# Campus Operations Best Current Practices

## Campus Network Design & Operations Workshop



UNIVERSITY OF OREGON

Last updated 22nd January 2017

NSRC
Network Startup Resource Center

# Core Network Services

- These are critical for the network to operate correctly. IP packets may flow in the network, but if these services don't reply or aren't configured correctly, users and devices won't be able to connect, authentication services may fail, and network applications won't be accessible.
- They are:
  1. DNS
  2. DHCP
  3. NTP

- In the next slides, we'll explain in turn
  - the importance of each service
  - guidelines on proper design and configuration
  - how to monitor them

# DNS: Domain Name Service

- Without DNS, there is effectively no network.
  - All users, and possibly backend services, are affected (authentication, mail, ...)
- There are two kinds of DNS servers
  - **Caching** (also called resolver):
    - look up (fetch and return) DNS information for clients
    - *“what's the IP address of www.nsrc.org ?”*
  - **Authoritative**
    - serve DNS data, reply to queries from Caching servers
    - “*I have the answer to your question, the IP address of www.nsrc.org is 128.223.157.25*”
  - We'll focus on **Caching** DNS service.

# DNS Design Recommendations

- Campus networks must offer reliable & fast (low latency) DNS service
  - Have on-campus, fast caching resolvers
  - Virtual machines OK, with enough RAM and CPU to deal with load

# DNS Design Recommendations (2)

- Fast and reliable local DNS caches gives better response times
  - Reduces the amount of DNS traffic that must leave the campus
  - Allows blocking access to undesirable domains (policy or other)
    - use DNSBL (DNS Blacklist) type services
    - no need for HTTP proxies or DPI (Deep Packet Inspection)
- Give DNS caches public IPv4 addresses. Avoid placing them behind NAT/firewalls at all costs (even if clients are on private space)

# DNS Software & configuration

- We recommend using either *Unbound* or *PowerDNS-recursor* as the caching resolver
  - Both of these are caching only
- Define which address ranges (v4 & v6) are allowed to use your cache
  - **Only** hosts and devices on the campus!
- No other configuration needed!

# DNS Redundancy

- Redundancy is critical
  - Have two caches on campus
- Larger campuses may have two layers of DNS servers
  - Core servers and client facing servers
  - IP addresses of servers for DNS given out using DHCP

# DNS Redundancy (2)

- DNS uses a simple client-based failover
  - If DNS1 doesn't answer, wait X seconds and try DNS2
  - For *every* query!
- Be aware of problems this can cause
  - There are ways to mitigate this

# DNS Monitoring

- Use a service monitoring tool (Nagios, SmokePing) to monitor availability and latency.
- For each cache
  - check regularly that a given name can be looked up
    - And the answer is the expected one
  - verify that the cache answers in a timely fashion
    - For example, below 10ms response time for cached data

# DHCP – Dynamic Host Configuration Protocol

- If DHCP is down, or leases full, new clients can't access the network!
  - DHCP hands out:
    - IP address and subnet information
    - Default gateway
    - DNS servers to use
    - Configuration server information (e.g. VoIP PBX, TFTP)

# DHCP: Design recommendations

- Place DHCP servers near the core
- Configure DHCP relaying on each subnet facing interfaces
- Broadcast DHCP messages from clients are *relayed* to DHCP servers in the core
- To avoid rogue DHCP servers, consider setting up DHCP snooping
  - blocks DHCP replies from non authorized DHCP servers

# DHCP: Design recommendations (2)

- Use DHCP even for fixed IP addresses (static leases)
  - Renumbering is easier
- Lease times of a few hours is ok
  - Reclaim IP addresses faster if clients leave network without releasing
- For IPv6: turn off SLAAC and use DHCPv6 if possible (we'll explain why)

# DHCP: Software & configuration

- We recommend something well known like ISC-DHCPD
- Configuration is not very difficult, but there are many options.

# DHCP: Redundancy

- For reliable DHCP, you need a pair of servers.
- Setting up redundant DHCP service isn't covered here
  - either have each server cover ½ subnet range
  - or have full failover and synchronization, which is complicated

# DHCP: Monitoring

- Keep an eye on the log files
  - Using, say, **swatch**
- Look for warnings about pool usage
  - Are the ranges allocated about to be full ?
- Network equipment can warn of rogue DHCP servers
  - See DHCP snooping

# NTP – Network Time Protocol

- Accurate time keeping is critical for the network to function properly, and to maintain synchronized logs across devices
  - If clocks are off, some authentication protocols, and DNS, may fail
  - Matching log information with incorrect timestamps is very time consuming
- In case of a security incident, you may need to:
  - Match DHCP log with NAT entries locally
  - And match those with information sent by a remote site administrator

# NTP: Design Recommendations

- For precise timekeeping, it's not recommended to run an NTP *server* inside a virtual machine
- NTP servers *can* live on the same servers (or VMSs) as the DNS resolvers and DHCP servers.
- But be aware that unpatched software can turn misconfigured NTP servers into attack amplifiers, and degrade DHCP and DNS service.
- If you are running a pair of ID management/DS servers (Active Directory) then they can, and probably already do, act as your DNS, NTP and DHCP servers.

# NTP: Software & configuration

- NTPD is well known but has a history of security issues.
- It may be worth looking at OpenNTPD.
- If there is a stratum 1 NTP clock nearby (local exchange point for example) then you can use that.
  - But it's also good enough to use *pool.ntp.org*
- Not all OSes and devices allow having more than one NTP server listed!

# Other recommendations

- We could fill a book with these, so here a few essential things worth considering
  - Implement anti-spoofing (BCP38) at the border of your campus
  - Block connections to port 25/TCP outbound except from a few trusted email servers
    - Configure other servers, and clients, to use those for outbound email
    - This gives you better control and insight into how mail is being (ab)used

# Other recommendations (2)

- Consider rate limiting UDP (except for known video conferencing devices) to slow down bit-torrent
  - blocking it entirely will make it switch to TCP.

# Questions?