NET-301 Anchor Reading Guide

4,937 words · ~22 min read

---

*VCA-NET-301 cross-chapter reading-guide handout. Companion to the catalog page at `https://virtuscyberacademy.org/vca-net-301`. Audience: Belt-5 networking-track students arriving from the catalog's distilled "What Belt-5 Networking Graduates Recognize" register. *

The catalog page tells you WHAT the course covers. This guide tells you HOW to read the canonical anchors that build the Belt-5: which books, which chapters, in which order, what to extract on each pass, and how the anchors compose into a coherent argument about networking at carrier, datacenter, line-rate, and adversary scale.

---

§0. What this guide is for

NET-301 is the academy's networking-track terminal course. Five anchors carry the Belt-5: Bejtlich's *Practice of Network Security Monitoring* for the analyst-watching-the-wire mindset, Stevens's *TCP/IP Illustrated Volume 1* for transport-layer dynamics revisited at advanced depth, and three sections of Kurose-Ross *Computer Networking: A Top-Down Approach* (9th edition) for the cellular core, the cellular authentication exchange, and the Mobile-IP architectural baseline that 5G mobility supersedes.

The five anchors do not compose a textbook tour. Each is opinionated about what matters at this level, each speaks to specific Belt-5 capstone moves, and the set has been chosen so that the anchors talk to each other across the course's Twelve-Module spine. By the end of NET-301 a student should be able to (a) deploy specific factual content from each anchor in a pentest-engagement conversation about modern networking, (b) recognize when a peer cybersecurity program made different anchor choices and what those choices commit them to, and (c) write a defensible Belt-5 capstone whose arguments cite these anchors at chapter and section depth.

This guide is opinionated by design. It is not a comprehensive bibliography; it is the academy's argument for these specific reads in this specific order at this specific depth. Anchors that other peer programs lean on (Tanenbaum's *Computer Networks*; the Cisco / Juniper certification reading lists; the IETF RFC corpus read directly) are

deliberately not the primary anchors at this level because they are encyclopedic rather than opinionated. NET-301 graduates know the comprehensive material; they were trained on the opinionated material.

---

§1. The anchor reading register

Five anchors. Read in this order on first pass; revisit per the per-anchor walks below for capstone preparation.

Anchor 1: Bejtlich, *The Practice of Network Security Monitoring*, Ch 1 (Network Security Monitoring rationale)

Edition / pointer: Richard Bejtlich, *The Practice of Network Security Monitoring*, No Starch Press, 2013 (no recent edition; the 2013 text remains canonical). Chapter 1, "Network Security Monitoring Rationale". Approximately 25 pages.

Why this matters at Belt-5: Bejtlich's argument in Chapter 1 is that the prevention paradigm has structurally failed and the operationally honest response is to assume compromise and instrument for it. The chapter's central operational claim is that NSM's value is asymmetric: building the telemetry costs a fixed amount; the value it returns scales with the sophistication of the adversaries the network encounters. NET-201 introduced Suricata signatures and Zeek scripts at single-sensor scale; NET-301 takes Bejtlich's four-data-types framework into a multi-sensor, log-pipeline, threat-hunting context. A Belt-5 graduate who has internalized Bejtlich's framework reads any production network through the four-data-types lens (full-content, session, statistical, alert) and treats prevention as one layer in a defensive depth, not as the central layer.

Suggested reading order: First. Read Ch 1 cover to cover before any other anchor in this guide. Bejtlich's mindset is the prerequisite for reading the other anchors as a security practitioner rather than as a network engineer.

Cross-link to academy artifacts: NET-301 Lab 8 (clustered Suricata + Zeek deployment against the academy production NSM corpus); SEC-101 cross-cut (the four-data-types framework appears as the canonical NSM reference); ADV-101 capstone (NSM telemetry is the audit surface that catches a successful CSRF reproduction in production).

Anchor 2: Stevens, *TCP/IP Illustrated Volume 1*, Ch 16 (TCP congestion control; advanced re-read)

Edition / pointer: W. Richard Stevens, *TCP/IP Illustrated Volume 1: The Protocols*, 1st edition (1994), Addison-Wesley. Chapter 16, "TCP Congestion Control". Approximately 25 pages. The 1st edition is canonical at the academy; later "second edition" reissues by Fall and Stevens are encyclopedic at a register Belt-5 students typically do not need.

