Mittuniversitetet
MID SWEDEN UNIVERSITY

Datornätverk
Routing, broadcast och multicast i fastighetsnät

Lennart Franked

20 augusti 2026

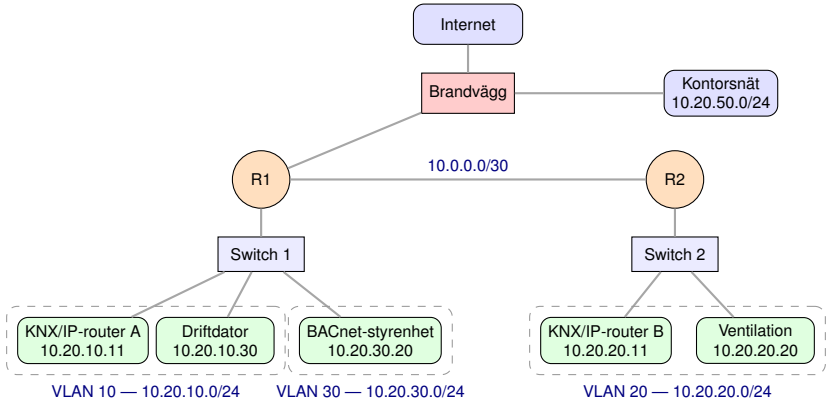
Mittuniversitetet
MID SWEDEN UNIVERSITY

1. Anläggningen
2. Routing
3. Broadcast och multicast stannar
4. KNXnet/IP
5. Portar och brandvägg
6. NAT och Säkerhet

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

Anläggningen vi ska felsöka



Switchar och VLAN från förra veckan, adressplanen från förra föreläsningen. Nu ska trafiken *mellan* segmenten fungera.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Två frågor

Fråga 1

Varför ser inte de här två KNX/IP-routrarna varandra?
Båda är påslagna, båda har rätt adress, båda svarar på `ping`. Ändå går ingen KNX-trafik mellan dem.

Fråga 2

Varför ligger det här segmentet på eget VLAN?
Det kostar arbete att hålla isär näten. Vad får vi tillbaka?

Denna föreläsning ämnar besvara dessa frågor.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

Vad en router gör

Repetition

- Enheter med *samma* prefix når varandra direkt över länklagret
- Enheter med *olika* prefix måste gå via en router

Routerns uppgift

- Ta emot ett paket på ett interface
- Slå upp destinationsadressen i *routingtabellen*
- Skicka vidare ut på rätt interface, till rätt *next-hop*

Nyckelinsikt

Routern fattar beslutet *ett hopp i taget*. Ingen enhet i nätet känner till hela vägen.

Konsekvens vid felsökning

Bara för att trafiken kommer fram åt ena hållet betyder inte det att den kommer tillbaka. Returvägen är ett eget beslut i en annan tabell/post.

Routingtabellen

Routingtabellen kollas varje gång ett IP-paket vidarebefordras.

På driftdatorn i VLAN 10

```
lennart@ET116G:~$ ip route list
default via 10.20.10.1 dev eth0  proto static
10.20.20.0/24 via 10.20.10.1 dev eth0  proto static
10.20.10.0/24 dev eth0  proto kernel  scope link  src 10.20.10.30
```

- `10.20.10.0/24 dev eth0`: *direkt anslutet*, ingen router behövs
- `via 10.20.10.1`: skicka till den routern som nästa hopp
- `default`: allt annat

Samma information i Windows: `route print`, eller `netstat -r` som ger exakt samma utdata [10].

Mittuniversitetet
MID SWEDEN UNIVERSITY

Default gateway

Definition

Dit paketet skickas när ingen annan post i tabellen matchar. Skrivs som `0.0.0.0/0`.

I praktiken

- En vanlig enhet har oftast bara sitt eget subnät plus en default gateway
- Gatewayen är routerns ben i *det egna* subnätet
- Fel gateway $\rightarrow$ allt lokalt fungerar, inget utanför

Vanligt fel

En styrenhet får rätt adress och rätt mask men *ingen* gateway. Den fungerar perfekt vid driftsättning, när alla tillhör samma segment, men slutar fungera då driftdatorn flyttas till kontorsnätet.

Längsta prefixmatchning

Regeln

Flera poster kan matcha samma destination. Routern väljer vägen med det längsta matchande prefixet.

