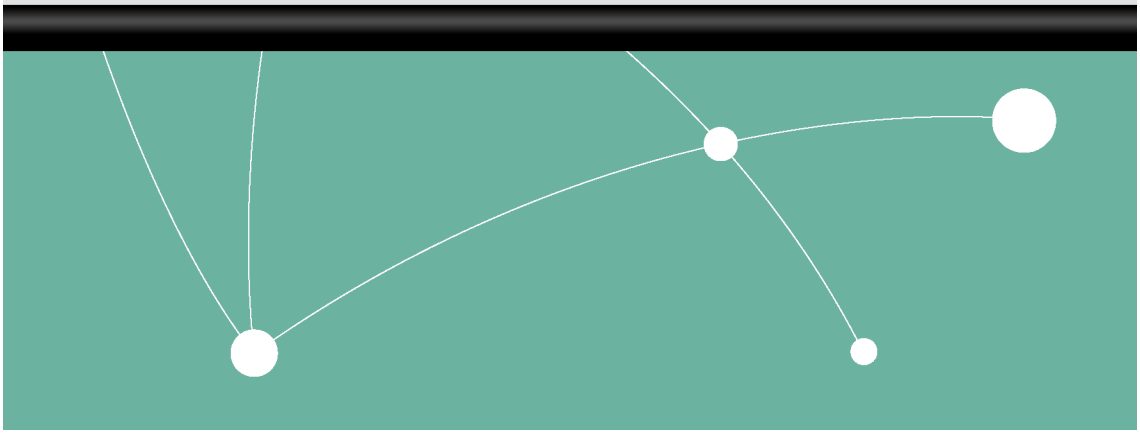
Netværksanbefalinger i forbindelse med Netprøver.dk - IT-drift.



NETDESIGN

Indholdsfortegnelse

1. Forord

Fra 2016/2017 skal alle gymnasiale skriftlige opgaver og prøver, distribueres og afleveres via et centralt IT-system Netprøver.dk.

Det er som hidtil den enkelte skoles ansvar at sikre tilfredsstillende afvikling af prøver. Med indførelsen af Netprøver.dk skal den enkelte skole således også sikre, at netværket er stabilt og kan håndtere den forventede trafik.

Nærværende er tænkt som inspiration og vejledning i forbindelse med opbygning eller udvidelse af trådløse netværk. Da det trådløse netværk er afhængig af det kablede netværk og de eksterne forbindelser, behandles disse overordnet.

Der er på nuværende tidspunkt ikke fremkommet konkrete krav fra Netprøver.dk, herunder svartidskrav og grænser for opgavesæts størrelse. Derfor er nærværende baseret på best practices i almindelighed.

Selve den centrale applikation Netprøver.dk og Internettet som sådan forudsættes at kunne håndtere den nødvendige trafik.

2. Om dette dokument

Nærværende er rettet mod den/de IT-drifts ansvarlige på skolerne.