Why this matters at Belt-5: Stevens's argument in Volume 1 Chapter 16 (revisited at NET-301 depth) is that congestion control is the single algorithm whose tuning has the largest practical impact on Internet performance for the largest number of users, and yet it is the algorithm the protocol stack was given the most difficult time to specify. The chapter walks the reader through Reno and NewReno; the modern algorithms that supplanted them are CUBIC (the Linux default since 2007, scaled-up for high-bandwidth long-haul links) and BBR (Google's 2016 algorithm, model-based rather than loss-based, designed for the bufferbloat-prone modern Internet). A Belt-5 graduate should be able to explain why the choice of congestion-control algorithm is an architectural decision visible from the wire: a CUBIC sender and a BBR sender, against the same bottleneck, leave structurally different signatures in `tcpdump` traces.

Suggested reading order: Second. Read Stevens after Bejtlich because Stevens is most useful when read with the analyst's mindset already installed. Approach Stevens looking for the parts of the algorithm visible to a packet-trace observer rather than for the parts visible only to a kernel author.

Cross-link to academy artifacts: NET-301 Lab 9 (capture both CUBIC and BBR streams against the same bottleneck topology in Containerlab; plot the goodput-over-time curves; explain the divergence). NET-201 introduced bufferbloat; NET-301 Stevens revisits the algorithmic landscape that bufferbloat surfaces.

Anchor 3: Kurose-Ross 9e, §7.4 (5G Core decomposition)

Edition / pointer: James Kurose and Keith Ross, *Computer Networking: A Top-Down Approach*, 9th edition (2024), Pearson. Section 7.4, "Cellular Networks: 4G LTE and 5G". The 9th edition is the canonical academy reference because the 9e treatment of 5G is substantially more architecturally serious than the 8e treatment was; per academy edition discipline (D7 net-track edition uplift), 9e is the only edition cited.

Why this matters at Belt-5: Kurose-Ross 9e §7.4 takes the architectural decomposition of the 5G Core seriously. The chapter walks the named Network Functions: AMF (Access and Mobility Management Function), SMF (Session Management Function), UDM (Unified Data Management), AUSF (Authentication Server Function), UPF

(User-Plane Function), plus the NRF (NF Repository) and NSSF (Network Slice Selection) helpers. The 9e frames the design as a deliberate move toward microservice-like functional decomposition: each NF owns one slice of the connection-lifecycle responsibility, NFs discover each other through the NRF, and the service-based interface (SBI) speaks HTTP/2 plus JSON. The 9e's central claim is that this looks superficially like a control-plane SDN move (logical centralization, separation of forwarding from control) but is in fact a different architectural philosophy: SDN centralizes control behind one logical authority; 5GC distributes control across named functional roles that coordinate over a service bus.

Suggested reading order: Third. Read after Bejtlich and Stevens. The 5G Core decomposition is most legible as an architectural argument when you have the analyst's mindset (Bejtlich) and the algorithmic awareness (Stevens) already installed. Without those, the named-NF taxonomy reads like a vendor brochure.

Cross-link to academy artifacts: The cross-chapter handout `handouts/cross-chapter-control-plane-architectures.md` (shared with vca-rf-301) walks the three-way comparison of 5G Core vs SDN vs Mobile-IP along three explicit axes (control-plane decomposition, routing model, state-management strategy). NET-301 Ch 8 wireless deep-dive pairs 5G against the 802.11 substrate; the joint reading at this level is that 5G and 802.11 are two architectural answers to the same wireless-attach question.

Anchor 4: Kurose-Ross 9e, §8.8.2 (5G-AKA authentication exchange)

Edition / pointer: Kurose-Ross 9e, §8.8.2, "5G-AKA Authentication". Read with §7.5.3 (5G mobility) as a coupled pair; the two sections compose one argument.

Why this matters at Belt-5: Kurose-Ross 9e §8.8.2 names the problem the protocol exists to solve. In 4G, 3G, and 2G, the IMSI (the long-lived subscriber identifier) was transmitted in cleartext during initial attach. A rogue base station broadcasting itself to nearby UEs would harvest the IMSI without the legitimate network ever being involved. The "IMSI-catcher" attack class is well documented in security literature, well-funded in surveillance practice, structurally unsolvable inside the legacy AKA design. 5G-AKA closes the gap by introducing the SUCI (Subscription Concealed Identifier), an ECIES-encrypted form of the SUPI (Subscription Permanent Identifier) computed using the home network's public key. Only the home network's AUSF can decrypt the SUCI back to the SUPI; the visited network sees only the encrypted form. The 9e's central observation is that 5G-AKA is not simply "AKA with one new field"; it is a redistribution of trust between the visited network and the home network, and the cryptographic side of that redistribution is what makes the design analyzable.

