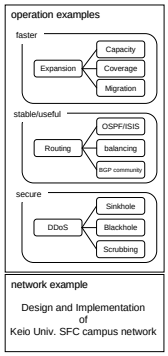
IT-Operation: Case Study (1)

Network Operation examples and Real network example

Yasuhiro Ohara
Seiji Ariga

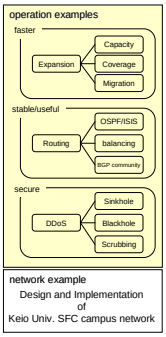
Contents

- Network operation examples
  - How to expand network
  - What we are doing in routing area
  - What is main issue on security operation in these days
- Real network example
  - Keio Univ. Shonan Fujisawa Campus



Network operation examples

An ISP engineer's daily(?) life



Introduction

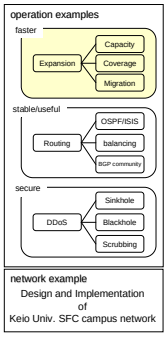
- Myself
  - I'm working at backbone ISP
- Today
  - I'll talk about my daily operation/work for an example of ISP operation
  - But I don't know how typical my daily life is …

Whose network is this ?

- Why do we operate our network ?
  - for users (in some case, customers) ☺
- What do we have to provide ?
  - faster network
  - stable network
  - secure network
  - useful network
- Then, let's think about what we should do

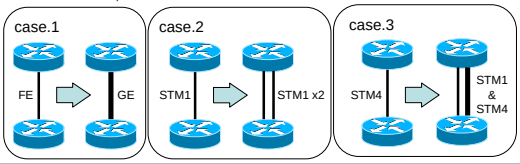
Faster network

- Network keeps changing (forever)
  - To meet user needs, to keep it efficient
- There are some types of expansions
  - Add more capacity in one place to accommodate growing traffic
  - Expand network coverage geographically for efficient operation
  - Network migration – If there are some 'networks' operated in the same manner, it should be migrated in one network



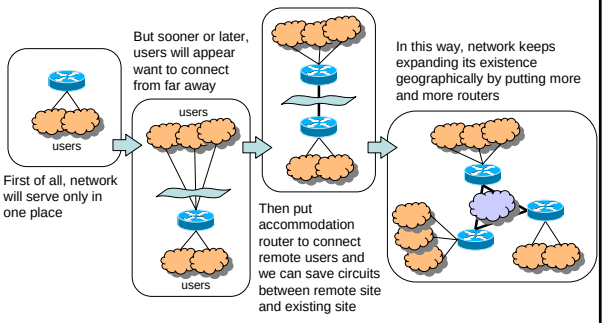
Capacity

- There are some ways just for upgrading
- What we should have in mind
  - Equipment constraints (“Is there any free ports ?”)
  - Operational constraints (“Can we interrupt our service ?”)
  - Circuit constraints (LAN or WAN)
  - Budget constraints
- Implementation
  - In case 3, we have to think about how to balance traffic



7

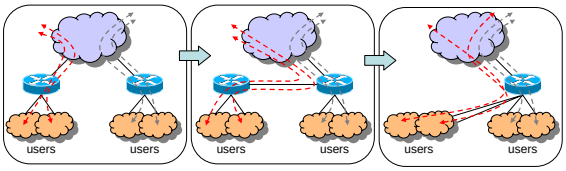
Coverage



8

Migration

- In some cases, we need to shrink network
  - user decreased, redundant nodes, budget
- What we have to care is to minimize
  - down time
  - impact on routing, etc.

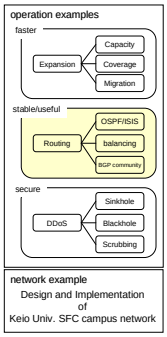


9

Stable and Useful network

- What is stability
  - No interruption
    - All sort of cause for interruption
  - I’m not vendor or L1 guy, so let me focus on Layer 3, “Routing”
- What is usefulness
  - There will be broad meaning
    - Fast, Secure, QoS, Multicast, …
  - In this session, I want to define as

    “Users can control their traffic to some extent”
  - How to give control to users ?
    - ex. BGP community

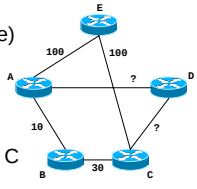


10

IGP

- IGP metric design is very important
  - especially in large/sparse network

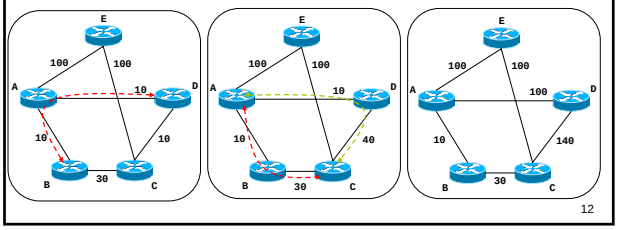
- Many protocols depends on IGP
  - just one small tweak will shift large amount of traffic and saturation starts suddenly (the same as BGP local-preference)
- For example,
  - D want to reach B via C
  - Try not to use A-E and C-E
  - But A don’t want to use D to reach C



11

IGP (cont.)

