29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

A System Dynamics Model for Systems Security Engineering Analysis of Internet Service Provider Customer Modem Cyber Defense

SD for SSE of ISP Modem Defense

Presented by David Eason, incose@eason.cc

Paper Co-Author: Don S. Gelosh, Ph.D., dsgelosh@wpi.edu

www.incose.org/symp2019

Copyright © 2019 by David Eason. Permission granted to INCOSE to publish and use.

Bandwidth Clutter Evidence & Impact

100ms Wait for Page Load

1% Profit Loss for Amazon >$1B in 2018

*Credits, respectively: https://news.mit.edu/2016/system-loads-web%20pages-34-percent-faster-0309, https://ir.aboutamazon.com/annual-reports/, https://www.statista.com/topics/3201/ad-blocking/?,

Bandwidth Clutter Evidence & Impact

Ad Blocker Usage in the U.S.

2016	2017
12%	27%

*Credits: https://www.statista.com/topics/3201/ad-blocking/?,

Probes Against My Home Server

- Within 5 hours:
  - dozens of foreign SSH probes received
- Within 5 days:
  - 1000+ probes daily

Malware Attacks per Year

…in BILLIONS

2017	2018
8.6	10.5

*Credits: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

Reducing Bandwidth Problems Would…

- Speed page loads
- Offer cleaner, distraction-free views
- Improve data privacy and safety

SSE using SD can help ISPs model improvements, benefiting customers and ISPs.

ISP Stakeholder Concerns

Customers

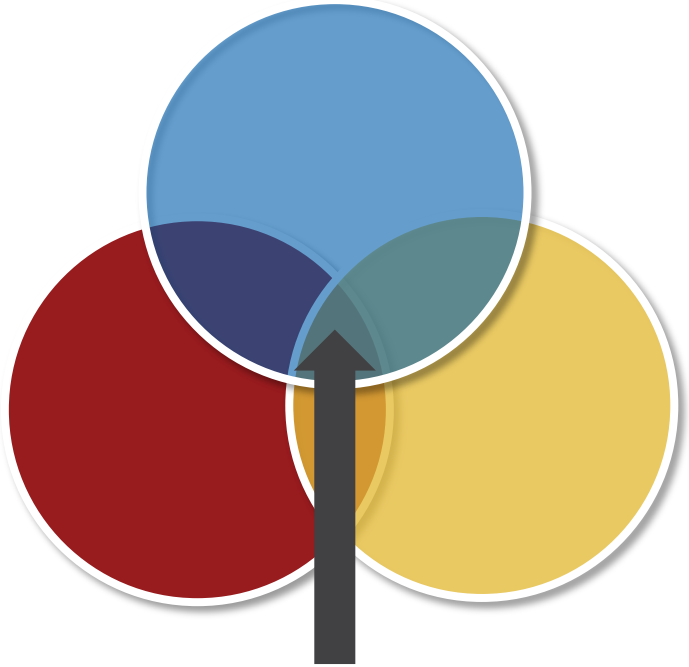
Fast, Cheap, Good

Data privacy and online safety too

Shareholders

Make money

Keep customers



Management

If it ain't broke…

… but keep everyone happy

Find the Sweet Spot!

Strategies for Improved ISP Service

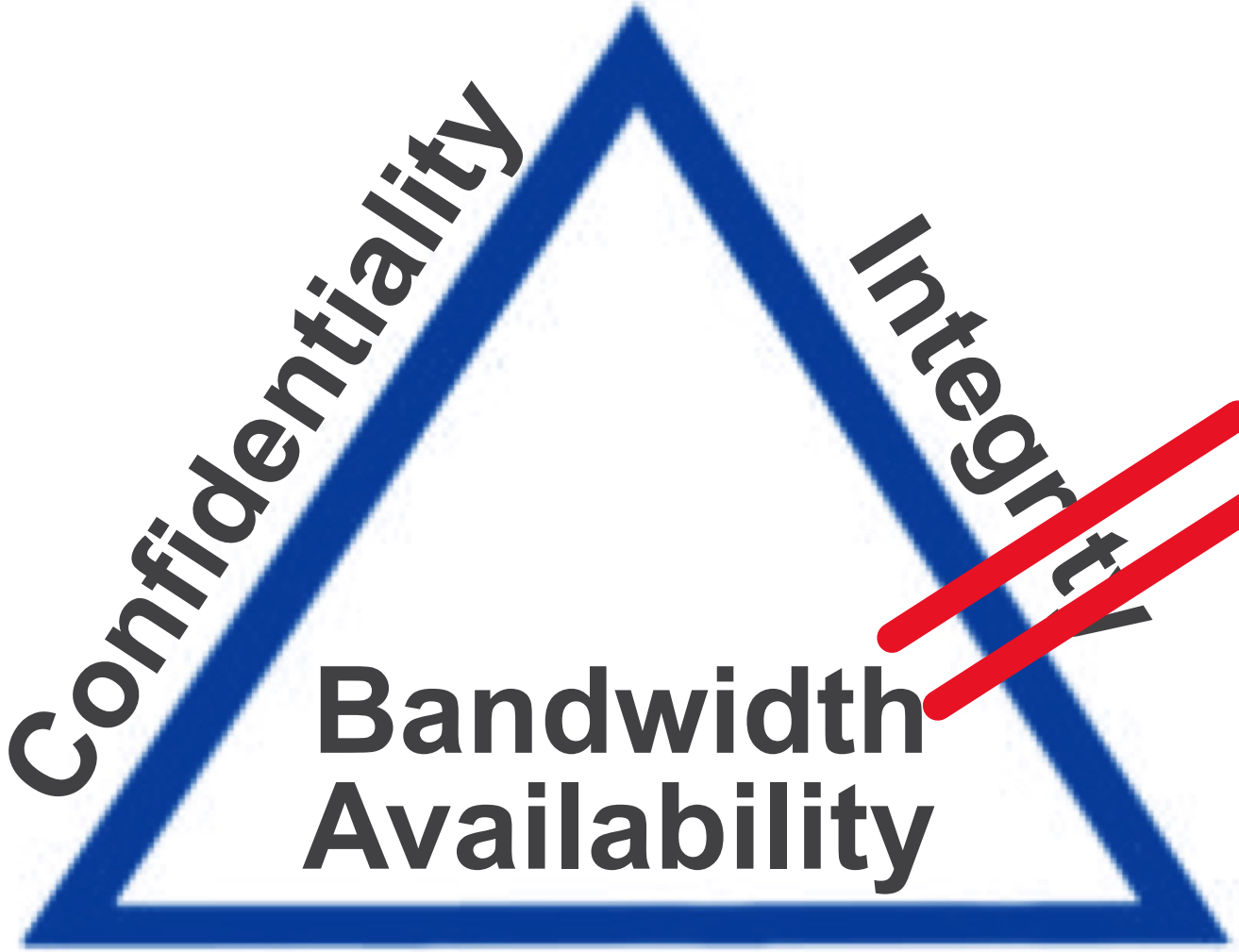
Serve More Customers
for less money

Create Competitive Moat
Add value beyond physical infrastructure, save time, protect data and bandwidth

Do It Faster
and better

Control Risk
Test process changes before broad application

Key Performance Indicators (KPI) from CIA



More & Happier Customers!

System Dynamics (SD) and KPIs

- **Define, rank, weigh KPIs**
- **Model** ISP systems with respect to **KPI**
- **Measure** actual KPIs and compare to model
- **Compare** process alternatives & pick one
- **Try it small** ←→ Validate & tweak model
- Repeat until satisfied, then **GO BIG**

Keys to Successful SD Modelling

- Management's involvement
- Iterative comparisons of diff. processes
- Compare SD model to the live system
- Improve model to make it match the system

The Data Is The Thing

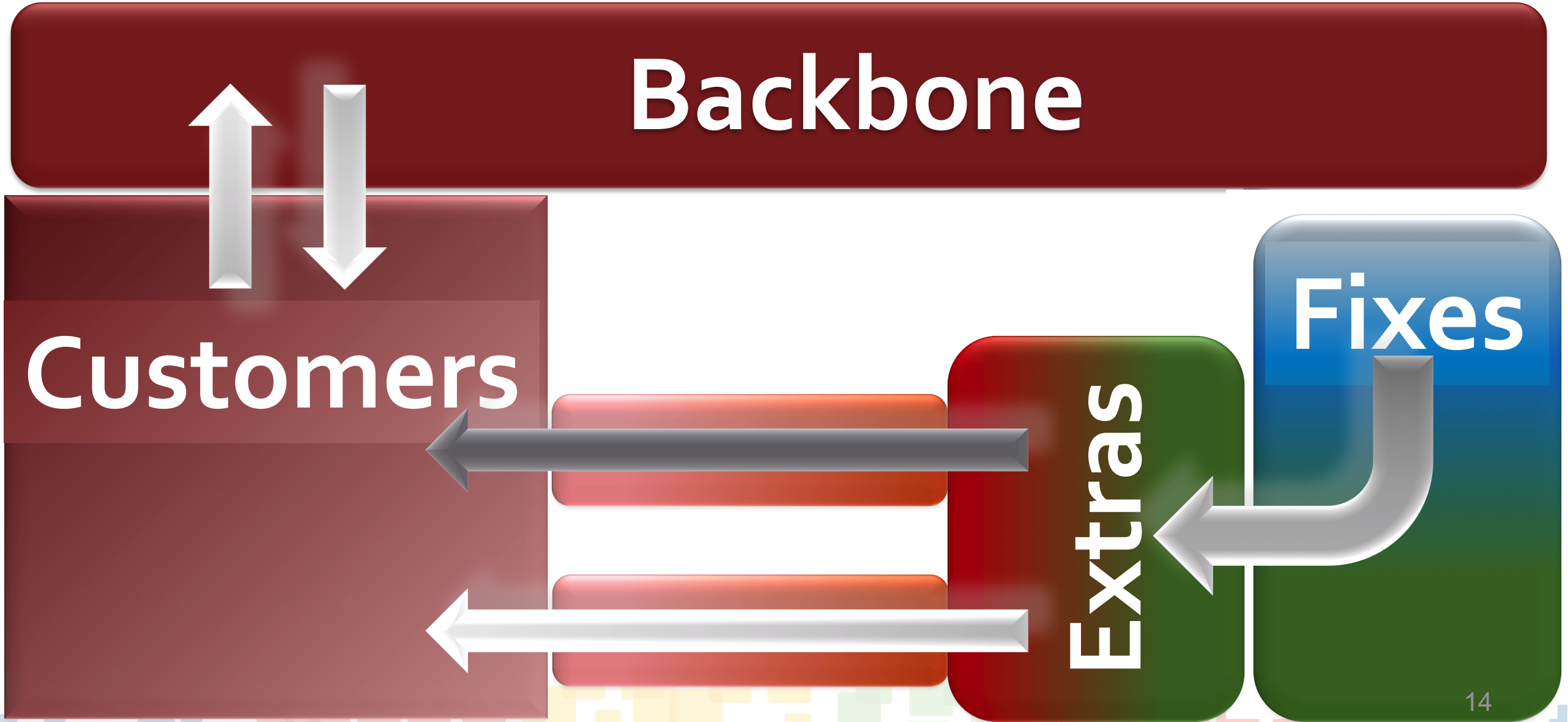
- Network engineers can measure actual bandwidth usage and types
- System Dynamics (SD) model output can be compared to live systems pre/post process changes