The mobility companion (§7.5.3) reads as a series of related decompositions: intra-RAN handover (gNB-to-gNB, AMF-stable); inter-AMF mobility (AMF context migrates between control-plane instances); inter-RAT mobility (4G-to-5G handover where the AKA generation itself changes mid-session). The pedagogical move at NET-301 register is to read 5G-AKA together with WPA-AKA (introduced in Ch 8 against the 802.11 substrate) as two AKA instantiations that share the same skeleton: challenge / response / sequence-number anti-replay / fresh session-key derivation. They diverge on exactly one architectural question: who anchors the long-term key, and how is the visiting network told what to trust?

Suggested reading order: Fourth. Read immediately after Anchor 3 (5G Core); the two are coupled. Treat them as one ~50-page Kurose-Ross block rather than two separate reads.

Cross-link to academy artifacts: The cross-chapter handout `handouts/cross-chapter-wireless-aka-progression.md` (shared with vca-wir-101 + vca-rf-301 + vca-net-201 + vca-sec-101) walks the wireless-AKA progression from 802.11i (2004) through WPA3 / Dragonfly (2018) to 5G-AKA (3GPP Rel-15, 2018) along three axes (trust-anchor model, long-term-identity privacy, forward-secrecy + replay-protection mechanism). KRACK, Dragonblood, and IMSI-catcher are named as the attack classes driving each redesign. A future SEC-101 advanced lab will pull forward from this prose to drive a hands-on capture-and-analyze exercise against an OAI 5G testbed.

Anchor 5: Kurose-Ross 9e, §7.5.4 (Mobile-IP and the architectural baseline)

Edition / pointer: Kurose-Ross 9e, §7.5.4, "Mobile-IP". The 9e §7.5.4 carries the Mobile-IP treatment that has been in the textbook since the 5th edition; the value at NET-301 register is that it surfaces the 1990s-IETF-era architectural baseline against which the 5G Core mobility design has to be read.

Why this matters at Belt-5: Mobile-IP's premise is transparent host mobility on the routed Internet. A mobile node registers a Care-of-Address with its Home Agent on its home network; subsequent traffic to the mobile node is intercepted by the HA and tunneled to the Foreign Agent on the visited network, which delivers the packet locally. The infamous criticism of the design is the triangle-routing pattern: sender to HA to FA to MN. MIPv6 introduces route-optimization to flatten the path. The 9e's central pedagogical move is to read Mobile-IP's per-mobile-node distributed-state design as a third architectural answer alongside 5G Core (microservice-like NF separation) and SDN

(logical centralization). Each of the three answers has a distinct failure-domain story: 5G Core fails per-NF; SDN fails behind the controller; Mobile-IP fails per-mobile-node-pair (HA outage strands one home network; FA outage strands one visited network).

Suggested reading order: Fifth. Read after Anchors 3 and 4 because Mobile-IP is most useful as a contrast against the 5G Core decomposition rather than as a standalone treatment.

Cross-link to academy artifacts: The same cross-chapter control-plane-architectures handout publishes the three-way comparison; this anchor is the third leg of the triangle (5G Core, SDN, Mobile-IP). A natural forward-stretch lab for students who reach NET-301 Ch 8 with extra time is an OAI 5G attach trace where the AMF-and-AUSF conversation is read alongside the radio-side primary synchronization.

---

§2. Bejtlich Ch 1 deep walk: Network Security Monitoring rationale

Bejtlich's Chapter 1 opens with the prevention-paradigm-failure thesis and closes with the asymmetric-value claim. Read for the four-data-types framework as the chapter's central operational primitive.

What to extract

A Belt-5 graduate should carry the following five facts from Ch 1 into engagement conversation:

1. **Prevention has structurally failed.** Bejtlich's argument is not that prevention is bad but that it is an incomplete defense. Sophisticated adversaries get past the prevention layer; the operationally honest response is to assume that and instrument for it.
2. **The four NSM data types are full-content, session, statistical, and alert.** Each is layered evidence: full-content is the wire; session is the per-flow summary; statistical is the per-interval aggregate; alert is the rule-driven trigger. A SOC analyst's investigation typically starts at alert and walks down to full-content.
3. **NSM's value is asymmetric.** Building the telemetry costs a fixed amount; the value it returns scales with the sophistication of the adversaries the network encounters. A network that only ever encounters commodity threats may never need the NSM stack; a network that encounters sophisticated threats finds the stack indispensable. The asymmetry is the chapter's central economic claim.