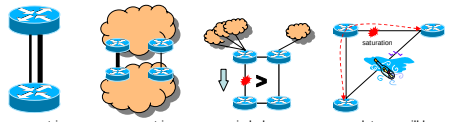
- There is no way to find “ideal” metric anyway
  - Try to pick all requirements up
  - From broad view point, try to find any impact on each change
    - Traffic flow itself
    - Effect on other protocols : PIM, MPLS, BGP …



12

Traffic Balancing

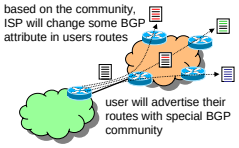
- There are many ways to do traffic balancing depends on the situation
- We will use following valuables for example
  - ASN
  - Prefix
  - BGP Community
- We're also able to use MPLS to some extent



asymmetric bandwidth | asymmetric bandwidth in geographically sparse network | imbalance input | latency will be very different

Traffic control by users

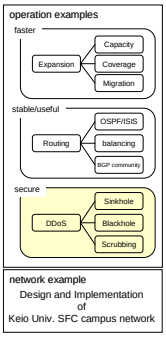
- Many ISP provide some ways to control users' traffic by themselves
  - mostly using BGP community (ex. http://info.us.bb.verio.net/routing.html)
  - example
    - prepend
    - stop announcing routes to certain party
    - change Local Preference



- Some ISP provide trigger for enabling filtering in case of, for example, DDoS attack

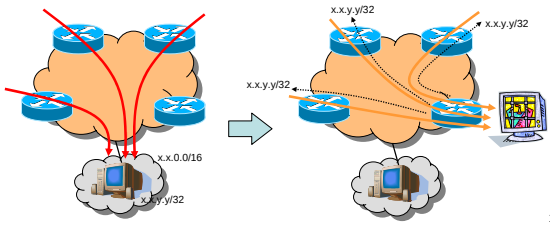
Secure network

- Nowadays, DDoS (Distributed Denial Service) attack is getting worse and worse …
  - Virus→Botnet→DDoS→Phishing
- ISP are try hard to mitigate junk traffic and save their users
  - They try to analyze/filter/clean up junk traffic



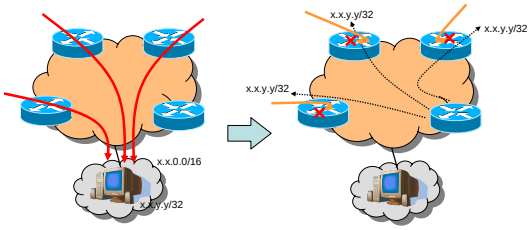
Sinkhole (analyze)

- Redirect attack traffic to certain place to analyze traffic
  - announcing more specific routes



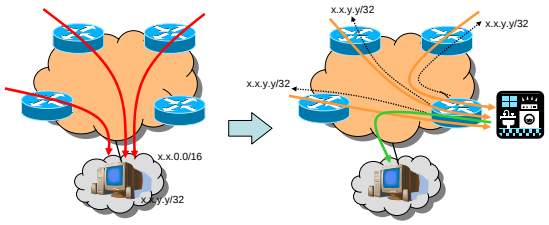
Blackhole (filtering)

- Discard attack packets at border routers
  - set null routed static on each border routers
  - announce specific route with BGP NextHop destined to that null routed static



Scrubbing (clean up)

- Try to clean attack traffic up
  - By using sinkhole/blackhole, communication to victim host is still incapable. This means DoS succeeded anyway.
  - By using scrubbing box, valid traffic can go to victim host during filtering attack traffic



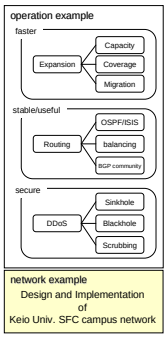
Summary for “Operation examples”

- Network operation is very interesting ☺
  - There are a lot of things to do (and will be forever)
  - Try to have micro/macro point of view at the same time
  - Be nice to users
    - They’re selfish, but they kindly help us to make things better at the same time
- Network operation is very boring ☹
  - There are still a lot of primitive/routine work
  - But we can eliminate them and improve quality of network and life