picture from https://ghidra-sre.org/

Presuming ISPs have the…

- **Motivation** to improve bandwidth
- **KPIs and measurability**

Now for the SD model…


Backbone
Customers
Extras
Fixes

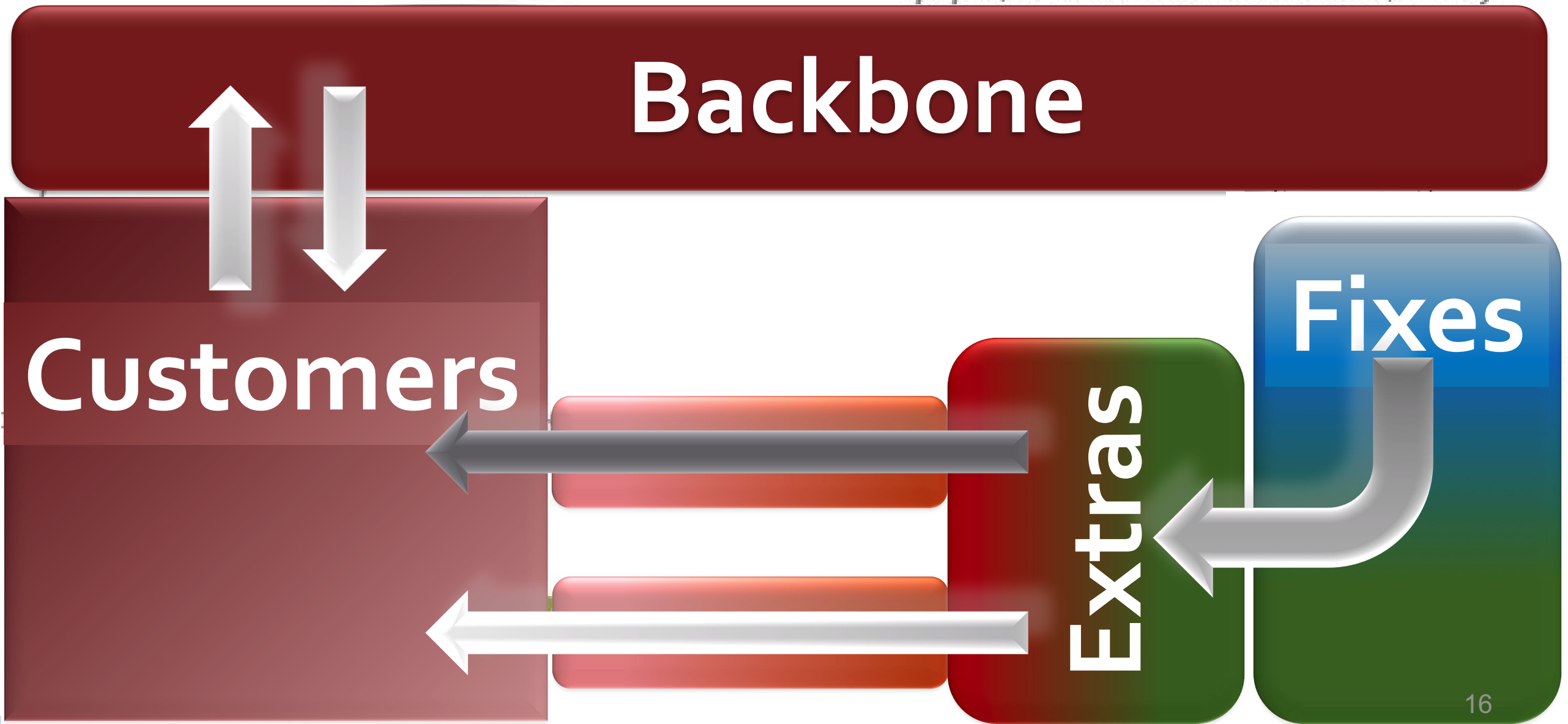
(Synonyms to Reduce Slide Clutter)

- odd = extra = undesired traffic
- fixed = mitigated = dampened
- user = customer = consumer
- will = goodwill = customer satisfaction