Paket till `10.20.20.11`:

Post i tabellen	Next-hop	Matchar?	Prefixlängd
`0.0.0.0/0`	brandväggen	ja	0
`10.0.0.0/8`	R2	ja	8
`10.20.20.0/24`	R3	ja	**24 — vinner**
`10.20.50.0/24`	R4	nej	—

- Det mest specifika svaret vinner alltid över det mer generella
- Därför fungerar default gateway: `/0` matchar allt, men förlorar mot varje annan träff

Next-hop måste vara nåbar på länklagret

Kravet

- Next-hop måste ligga i *samma subnät* som ett av enhetens egna interface
- Annars går det inte att ARP:a fram en MAC-adress
- Utan MAC-adress kan ramen inte skickas.

Symptomet

Konfigurationen *ser* rätt ut. Routen finns i tabellen. Men inget går fram, och `arp -a` visar `(incomplete)` för gatewayadressen.

Exempel på felet

Enheten har `10.20.10.30/24` och man sätter gateway till `10.20.11.1`.

`10.20.11.1` ligger *inte* i `10.20.10.0/24`. Enheten kan aldrig fråga efter dess MAC-adress, och därmed aldrig skicka något till den.

Hur routern lär sig vägarna

Statiska routes

- Någon skriver in dem för hand
- Ändras aldrig av sig själva
- Fullt tillräckligt för ett fastighetsnät med en handfull segment

Routingprotokoll

- Routrarna berättar för varandra vilka nät de känner till
- **OSPF** inom en organisation, **BGP** mellan operatörer på internet
- Behövs när topologin är stor eller ändrar sig

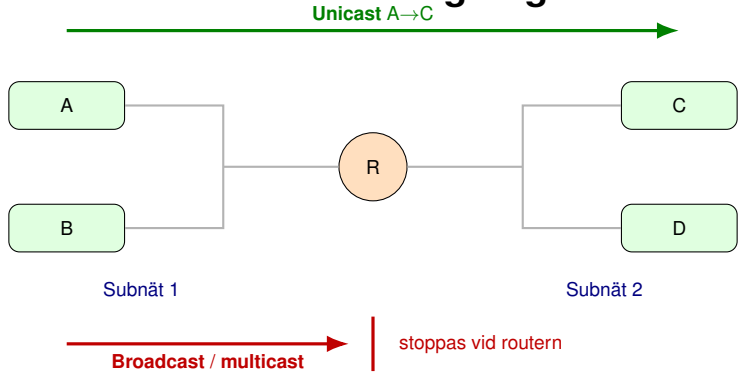
För er del

Underliggande IP-infrastruktur hanteras av IT-avdelningen. Men det är viktigt att förstå subnät, segmentering och routing för konfigurering och felsökning.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

Vad som stannar och vad som går igenom



- **Unicast** En mottagare, en adress. Routas som vanligt.
- **Broadcast** Alla i det egna subnätet. Stannar där.
- **Multicast** Alla som *anmält intresse*. Går vidare bara om routern konfigurerats för det.

Broadcast och Multicast

Broadcast passerar *aldrig* en router.
Multicast passerar bara om någon konfigurerat det.

Varför

- En broadcast är adresserad till *alla i det egna nätet*. Routern vidarebefordrar den aldrig, därav namnet broadcastdomän
- En multicast är adresserad till en *grupp*. Routern vidarebefordrar den om, och bara om, den är konfigurerad för det

Konsekvensen

- **BACnet/IP** bygger på broadcast
- **KNXnet/IP routing** bygger på multicast
- Båda stoppas vid en routergräns om inget görs åt saken

Mittuniversitetet
MID SWEDEN UNIVERSITY

Multicast och IGMP

Idén

- Adressen `224.0.0.0/4` pekar ut en *grupp*, inte en enhet [3]
- En enhet som vill ta emot går med i gruppen
- Anmälan görs med **IGMP** [1]

Skillnaden mot broadcast

- En broadcast går till *alla* på länken, vare sig de vill eller inte
- En multicast går bara till dem som anmält sig — och kan därför också ta sig vidare till nästa subnät, om nätet är konfigurerat för det

KNXnet/IP i routing-läge använder gruppen `224.0.23.12` [7]. Samma adress som i laborationen.

Mittuniversitetet
MID SWEDEN UNIVERSITY

IGMP: så anmäler man sig till en grupp

Mottagaren anmäler sig

- Enheten som vill lyssna skickar ett **Membership Report** till `224.0.0.22`, dit alla IGMPv3-routrar lyssnar [1]
- Routern frågar med jämna mellanrum **Membership Query** till `224.0.0.1` om någon fortfarande vill ha trafiken [1]
- Svarar ingen slutar routern skicka gruppen till det subnätet

Notera

Sändaren anmäler ingenting. Den skickar bara iväg sina paket. Det är *mottagarna* som styr vart trafiken tar vägen.