19

Real network example

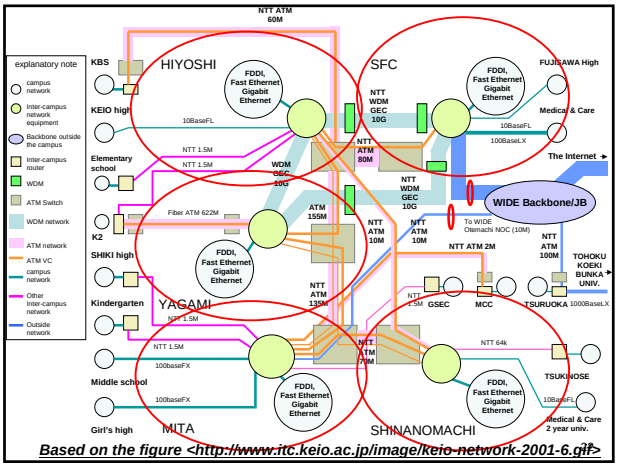
Design and Implementation
of
Keio Univ. SFC campus network



Keio Univ. and its SFC campus

- Keio Univ.
  - Private university, since 1858 (First university in Japan)
  - 8 Campuses:
    - Mita, Hiyoshi, Shinanomachi, Yagami, Shonan Fujsiawa (SFC), Tsuruoka, Kawasaki(K2), Marunouchi (MCC)
- SFC campus
  - Since 1990, Junior, Senior High school, 3 faculties and graduate school
  - Area: over 230,000 square meters, 17 bldg
  - approx. #students:
    - Bachelor 4,430
    - Master 370
    - Doctoral 170

21

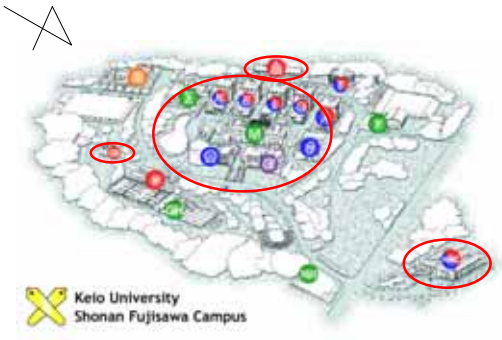


design policy and its goal for SFC campus

1. usability / flexibility
   - various research labs have various demand
   - loose policy to respond to them
2. Security
   - public trend, provides least security
3. cost performance balance
   - operational cost will lead employment cost
   - trade-offs: which is preferred above 1 or 2 ?
   - trade-offs: a few fine devices or poor but many devices?

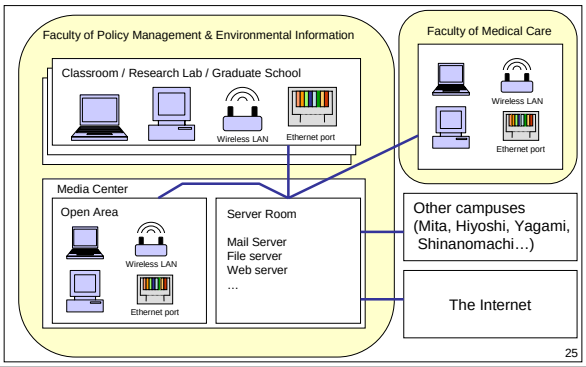
23

Keio Univ. SFC Campus



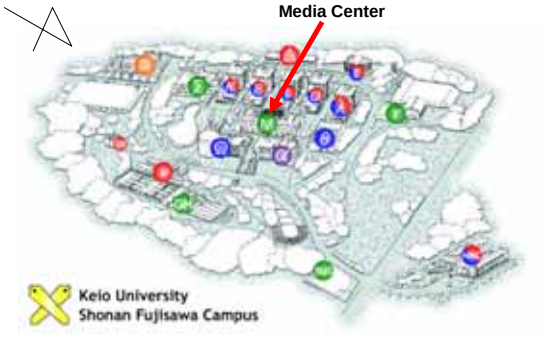
24

Centralized operation model (Media Center)