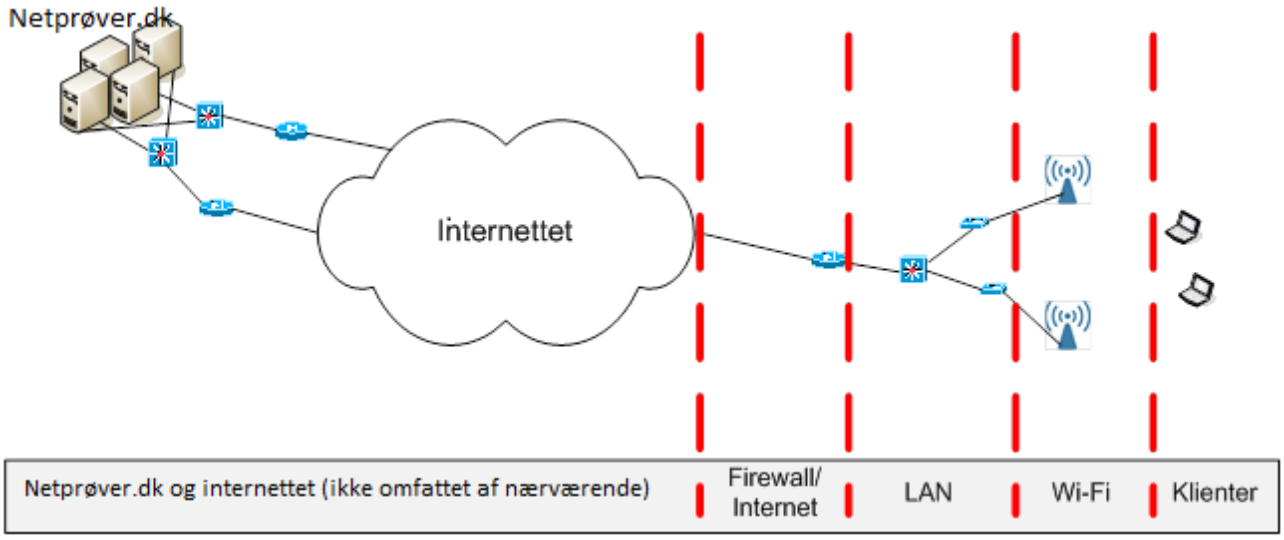
3. Netværk

Opbygning af højtydende og stabile netværk kræver en del specialviden. Hvis skolen ikke har en netværksafdeling med den fornødne ekspertise, må det overvejes, om skolen skal deltage i et IT-fællesskab, eller lade opbygning og vedligeholdelse af netværk udføre af anderkendte netværksleverandører.

Herudover kan følgende anbefales:

- Det bør sikres, at der ikke udføres anlægs- og reparationsarbejder i prøveperioderne, som kan medføre afbrydelse af netværk eller forbindelser.
- Alt netværksudstyr bør være beskyttet af gode passwords, som yderligere bør skiftes mindst én gang om året, f.eks. i forbindelse med sommerferien.
- Der bør ikke være adgang fra elev-VLAN til udstyrets managementadresser.
- Udstyr bør installeres i aflåste rackskabe, så uvedkommende ikke har adgang.

Forbindelsen fra klientenhed til Netprøver.dk kan opdeles i følgende elementer.



3.1 Redundans

I en verden uden ressourcebegrænsninger, ville man opbygge fuldstændigt redundante systemer. Alt lige fra AP til Internetforbindelse skulle være dubleret, så hvilket som helst udstyr kunne fejle og driften alligevel fortsætte upåvirket.

Dette ville selvfølgelig koste mindst det dobbelte af en løsning uden redundans.

Et system opbygget af kvalitetskomponenter, ordentlig implementering, seriøs overvågning, løbende vedligeholdelse og gode procedurer burde i langt de fleste tilfælde være tilstrækkeligt.

I den sidste ende skal prøverne jo kunne afvikles med nødprocedurer, der selvsagt bør vær kendte og afprøvede.

3.2 Wi-Fi

Wi-Fi systemer bruger nogle frekvensområder i 2,4 GHz og 5 GHz båndet. I 2,4 GHz området er dette organiseret i 13 kanaler. Disse er imidlertid overlappende og i praksis kan man kun benytte 3 kanaler (1, 6 og 11) samtidigt. Hvis man f.eks. opsætter 3 AP'er i samme lokale på hver sin kanal (1, 6 og 11) vil den samlede kapacitet være 3 gange kapaciteten for ét AP. Men hvis der opsættes 6 AP'er i lokalet vil disse, to og to, skulle benytte de samme kanaler og man vil ikke få væsentlig højere kapacitet.

I 5 GHz området er der 18 ikke-overlappende kanaler til rådighed og den samlede kapacitet langt større. Der er yderligere større frihed med hensyn til antal og placering af AP'er.

Det er efterhånden almindeligt i skoleløsninger, at der opsættes et AP pr. klasselokale. Hertil kommer AP'er på gange og fællesområder.
Hvis der er behov for mere end 3 AP'er indenfor et mindre område, skal der anvendes forskellige metoder for at sikre tilfredsstillende funktion.

- Brug af retningsbestemte antenner, så udbredelsen af det enkelte AP begrænses
- Brug af 20 MHz brede kanaler, så der er flest mulige kanaler til rådighed

- Brug af nogle AP'er, der kun benytter 5 GHz.
- Kun tillade høje associeringshastigheder, så klienterne er tættere på AP'et.
- Hvis der er mange klienter i ét lokale kan man yderligere formindske AP'ernes følsomhed.

