,2,\dots,k-1} D(e_i)$$

$$L(P) = 1 - \prod_{i=1}^{k-1} (1 - L(e_i))$$

- **Network tomography: link quality**

- Status of one-hop link  $E_i$  can be deduced from the qualities of known links  $(v_0, v_i)$  and  $(v_0, v_{i-1})$



- **Network tomography: quality metrics**

$$B(e_i) = B(P_1^i) \text{ if } B(P_1^i) < B(P_1^{i-1})$$

$$D(e_i) = D(P_1^i) - D(P_1^{i-1})$$

$$L(e_i) = 1 - \frac{1 - L(P_1^i)}{1 - L(P_1^{i-1})}$$

- **IPLR measuring**

- **Continuous observations**

$$L_i = \begin{cases} SEQ_i - SEQ_{\max} - 1 & (SEQ_i > SEQ_{\max}) \\ 0 & (SEQ_i \leq SEQ_{\max}) \end{cases}$$

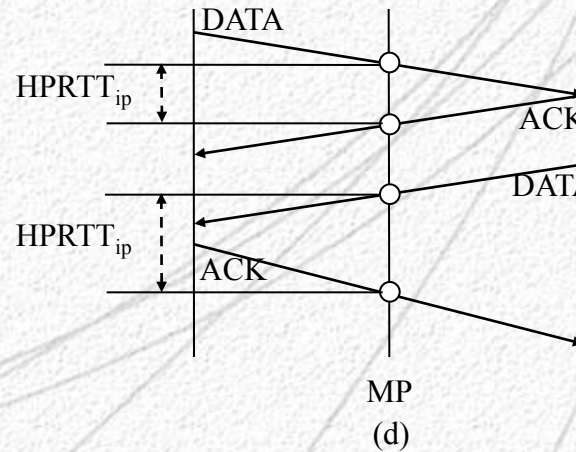
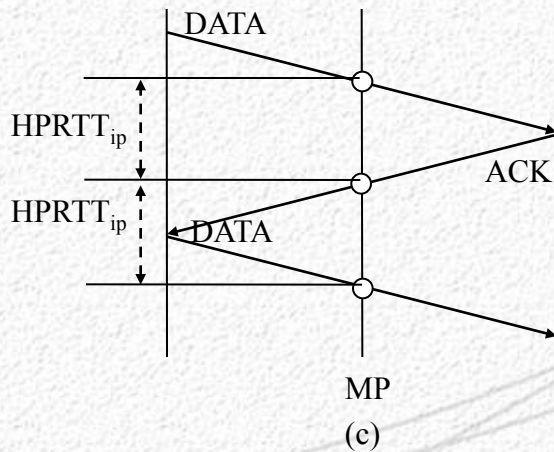
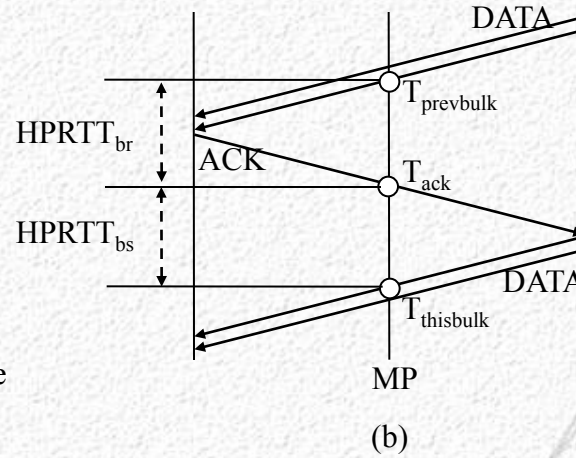
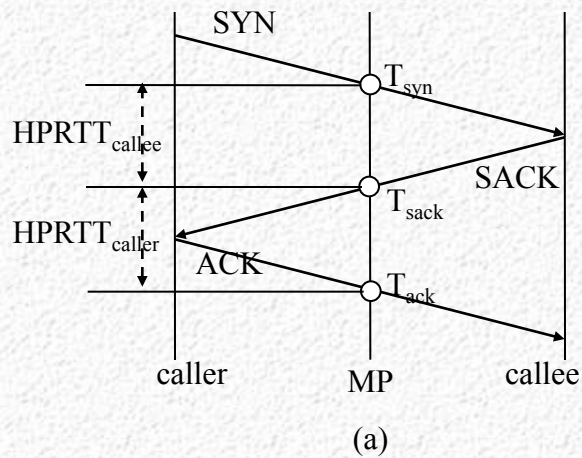
$$IPLR_a = \frac{\sum_{k=1}^i L_i}{(i + \sum_{k=1}^i L_i)}$$

