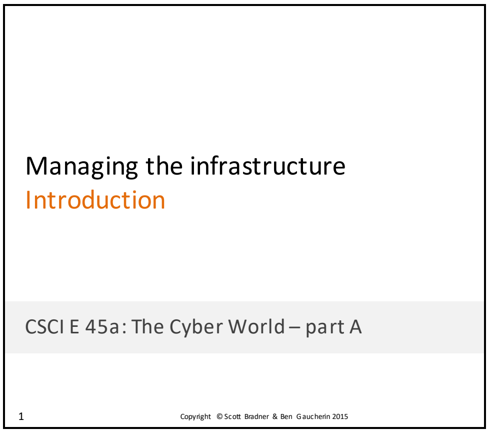
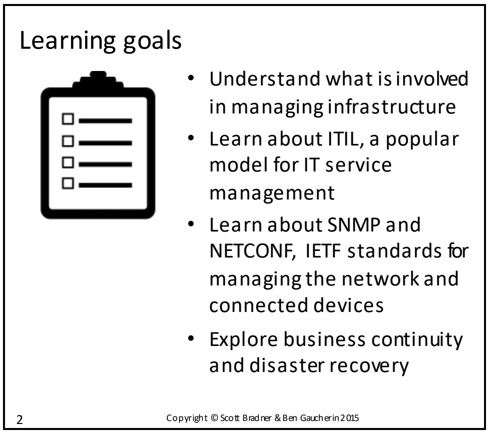


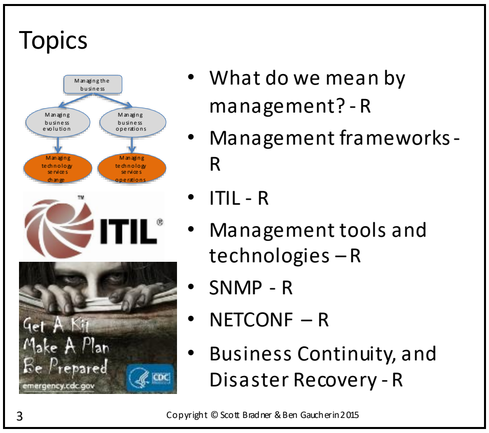
Managing the infrastructure
Introduction

CSCI E 45a: The Cyber World – part A



Learning goals

- Understand what is involved in managing infrastructure
- Learn about ITIL, a popular model for IT service management
- Learn about SNMP and NETCONF, IETF standards for managing the network and connected devices
- Explore business continuity and disaster recovery



Topics

Managing the business
Managing business evolution
Managing business operations
Managing technology services change
Managing technology services operations
ITIL
Get A Kit
Make A Plan
Be Prepared
emergency.cdc.gov
CDC

- What do we mean by management? - R
- Management frameworks - R
- ITIL - R
- Management tools and technologies – R
- SNMP - R
- NETCONF – R
- Business Continuity, and Disaster Recovery - R

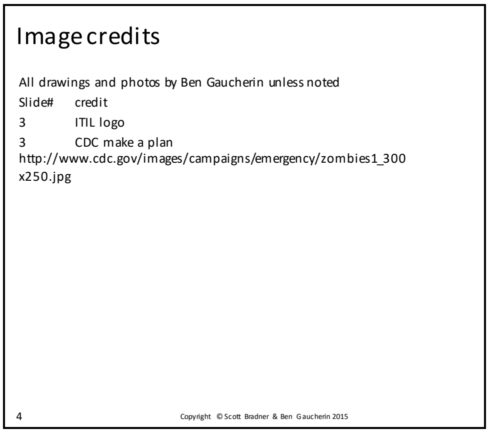
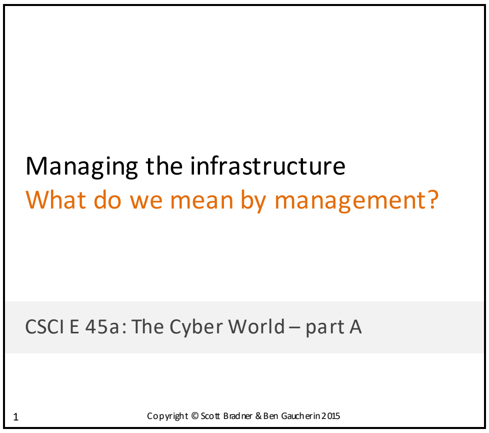


Image credits

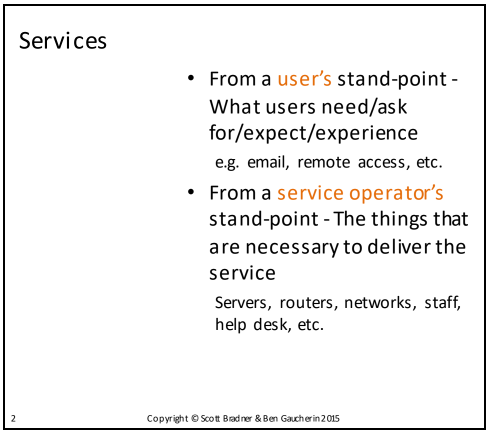
All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
3	ITIL logo
3	CDC make a plan http://www.cdc.gov/images/campaigns/emergency/zombies1_300x250.jpg



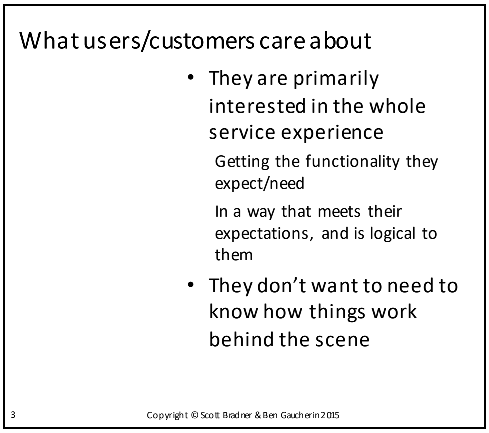
Managing the infrastructure
What do we mean by management?

CSCI E 45a: The Cyber World – part A



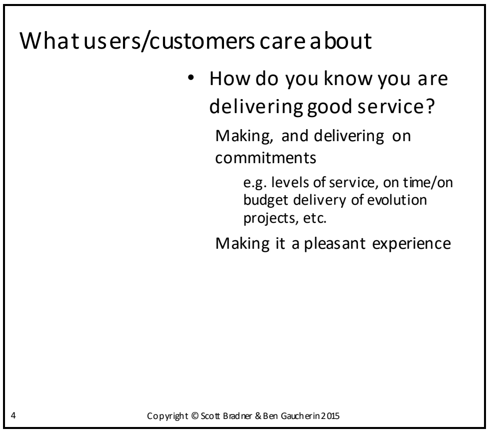
Services

- From a user's stand-point - What users need/ask for/expect/experience
  - e.g. email, remote access, etc.
- From a service operator's stand-point - The things that are necessary to deliver the service
  - Servers, routers, networks, staff, help desk, etc.



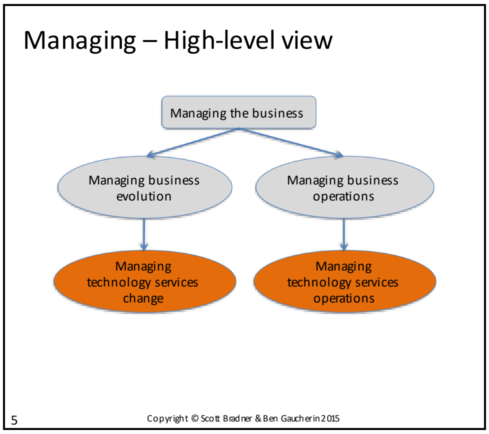
What users/customers care about

- They are primarily interested in the whole service experience
  - Getting the functionality they expect/need
  - In a way that meets their expectations, and is logical to them
- They don't want to need to know how things work behind the scene



What users/customers care about

- How do you know you are delivering good service?
  - Making, and delivering on commitments
    - e.g. levels of service, on time/on budget delivery of evolution projects, etc.
  - Making it a pleasant experience



Managing – High-level view

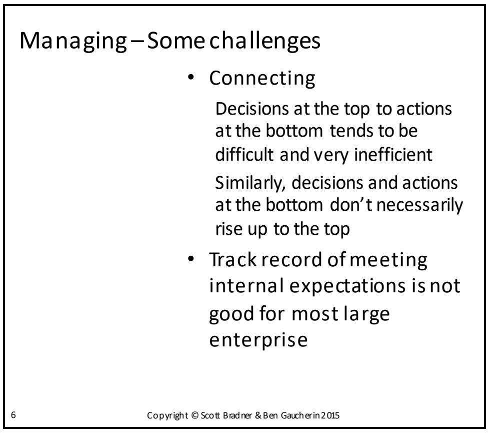
Managing the business

Managing business evolution

Managing business operations

Managing technology services change

Managing technology services operations



Managing – Some challenges

- Connecting
  - Decisions at the top to actions at the bottom tends to be difficult and very inefficient
  - Similarly, decisions and actions at the bottom don't necessarily rise up to the top
- Track record of meeting internal expectations is not good for most large enterprise

Managing – Activities

- Strategic management
  - Mid/long range planning
  - Assessment of high-level opportunities and risks
  - Deciding direction/technologies/products
- Managing evolution
  - Deciding direction/technologies/products
  - Design, Development/Configuration, Deployment, Decommissioning

Managing – Activities

- Managing operations
  - Operators - Who is doing what, to what/whom
  - Things - What's where, and how it is performing
  - User/customer experiences

