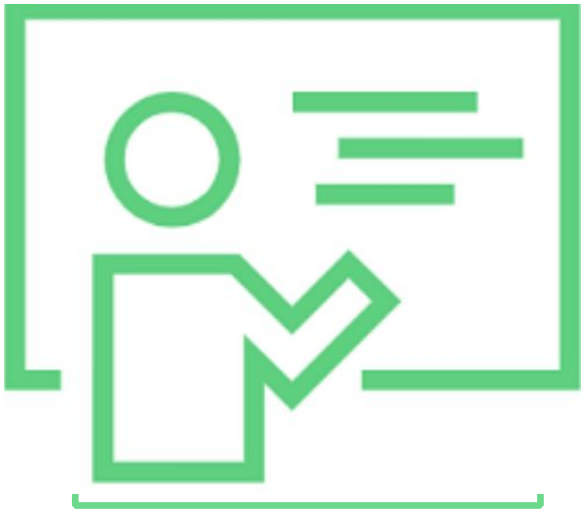

Nätverksutrustning, segmentering och åtkomst

Joakim Englund, Systementor AB

Repetition från dag 5

- Sensor → broker → adapter → API → konsument
- Varje tjänst har ett avgränsat ansvar
- Request/response och publish/subscribe
- Ett delsystem kan fungera när ett annat har fel

Dagens mål

- Förklara nätverksutrustningens roller
- Planera IP-adresser och separata nät
- Tillåta och blockera rätt anslutningar
- Testa regler och återställa konfigurationen

Switch, router och brandvägg

- Switch: skickar ramar (frames) inom ett lokalt nät
- Router: skickar IP-paket mellan nät
- Brandvägg: tillåter eller blockerar trafik
- Samma apparat kan ha flera av rollerna

WiFi och accesspunkter

- Accesspunkten ansluter trådlösa klienter
- SSID är namnet på det trådlösa nätet
- Olika SSID kan kopplas till olika VLAN
- Separera IoT från administration
- Verifiera isoleringen med trafiktester

En enkel IP-plan

Segment	***IP-nät / gateway***
IoT	10.60.10.0/24
Tjänster	10.60.20.0/24
Administration	10.60.30.0/24
Gateway	Routern har .1 i varje nät

IP-adress, prefix och gateway

10.60.10.10/24 → gateway 10.60.10.1

- Adressen identifierar ett interface i nätet
- /24: nät 10.60.10.0, mask 255.255.255.0
- Trafik till andra nät går via en gateway

Segmentering med VLAN

- VLAN delar upp ett switchat nät logiskt
- Accessport: ett VLAN till slutenheten
- Trunk: flera VLAN över samma länk
- Mellan VLAN behövs routing och åtkomstregler

Paketets väg till ett annat nät

1. Avsändaren ser att målet ligger i ett annat nät
2. Paketet skickas till standardgatewayen
3. Routern väljer väg; brandväggen prövar regeln
4. Svaret behöver också en fungerande returväg

Vilka anslutningar ska tillåtas?

Målserver: 10.60.20.10 | Transport: TCP

- IoT → server: 1883 tillåts (MQTT)
- IoT → server: 8080 blockeras
- Admin → server: 8080 tillåts (API)
- Admin → server: 1883 blockeras

Brandväggens kedjor

Kedja	***Vilken trafik?***
input	Till routern själv
forward	Genom routern mellan näten
output	Från routern själv

Tillstånd och returtrafik

- Nya anslutningar prövas mot åtkomstreglerna
- Tillåt returtrafik med established,related
- MQTT-klienten initierar anslutningen till brokern
- Brokern kan skicka data tillbaka på samma anslutning

NAT och VPN

- NAT översätter IP-adresser och ibland portar
- Vanligt när privata IoT-nät når internet
- En krypterad VPN skyddar trafik mellan ändpunkter
- Båda behöver fortfarande rätt åtkomstregler

Underhåll och säker återställning

- Dokumentera modell, version och ansvarig
- Spara konfigurationen före en ändring
- Kontrollera uppdateringar och kompatibilitet
- Verifiera efteråt; återställ om testerna fallerar

Demo: ett nät, en terminal

1. Starta labben med up
2. Kör sex tester med test
3. Kontrollera tillåten trafik
4. Verifiera blockerad trafik
5. Prova ändring och återställning

Eftermiddagens arbete

- Kör referenslabben i en Linux-terminal
- Rita nät och IP-plan för gruppens IoT-case
- Motivera och testa tillåten och blockerad trafik
- Spara skiss, regler och testresultat i Git