4. **NSM is a discipline, not a product.** Bejtlich is explicit: NSM is a methodology students adopt and practice; the tooling is interchangeable (Suricata or Zeek or Snort or commercial platforms). The discipline is what differentiates an NSM analyst from a SIEM-rule-author.
5. **NSM is investigative, not preventive.** The output of an NSM operation is a finding, an explanation, and a remediation; it is not a block. The block belongs to the prevention layer. A Belt-5 graduate should be precise about this distinction in any defensive architecture conversation.

What is out-of-scope at Belt-5

Bejtlich's later chapters (Ch 4 onward) walk the technical Suricata-and-Zeek deployment in detail. NET-301 students should be familiar with these chapters at the technical-reference register but not as primary reading; the academy's NET-201 and NET-301 lab manifest covers the same territory at the practitioner register. Bejtlich's appendices on disk-and-bandwidth-budget for full-content storage are useful for production deployment planning and out-of-scope for the Belt-5 reading.

Cross-anchor connections

Bejtlich's four-data-types framework lands directly on Stevens's congestion-control material: a CUBIC-vs-BBR signature analysis (Lab 9) is exactly a session-data plus statistical-data investigation. Bejtlich's prevention-failure thesis lands on the 5G Core anchors: 5G's UDM/AUSF decomposition is a control-plane prevention strategy; an NSM-mindset graduate asks immediately what telemetry the NRF service-bus exposes for post-compromise investigation. Bejtlich's discipline-not-product framing lands on Mobile-IP: the discipline says you instrument the home-agent and foreign-agent endpoints regardless of whether the deployment is a textbook Mobile-IP rollout or a 5G-Core inheritor.

---

§3. Stevens Ch 16 deep walk: TCP congestion control at advanced depth

Stevens's Chapter 16 is the canonical reading on TCP's congestion-control algorithm. At NET-301 register the chapter is revisited rather than introduced; NET-101 walked Reno and the slow-start / congestion-avoidance / fast-retransmit sequence at the introduction depth.

What to extract

A Belt-5 graduate should carry the following five facts from Ch 16 (revisited at advanced depth):

1. **Reno is the historical baseline; NewReno fixed the partial-ACK problem.** Reno's fast-retransmit assumed one packet lost per RTT; NewReno generalized to multiple losses. SACK extends the signaling so the receiver can name exactly which packets are missing. Belt-5 graduates should be able to read a `tcpdump` trace and tell whether the sender is using SACK from the options-field shape.
2. **CUBIC is the Linux default since 2007 and scales to high-bandwidth long-haul links.** CUBIC's congestion-window growth is a cubic function of time-since-last-loss rather than the linear function Reno uses. The cubic shape lets the window grow quickly on under-utilized fat pipes without overshooting on near-capacity links. Belt-5 graduates should be able to identify CUBIC behavior in a goodput-over-time plot.
3. **BBR is Google's 2016 algorithm; model-based, not loss-based.** BBR explicitly models the bottleneck bandwidth and the round-trip propagation delay and drives the sending rate to fill the bandwidth without filling the queue. The design is opinionated about bufferbloat: BBR refuses to use the buffer as signaling, where Reno-and-CUBIC use buffer fill as the loss-precursor signal. Belt-5 graduates should be able to identify BBR behavior from an absent loss-and-retransmit pattern.
4. **The choice is visible from the wire.** A CUBIC sender's `tcpdump` trace shows the cubic-curve goodput envelope; a BBR sender's shows a stable plateau punctuated by periodic probing for additional bandwidth. The two senders against the same bottleneck topology produce structurally different traces. This is Stevens's central pedagogical move at advanced depth: the wire is the right place to read the algorithm.
5. **Bufferbloat is the architectural failure mode the modern algorithms address.** The modern Internet has more buffer at every hop than the algorithm authors of the 1990s anticipated, and Reno-style loss-based congestion control mistakes long buffers for absent congestion. The result is increased latency without increased loss, which is the bufferbloat phenomenon NET-201 introduced. CUBIC partially addresses this; BBR addresses it directly; commodity home-router default queues remain a substantial unresolved problem.

What is out-of-scope at Belt-5

Stevens's mathematical derivations of the AIMD steady-state behavior are useful for academic reading and out-of-scope at the engagement register. NET-301 students should know that the derivations exist and that the steady-state is well-characterized; the engagement register cares about the wire-level signature, not the closed-form analysis. Stevens's earlier chapters on slow-start and the RFC 793 state machine are NET-101 register material and only revisited if a specific lab artifact requires them.