Management of IP networks

- No "Minority Report" for systems and networks
- Driven by user detected failures
  - Logging? Who's watching the logs?
  - What if your monitoring tools are down?
- Rarely, if ever, pro-actively identify early signs of service degradation and pending failures

Management of IP networks

Let's keep the tools in our toolkit simple and easy to use
I'm just going to knock this nail in
So why over complicate things? THIS would do the job perfectly well
©ogliviedesign.co.uk

- Blind reliance on "fancy" tools and process over simple validation that things are working
  - There are lots of management frameworks you can "blindly" follow to solve your management problems
  - Network, systems, security technology vendors have lots of tools to solve your management problems
    - Tend to assume somebody is watching each of the screens

10 Copyright © Scott Bradner & Ben Gaucherin 2015

Management of IP networks

- In case of failure/degradation: who is affected?
  - Who gets notified?
  - What are they being told?
- Completely different philosophy for Telecommunications network operators
  - Active, in-band monitoring of service levels

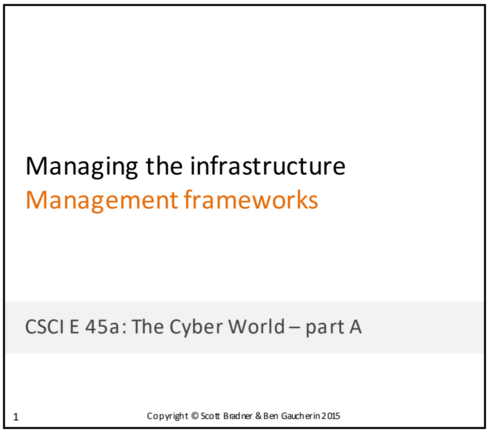
11 Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Ben Gaucherin unless noted

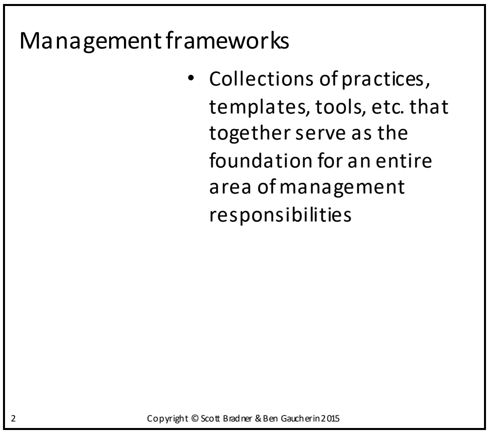
Slide#	credit
9	http://static.ddmcdn.com/gif/blogs/Minority-Report-Info-Main.jpg
10	Cartoon – ogliviedesign.co.uk

12 Copyright © Scott Bradner & Ben Gaucherin 2015



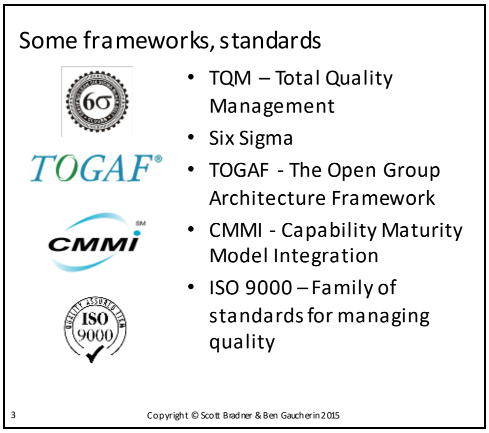
Managing the infrastructure
Management frameworks

CSCI E 45a: The Cyber World – part A



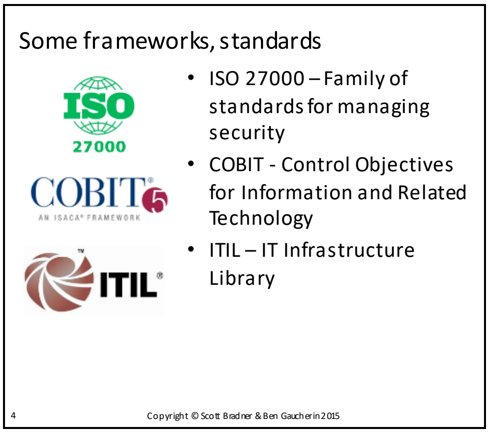
Management frameworks

- Collections of practices, templates, tools, etc. that together serve as the foundation for an entire area of management responsibilities



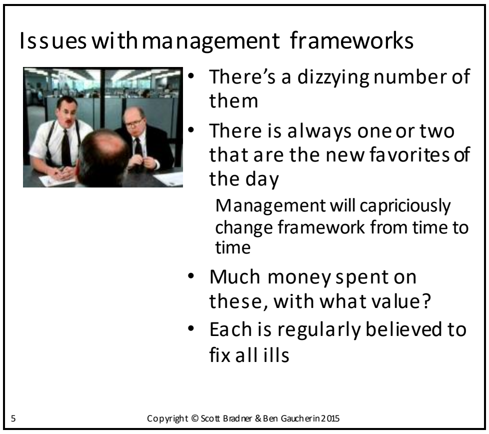
Some frameworks, standards

- TQM – Total Quality Management
- Six Sigma
- TOGAF - The Open Group Architecture Framework
- CMMI - Capability Maturity Model Integration
- ISO 9000 – Family of standards for managing quality



Some frameworks, standards

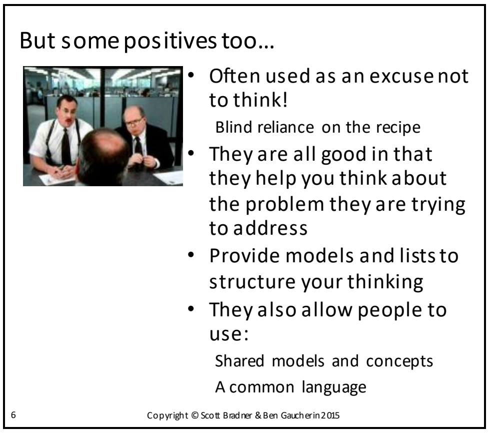
- ISO 27000 – Family of standards for managing security
- COBIT - Control Objectives for Information and Related Technology
- ITIL – IT Infrastructure Library



Issues with management frameworks

- There's a dizzying number of them
- There is always one or two that are the new favorites of the day

  Management will capriciously change framework from time to time
- Much money spent on these, with what value?
- Each is regularly believed to fix all ills



But some positives too…

- Often used as an excuse not to think!

  Blind reliance on the recipe
- They are all good in that they help you think about the problem they are trying to address
- Provide models and lists to structure your thinking
- They also allow people to use:

  Shared models and concepts

  A common language

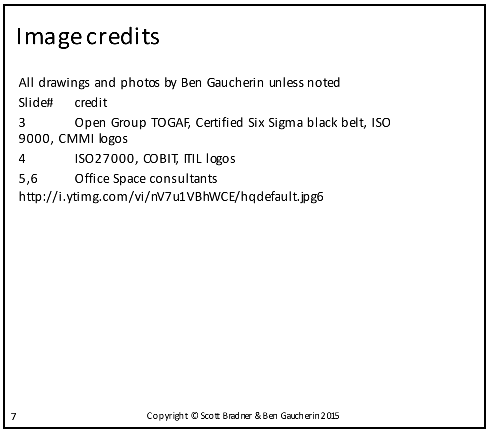
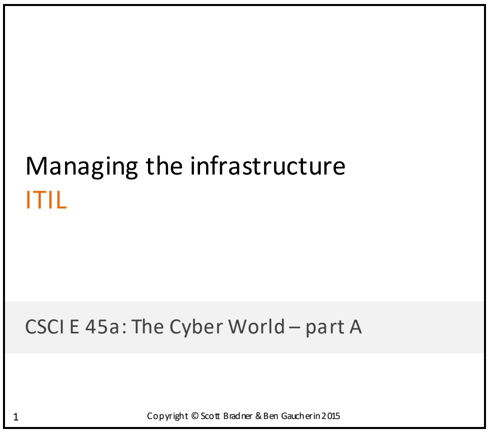


Image credits

All drawings and photos by Ben Gaucherin unless noted

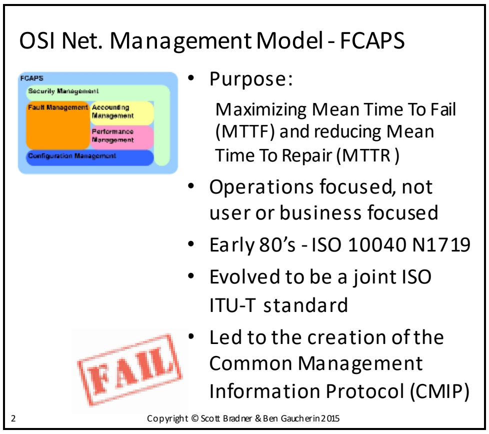
Slide#	credit
3	Open Group TOGAF, Certified Six Sigma black belt, ISO 9000, CMMI logos
4	ISO27000, COBIT, ITIL logos
5,6	Office Space consultants http://i.ytimg.com/vi/nV7u1VBhWCE/hqdefault.jpg6