Generelt kan følgende anbefales:

- Wi-Fi systemet bør være styret via en central WLAN kontroller, så der er samlet styring af både sikkerhed og radiomæssige forhold. Herudover giver en centraliseret løsning normalt et godt overblik.

- Nye AP'er bør understøtte IEEE802.11ac (5 GHz) og yderligere samtidigt understøtte 2,4 GHz (IEEE802.11n).

- Som tommelfingerregel regnes med 20-40 klienter pr. AP.

- IEEE802.11b og de langsomme hastigheder (1,2,5,11,6,9,12,18…..) bør deaktiveres. Den præcise konfiguration afhænger af hvor tæt AP'erne er opsat.

- Brug altid kun kanal 1, 6 og 11 på 2,4 GHz båndet

- Brug mekanismer for at få klienterne til at benytte 5 GHz (Bandselect, Bandsteering etc.)

- Under prøverne kan der eventuelt benyttes et specielt SSID (WLAN) og tilhørende VLAN. Således kan dette forholdsvist enkelt prioriteres i forhold til de øvrige anvendelser. Omvendt kan det generelle elevnet nemt nedprioriteres i tilfælde af flaskehalsproblemer.

3.3 Klienterne

Elevernes enheder udgør halvdelen af hver forbindelse og samlet set langt den største del af det trådløse netværk. Det er yderligere klientenhederne der primært styrer forholdene omkring den trådløse forbindelse, herunder protokol og hastighed, hvilket AP der kommunikeres med og hvornår der eventuelt skiftes til et andet AP.

AP'erne i netværket kan kommunikere med forskellige hastigheder mod de enkelte klienter, men den samlede kapacitet bliver naturligvis størst hvis der primært kommunikeres med høje hastigheder. Med andre ord – enkelte klienter der kommunikerer med lave hastigheder, f.eks. IEEE802.11b, vil trække den samlede ydeevne ned.

Det er derfor vigtigt at disse enheder og specielt netværkskortene, er nyere og understøtter de protokoller og mekanismer som netværket tilbyder.

Specielt er det vigtigt at de trådløse enheder understøtter 5 GHz båndet (IEEE802.11a eller IEEE802.11ac), som tilbyder langt flere kanaler og dermed samlet større kapacitet.

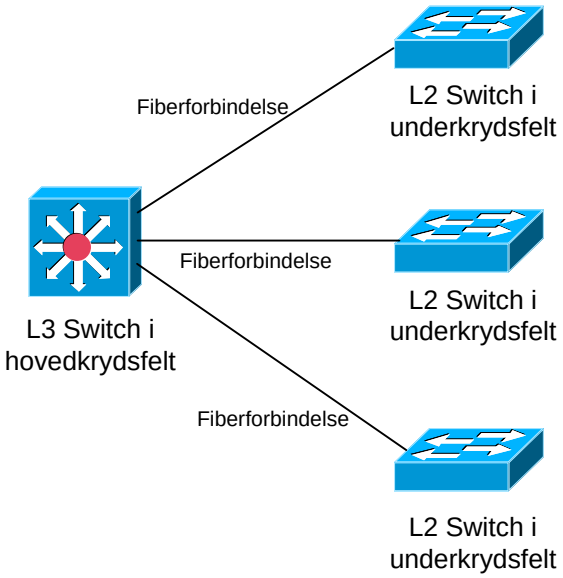
Derfor er yderligere vigtigt at enhedernes drivere er opdateret til seneste version.

Den enkelte skole bør udarbejde anbefalinger vedrørende PC anskaffelser og i øvrigt tilbyde de studerende mulighed for at teste udstyr mod netværket. Skolen kan yderligere anskaffe et antal Wi-Fi dongles til udlån, hvis enkelte elevmaskiner ikke kan bringes til at fungere tilfredsstillende.

De fleste professionelle trådløse netværk giver mulighed for at se hvilke protokoller og hastigheder klienterne benytter. Dette kan blandt andet benyttes til at justere forskellige parametre i de trådløse netværk.

3.4 LAN

Det kablede netværk, LAN'et, skal sammenbinde alle enheder, herunder AP'er og firewall.



