CSF 432: Intro to Network and System Security

Week 09 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

Network Documentation

Network Documentation

Internal operating procedures

- Organizations have different business objectives
  - Processes and procedures
- Operational procedures
  - Downtime notifications
  - Facilities issues
- Software upgrades - Testing, change control
- Documentation is the key
  - Everyone can review and understand the policies

Network Documentation

Mapping the network

- Networks are built in phases
  - Large chunks at a time
- You can't see most of it
  - Fiber and wires in the walls and ceiling
- Documentation is essential
  - Both physical and logical
- One of the best things you can do
  - Especially as the new hire

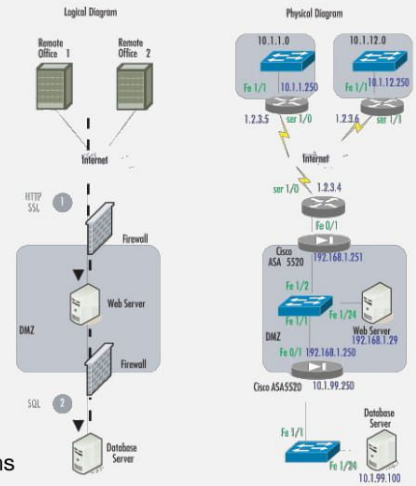
Network Documentation

Logical network maps

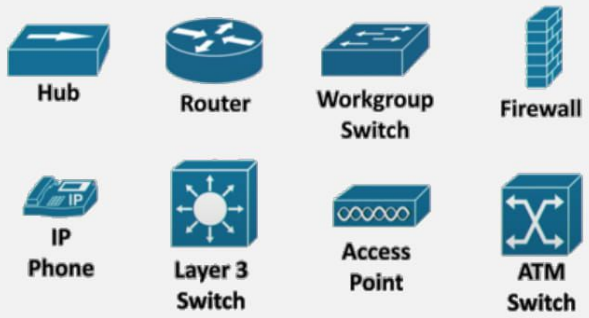
- Specialized software
  - Visio, OmniGraffle, Gliffy.com
- High level views
  - WAN layout, application flows
- Useful for planning and collaboration

Physical network maps

- Follows the physical wire and device
  - Can include physical rack locations



Network Documentation



Network Documentation

Change management

- How to make a change
  - Upgrade software, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored
  - Did you feel that bite?
- Have clear policies
  - Frequency, duration, installation process, fallback procedures
- Sometimes extremely difficult to implement
  - It's hard to change corporate culture

Network Documentation

Managing your cables

- ANSI/TIA/EIA 606
  - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- Presentation of information
  - Reports, drawings, work orders
- Pathway, space, grounding
  - Identifiers, Labeling
- Cables
  - Identifiers, labels, color coding, bar coding

Network Documentation

Labeling

- Everything is tagged and labeled
  - A standard format
- Port labeling
  - CB01-01A-D088
  - CB01 - Main facility
  - 01A - Floor 1, space A
  - D088 - Data port 88
- All cables are documented
  - Central database

Network Documentation

System labeling

- Many people will work on a single workstation or server
  - There needs to be a standard reference
- Unique system ID
  - Asset tag
  - System name
  - Serial number
- Clearly visible
  - Especially in a data center

Network Documentation

Circuit labeling

- WAN circuits aren't a problem
  - Until they are a problem
  - It's outside your control
- All components of the WAN
  - Demarc interface
  - CSU/DSU
  - Router
- Label information
  - WAN provider Circuit ID
  - WAN provider phone number
  - Internal reference name

Network Documentation

Patch panel labeling

- Not much real estate
  - Fit a lot into a small space
- Number each side of the link
  - Incremental
  - Geographically descriptive

Network Documentation

Baselines

- Broadly defined
  - What does it mean to you?
  - Application response time, network throughput, etc.
- Point of reference
  - Accumulated knowledge
  - Examine the past to predict the future
  - Useful for planning