Managing the infrastructure

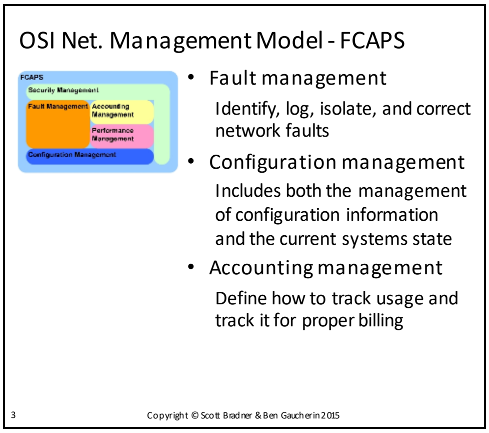
ITIL

CSCI E 45a: The Cyber World – part A



OSI Net. Management Model - FCAPS

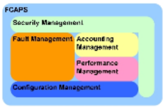
- Purpose:
  Maximizing Mean Time To Fail (MTTF) and reducing Mean Time To Repair (MTTR)
- Operations focused, not user or business focused
- Early 80's - ISO 10040 N1719
- Evolved to be a joint ISO ITU-T standard
- Led to the creation of the Common Management Information Protocol (CMIP)



OSI Net. Management Model - FCAPS

- Fault management
  Identify, log, isolate, and correct network faults
- Configuration management
  Includes both the management of configuration information and the current systems state
- Accounting management
  Define how to track usage and track it for proper billing

OSI Net. Management Model - FCAPS



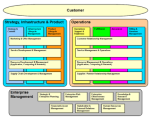
- Performance management

  Manage the performance of the network and plan for future needs

- Security management

  Ensure the proper securing of the network, and the collection & analysis of security information/logs

Evolved as part of eTOM's BPF



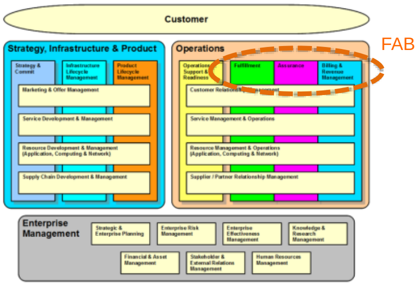
- Enhanced Telecom Operations Map (eTOM)
- Business Process Framework (BPF)
- Started in 2000
- Evolves FCAPS to FAB

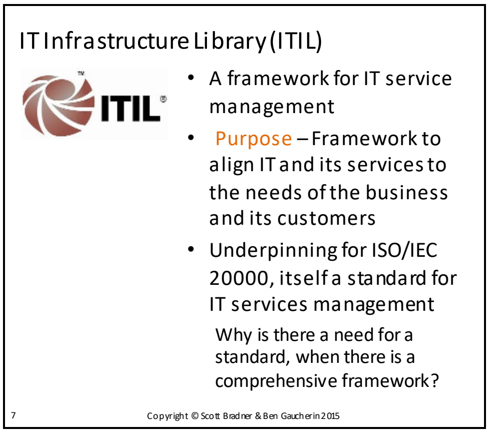
  Fulfillment – Configuration, Security

  Assurance – Fault, Performance

  Billing - Accounting

enhanced Telecom Operations Map

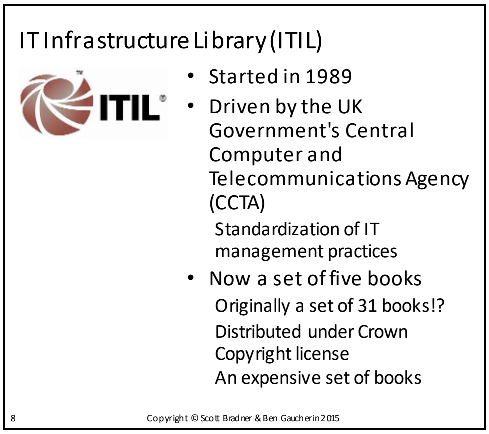

Customer
Strategy, Infrastructure & Product
Strategy & Commit
Infrastructure Lifecycle Management
Product Lifecycle Management
Marketing & Offer Management
Service Development & Management
Resource Development & Management (Application, Computing & Network)
Supply Chain Development & Management
Operations
Operations Support & Readiness
Fulfillment
Assurance
Billing & Revenue Management
Customer Relationship Management
Service Management & Operations
Resource Management & Operations (Application, Computing & Network)
Supplier / Partner Relationship Management
Enterprise Management
Strategic & Enterprise Planning
Enterprise Risk Management
Enterprise Effectiveness Management
Knowledge & Research Management
Financial & Asset Management
Stakeholder & External Relations Management
Human Resources Management
FAB



IT Infrastructure Library (ITIL)

- A framework for IT service management
- Purpose – Framework to align IT and its services to the needs of the business and its customers
- Underpinning for ISO/IEC 20000, itself a standard for IT services management
  - Why is there a need for a standard, when there is a comprehensive framework?

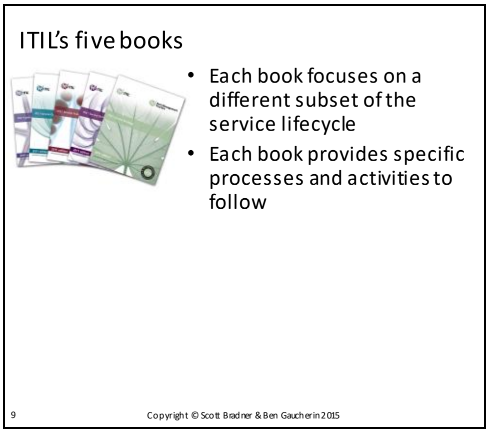
7



IT Infrastructure Library (ITIL)

- Started in 1989
- Driven by the UK Government's Central Computer and Telecommunications Agency (CCTA)
  - Standardization of IT management practices
- Now a set of five books
  - Originally a set of 31 books!?
  - Distributed under Crown Copyright license
  - An expensive set of books

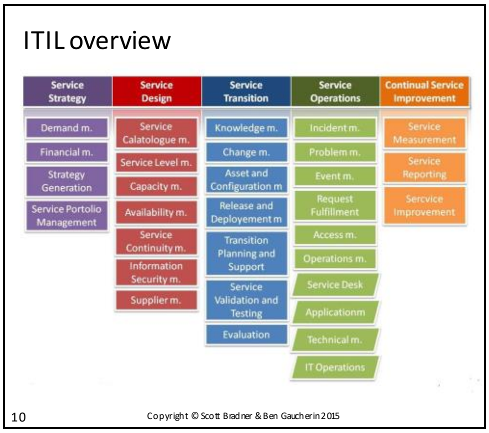
8



ITIL's five books

- Each book focuses on a different subset of the service lifecycle
- Each book provides specific processes and activities to follow

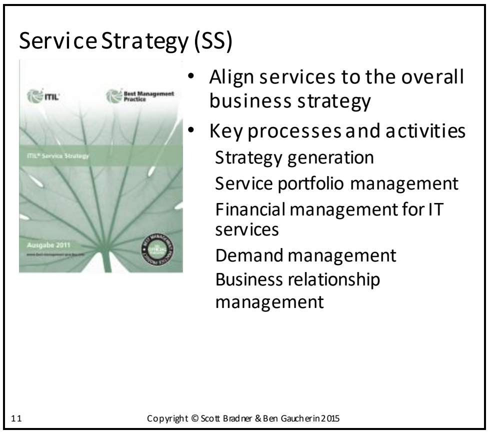
9



ITIL overview

Service Strategy	Service Design	Service Transition	Service Operations	Continual Service Improvement
Demand m.	Service Calatologue m.	Knowledge m.	Incident m.	Service Measurement
Financial m.	Service Level m.	Change m.	Problem m.	Service Reporting
Strategy Generation	Capacity m.	Asset and Configuration m	Event m.	Sercvice Improvement
Service Portolio Management	Availability m.	Release and Deployement m	Request Fulfillment	
	Service Continuity m.	Transition Planning and Support	Access m.	
	Information Security m.	Service Validation and Testing	Operations m.	
	Supplier m.	Evaluation	Service Desk	
			Applicationm	
			Technical m.	
			IT Operations	

10



Service Strategy (SS)

- Align services to the overall business strategy
- Key processes and activities

  Strategy generation

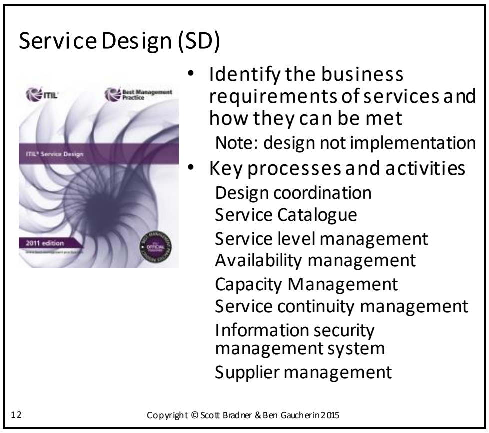
  Service portfolio management

  Financial management for IT services

  Demand management

  Business relationship management

11



Service Design (SD)