Vem gör vad

- **Switchen** lyssnar på IGMP-trafiken — *IGMP snooping* — och skickar gruppen bara till de portar som anmält sig [2]
- **Routern** måste ha multicastrouting påslagen för att gruppen ska nå nästa subnät
- Routrarna bygger vägen mellan sig med **PIM**, ett eget protokoll för multicast [6]

Alla IGMP-meddelanden skickas med `TTL=1` [1].

Mittuniversitetet
MID SWEDEN UNIVERSITY

Tre saker att kontrollera

1. **Multicastrouting i routern.** Utan den stannar trafiken i sitt eget subnät, precis som en broadcast. Kräver PIM på *varje* interface trafiken ska passera [6].
2. **Tillräckligt TTL i avsändarens paket.** Varje router drar ett från TTL. `TTL=1` betyder ”lämna aldrig det egna nätet” [4].
3. **IGMP snooping i switchen.** Switchen lyssnar på IGMP och skickar gruppens trafik bara till de portar som anmält sig. Utan snooping går den till *alla* portar i VLAN:et [2].

Felsökningspoängen

De två första måste båda stämma. Är multicastroutingen perfekt konfigurerad men TTL är 1, ser symptomet likadant ut som om ingenting alls var gjort.

`224.0.0.0/24` vidarebefordras *aldrig* utanför länken — den är reserverad för routrarnas egen kontrolltrafik [3].

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

Mittuniversitetet
MID SWEDEN UNIVERSITY

KNXnet/IP: två helt olika driftsätt

	Tunnelling	**Routing**
Trafiktyp	*Unicast* UDP	*Multicast* UDP
Adress	Gatewayens IP-adress	`224.0.23.12` [7]
Port	3671 [8]	3671 [8]
Används för	En klient (t.ex. ETS eller en visualisering) mot en KNX-installation	Att koppla ihop flera KNX-linjer eller byggnader över IP
Över routergräns	Vanlig unicast-routing	Kräver korrekt konfigurerad multicastrouting

Tillbaka till fråga 1

Varför ser inte de två KNX/IP-routrarna varandra?

De står i *olika subnät* och kör KNXnet/IP i *routing*-läge. Deras multicasttrafik till `224.0.23.12` stoppas vid routern.

Vad som skulle lösa det

- Konfigurera multicastrouting mellan segmenten, och kontrollera TTL
- Eller: byt till tunnelling där det passar, unicast routas av sig själv
- Samma VLAN löser det också, men de sitter oftast i var sin del av byggnaden

Varför `ping` lurade oss

`ping` är *unicast* ICMP [11]. Att den fungerar bevisar bara att unicast-routingen är hel. Den säger ingenting alls om multicast.

Ett fungerande `ping` är inte samma sak som ett fungerande system.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

Portar

Vad är en port

IP-adressen pekar ut *enheten*. Portnumret pekar ut *vilken tjänst* i enheten. Brandväggsregler skrivs i termer av adress *och* port.

Protokoll	Port	Transport
KNXnet/IP	3671	UDP
BACnet/IP	47808	UDP
Modbus TCP	502	TCP

Samtliga registrerade hos IANA [8].

TCP eller UDP

- **TCP:** upprättar en förbindelse, kvitterar och skickar om det som tappats. Kostar en handskakning innan första nyttopaketet, och ett tappat paket ger fördröjning när det skickas om. Tillförlitligt.
- **UDP:** ingen förbindelse och ingen omsändning. Inget att vänta på innan man börjar skicka, och det enda som kan bära broadcast och multicast.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

NAT

Vad NAT gör

- Fastigheten har privata adresser (RFC 1918) som inte kan routas på internet [12]
- Routern byter ut avsändaradressen mot sin egen publika adress och håller reda på vem som frågade [14]
- Svaret översätts tillbaka på vägen in

Följden

- Trafik *ut* fungerar av sig själv
- Trafik *in* fungerar inte, routern vet inte vem den skulle gå till

Portöppning — och varför inte

Det frestande

Öppna UDP 3671 in mot KNX-gatewayen i brandväggen, så kommer man åt anläggningen hemifrån. Fem minuters arbete.

Det som händer

- Hela internet kan nu nå gatewayen
- Sökmotorer för uppkopplade enheter, som Shodan, indexerar den inom timmar
- KNXnet/IP utan KNX Secure har ingen autentisering — den som når porten kan styra installationen

Det är inte hypotetiskt

En systematisk genomsökning av internet 2025 hittade **68 243** publikt exponerade OT-enheter globalt. BACnet och KNX var två av de femton protokoll som söktes [13]. Motsvarande genomgång av KNXnet/IP-protokollet finns i [5].