- [subset] refers to another (1 or more) sets

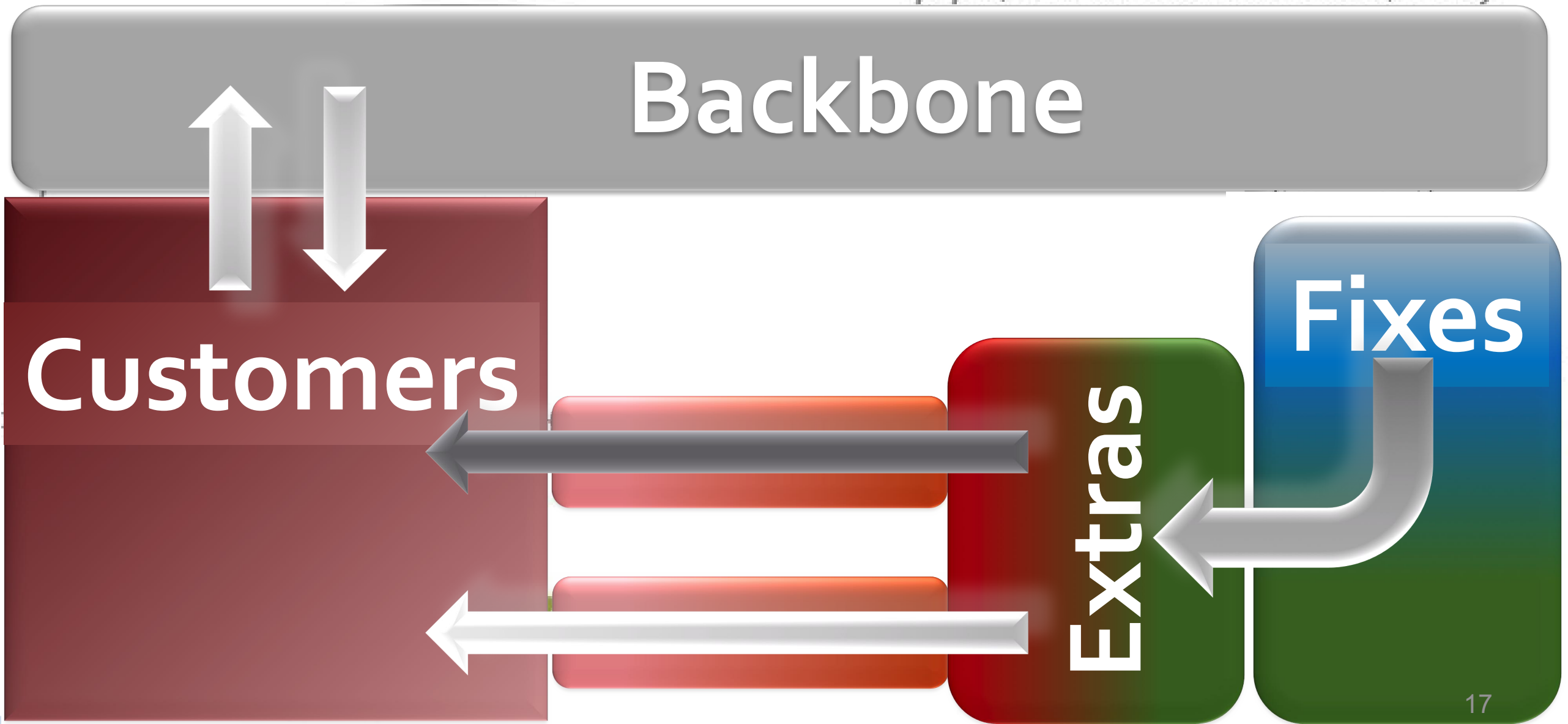
ISP overview

SUFFIX KEY: B=bits, P=percent, H=hour, p=per, N=dimensionless number, D=day



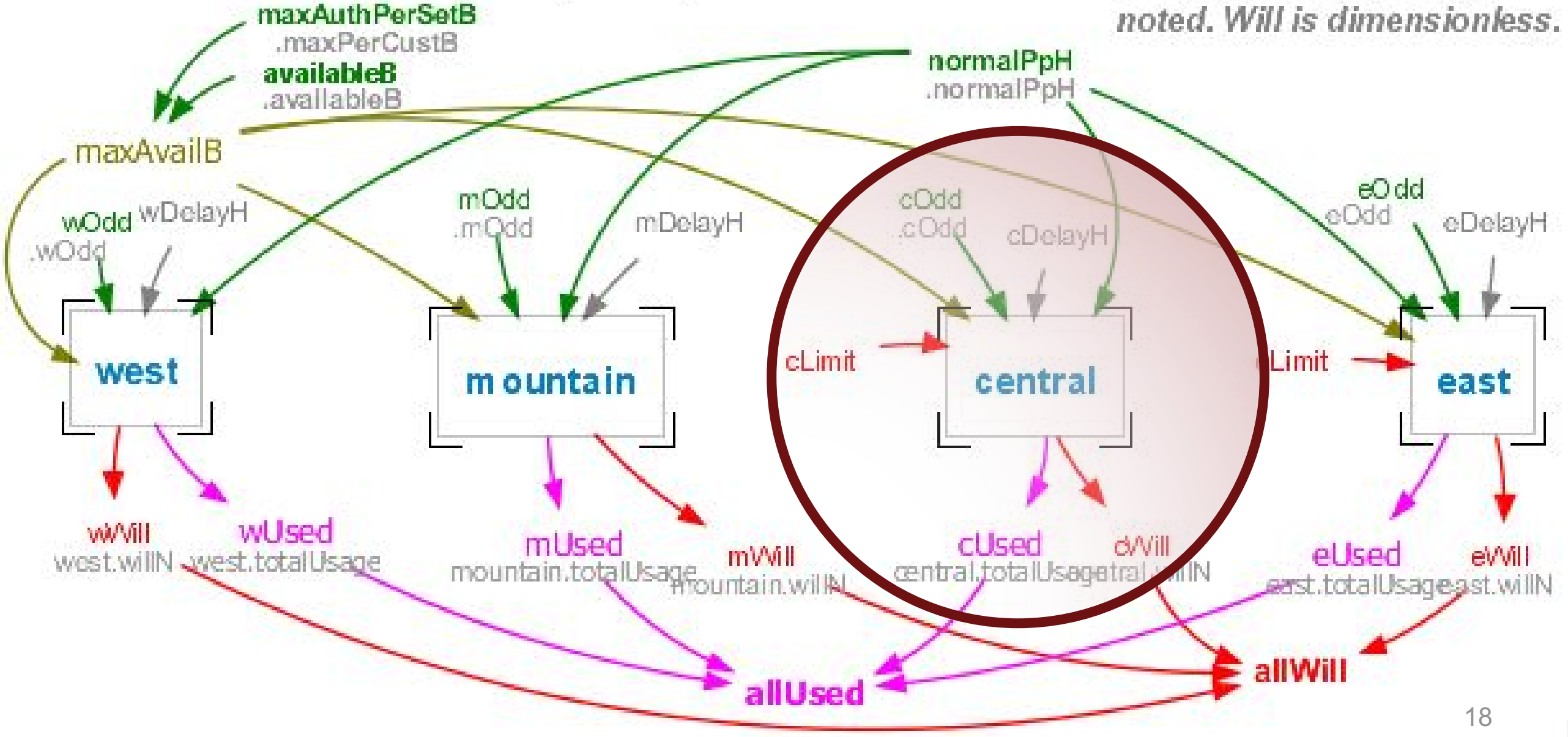
ISP overview

SUFFIX KEY: B=bits, P=percent, H=hour, p=per, N=dimensionless number, D=day



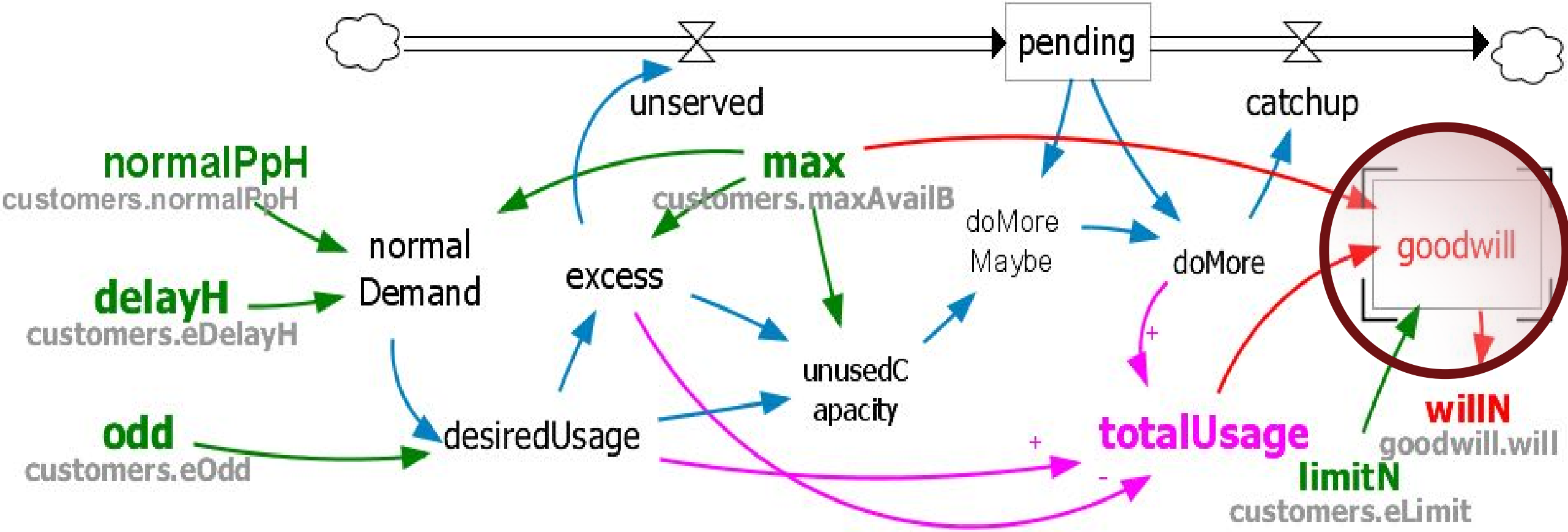
Customers: all sets, shown separately and summed

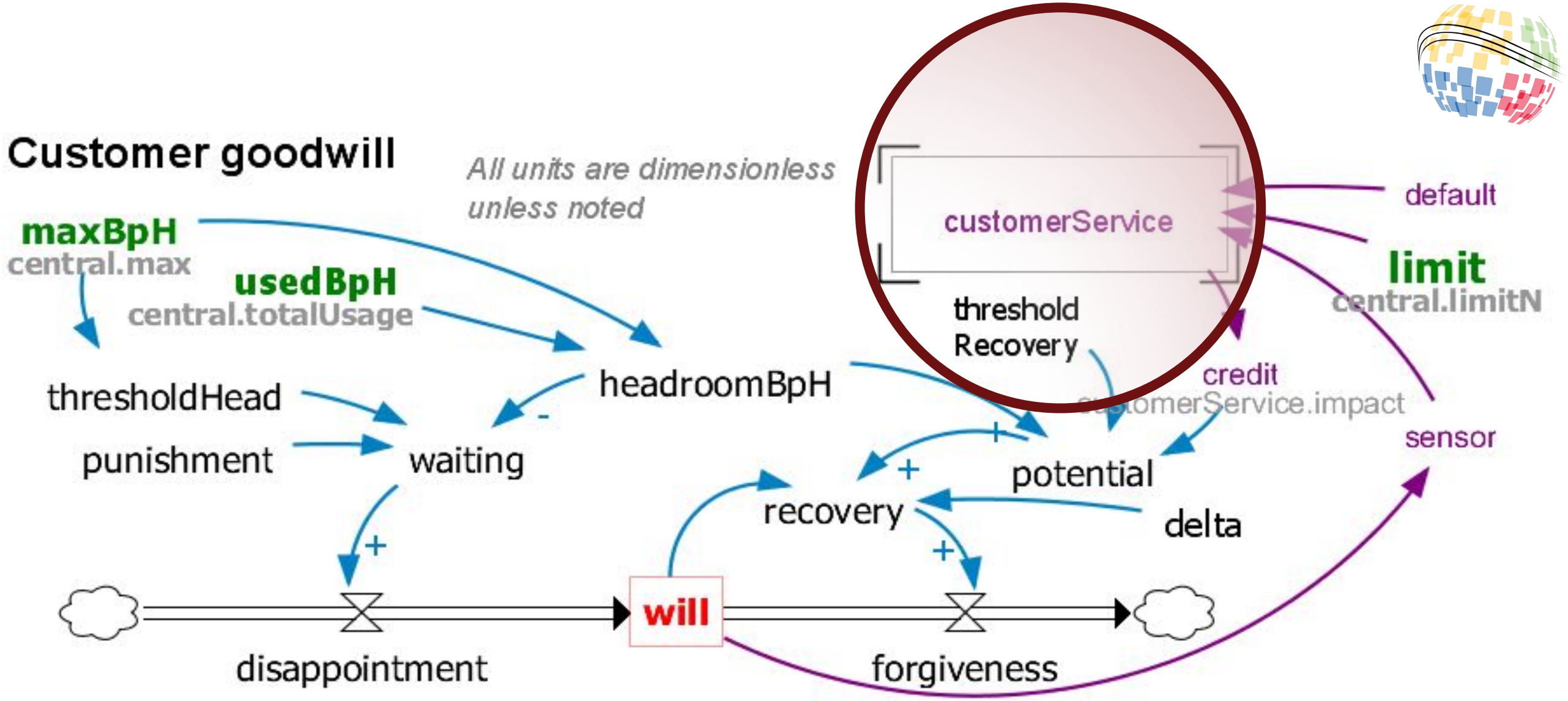
All units are BpH unless noted. Will is dimensionless.

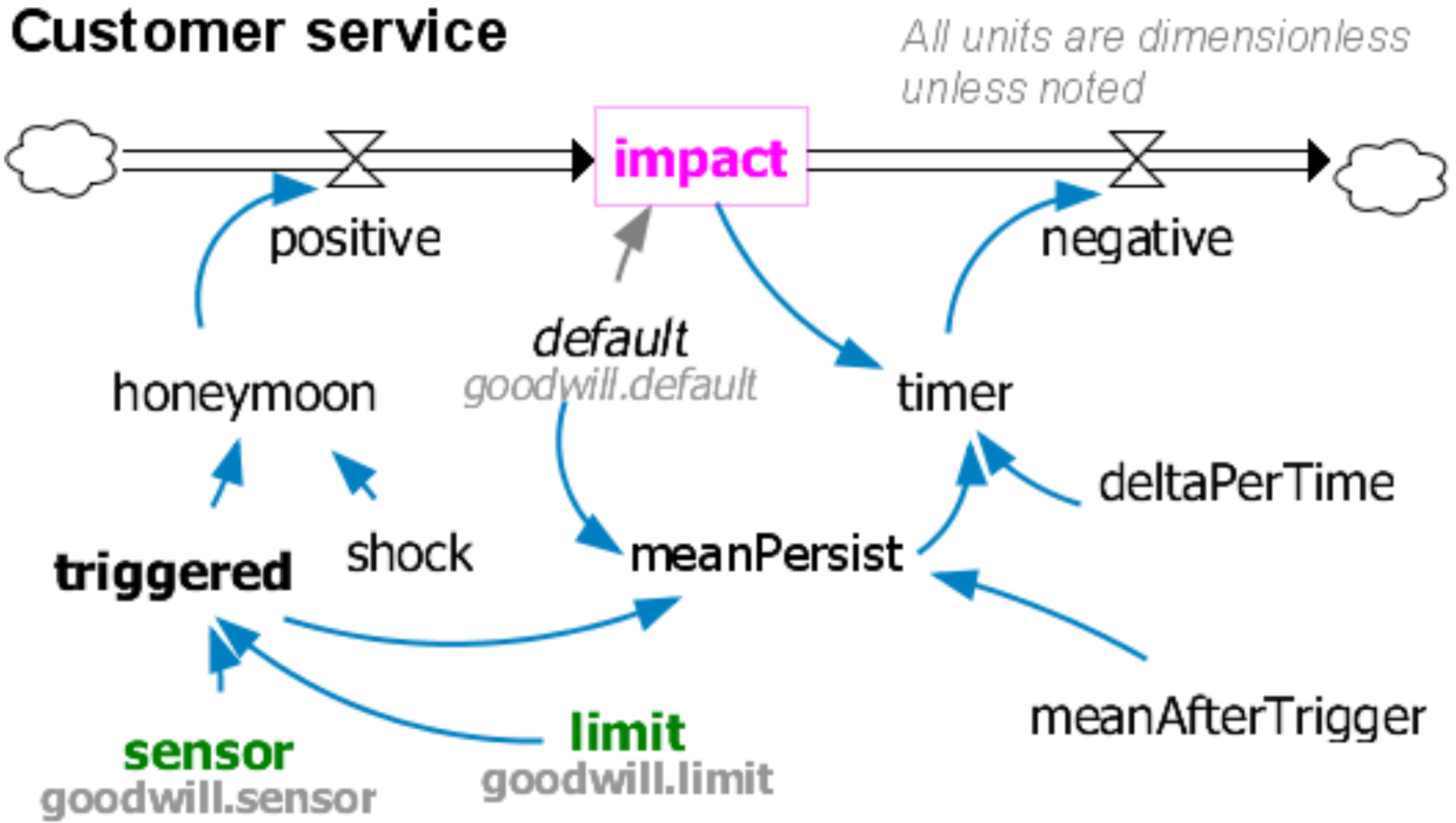


Customer traffic (normal+odd+pending) and Goodwill

All units are BpH unless noted



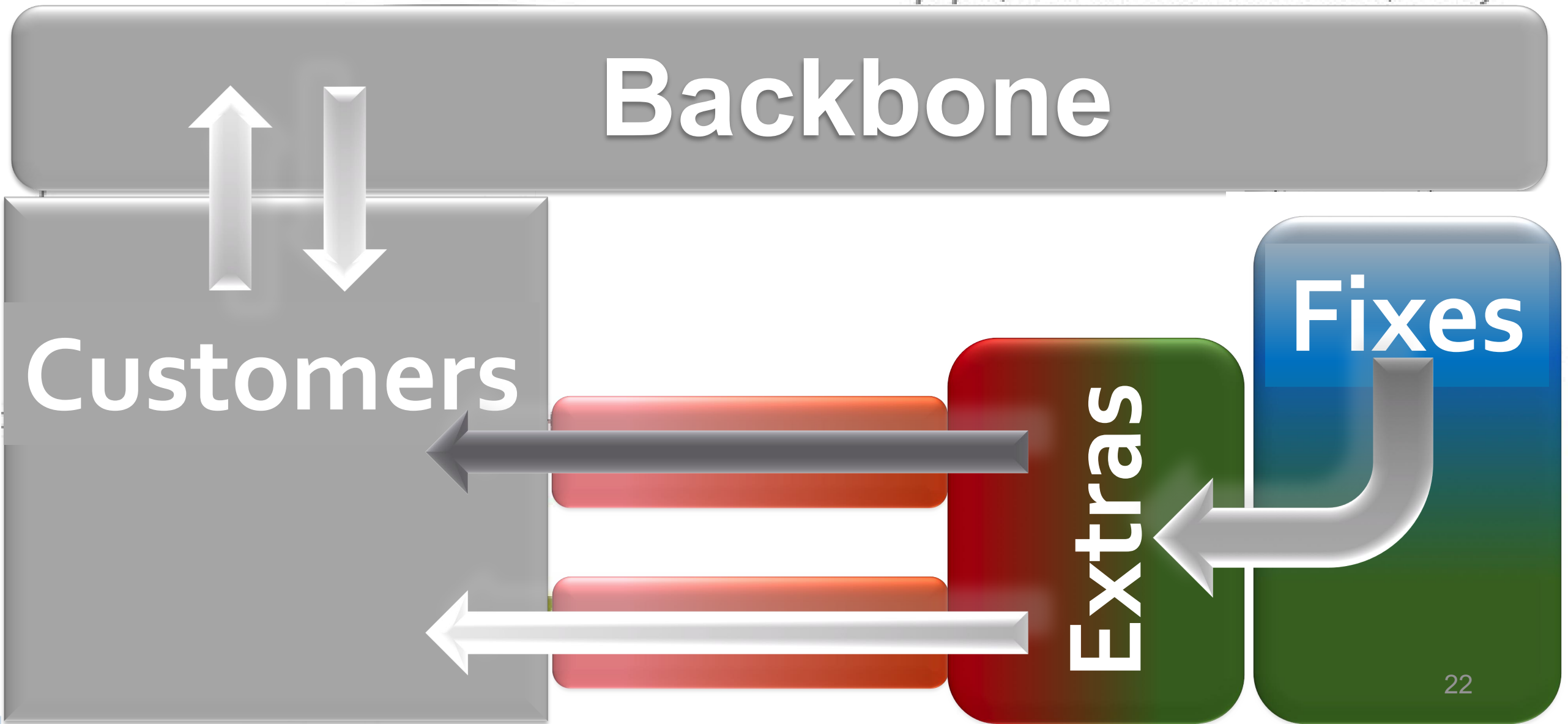

Customer goodwill
All units are dimensionless unless noted
maxBpH
central.max
usedBpH
central.totalUsage
thresholdHead
punishment
waiting
headroomBpH
customerService
threshold
Recovery
default
limit
central.limitN
credit
customerService.impact
potential
sensor
recovery
delta
will
disappointment
forgiveness