Normalt opbygges LAN med L3 switche i hovedkrydsfeltet og L2 switche i underkrydsfelterne. Herved kan netværket opdeles i VLAN der routes sammen. Herved kan eventuelle problemer (broadcast-storme) ikke umiddelbart brede sig ukontrolleret i netværket.
VLAN kan yderligere bruges som sikkerhed, da adgangen mellem VLAN kan begrænses eller forhindres via routerfunktionen eller firewallen.

Der bør etableres QoS i netværket således, at visse anvendelser kan prioriteres over andre. For eksempel vil det jo være uheldigt hvis ikke-prøverelateret brug af YouTube eller lignende påvirker afholdelsen af eksamen.

Forbindelser mellem krydsfelter bør være fiber og minimum 1 Gbit/s. Ved ny-anlæg bør Single Mode Fiber (SM) vælges.

Switchene i underkrydsfelter bør understøtte PoE+ (Power over Ethernet) – IEEE802.3at. Herved kan AP'er strømforsynes direkte fra switchene og man undgår strømforsyninger og powerinjektorer.
IEEE802.3at (30W) anbefales fordi mange nyere AP'er kræver mere effekt end den gamle standard IEEE802.3af (15,4W) kan levere.

3.5 Firewall/Internet

Internetforbindelsen bør være baseret på fiber med symmetrisk båndbredde. Herved kan trafik til og fra Internettet foregå lige hurtigt.

Forbindelsen bør kun være ca. 50% belastet på normale dage.

Forbindelsen bør være beskyttet af en firewall med en kapacitet der matcher Internetforbindelsen.

3.5.1 Beskyttelse mod DDOS angreb

Det kan overvejes om forbindelsen skal beskyttes mod DDOS angreb.

I modsætning til de angreb almindelige firewalls beskytter mod, er formålet med DDoS-angreb (Distributed Denial of Service) som regel ikke at trænge ind gennem forsvaret, men simpelthen at gøre målet, fx en webserver, utilgængelig for omverden. Det sker oftest ved at sende meget store mængder datapakker fra mange forskellige kilder mod målet. Det spænder fra simple datapakker, der tilsammen opbruger al båndbredden på forbindelsen, til avancerede datapakker som angriberen har designet til at være meget krævende for målmaskinen at behandle, og derfor opbruger alt CPU og RAM. Resultatet er det samme; målet er afskåret fra omverdenen.
For nogle få $ kan man bestille et angreb mod en given server.

Beskyttelsen skal implementeres af leverandøren af Internetforbindelsen.

Læs eventuelt mere hos disse udvalgte leverandører:

http://erhverv.tdc.dk/element.php?dogtag=e_prod_net_sik_dos

https://nianet.dk/produkter/anti-ddos/?gclid=CNWyqbbUhMMCFcECcwod7SEAKw

4. Trådløse netværk – Lidt teori

Trådløse netværk (WLAN - Wi-Fi) opererer i 2 frekvensområder omkring 2,4 GHz og 5 GHz.

Standardiseringsorganisationen IEEE, nærmere bestemt IEEE802.11 og de underliggende arbejdsgrupper, styrer udviklingen af standarderne indenfor trådløse netværk i disse frekvensområder. Cisco deltager aktivt i flere arbejdsgrupper og er således med til at præge udviklingen.

Følgende arbejdsgrupper kan nævnes:

- 802.11a (op til 54 Mbit/s på 5 GHz)
- 802.11b (op til 11 Mbit/s på 2,4 GHz)
- 802.11g (op til 54 Mbit/s på 2,4 GHz)
- 802.11n (op til 300 Mbit/s på 2,4 GHz og 5 GHz)
- 802.11ac (op til 1,3 Gbit/s på 5 GHz)
- 802.11e (QoS i WLAN)
- 802.11i (Sikkerhed i WLAN)
- 802.11r (Roaming i WLAN)

Jævnfør IEEE802.11 er frekvensområderne organiseret i kanaler. I 2,4 GHz området er der 3 brugbare (ikke overlappende) kanaler og i 5,0 GHz området er der 19 kanaler.