- Identify the business requirements of services and how they can be met

  Note: design not implementation
- Key processes and activities

  Design coordination

  Service Catalogue

  Service level management

  Availability management

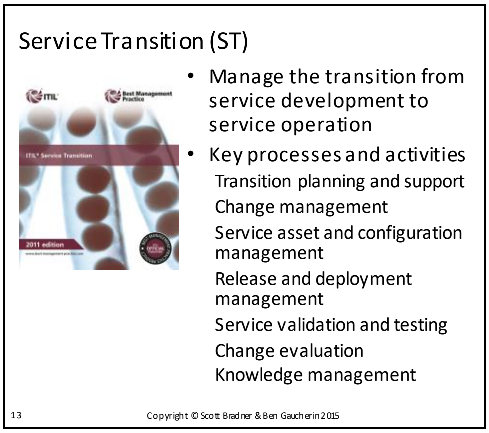
  Capacity Management

  Service continuity management

  Information security management system

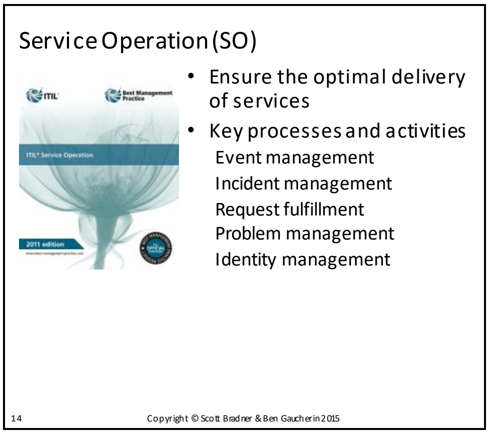
  Supplier management

12



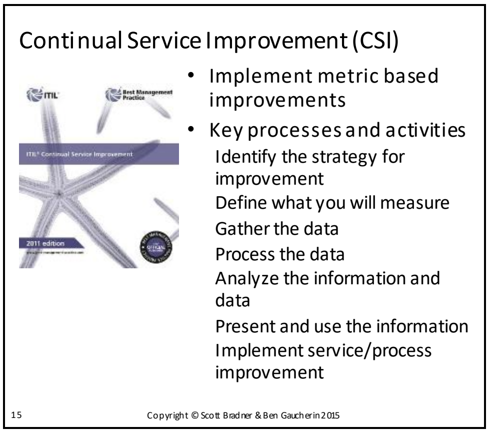
Service Transition (ST)

- Manage the transition from service development to service operation
- Key processes and activities
  - Transition planning and support
  - Change management
  - Service asset and configuration management
  - Release and deployment management
  - Service validation and testing
  - Change evaluation
  - Knowledge management



Service Operation (SO)

- Ensure the optimal delivery of services
- Key processes and activities
  - Event management
  - Incident management
  - Request fulfillment
  - Problem management
  - Identity management



Continual Service Improvement (CSI)

- Implement metric based improvements
- Key processes and activities
  - Identify the strategy for improvement
  - Define what you will measure
  - Gather the data
  - Process the data
  - Analyze the information and data
  - Present and use the information
  - Implement service/process improvement

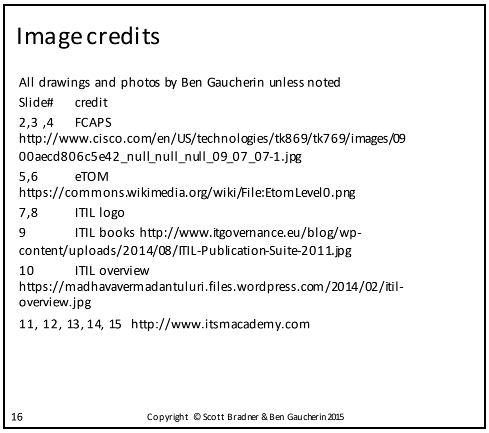


Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2,3 ,4	FCAPS http://www.cisco.com/en/US/technologies/tk869/tk769/images/0900aecd806c5e42_null_null_null_09_07_07-1.jpg
5,6	eTOM https://commons.wikimedia.org/wiki/File:EtomLevel0.png
7,8	ITIL logo
9	ITIL books http://www.itgovernance.eu/blog/wp-content/uploads/2014/08/ITIL-Publication-Suite-2011.jpg
10	ITIL overview https://madhavavermadantuluri.files.wordpress.com/2014/02/itil-overview.jpg
11, 12, 13, 14, 15	http://www.itsmacademy.com

Managing the infrastructure

Management tools and technologies

CSCI E 45a: The Cyber World – part A

What tools?

- Three useful categories:
  - Managing the processes
  - Managing the "applications"
  - Managing the network (the devices that comprise the network)
- There are some tools that are gaining momentum in the market to manage processes

Management tools - "silicon snake oil"

- Tools are either
  - Very narrowly focused
  - OR try to boil the ocean – CA Unicenter, IBM's Tivoli
- GUI tools getting better
  - Mostly useful to do simple things you do infrequently
  - Command line better for routine (complicated) tasks
- Still today, much of management tasks are done using basic command line tools, shell/Perl/Python scripts, and text logs

One of Ben’s home PIX config (partial)

```
: Saved
: Written by enable_15 at 19:24:59.956 UTC Mon Apr 9 2012
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password ************ encrypted
passwd ************* encrypted
hostname pixy
domain-name gaucherin.org
fixup protocol dns maximum-length 512
names
access-list inside_outbound_nat0_acl permit ip any 10.0.0.16 255.255.255.240
pager lines 24
logging on
logging timestamp
logging trap notifications
logging host inside 10.0.0.3 format emblem
mtu outside 1500
mtu inside 1500
ip address outside 192.168.1.30 255.255.255.0
ip address inside 10.0.0.1 255.255.255.0
ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip audit info action alarm
ip audit attack action alarm
ip local pool pixy_vpn_pool 10.0.0.20-10.0.0.30
```

Mindset mismatch, again

- People used to manage large Telco structures
  - Large complex set of expensive (multi million $) tools to manage all aspects of the “smart network”
  - Large headcount of people
    - Front-line people with limited training
    - People configuring the tools need to be well trained

Mindset mismatch, again

- People running IP based networks
  - Mostly use simple ping, traceroute, configs managed as text files, and answering phone calls
  - Lower headcount
    - Front-line people need more expertise

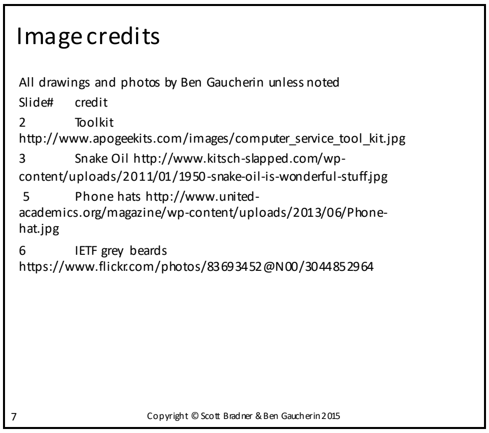


Image credits

All drawings and photos by Ben Gaucherin unless noted

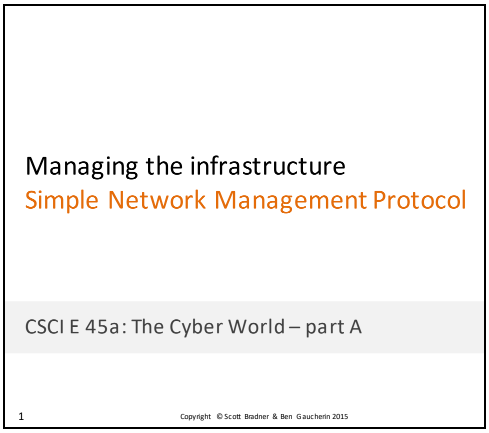
Slide# credit

2 Toolkit http://www.apogeekits.com/images/computer_service_tool_kit.jpg

3 Snake Oil http://www.kitsch-slapped.com/wp-content/uploads/2011/01/1950-snake-oil-is-wonderful-stuff.jpg

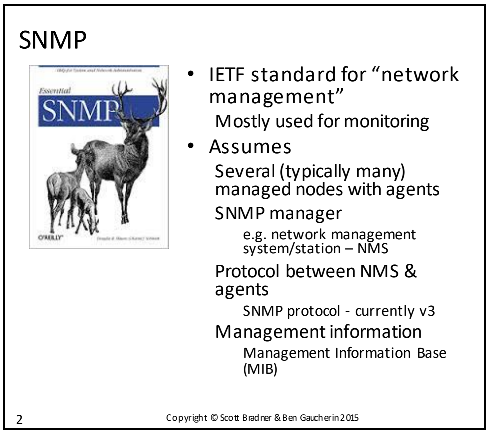
5 Phone hats http://www.united-academics.org/magazine/wp-content/uploads/2013/06/Phone-hat.jpg

6 IETF grey beards https://www.flickr.com/photos/83693452@N00/3044852964



Managing the infrastructure
Simple Network Management Protocol

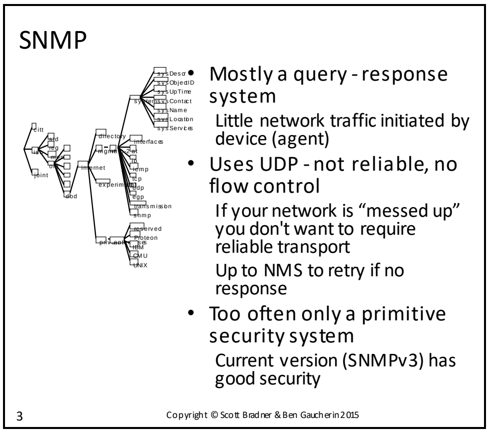
CSCI E 45a: The Cyber World – part A



Essential
SNMP
O'REILLY

SNMP

- IETF standard for “network management”
  - Mostly used for monitoring
- Assumes
  - Several (typically many) managed nodes with agents
  - SNMP manager
    - e.g. network management system/station – NMS
  - Protocol between NMS & agents
    - SNMP protocol - currently v3
  - Management information
    - Management Information Base (MIB)

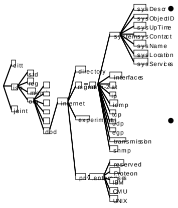


citt
iso
joint
std
reg
mem
org
dod
internet
directory
mgmt
mib-2
experimental
private
enterprises
system
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
interfaces
at
ip
icmp
tcp
udp
egp
transmission
snmp
reserved
Proteon
IBM
CMU
UNIX