- **Statics over prediction**

$$IPLR_a = \frac{R_{\text{predict}}}{R_{\text{measure}}}$$

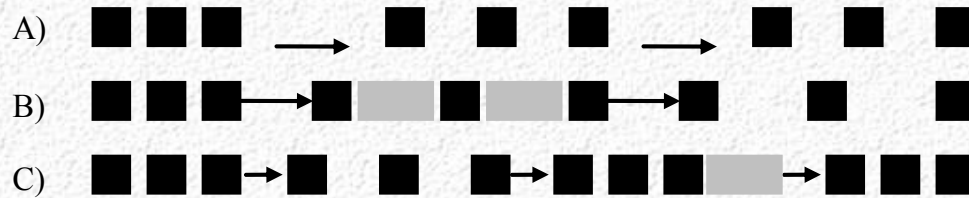
$$R_{\text{predict}} = \frac{1}{T} = \frac{1}{(TS_i - TS_{i-1})/R} = \frac{R}{(TS_i - TS_{i-1})}$$

# • Bi-directional half-path RTT



- **Path bandwidth and bandwidth available**

- **Short Equal-Dispersion Train**



- **Kernel density estimation**

$$d(x) = \frac{1}{n} \sum_{i=1}^n K\left(\frac{x - x_i}{c_x}\right)$$

- **VoIP QoE evaluation**

- **E-Model**

$$R = R_0 - I_s - I_d - I_e + A$$

- **Mathematic Curve fitting**

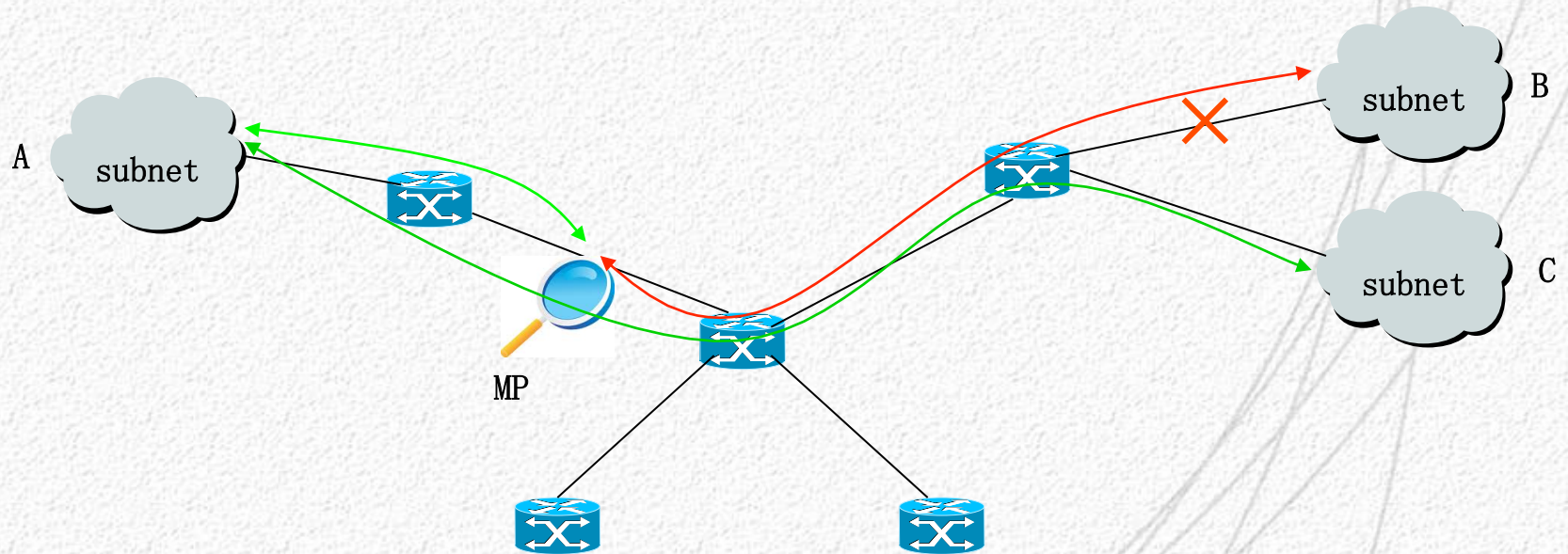
$$\begin{aligned} R &= R_0 - I_d - I_e \\ &= 100 - 0.024d + 0.11(d - 177.3)H(d - 177.3) + a \ln(1 + bp) + c \end{aligned}$$

- **What measurement can do?**
  - **Traffic statics**
  - **Services and behaviors analysis**
  - **Events alarm**
  - **E2E QoE tracking**
  - **Route topology deduction**
  - **Fault discovery**
  - ... ..