Availability Concepts

Availability Concepts

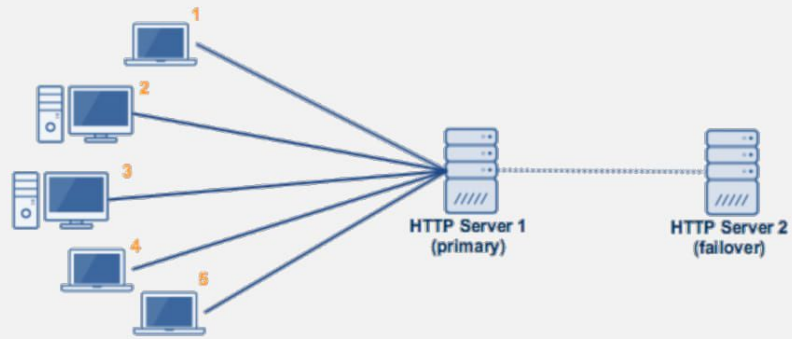
Fault tolerance

- Maintain uptime in the case of a failure
  - If a problem occurs, what happens?
  - Can degrade performance
- Fault tolerance adds complexity
  - The cost of managing the environment increases
- Single device fault tolerance
  - RAID, redundant power supplies, redundant NICs
- Multiple device fault tolerance
  - Server farms with load balancing
  - Multiple network paths

Availability Concepts

Active/Passive

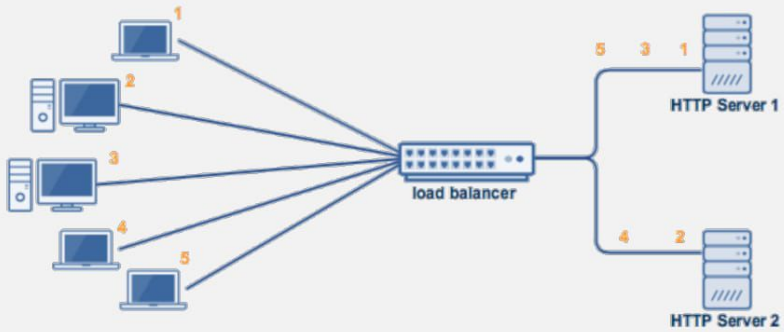
- Some servers active, others on standby (active/passive)



Availability Concepts

Active/Active

- Share the load to reduce stress on one device. If one server fails, distribute that load among the other servers



Availability Concepts

Redundancy and fault tolerance

- Redundant hardware components
  - Multiple devices, load balancing power supplies
- RAID
  - Redundant Array of Independent Disks
- Uninterruptible power supplies (UPS)
  - Prepare for the disconnections
- Clustering
  - A logical collective of servers
- Load balancing
  - Shared service load across components

Availability Concepts

High availability

- Redundancy doesn't always mean always available
  - May need to be enabled manually
- HA (high availability)
  - Always on, always available
- May include many different components working together
  - Watch for single points of failure
- Higher availability almost always means higher costs
  - There's always another contingency you could add
  - Upgraded power, high-quality server components, etc.

Availability Concepts

NIC teaming

- Load Balancing / Fail Over (LBFO)
  - Aggregate bandwidth, redundant paths
  - Becomes more important in the virtual world
- Multiple network adapters
  - Looks like a single adapter
  - Integrate with switches
- NICs talk to each other
  - Usually multicast instead of broadcast
  - Fails over when a NIC doesn't respond

Power Management

Power Management

UPS

- Uninterruptible Power Supply
  - Short-term backup power
  - Blackouts, brownouts, surges
- UPS types
  - Standby UPS, line-interactive UPS, and on-line UPS
- Features
  - Auto shutdown, battery capacity, outlets, phone line suppression

Power Management

Generators

- Long-term power backup
  - Fuel storage required
- Power an entire building
  - Some power outlets may be marked as generator-powered
- It may take a few minutes to get the generator up to speed
  - Use a battery UPS while the generator is starting