End of Customer Deep-Dive

ISP overview

SUFFIX KEY: B=bits, P=percent, H=hour, p=per, N=dimensionless number, D=day



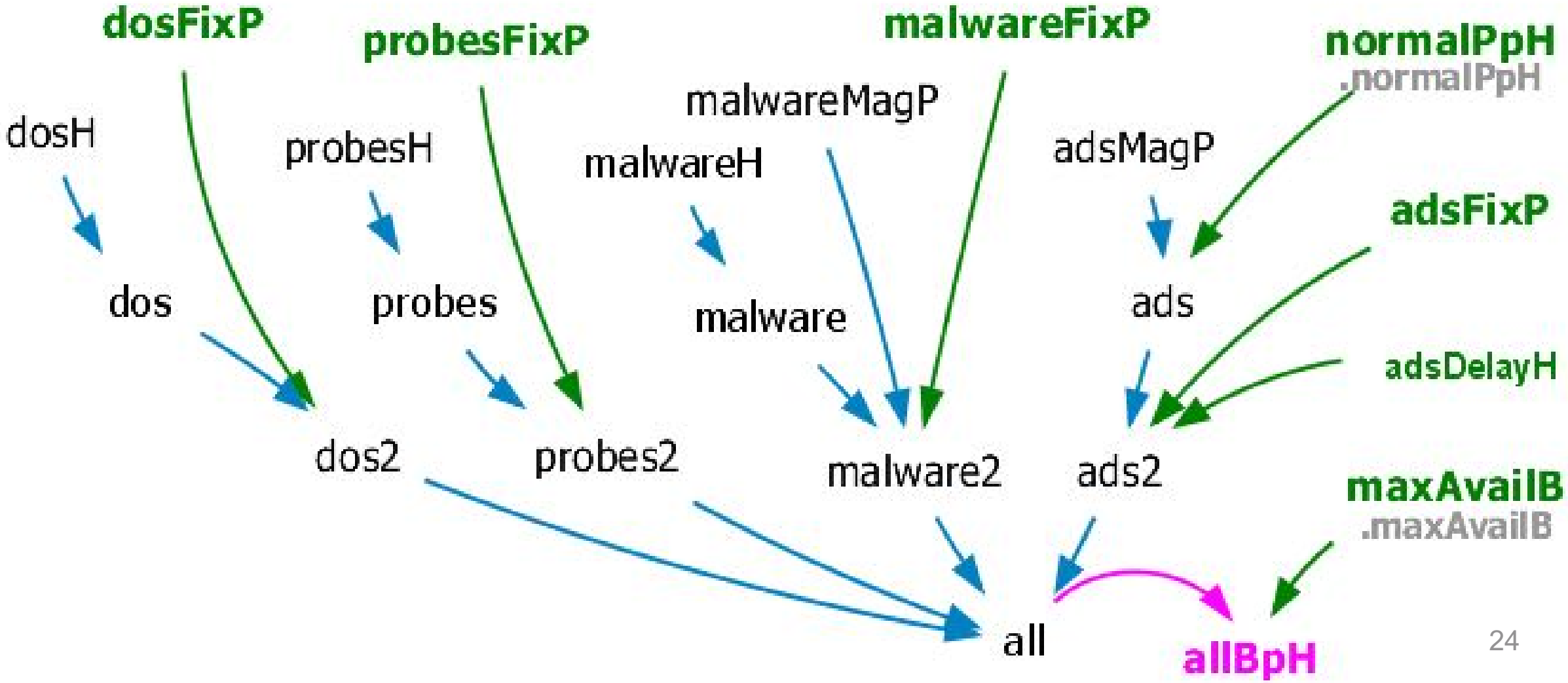
Extras Add to Normal User Traffic

Name	Frequency	Volume	Impact
Ads	High	Low/Moderate	Low
Probes	High	Low	Low
Malware	Low	Low/Moderate	High
DoS/DDoS	Low	High	High

“The Data is the Thing”: measure actual frequency and volume of each. Prioritize and model the “signals” from each. Use data as input to the model (next slide).

Extras: Undesired traffic contributing to total customer traffic usage

All units are BpH unless noted



Sample Modem Bandwidth, 1 Customer

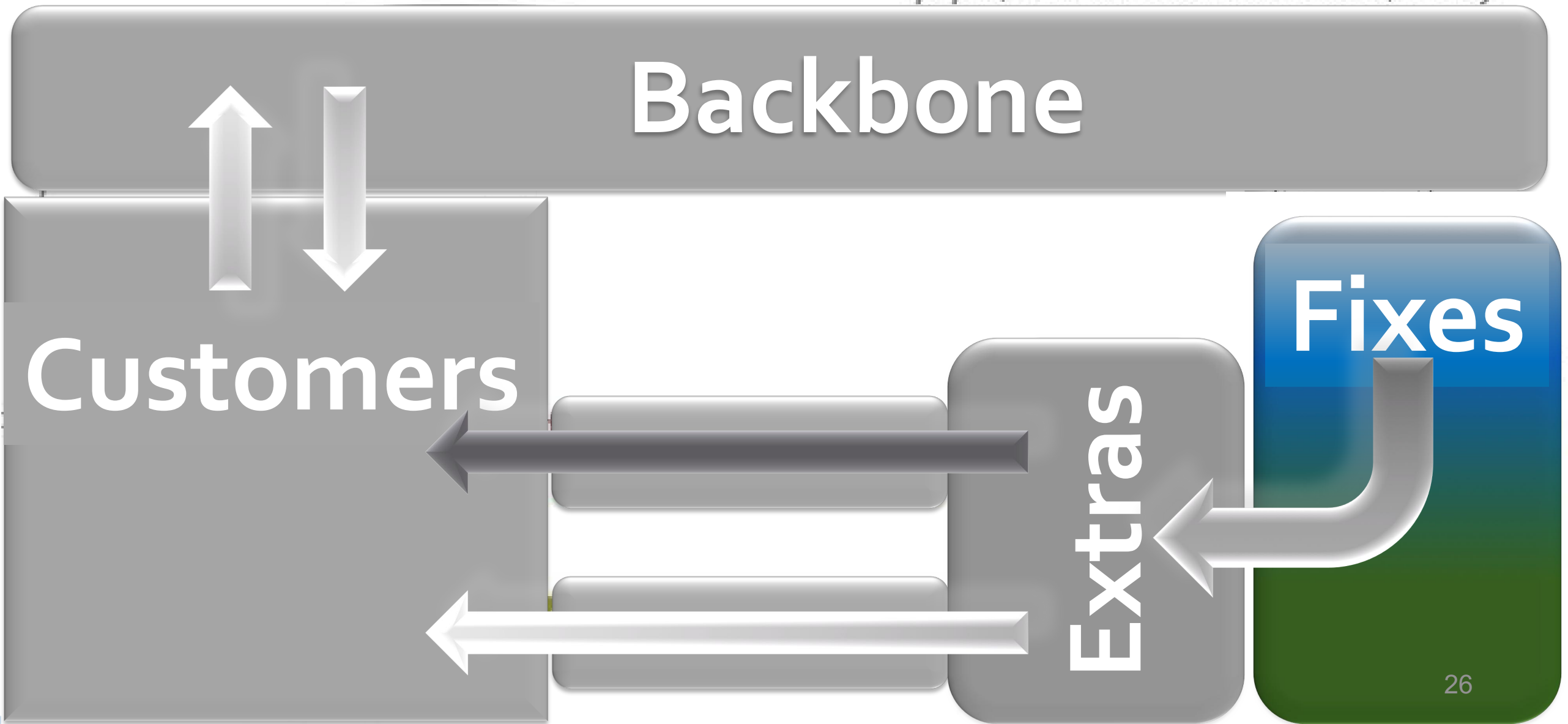
This 30-hour graph is the sum of all signals, capped by user limits, from:

- **normal traffic**
- **extra bandwidth types** (DoS, probes, malware, ads)

Note: this is ONE customer. Later graphs represent SETS of customers.

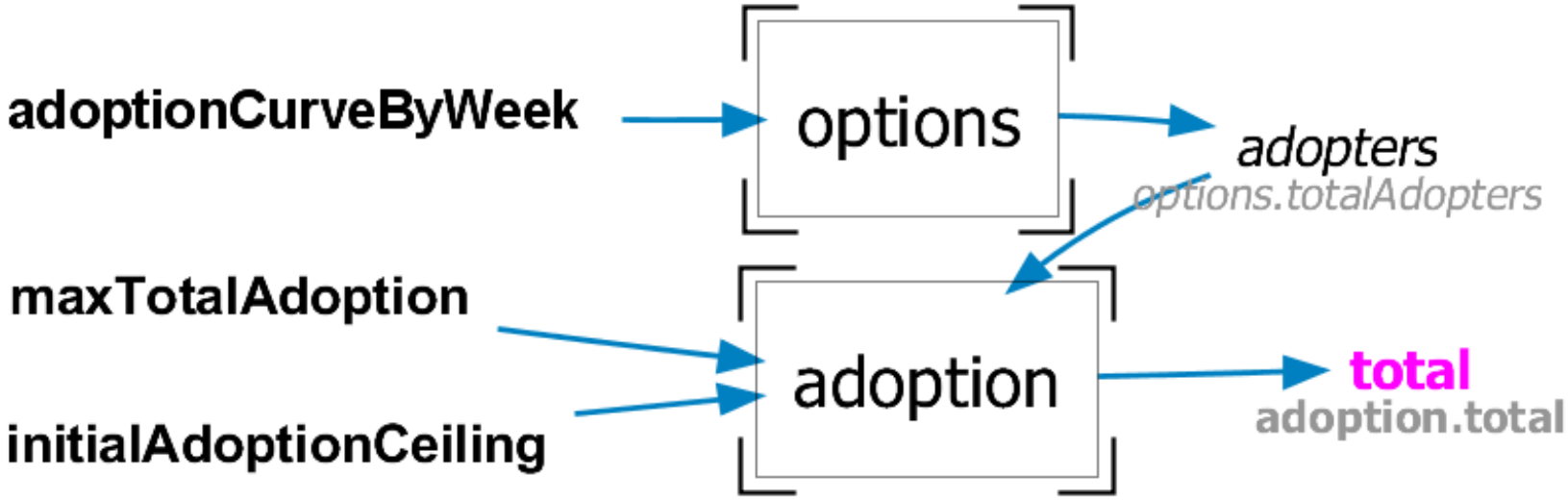
ISP overview

SUFFIX KEY: B=bits, P=percent, H=hour, p=per, N=dimensionless number, D=day



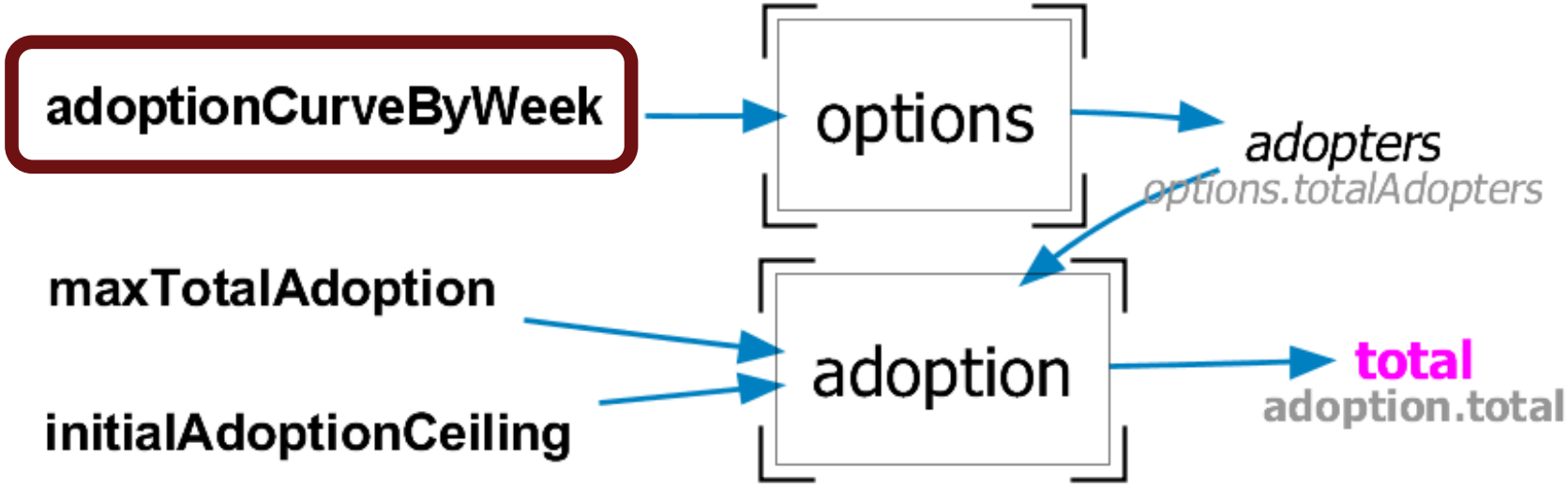
Fixes: Dampening of odd traffic by increasing P of adopted improvements

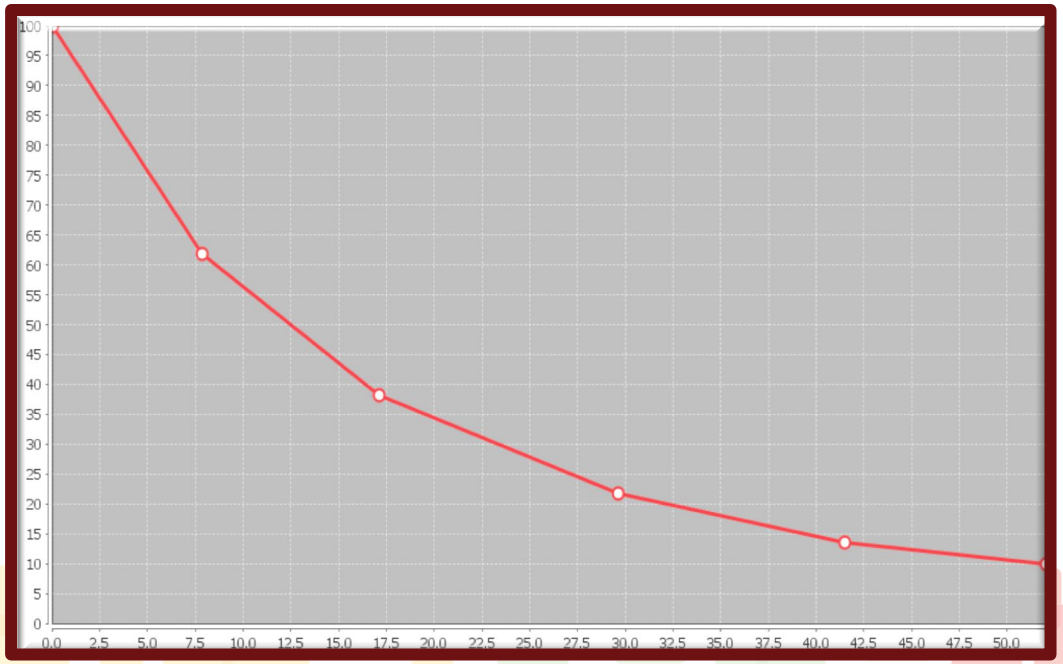
All units are PpH



Fixes: Dampening of odd traffic by increasing P of adopted improvements

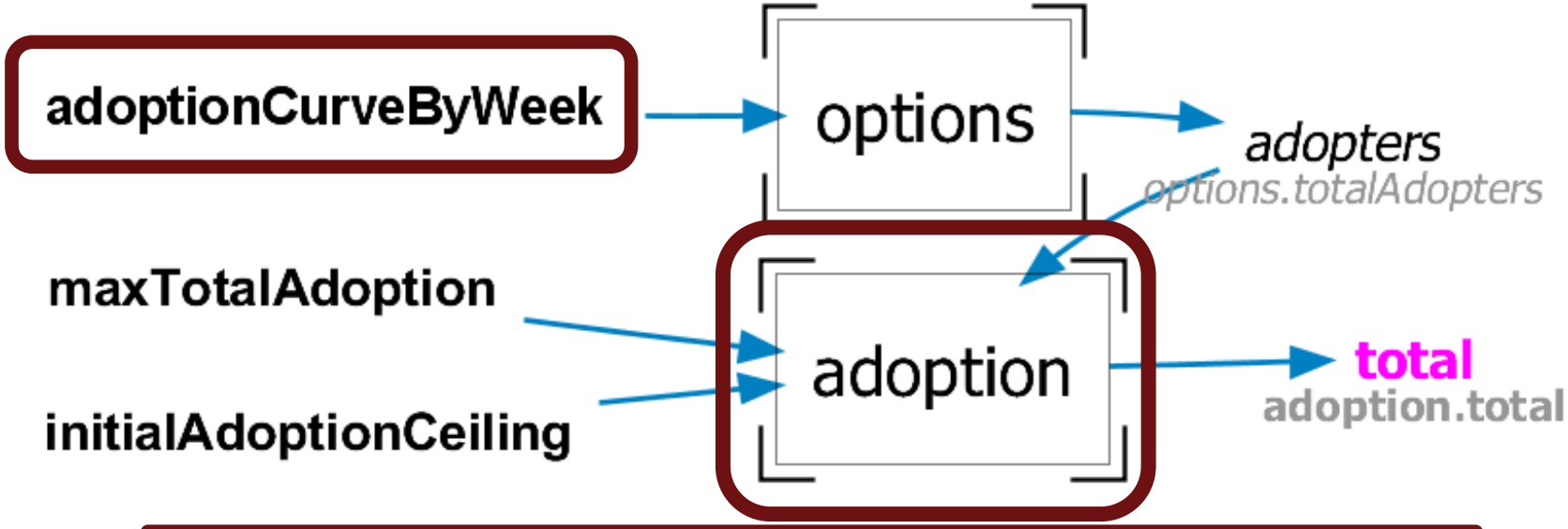
All units are PpH





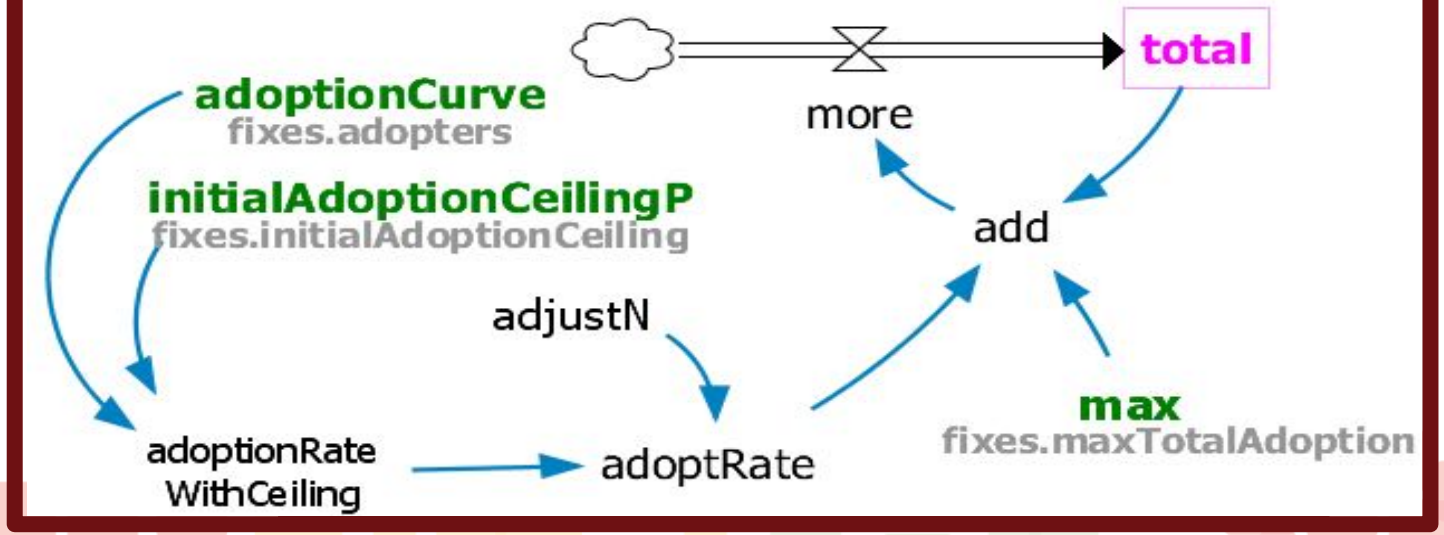
Fixes: Dampening of odd traffic by increasing P of adopted improvements

All units are PpH



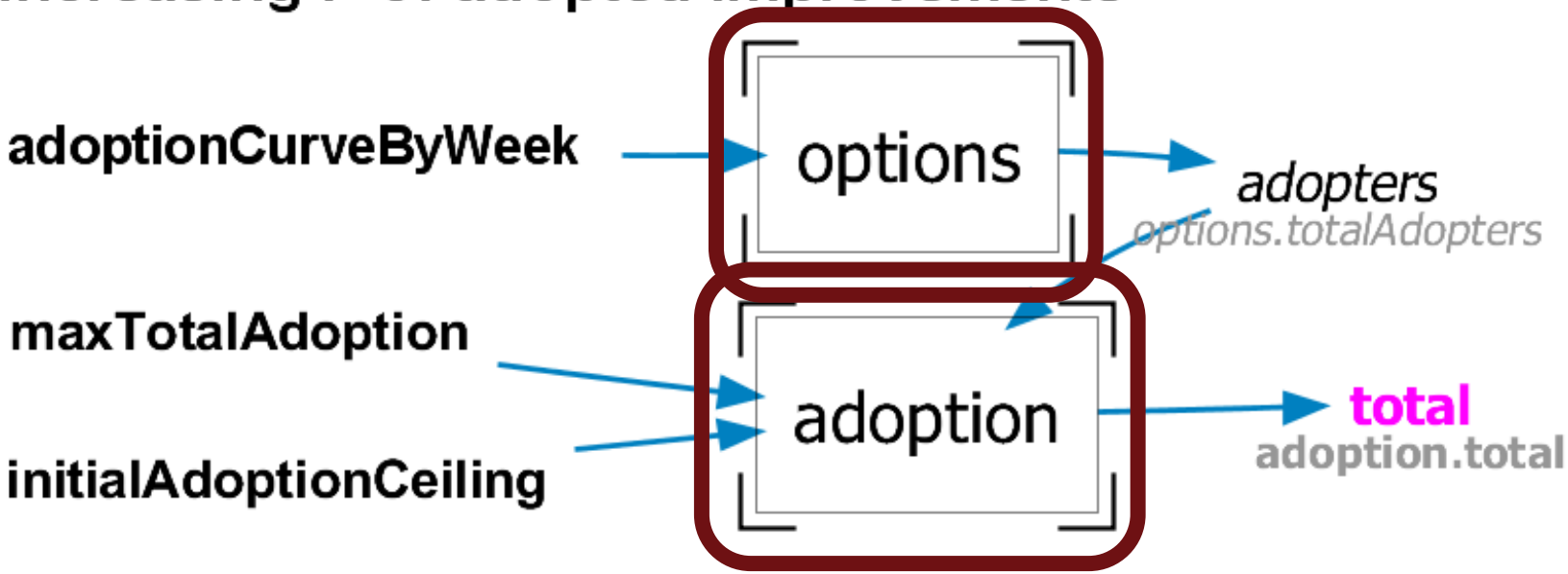
Adoption: accumulation of fix-adoption percentages over time

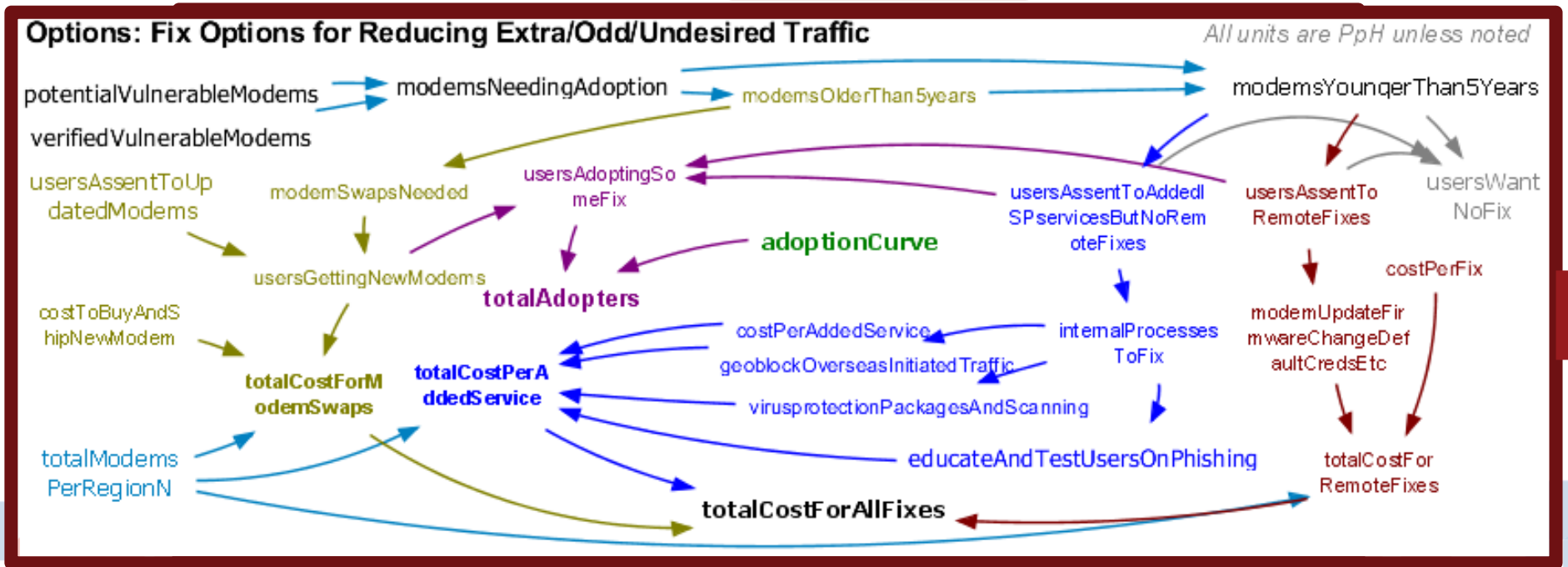
All units are PpH unless noted



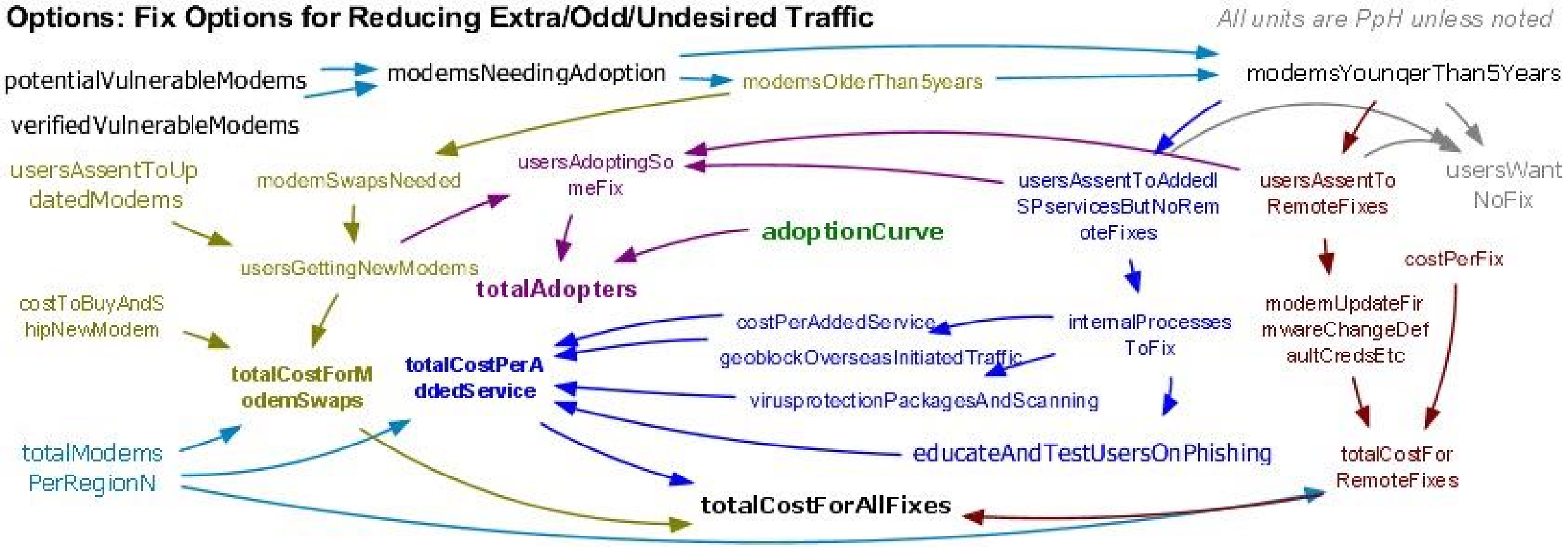
Fixes: Dampening of odd traffic by increasing P of adopted improvements

All units are PpH

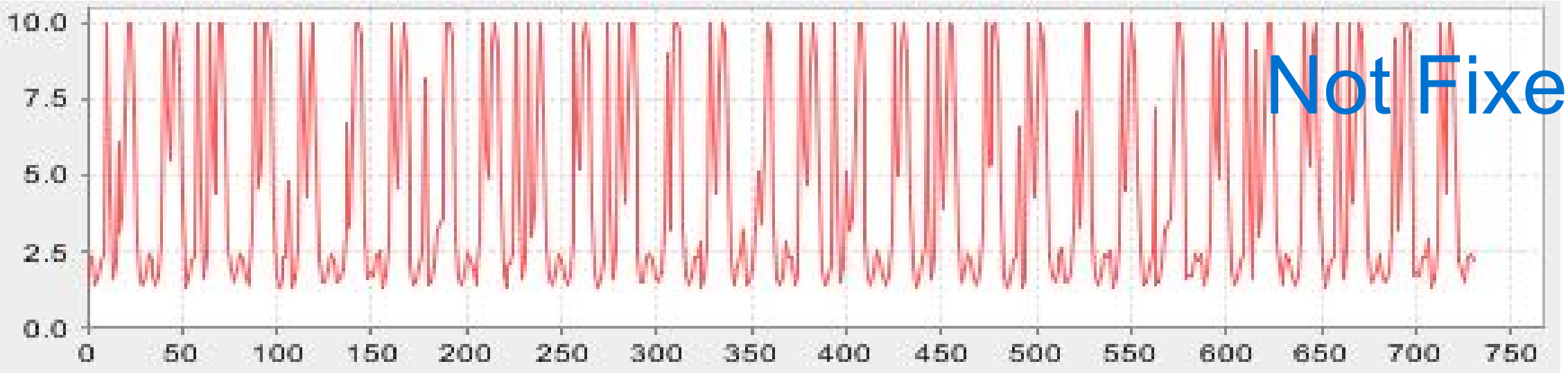




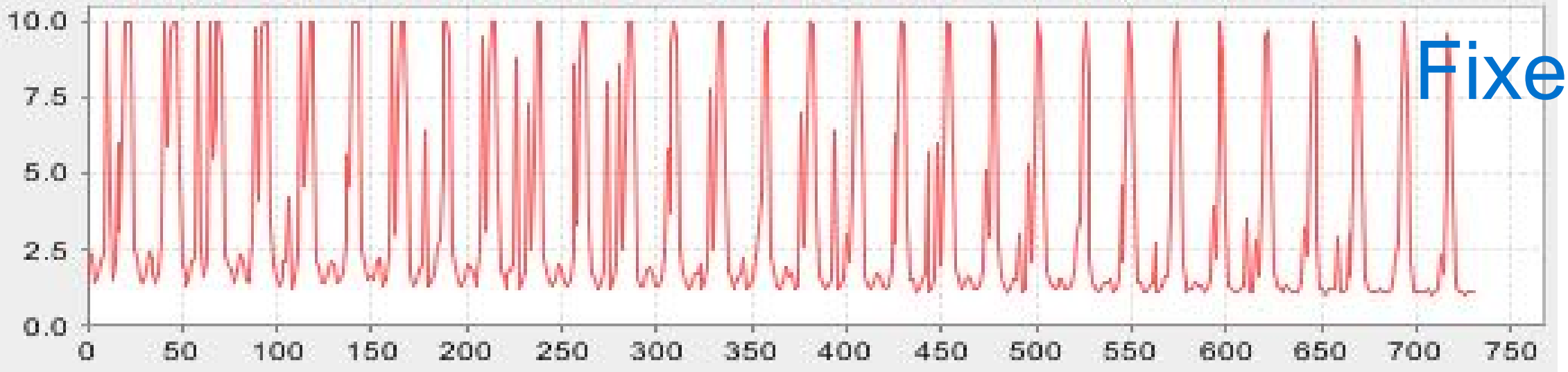
Fix Options


Options: Fix Options for Reducing Extra/Odd/Undesired Traffic
All units are PpH unless noted
potentialVulnerableModems
verifiedVulnerableModems
modemsNeedingAdoption
modemsOlderThan5years
modemsYounqerThan5Years
usersAssentToUpdatedModems
modemSwapsNeeded
usersAdoptingSomeFix
usersAssentToAddedISPservicesButNoRemoteFixes
usersAssentToRemoteFixes
usersWantNoFix
adoptionCurve
usersGettingNewModems
totalAdopters
costPerFix
costToBuyAndShipNewModem
costPerAddedService
internalProcessesToFix
modemUpdateFirmwareChangeDefaultCredsEtc
totalCostForModemSwaps
totalCostPerAddedService
geoblockOverseasInitiatedTraffic
virusprotectionPackagesAndScanning
totalModemsPerRegionN
educateAndTestUsersOnPhishing
totalCostForRemoteFixes
totalCostForAllFixes

Traffic for a **Set of Users** Over ~1 Month

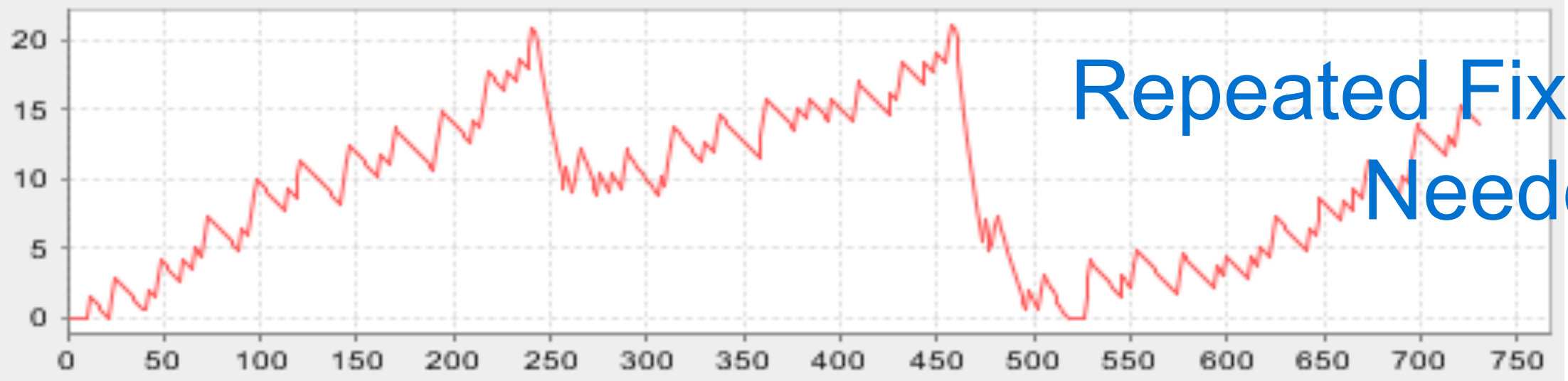


Not Fixed

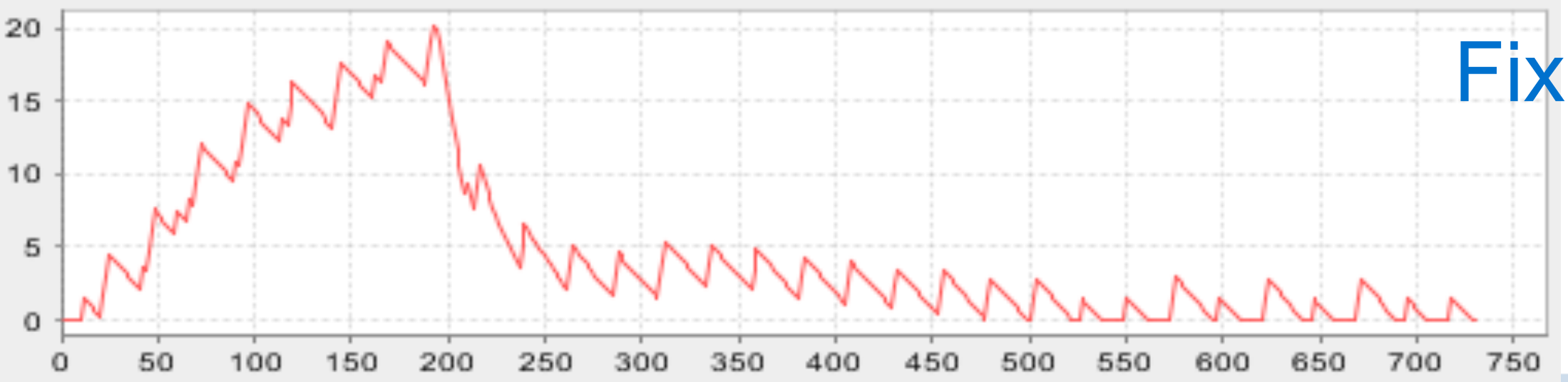


Fixed

Customer **Dis**satisfaction Over ~1 Month



Repeated Fixes Needed



Fixed

Next Steps – High Level

- **Validate and apply the SD model**
  - Meet with stakeholders & get KPIs
  - Measure KPIs & develop targets
  - Make & model competing fix processes
  - Apply process & do pre/post KPI measures

Next Steps – More Improvements

- **Sensitivity analysis** and magnitude measurements for contributing factors
- **Adjust customer sets** to infrastructure and applicability of processes

SD for SSE is Good for ISP Business

Service More Customers
for less money

Do It Faster
and with more precision

Create Competitive Moat
Add value beyond physical infrastructure, save time, protect data and bandwidth

Control Risk
Test process changes before broad application

Your Turn!

- Work within your ISP to develop a better internet experience using SD for SSE

David Eason: incose@eason.cc

All system dynamics diagrams and graph outputs came from the paper title on the cover slide, available at INCOSE.org and eason.cc
All slides Copyright © 2019 by David Eason. Permission granted to INCOSE to publish and use.

29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

www.incose.org/symp2019