For at sikre fredelig sameksistens og kompabilitet mellem WLAN udstyr fra forskellige producenter, er der oprettet en uafhængig organisation, Wi-Fi Alliance, der tester og godkender WLAN udstyr. Således vil en Wi-Fi certificeret klient kunne koble op mod et certificeret WLAN system.
Wi-Fi Alliance har naturligvis kun indflydelse på udstyr der testes med henblik på certificering og Wi-Fi certificeret udstyr vil kunne generes af udstyr der ikke er certificeret. Det kan nævnes, at Wi-Fi Alliance har en sikkerhedsspecifikation WPA2 som er sammenfaldende med IEEE802.11i.

4.1 IEEE802.11 grundlæggende teknik

Der er en række grundlæggende karakteristika ved radiokommunikation og IEEE802.11.

Disse forhold er lige for alle fabrikater, men måden hvorpå den enkelte leverandør forsøger at overkomme eller minimere virkningerne af disse karakteristika varierer.

- Den opnåelige hastighed (datarate[1]) afhænger af signalkvaliteten (signalstyrke og forholdet mellem signal og støj). Jo længere væk man er fra et AP jo lavere hastighed er mulig. Således kan en klient tæt på et AP tilknytte sig med 54 Mbit/s medens klienter længere væk kun kan opnå tilknytning med måske 1 Mbit/s.

- For at sikre tilpas høj associeringshastighed for den enkelte klient vi man sætte AP'er tættere – lave mikroceller. Der kan yderligere være kapacitetsmæssige grunde til at opsætte mange AP'er – hvis klienterne fordeles over flere AP'er bliver den samlede båndbredde højere. Hvis man opsætter mange AP'er vil den samme kanal skulle bruges flere gange.

[1] Datarate eller tilknytningshastighed (associeringshastighed) er den hastighed hvormed data signaleres på den aktuelle forbindelse. På grund af protokol ineffektivitet og halv dupleks er den effektive båndbredde kun ca. 50 % af datarate. En PC med 54 Mbit/s datarate kan således forvente at kunne flytte maksimalt 22 Mbit/s.

- Når der er mange AP'er vil der oftere skulle foregå overdragelse af dataforbindelsen (handover/roaming) fra et AP til et andet. I forbindelse med for eksempel trådløs IP telefoni bliver denne roaming en kritisk funktion.

4.2 Co-Channel Interference

IEEE802.11 er af natur et delt medie - alle enheder på samme kanal kan høre hinanden og hvis flere enheder sender samtidigt (i samme fysiske område) vil radiosignalerne ødelægge hinanden. Dette kaldes Co-channel Interference (Interferens fra enheder på samme kanal). Dette har specielt betydning i 2,4 GHz området hvor der kun er 3 kanaler og samme kanal derfor hurtigere bliver genbrugt.

IEEE802.11 benytter CSMA/CA til at styre hvornår de enkelte enheder har adgang til mediet (kanalen). Dette sker blandt andet ved at der i alle pakker er et varighedsfelt (duration), der fortæller alle enhederne hvor længe en given transmission forventes at vare. Andre enheder undlader at transmittere data imens og er således med til at forhindre kollisioner. IEEE802.11 specifikationerne fastlægger de mulige værdier og der sikres herigennem fair og lige adgang til mediet.

Både AP'er og klienter bidrager til Co-Cannel Interference.

Når mikroceller benyttes ønsker man derfor ofte at reducere sendestyrken på AP'er og klienter, så udbredelsesområdet minimeres. Yderligere reducerer man problemet hvor klienter kommunikerer med samme AP, men ikke kan høre hinanden. Dette fænomen "hidden nodes" medfører, at klienterne uforvarende kommer til at kommunikere samtidigt og kollisioner opstår.

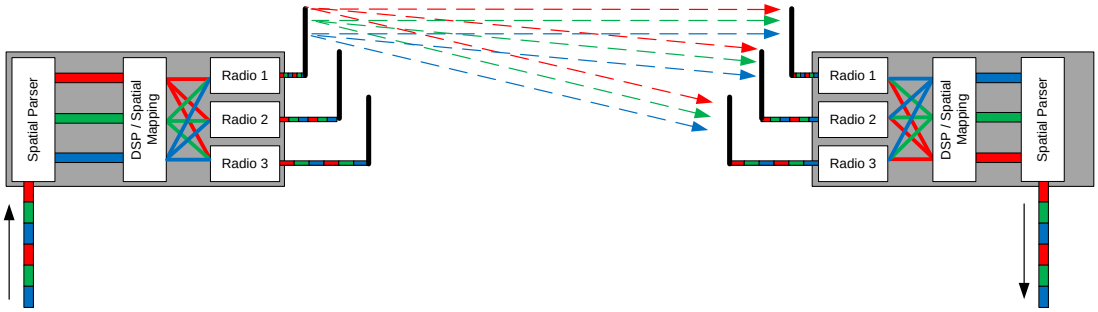
Hvis mange AP'er i samme område benytter samme kanal vil den samlede kapacitet, uanset antallet af AP'er i bedste fald svare til kapaciteten af ét AP (pr. ikke-overlappende kanal).

4.3 IEEE802.11n og 11ac

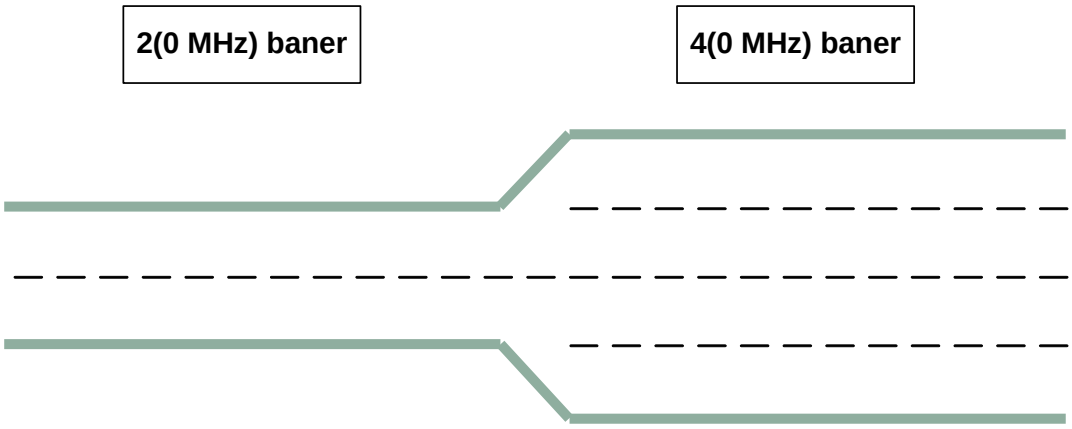
Der benyttes forskellige teknikker til at opnå de højere hastigheder med 11n og 11ac. Selv om der er forskelle er der alligevel mange lighedspunkter. For at opnå de maksimale hastigheder skal alle teknikker anvendes og radioforholdene skal være optimale.

I det følgende nævnes de vigtigste.
MIMO teknikken (Multiple-In, multiple-Out), hvor anvendelse af op til 4 radioer/antenner samtidigt (på samme frekvensbånd/kanal) giver forbedret rækkevidde og performance.

Flere Spatial Streams (MSS - Multiple Spatial Streams). Forskellige datastrømme afsendelse samtidigt af de forskellige radioer.
Når der er tale om 3 spatial streams deles den indkomne datastrøm op i tre (rød, grøn og blå) som hver sendes til alle 3 radioer. Man sender de 3 dele samtidigt ved at ændre fase og amplitude og kan på denne måde holde data adskilt. Man opnår højere båndbredde. Teknikken kræver naturligvis at modtageren også kan modtage/kombinere datastrømmene og er derfor kun relevant mellem to IEEE802.11n produkter.
Tegningen viser kun datastrømmen fra den øverste antenne.



Brug af brede kanaler. Ved at bundle 2, 4 eller 8 almindelige 20 MHz kanaler opnås højere båndbredde. Som tidligere nævnt er der kun 3 kanaler i 2,4 GHz området og hvis 2 kanaler bundles er der i praksis kun mulighed for én kanal. Derfor er denne teknik kun relevant i 5 GHz området.



Hvis mange AP'er opsættes tæt, som det typisk er tilfældet på skoler, vil teknikken ikke være umiddelbart være relevant.