SNMP

- Mostly a query - response system
  - Little network traffic initiated by device (agent)
- Uses UDP - not reliable, no flow control
  - If your network is “messed up” you don't want to require reliable transport
  - Up to NMS to retry if no response
- Too often only a primitive security system
  - Current version (SNMPv3) has good security

SNMP



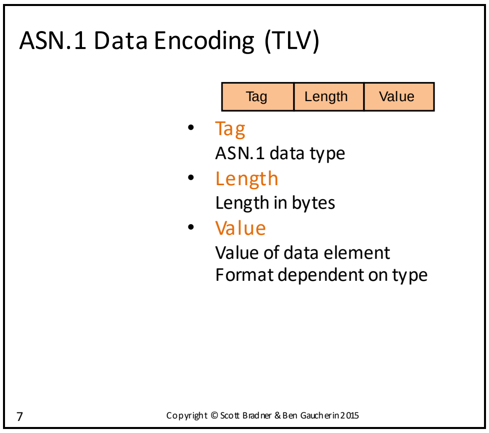
- Uses database defined in the Management Information Base (MIB)
  - Can have "enterprise" extensions to MIB
- Structure of Management Information (SMI) document defines structure of MIB
  - SMI defines data structure using ASN.1

ASN.1

- Joint ISO, IEC, ITU standard
- Abstract Syntax Notation One (ASN.1)
  - Defines a language used to describe data types
- Basic Encoding Rules for Abstract Notation One
  - Defines a method for unambiguous transmission of data
  - Data is self identifying on the wire

ASN.1

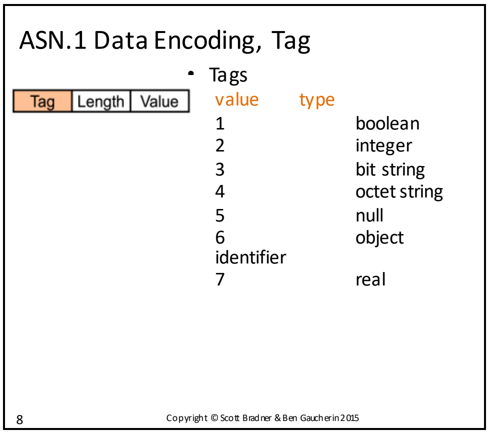
- Machine architecture independent
- Operating system independent
- Network protocol independent
- Native language independent



ASN.1 Data Encoding (TLV)

Tag	Length	Value

- Tag
  ASN.1 data type
- Length
  Length in bytes
- Value
  Value of data element
  Format dependent on type

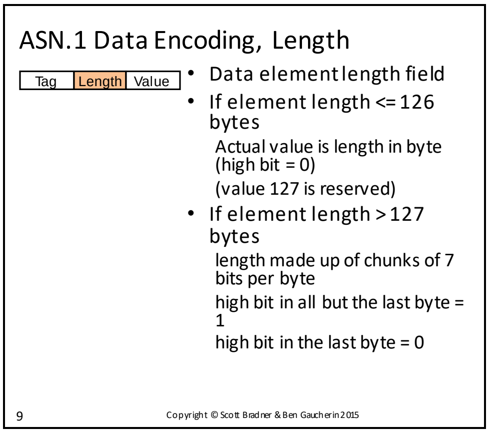


ASN.1 Data Encoding, Tag

Tag	Length	Value

- Tags

value	type
1	boolean
2	integer
3	bit string
4	octet string
5	null
6	object identifier
7	real

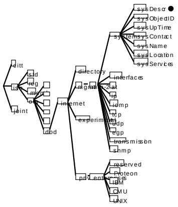


ASN.1 Data Encoding, Length

Tag	Length	Value

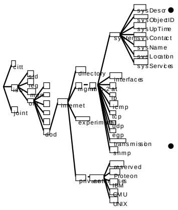
- Data element length field
- If element length <= 126 bytes
  Actual value is length in byte (high bit = 0)
  (value 127 is reserved)
- If element length > 127 bytes
  length made up of chunks of 7 bits per byte
  high bit in all but the last byte = 1
  high bit in the last byte = 0

ASN.1 Data Encoding, OID



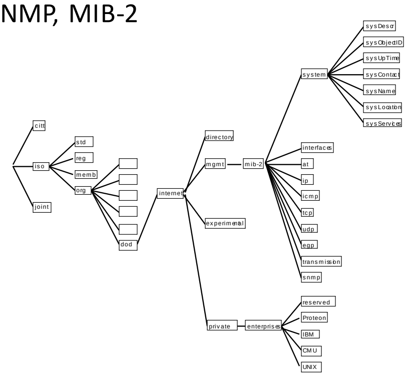
- OBJECT IDENTIFIER (OID)
  - Sequence of integers that describe a pathway taken in traversing a tree of options, must be unique
    - e.g. 1.3.6.1.2.1.1.1
    - or
    - iso.org.dod.internet.mgmt.mib-2.system.sysDescr
  - The base of the tree is defined by ISO
  - Layers (branches) are defined by other authorities

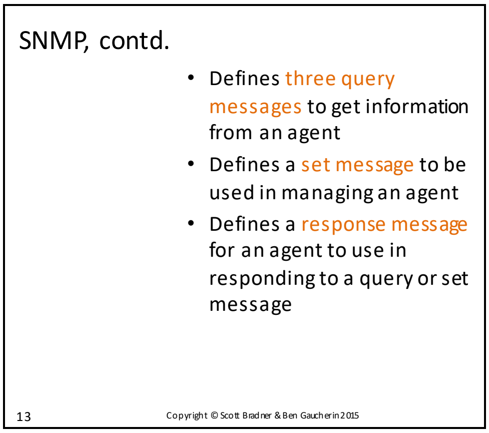
ASN.1 in retrospect



- Choice to use ASN.1 was (to some) political
  - To enable migration to CMIP
  - Because OSI was the future
  - But SNMP was ok for the short term
- Quite a few people in the IETF now think that using ASN.1 was a mistake
  - Too complex
  - ASN.1 standards people seen as too inflexible
  - Set expectations of interoperability that were not met

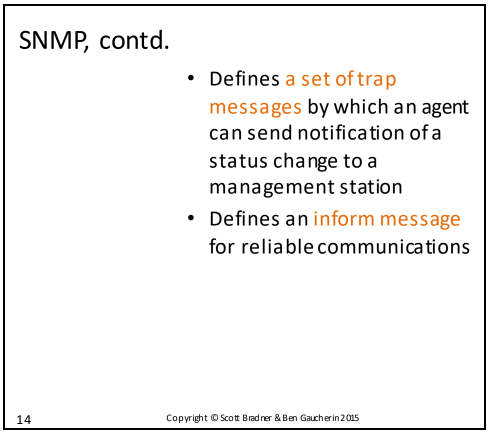
SNMP, MIB-2





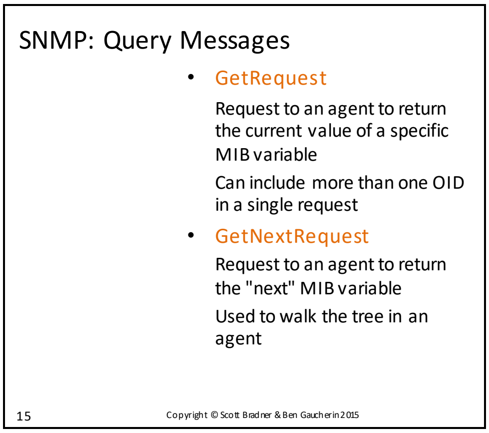
SNMP, contd.

- Defines three query messages to get information from an agent
- Defines a set message to be used in managing an agent
- Defines a response message for an agent to use in responding to a query or set message



SNMP, contd.

- Defines a set of trap messages by which an agent can send notification of a status change to a management station
- Defines an inform message for reliable communications



SNMP: Query Messages

- GetRequest

  Request to an agent to return the current value of a specific MIB variable

  Can include more than one OID in a single request
- GetNextRequest

  Request to an agent to return the "next" MIB variable

  Used to walk the tree in an agent

SNMP: Query Messages

- GetBulkRequest

  Request to an agent to return large blocks of data

  Problem - no flow control, can congest network

  see SNMP over TCP, RFC 3430

SNMP: Response Message

- Response

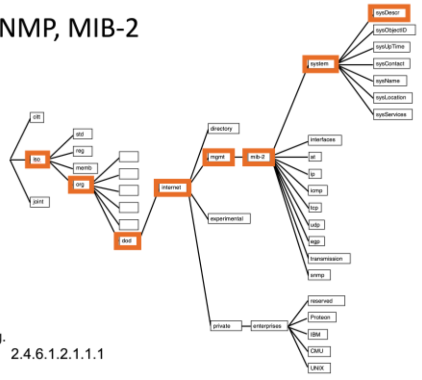
  Message from an agent to a NMS in response to an SNMP request message

  Used to return requested values or to indicate success or failure of set request

  Includes OID and value

  May include an error status and an error index

SNMP, MIB-2

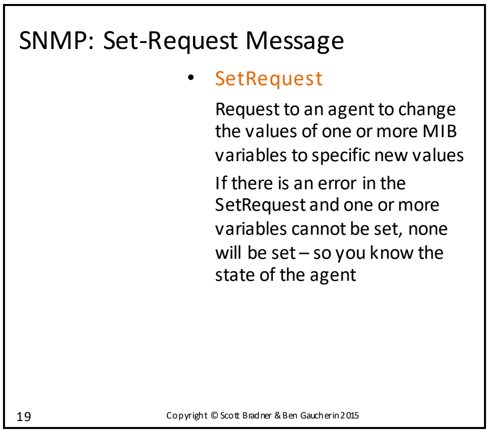


e.g.