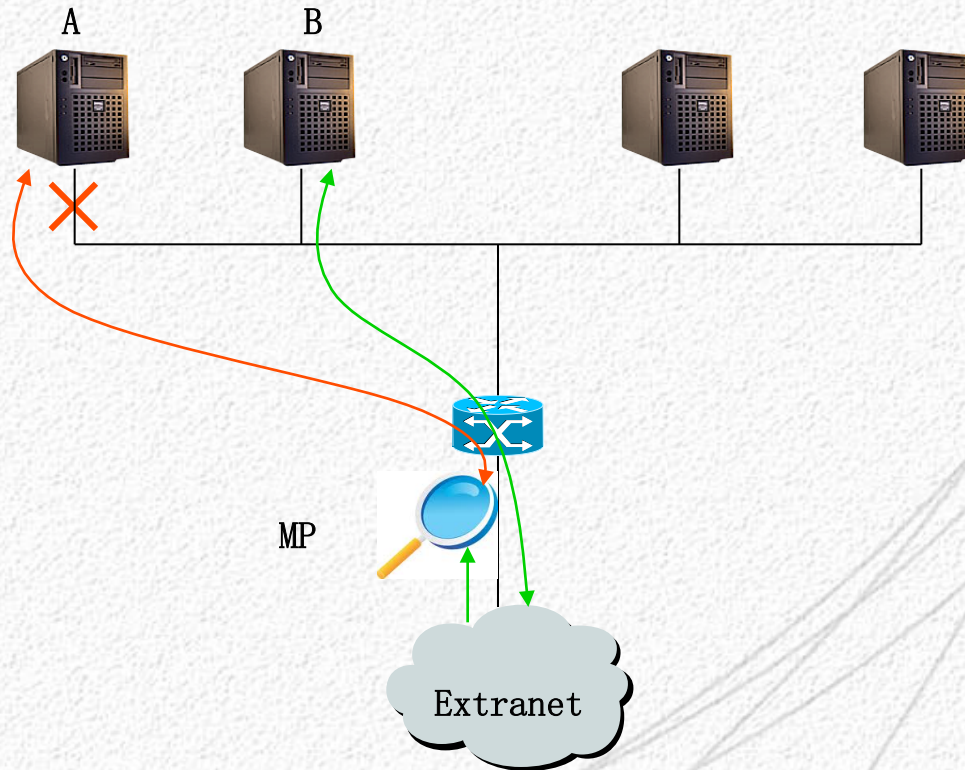
- **Corelations between traffic measurement and fault management**

<b>faults</b>	<b>measurement</b>
<b>Path broken/port loss</b>	<b>Continuous access fail to a specific subnet</b>
<b>Server down</b>	<b>Continuous access fail to a specific host</b>
<b>Network congestion</b>	<b>QoS/QoE varying</b>
<b>Trojan/worm/attack</b>	<b>Direct attack flow or abnormal flow</b>
<b>Terminal fault</b>	<b>varying on user unilateral QoE</b>
<b>Route change/balance fault</b>	<b>Varying on TTL/statics unusual</b>
<b>...</b>	<b>...</b>