En glömd gateway från byggtiden är ett återkommande fynd.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Säkra OT-nät

VPN i stället för portöppning

- Teknikern kopplar upp sig mot fastighetens nät
- Autentisering och kryptering sköts av VPN-lösningen
- Ingenting exponeras utåt

KNX Secure

KNX IP Secure krypterar KNX-telegrammen över IP. **KNX Data Secure** skyddar användardata med kryptering och autentisering oavsett medium. Bygger på AES 128 CCM [9].

OT-segmentering

- Fastighetssystemen i egna VLAN, skilda från kontorsnätet
- Brandväggsregler som släpper igenom *bara* det som behövs, i *en* riktning
- Driftdator och styrenheter i samma segment. Åtkomst utifrån går via VPN

Mittuniversitetet
MID SWEDEN UNIVERSITY

Tillbaka till fråga 2

Varför ligger det här segmentet på eget VLAN?

För att en dator med skadlig kod i kontorsnätet inte ska kunna nå brandlarmet och ventilationsstyrningen.

Vad segmenteringen kostar

Egna VLAN, egna subnät, en router emellan — och därmed allt vi gått igenom idag: default gateway, multicastrouting, IGMP.

Vad den ger

En begränsad skada. Det som händer i kontorsnätet stannar i kontorsnätet, och fastighetssystemen når man bara via VPN och genom brandväggens regler.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser I

[1] B. Cain m. fl. *Internet Group Management Protocol, Version 3*. Request for Comments RFC 3376. Internet Engineering Task Force, okt. 2002. URL: https://www.rfc-editor.org/rfc/rfc3376 (hämtad 2026-08-17).

[2] M. Christensen, K. Kimball och F. Solensky. *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*. Request for Comments RFC 4541. Internet Engineering Task Force, maj 2006. URL: https://www.rfc-editor.org/rfc/rfc4541 (hämtad 2026-08-17).

[3] M. Cotton, L. Vegoda och D. Meyer. *IANA Guidelines for IPv4 Multicast Address Assignments*. Request for Comments RFC 5771. Internet Engineering Task Force, mars 2010. URL: https://www.rfc-editor.org/rfc/rfc5771 (hämtad 2026-08-17).

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser II

[4] S. Deering. *Host Extensions for IP Multicasting*. Request for Comments RFC 1112. Internet Engineering Task Force, aug. 1989. URL: https://www.rfc-editor.org/rfc/rfc1112 (hämtad 2026-08-17).

[5] Tao Feng m. fl. ”Security assessment and improvement of building ethernet KNXnet/IP protocol”. I: *Discover Applied Sciences* 6.4 (2024), s. 162. DOI: 10.1007/s42452-024-05707-6.

[6] B. Fenner m. fl. *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. Request for Comments RFC 7761. Internet Engineering Task Force, mars 2016. URL: https://www.rfc-editor.org/rfc/rfc7761 (hämtad 2026-08-20).

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser III

[7] Internet Assigned Numbers Authority. *IPv4 Multicast Address Space Registry*. Online registry. URL: https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml (hämtad 2026-08-17).

[8] Internet Assigned Numbers Authority. *Service Name and Transport Protocol Port Number Registry*. Online registry. URL: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml (hämtad 2026-08-17).

[9] KNX Association. *What makes KNX the secure solution for your smart building?* KNX Association, nyhetsartikel. Okt. 2024. URL: https://www.knx.org/news/what-makes-knx-secure-solution-your-smart-building (hämtad 2026-08-17).

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser IV

[10] Microsoft. *netstat*. Windows Commands, Microsoft Learn. 2025. URL: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat (hämtad 2026-08-20).

[11] J. Postel. *Internet Control Message Protocol*. Request for Comments RFC 792. Internet Engineering Task Force, sept. 1981. URL: https://www.rfc-editor.org/rfc/rfc792 (hämtad 2026-08-17).

[12] Y. Rekhter m. fl. *Address Allocation for Private Internets*. Request for Comments RFC 1918. Internet Engineering Task Force, febr. 1996. URL: https://www.rfc-editor.org/rfc/rfc1918 (hämtad 2026-08-17).

Mittuniversitetet
MID SWEDEN UNIVERSITY

Referenser V

[13] Matthew Rodda och Vasilios Mavroudis. ”Analysis of Publicly Accessible Operational Technology and Associated Risks”. I: *arXiv preprint arXiv:2508.02375* (aug. 2025). URL: https://arxiv.org/abs/2508.02375 (hämtad 2026-08-17).

[14] P. Srisuresh och K. Egevang. *Traditional IP Network Address Translator (Traditional NAT)*. Request for Comments RFC 3022. Internet Engineering Task Force, jan. 2001. URL: https://www.rfc-editor.org/rfc/rfc3022 (hämtad 2026-08-17).

Mittuniversitetet
MID SWEDEN UNIVERSITY