Power Management

Dual-power supplies

- Redundancy
  - Internal server power supplies
  - External power circuits
- Each power supply can handle 100% of the load
  - Would normally run at 50% of the load
- Hot-swappable
  - Replace a faulty power supply without powering down

Recovery Sites

Recovery Sites

Cold site

- No hardware - empty building
- No data - bring it with you
- No people - bus in your team

Warm site

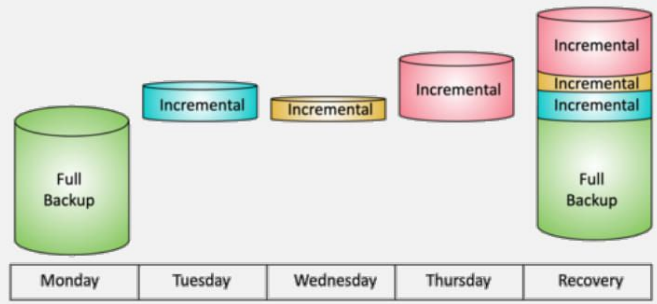
- Somewhere between cold and hot
  - Just enough to get going
- Big room with rack space
  - You bring the hardware
- Hardware is ready and waiting
  - You bring the software and data

Recovery Sites

Hot site

- An exact replica
  - Duplicate everything
- Stocked with hardware
  - Constantly updated
  - You buy two of everything
- Applications and software are constantly updated
  - Automated replication
- Flip a switch and everything moves
  - This may be quite a few switches

Backup and Recovery



Backup and Recovery

File backups

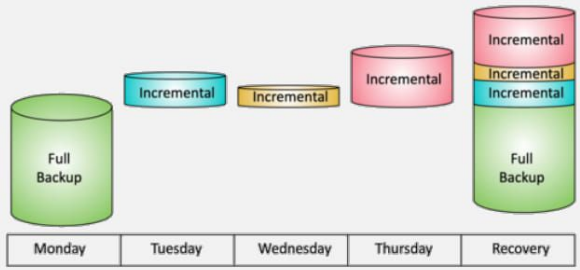
- The archive attribute
  - Set when a file is modified
- Full - Everything
  - You'll want this one first
- Incremental
  - All files changed since the last incremental backup
- Differential
  - All files changed since the last full backup

Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data	High / Low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / High (Multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / Moderate (No more than 2 sets)	Not Cleared

Backup and Recovery

Incremental Backup

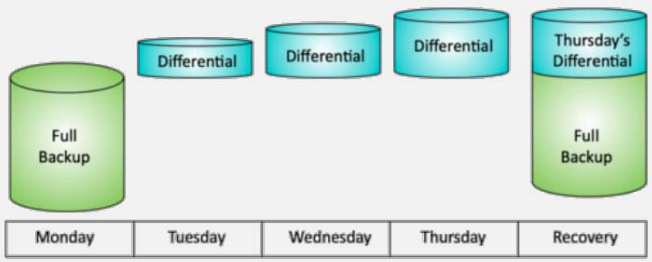
- A full backup is taken first
- Subsequent backups contain data changed since the last full backup and last incremental backup
  - These are usually smaller than the full backup
- A restoration requires the full back and all of the incremental backups



Backup and Recovery

Differential Backup

- A full backup is taken first
- Subsequent backups contain data changed since the last full backup
  - These usually grow larger as data is changed
- A restoration requires the full back and the last differential backup



Backup and Recovery

Taking snapshots

- The cloud is always in motion
  - Application instances are constantly built and torn down
- Snapshots can capture the current configuration and data
  - Preserve the complete state of a device, or just the configuration
- Revert to known state
  - Fall back to a previous snapshot
- Rollback to known configuration
  - Don't modify the data, but use a previous configuration
- Live boot media
  - Run the operating system from removable media - very portable!

CSF 432: Intro to Network and System Security

Week 09 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes