Campus Core Services

Campus Network Design & Operations Workshop

UNIVERSITY OF OREGON

Last updated 3rd October 2024

NSRC Network Startup Resource Center

Core Network Services

- These are critical for the network to operate correctly. Packets may flow in the network, but if these services don’t respond or aren’t configured correctly, users will say "the network is down"
- They are:
  1. DNS
  2. DHCP
  3. NTP
  4. Authentication services

Service-by-Service

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

DOMAIN NAME SERVICE

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

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 or recursor):
    - 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 know about nsrc.org, the IP address of www.nsrc.org is 128.223.157.25*"
  - We'll focus on **Caching** DNS service.

DNS Design Recommendations (1)

- Provide on-campus, fast, reliable caching resolvers
  - Avoid giving users resolvers which are tens or hundreds of milliseconds away
  - Reduces the amount of DNS traffic that must leave the campus
  - Virtual machines are OK, with enough RAM and CPU to deal with load

DNS Design Recommendations (2)

- If you can, give DNS caches **public** IPv4 addresses
  - Avoid placing them behind NAT/firewalls (even if clients are on private space) as this will rapidly consume NAT states
- Do you also want to block access to bad domains?
  - Configure your *caches* (not your clients) to forward to Quad9 (9.9.9.9) or Cloudflare for Families (1.1.1.2) to block malware domains
  - Cloudflare 1.1.1.3 will block “adult” domains as well
  - Free and simple to deploy – does not require HTTP proxies or DPI

DNS Design Recommendations (3)

- If your campus runs authoritative DNS as well:
  - Don’t use your authoritative DNS as a resolver
  - Use separate system/VM for authoritative DNS
  - If you have Active Directory, then assign it a subdomain of a real domain you own, e.g. **`ad.myuniv.edu`**
- Totally different functions – keep them apart!
  - Authoritative DNS is queried by the *world* and gives out information about your domains and your IPv4/IPv6 addresses (reverse DNS)
  - Caching DNS is for your *on-site* users, and keeps cache of frequently used names and addresses learned from the Internet

DNS Software & configuration

- We recommend using either **Unbound** or **PowerDNS-recursor** as the caching resolver
  - Both of these are caching only
  - https://nlnetlabs.nl/projects/unbound/about/
  - https://www.powerdns.com/powerdns-recursor
- Define which address ranges (v4 & v6) are allowed to use your cache
  - **Only** permit access from hosts and devices on the campus!
- No other configuration needed!

DNS Redundancy (1)

- Redundancy is critical
  - Have two caches on campus
- Very large campuses may have two or more sets of DNS caches
  - e.g. for internal servers and for clients
  - IP addresses of servers for DNS are given out using DHCP, and can vary by subnet

DNS Redundancy (2)

- DNS uses a simple client-based failover
  - If DNS1 doesn't answer, wait X seconds and try DNS2
  - Some clients do this for *every* query!
- Can cause noticeable degradation
  - Be prepared to get DNS1 back online quickly
  - There are more complex solutions to deal with this, but probably not worth the effort

DNS Monitoring

- Use a service monitoring tool (e.g. 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

DYNAMIC HOST CONFIGURATION PROTOCOL

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Dynamic Host Configuration Protocol (DHCP)

- If DHCP is down, or pools are 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 (1)

- 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

DHCP: Design recommendations (2)

- Use DHCP even for fixed IP addresses for printers etc (static leases)
  - Renumbering is easier
- Sensible lease times are 4-12 hours for wired, 30 mins for wireless to reclaim addresses faster
  - Windows DHCP server defaults to 7 days!
  - Mikrotik DHCP server defaults to 10 minutes!

DHCP: Software & configuration

- We recommend something well known like ISC DHCP or Kea DHCP
- Configuration is not very difficult, but there are many options
- If you already have Active Directory, it's fine as a DHCP server

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

- Check if your server supports active monitoring
  - e.g. Kea + stork (+ prometheus + grafana)
- Otherwise, monitor the log files
- 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. Requires managed edge switches.

NETWORK TIME PROTOCOL

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

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 DNSSEC, may fail
  - Matching log information with incorrect timestamps is very difficult
  - Use consistent timezones: either UTC or your local time zone
- In case of a security incident, you may need to:
  - Match DHCP and auth logs with flow data
  - And match those with information sent by a remote site administrator

NTP: Design Recommendations

- For precise timekeeping, it's better to run an NTP server on hardware rather than inside a virtual machine (but VM is acceptable)
- NTP servers can live on the same servers as the DNS caches and DHCP servers. Or you can use routers as NTP servers.
- Be aware that unpatched software can turn misconfigured NTP servers into attack amplifiers
- If you are running Active Directory servers then they can, and probably already do, act as your DNS, NTP and DHCP servers.

NTP: Deployment Recommendations

- Two local NTP servers sync with external NTP servers
- If there is a stratum 1 NTP clock nearby (at a local exchange point for example) then you can sync to that.
  - But it's also good enough to use pool.ntp.org
    - Note that 2.pool.ntp.org is the only one handing out IPv6 addresses
- Rest of the network devices configured to sync with the local servers
  - Not all OSes and devices allow having more than one NTP server listed!

NTP: Software & configuration

- NTPD is well known but has a history of security issues.
- It may be worth looking at Chrony or OpenNTPD.

AUTHENTICATION SERVICES

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Authentication Services

- Many possibilities, you might have:
  - User database including any of Active Directory, Samba4, FreeIPA, LDAP, SQL...
  - RADIUS server (802.1x wireless authentication)
  - Captive portal
  - ...
- Without any user database, you have no way of knowing or controlling who can access the campus network

Authentication Services

- Users cannot access the network without authenticating
  - Pre-shared Key strongly discouraged
- Have replicated instances of authentication servers, preferably live-live
- Implement active monitoring (e.g. Nagios plugins)
- With 802.1X for wireless, campus can join Eduroam
  - https://eduroam.org/
  - "*Eduroam is based on 802.1X and a linked hierarchy of RADIUS servers containing users' data (usernames and passwords). Participating institutions must have operating RADIUS infrastructure…*"

Questions?