2.4.6.1.2.1.1.1

or

iso.org.dod.internet.mgmt.mib-2.system.sysDescr

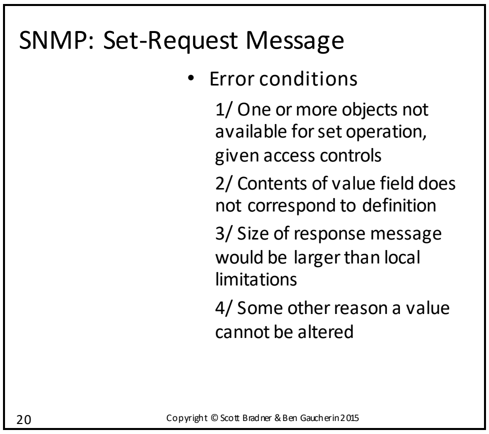


SNMP: Set-Request Message

- SetRequest

  Request to an agent to change the values of one or more MIB variables to specific new values

  If there is an error in the SetRequest and one or more variables cannot be set, none will be set – so you know the state of the agent



SNMP: Set-Request Message

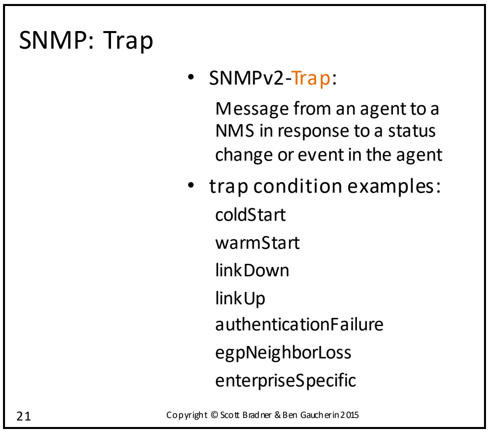
- Error conditions

  1/ One or more objects not available for set operation, given access controls

  2/ Contents of value field does not correspond to definition

  3/ Size of response message would be larger than local limitations

  4/ Some other reason a value cannot be altered



SNMP: Trap

- SNMPv2-Trap:

  Message from an agent to a NMS in response to a status change or event in the agent

- trap condition examples:

  coldStart

  warmStart

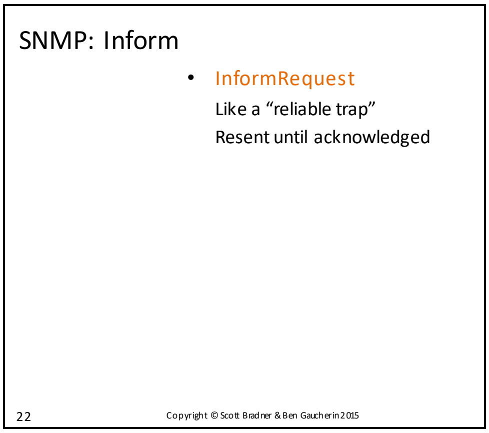
  linkDown

  linkUp

  authenticationFailure

  egpNeighborLoss

  enterpriseSpecific



SNMP: Inform

- InformRequest

  Like a “reliable trap”

  Resent until acknowledged

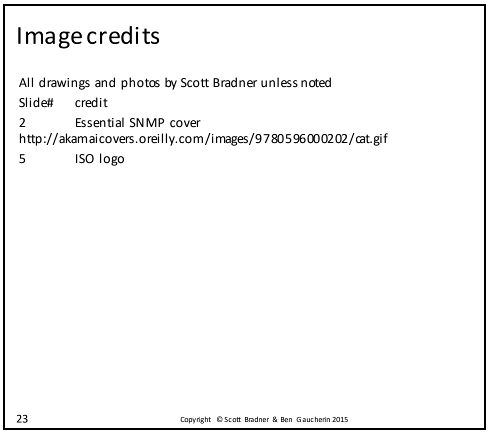


Image credits

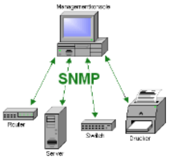
All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	Essential SNMP cover http://akamaicovers.oreilly.com/images/9780596000202/cat.gif
5	ISO logo

Managing the infrastructure
NETCONF

CSCI E 45a: The Cyber World – part A

Problems with SNMP



- Few MIBs support the set command
- SNMP does not provide a holistic view of the configuration of a device, or network
- Thus, SNMP is not seen as a good tool to use for configuring networks of devices
- NETCONF was developed by the IETF to fill the gap

NETCONF

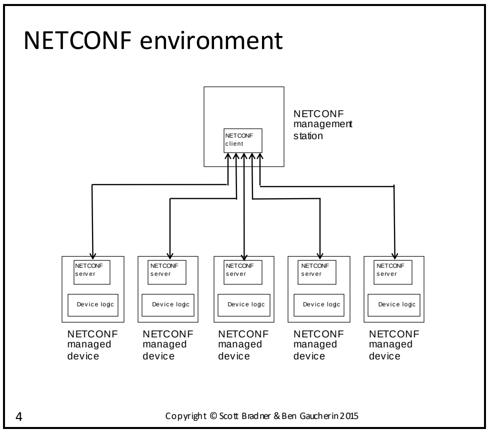
- Network Configuration Protocol
- Specification published by the IETF in December 2006
- Works on device & multi-device configurations

  Retrieve current device configuration files

  Modify configuration files

  Install modified configuration files

  On one or more devices



NETCONF environment

NETCONF management station

NETCONF client

NETCONF server

Device logic

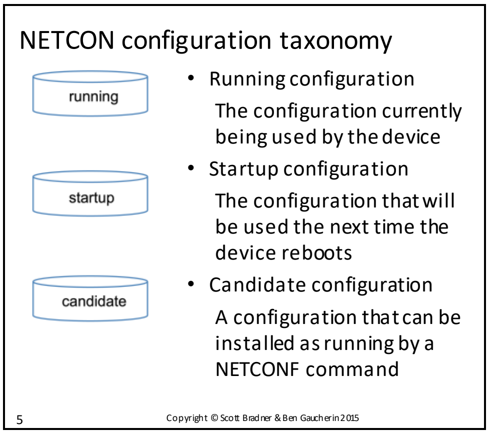
NETCONF managed device

NETCONF managed device

NETCONF managed device

NETCONF managed device

NETCONF managed device



NETCON configuration taxonomy

running

startup

candidate

- Running configuration

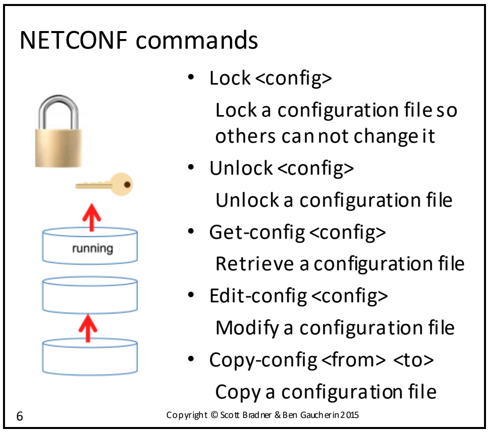
  The configuration currently being used by the device

- Startup configuration

  The configuration that will be used the next time the device reboots

- Candidate configuration

  A configuration that can be installed as running by a NETCONF command



NETCONF commands

running

- Lock <config>

  Lock a configuration file so others can not change it

- Unlock <config>

  Unlock a configuration file

- Get-config <config>

  Retrieve a configuration file

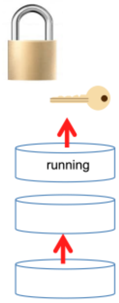
- Edit-config <config>

  Modify a configuration file

- Copy-config <from> <to>

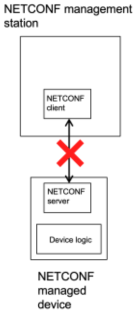
  Copy a configuration file

NETCONF commands, contd.



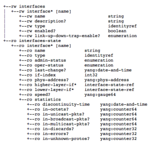
- Discard-changes <config>
  - Discard the changes made to a configuration file
- Delete <config>
  - Delete a configuration file
- Commit <candidate, ID>
  - Move a candidate configuration file into the running configuration
- Cancel-commit <ID>
  - Cancel a particular commit command

NETCONF commands & misc.