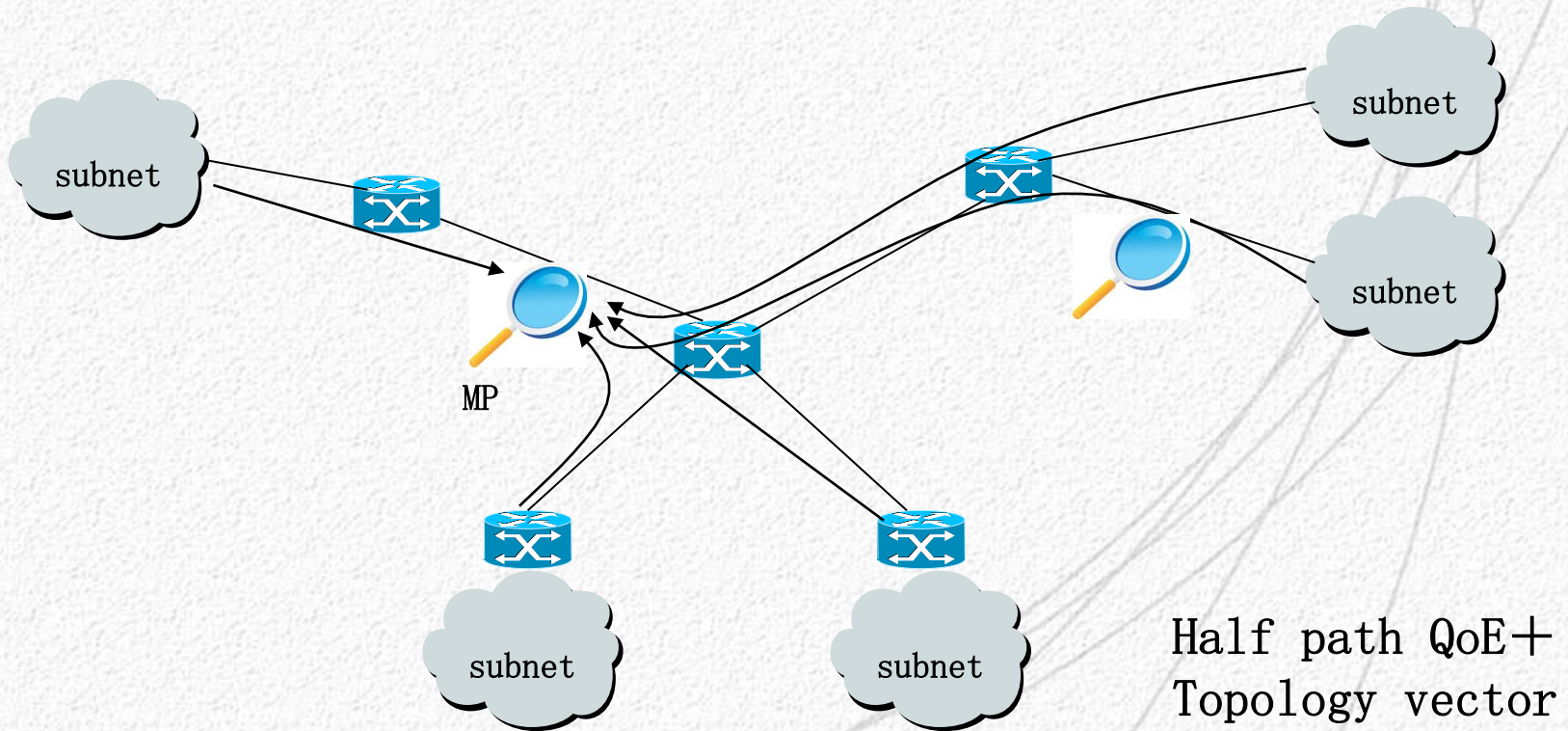
- IP path broken



- **Server down**

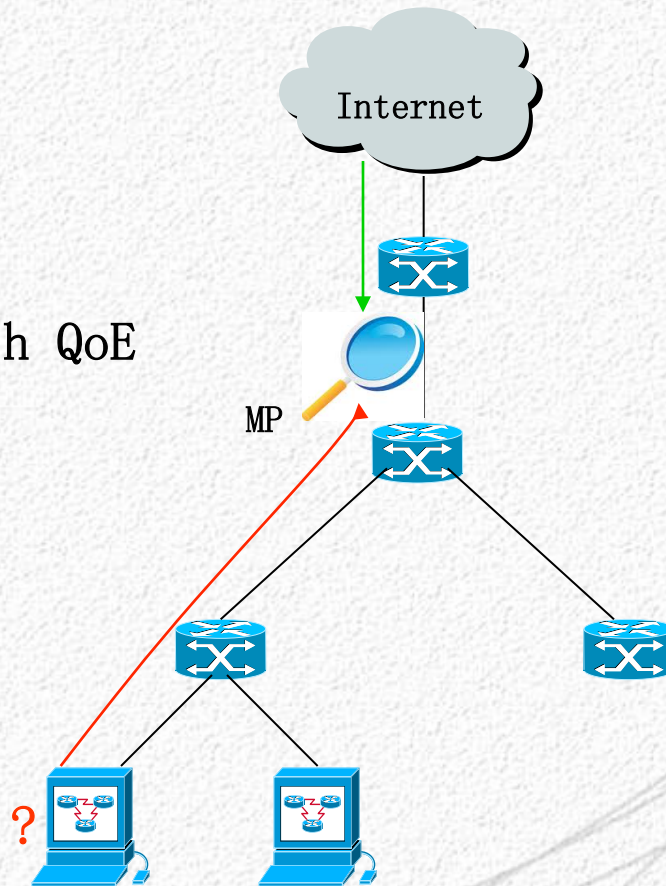


- **Network congestion**

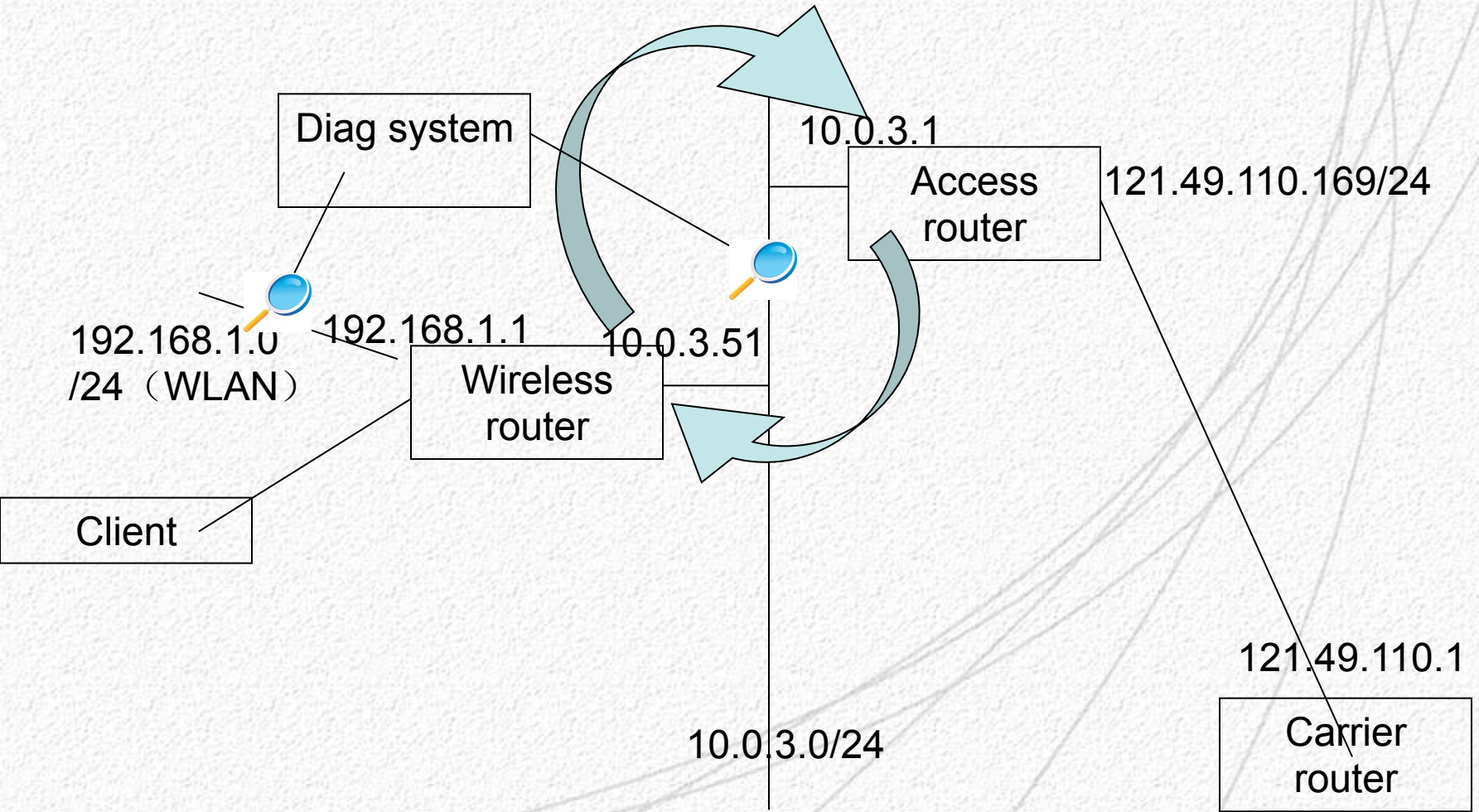


- Terminal fault

Half path QoE



# • IP loop



- VoIP QoE
- IP loop
- IP blackhole
- Route deduction



电子科技大学  
University of Electronic Science and Technology of China

[www.uestc.edu.cn](http://www.uestc.edu.cn)

Thanks