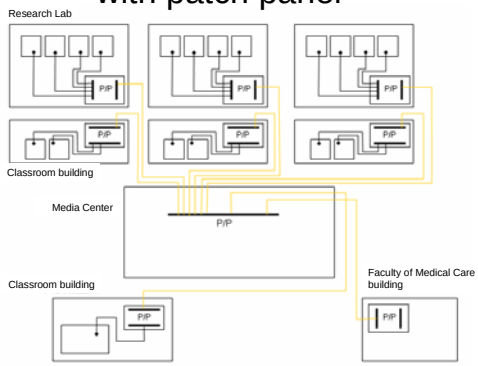
25

Keio Univ. SFC Campus



26

Inter building connection with patch panel



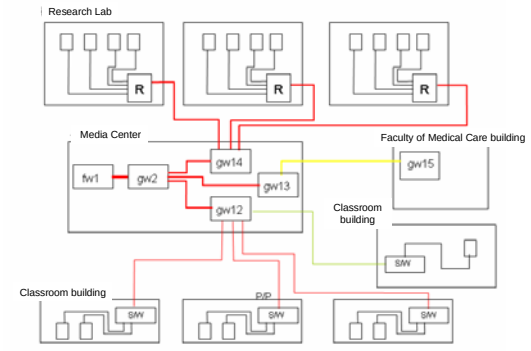
27

Necessity of Patch Panel

- Flexibility
- Unknown usage for future, e.g.
  - Link aggregation by user demand
    - GEC (Gigabit Ether Channel), IEEE 802.3ad, even WDM in future, etc...
  - Alternative/backup for other circuit's line cut
    - Change only patching port of troubled circuit/link
- Operational cost can be decreased
  - e.g. moving the terminating device in remodeling the NOC room, the length of cable needed may change

28

Abstracted connection between L2/L3 devices



29

Abstracted Physical connection in SFC campus

30

Ethernet Specification

– SMF: SI: Step-Index, <10μm, 125μm
– MMF: GI: Graded-Index, 50μm or 62.5 μm, 125 μm

spec name	IEEE spec	media (wave-length)	operating distance
10Base-FL	802.3j	MMF (850nm)	2km
100Base-TX	802.3u	UTP	100m
100Base-FX		MMF (1310nm)	2km
		SMF (1310nm)	10km
100Base-SX		MMF (850nm)	2km
1000Base-T	802.3ab	UTP	100m
1000Base-SX	802.3z	MMF (850nm)	550m
1000Base-LX		MMF (1310nm)	550m
		SMF (1310nm)	5km
10GBase-SR	802.3ae	MMF (850nm)	65m
10GBase-LR		SMF (1310nm)	10km
10GBase-ER		SMF (1550nm)	40km

31

Network Configuration Summary

- Backbone consist of 3 (high-performance) L3 switches and aggregated link e.g. 4Gbps
- Most edge segments support 1Gbps
- Tree form (basically no physical loop)
  - redundancy is provided by technologies below L2
    - link-aggregation
    - redundant module/power unit
- VLANs: IEEE 802.1q
- Link Agg: GEC (v.s. IEEE 802.3ad)
- STP (IEEE 802.1d) enabled in core networks
- STP not enabled in edge networks
  - user may accidentally create L2 loops ...

32

IP/Routing

- Class B address space (/16)
- OSPF with 2 stub area
  - most are static
- static route between SFC and WIDE
  - aggregate 8 links by GEC, HSRP enabled
- Employs static IP packet filtering
  - need-to-apply basis
- applies MAC-based black-list filtering in DHCP

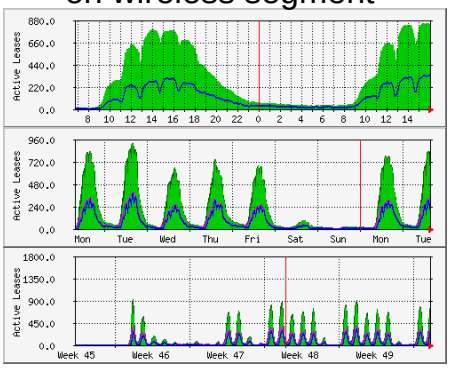
33

Wireless Operation

- Operating IEEE802.11b
  - Covers almost all field as well as all room in buildings (approx. 200 APs)
  - APs are from multiple vendors (3 vendors)
  - Type of AP depends on the usage (i.e. #users) at each location
- Policy
  - Roaming is demanded (Ubiquity)
    - AP areas as a whole forms one IP segment (/21 !)
  - No security / authentication
    - Easy-to-use for many guests visiting here
  - security can be provided by upper layer
    - HTTPS, SSL, ssh, etc ...

34

DHCP statistics on wireless segment



35

Traffic

- peak traffic is around 100Mbps

36

Miscellaneous

- Strategy (loose, changing)
  - bandwidth estimation
    - *Upstream bw* > *edge segment bw* x 10
      - if port many then additional x 2
    - *Upstream bw* > *actual traffic* x 2
  - upgrading facilities
    - Incremental upgrades on user demand
    - e.g. additional installation of inter-building fibers
- Empirical feelings
  - Upgrading fiber is necessary at an interval of about 10 year (About to upgrade from MMF to SMF to support 10G)
  - Upgrading metal is necessary at an interval of about 4 year (CAT3, CAT5, CAT5e, CAT6)
- Everything falls in cost-performance balance problems

37

THE END

Any questions ?