- Close-session
  - Gracefully close current NETCONF client-server session
- Kill-session <ID>
  - Force a NETCONF session to terminate
- Miscellaneous
  - Runs over SSH or TSL
  - Uses RPC
  - Communication format is XML
  - Uses YANG data models

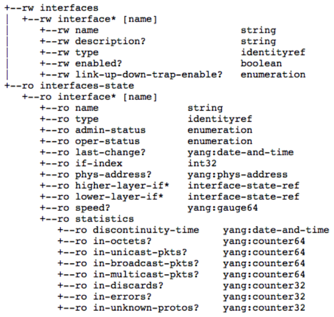
YANG



```
+--rw interfaces
|  +--rw interface* [name]
|     +--rw name                        string
|     +--rw description?                string
|     +--rw type                        identityref
|     +--rw enabled?                    boolean
|     +--rw link-up-down-trap-enable?   enumeration
+--ro interfaces-state
   +--ro interface* [name]
      +--ro name               string
      +--ro type               identityref
      +--ro admin-status       enumeration
      +--ro oper-status        enumeration
      +--ro last-change?       yang:date-and-time
      +--ro if-index           int32
      +--ro phys-address?      yang:phys-address
      +--ro higher-layer-if*   interface-state-ref
      +--ro lower-layer-if*    interface-state-ref
      +--ro speed?             yang:gauge64
      +--ro statistics
         +--ro discontinuity-time    yang:date-and-time
         +--ro in-octets?            yang:counter64
         +--ro in-unicast-pkts?      yang:counter64
         +--ro in-broadcast-pkts?    yang:counter64
         +--ro in-multicast-pkts?    yang:counter64
         +--ro in-discards?          yang:counter32
         +--ro in-errors?            yang:counter32
         +--ro in-unknown-protos?    yang:counter32
```

- Stands for “Yet Another Next Generation”
- Data modeling language
- YANG module defines a hierarchy of data
  - Most MIBs can be mapped into YANG modules
- Modeled as a tree of nodes
- Each node has a value or list of child nodes

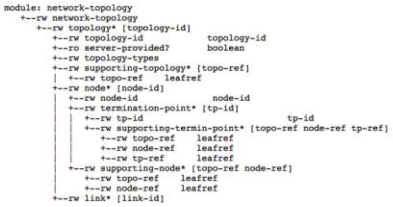
YANG IETF Interfaces Module



```
+--rw interfaces
|  +--rw interface* [name]
|     +--rw name                        string
|     +--rw description?                string
|     +--rw type                        identityref
|     +--rw enabled?                    boolean
|     +--rw link-up-down-trap-enable?   enumeration
+--ro interfaces-state
   +--ro interface* [name]
      +--ro name               string
      +--ro type               identityref
      +--ro admin-status       enumeration
      +--ro oper-status        enumeration
      +--ro last-change?       yang:date-and-time
      +--ro if-index           int32
      +--ro phys-address?      yang:phys-address
      +--ro higher-layer-if*   interface-state-ref
      +--ro lower-layer-if*    interface-state-ref
      +--ro speed?             yang:gauge64
      +--ro statistics
         +--ro discontinuity-time    yang:date-and-time
         +--ro in-octets?            yang:counter64
         +--ro in-unicast-pkts?      yang:counter64
         +--ro in-broadcast-pkts?    yang:counter64
         +--ro in-multicast-pkts?    yang:counter64
         +--ro in-discards?          yang:counter32
         +--ro in-errors?            yang:counter32
         +--ro in-unknown-protos?    yang:counter32
```

YANG modules

- YANG can model a router e,g., previous slide
- Can also model network & service topologies



```
module: network-topology
   +--rw network-topology
      +--rw topology* [topology-id]
         +--rw topology-id            topology-id
         +--ro server-provided?       boolean
         +--rw topology-types
         +--rw supporting-topology* [topo-ref]
         |  +--rw topo-ref    leafref
         +--rw node* [node-id]
         |  +--rw node-id              node-id
         |  +--rw termination-point* [tp-id]
         |  |  +--rw tp-id                           tp-id
         |  |  +--rw supporting-termin-point* [topo-ref node-ref tp-ref]
         |  |     +--rw topo-ref    leafref
         |  |     +--rw node-ref    leafref
         |  |     +--rw tp-ref      leafref
         |  +--rw supporting-node* [topo-ref node-ref]
         |     +--rw topo-ref    leafref
         |     +--rw node-ref    leafref
         +--rw link* [link-id]
```

NETCONF/YANG vs. SNMP

SNMP

v

NETCONF/
YANG

- SNMP does very well at monitoring individual devices
- SNMP does less well at configuring individual devices
- NETCONF is targeted at configuring sets of devices
- NETCONF does less well at monitoring individual devices

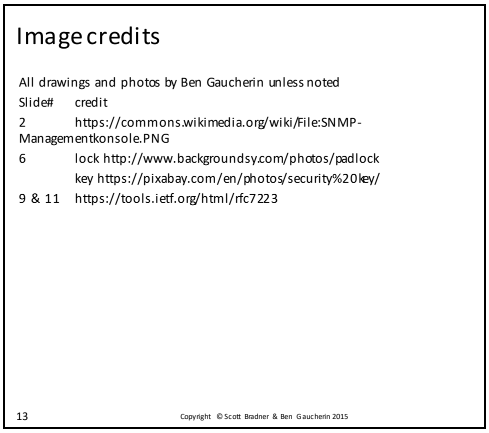


Image credits

All drawings and photos by Ben Gaucherin unless noted

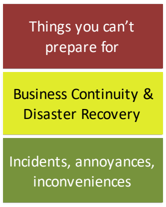
Slide#	credit
2	https://commons.wikimedia.org/wiki/File:SNMP-Managementkonsole.PNG
6	lock http://www.backgroundsy.com/photos/padlock
	key https://pixabay.com/en/photos/security%20key/
9 & 11	https://tools.ietf.org/html/rfc7223

13

Managing the infrastructure
Business Continuity & Disaster Recovery

CSCI E 45a: The Cyber World – part A

A continuum


Things you can't prepare for

Business Continuity & Disaster Recovery

Incidents, annoyances, inconveniences

- Incident Management (ITIL) allows for the management of incidents big and small
- Understanding the thresholds is important

  When do you go from incident to crisis/disaster?

  Tends to be industry, organization specific

Business Continuity (BC)

- Maintaining continuity of key business operations through suddenly changing conditions
- Not always physical destruction

  e.g., H1N1 planning
- Broader risk management

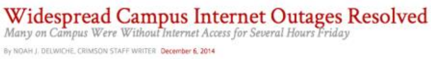
  e.g., changes in market conditions, competitive landscape, etc.

Business Continuity (BC)

- When are changing business conditions disasters?
- Is the rapid disappearance of your entire product market a disaster?
  - See Blackberry
- Some standards
  - e.g., BS 25999-2
- Some business continuity is mandated
  - e.g., FFIEC "guidance"
  - e.g., Payroll for State of Mass. employees

Disaster Recovery (DR)

- A disaster does not always affect technology
  - But technology can be critical to recovery efforts
- And sometime technology is the disaster



Widespread Campus Internet Outages Resolved

Many on Campus Were Without Internet Access for Several Hours Friday

By NOAH J. DELWICHE, CRIMSON STAFF WRITER December 6, 2014

Disaster Recovery (DR)

- For the technology
  - Synchronous resiliency is what you factor in to your system design
    - Resiliency in the design reduces the need for DR or at least changes the concept
  - So DR is Asynchronous resiliency
    - With varying time lag

Disaster Recovery (DR)

Paula Deen's DIET LIES!
NATIONAL ENQUIRER
Inside Tom's HOUSE OF HORRORS!
THE ABUSE PUNISHMENTS HUMILIATION
Katie's tortured life exposed!

- May need to be able to operate even if you cannot get to the office
  - e.g., American Media Inc. (National Enquirer) anthrax letter received & building evacuated October 2001
    - Federal authorities OK'd building on 8 Feb 2007
  - e.g., 100s of companies in World Trade Center
    - Some went out of business because of data (not people) loss

7 Copyright © Scott Bradner & Ben Gaucherin 2015

Some important acronyms

- Business Impact Analysis – BIA
  - Analysis of risks, tolerance for loss/degradation of service, and recovery requirements
- Mean Time To Fail – MTTF
  - The mean time between outages
- Mean Time To Repair – MTTR
  - The mean time ot bring the service back up from an outage

8 Copyright © Scott Bradner & Ben Gaucherin 2015

Some important acronyms, contd.

- Recovery Time Objective – RTO
  - Target time to bring a service back to an acceptable state of performance
- Recovery Point Objective – RPO
  - Defines how much data you can afford to loose – i.e., the frequency of backups

9 Copyright © Scott Bradner & Ben Gaucherin 2015

DR planning

- Step 0: Figure out what outage is acceptable
  - Before the event!!
  - i.e., do a risk model for an outage
    - What is at risk if you cannot operate and over what timeframe?
  - e.g., payroll system: checks needed within 3 business days, updates can take months
  - e.g., employee Christmas party planning site: unused 11 months of the year
    - Understand seasonality
  - Assume that you cannot tolerate any data loss
    - i.e., good backup process (including off site storage

DR planning

- Step 1: Define key roles and responsibilities
  - Who will make decisions? Who will communicate? Etc.
  - And if that person is unreachable?
- Step 2: Decide how you will communicate with employees, the press, the public?
  - Who will speak for the organization?

DR planning

- Step 3: Think about the people
  - Who is needed when?
  - Where will people work if office is closed?
  - What if the people cannot travel to the office or to an alternate site?
    - 9/11 flight shutdown, blizzard of '78, bird flu, ...

DR planning

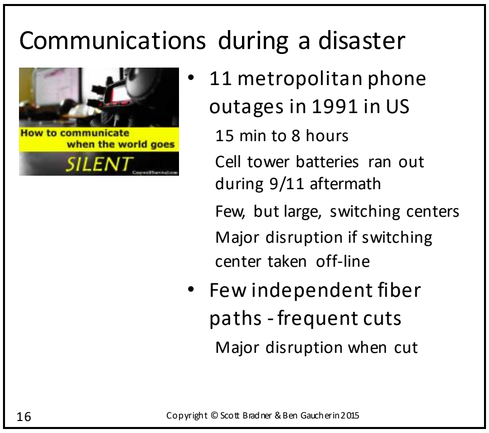
- Step 4: Think about the systems
  - What systems are needed when?
  - How are they going to be accessed?
- Step 5: Think about the data
  - What data will be needed when and where?
  - How is the data going to get to where it is needed?

DR planning

- Step 6: Plan the backup systems
  - Do you need your own redundant system?
  - Does the data need to be in sync in real time?
- Step 7: Plan the communications
  - Communicate the plan
  - to support decision makers
  - to support user and staff access
  - to support data transfers

Communications during a disaster

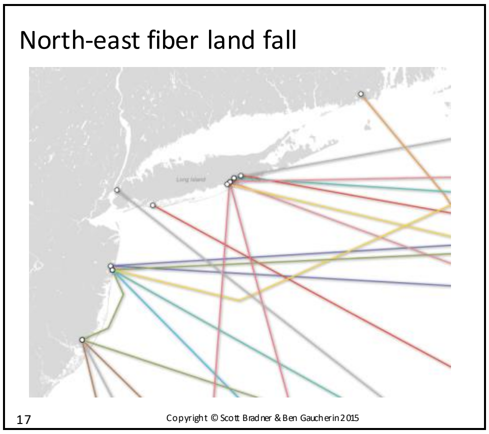
- Cannot assume phone system will work
  - Phone system gets clogged during most major emergencies
  - Both land-line and cellular
- Internet may work better



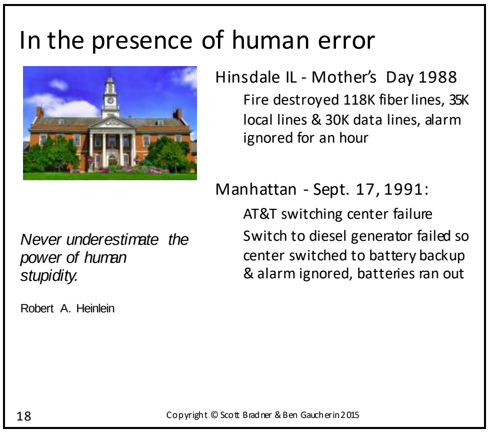
Communications during a disaster

How to communicate
when the world goes
SILENT

- 11 metropolitan phone outages in 1991 in US
  - 15 min to 8 hours
  - Cell tower batteries ran out during 9/11 aftermath
  - Few, but large, switching centers
  - Major disruption if switching center taken off-line
- Few independent fiber paths - frequent cuts
  - Major disruption when cut



North-east fiber land fall



In the presence of human error

Hinsdale IL - Mother's Day 1988

Fire destroyed 118K fiber lines, 35K local lines & 30K data lines, alarm ignored for an hour

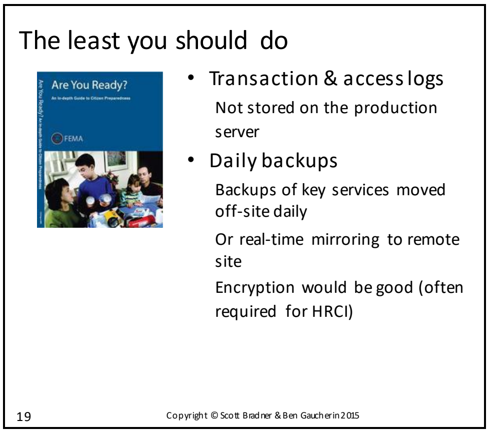
Manhattan - Sept. 17, 1991:

AT&T switching center failure

Switch to diesel generator failed so center switched to battery backup & alarm ignored, batteries ran out

Never underestimate the power of human stupidity.

Robert A. Heinlein


Are You Ready?
An In-depth Guide to Citizen Preparedness
FEMA

The least you should do

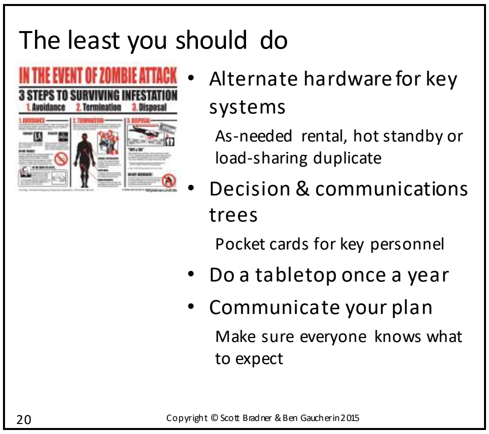
- Transaction & access logs

  Not stored on the production server
- Daily backups

  Backups of key services moved off-site daily

  Or real-time mirroring to remote site

  Encryption would be good (often required for HRCI)


IN THE EVENT OF ZOMBIE ATTACK
3 STEPS TO SURVIVING INFESTATION
1. Avoidance
2. Termination
3. Disposal

The least you should do

- Alternate hardware for key systems

  As-needed rental, hot standby or load-sharing duplicate
- Decision & communications trees

  Pocket cards for key personnel
- Do a tabletop once a year
- Communicate your plan

  Make sure everyone knows what to expect

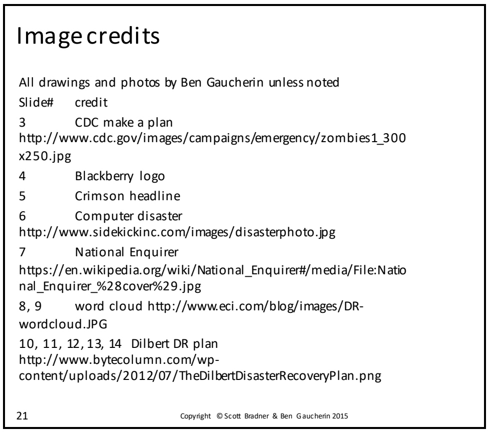


Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

3 CDC make a plan http://www.cdc.gov/images/campaigns/emergency/zombies1_300x250.jpg

4 Blackberry logo

5 Crimson headline

6 Computer disaster http://www.sidekickinc.com/images/disasterphoto.jpg

7 National Enquirer https://en.wikipedia.org/wiki/National_Enquirer#/media/File:National_Enquirer_%28cover%29.jpg

8, 9 word cloud http://www.eci.com/blog/images/DR-wordcloud.JPG

10, 11, 12, 13, 14 Dilbert DR plan http://www.bytecolumn.com/wp-content/uploads/2012/07/TheDilbertDisasterRecoveryPlan.png

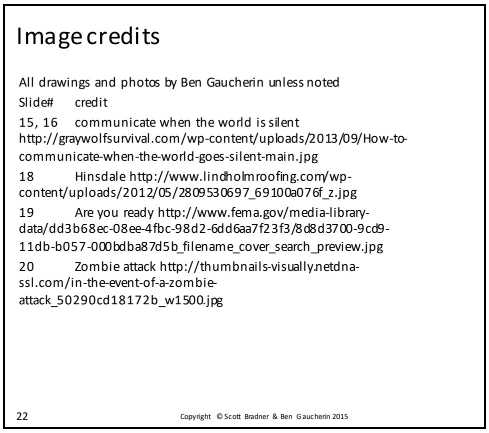


Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
15, 16	communicate when the world is silent http://graywolfsurvival.com/wp-content/uploads/2013/09/How-to-communicate-when-the-world-goes-silent-main.jpg
18	Hinsdale http://www.lindholmroofing.com/wp-content/uploads/2012/05/2809530697_69100a076f_z.jpg
19	Are you ready http://www.fema.gov/media-library-data/dd3b68ec-08ee-4fbc-98d2-6dd6aa7f23f3/8d8d3700-9cd9-11db-b057-000bdba87d5b_filename_cover_search_preview.jpg
20	Zombie attack http://thumbnails-visually.netdna-ssl.com/in-the-event-of-a-zombie-attack_50290cd18172b_w1500.jpg

Managing the infrastructure

Conclusion

CSCI E 45a: The Cyber World – part A

In summary…

ISO 27000

COBIT 5 AN ISACA® FRAMEWORK

ITIL®

- Delivering technology services requires managing everything involved in delivering the service
- There is no shortage of management frameworks and tools
  - Some are useful
  - None are the answer to everything
- ITIL is a comprehensive framework for managing technology services

In summary…

I E T F

Paula Deen's DIET LIES!
BRUCE CATCHES KRIS WITH HER EX-LOVER!
NATIONAL ENQUIRER
KATIE'S SECRET BREAKDOWN
Inside Tom's HOUSE OF HORRORS!
THE REAL TOM IS A MONSTER!
THE ABUSE PUNISHMENTS HUMILIATION
Katie's tortured life exposed!

- IETF standards include management technology standards such as SNMP, NETCONF
- Disasters happen, not planning for them is irresponsible

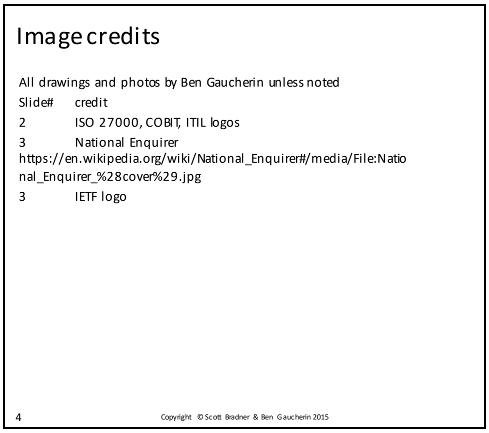


Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	ISO 27000, COBIT, ITIL logos
3	National Enquirer https://en.wikipedia.org/wiki/National_Enquirer#/media/File:National_Enquirer_%28cover%29.jpg
3	IETF logo