Cross-anchor connections

Stevens's congestion-control material is the analytical foundation for Bejtlich's session-data and statistical-data layers: a Belt-5 SOC analyst reading a session-data summary is reading aggregate congestion-control behavior and inferring application traffic patterns from it. Stevens's wire-visible-algorithm thesis lands on the 5G Core anchors: the 5G UPF's congestion management is the same algorithm-on-the-wire question at the cellular tier, and a Belt-5 graduate should ask immediately what congestion-control discipline the UPF defaults to. Stevens's bufferbloat lens lands on the Mobile-IP triangle-routing pattern: triangle routing's path-stretch is itself a buffering problem at the architectural tier, and route-optimization (MIPv6) addresses it the same way BBR addresses queue buildup at the host tier.

---

§4. Kurose-Ross 9e §7.4 deep walk: 5G Core decomposition

The 5G Core treatment in Kurose-Ross 9e §7.4 is the academy's canonical anchor for understanding the architectural shift from 4G EPC to 5G. Read with attention to the named Network Functions and the service-based interface; the architecture's distinctive choices live there.

What to extract

A Belt-5 graduate should carry the following six facts from §7.4:

1. **Five primary 5G Core Network Functions (NFs) plus two helpers.** AMF (Access and Mobility Management); SMF (Session Management); UDM (Unified Data Management); AUSF (Authentication Server); UPF (User-Plane Forwarding); plus NRF (NF Repository) and NSSF (Network Slice Selection). Each owns one slice of connection-lifecycle responsibility.

2. **NFs discover each other through the NRF.** The NRF is the service registry; NFs register at startup and look up peers by capability. This is the architectural primitive that distinguishes 5G Core from EPC's monolithic gateway; EPC peers were configured statically.
3. **The service-based interface (SBI) speaks HTTP/2 plus JSON.** The 5G Core NFs talk to each other over a standard web-services protocol stack rather than over the bespoke Diameter and GTP protocols that 4G EPC inherited. The choice has operational consequences (logs are HTTP-shape; observability tooling extends naturally) and security consequences (the attack surface includes HTTP/2 framing bugs and JSON parser bugs).
4. **Control-plane and user-plane are explicitly separated (CUPS).** The user-plane (UPF) carries packet forwarding; the control-plane NFs (AMF, SMF, UDM, AUSF) carry signaling. The separation is a 4G LTE inheritance taken seriously in 5G; the operational consequence is that user-plane and control-plane scale independently.
5. **The architecture is not SDN.** SDN's premise is logical centralization of control behind one controller; 5G Core's premise is functional decomposition of control across multiple peer NFs that coordinate through the service bus. The two architectures answer the same underlying question (where does per-flow state live?) with different commitments.
6. **Network slicing is a first-class architectural primitive.** The NSSF selects a slice at attach time; the slice carries its own NF instances or its own NF configurations; the user's traffic is logically isolated within the slice. Belt-5 graduates should be precise about what slicing isolates (configuration, signaling, sometimes data-plane forwarding) and what it does not (the underlying physical hardware in most deployments).

What is out-of-scope at Belt-5

Kurose-Ross 9e §7.4 covers the architecture at the textbook register; the 3GPP TS 23.501 specification is the authoritative reference for an engineer who needs every parameter and every interface. Belt-5 NET-301 students should know that the 3GPP spec exists and where to look; they should not be expected to read it cover to cover. The 9e's coverage of the 4G EPC is brief and adequate for context; students should be able to name the EPC's MME, SGW, and PGW components without being asked to walk their interfaces in detail.

Cross-anchor connections

The 5G Core decomposition reads against Mobile-IP (§7.5.4 anchor) as a different architectural answer to per-flow state localization; the cross-chapter handout walks both. The 5G Core's HTTP/2-plus-JSON service bus reads against Bejtlich's NSM framework: the SBI is a telemetry surface that an NSM-mindset graduate instruments first. The 5G UPF's congestion management reads against Stevens's congestion-control material at the cellular tier. The 5G-AKA exchange (anchor 4) is the authentication primitive that the AUSF NF actually executes; reading anchor 4 immediately after anchor 3 is the right pedagogical sequence.

---

§5. Kurose-Ross 9e §8.8.2 plus §7.5.3 deep walk: 5G-AKA and 5G mobility

The §8.8.2 / §7.5.3 pair is the academy's coupled treatment of the cellular authentication exchange and the mobility procedures it composes with. Read as one block.

What to extract

A Belt-5 graduate should carry the following six facts:

1. **The IMSI-catcher attack class is what 5G-AKA exists to close.** Pre-5G AKA generations transmitted the IMSI in cleartext during initial attach; rogue base stations harvested it without the legitimate network's involvement. The attack class is well-documented (the OsmocomBB project's `IMSI-catcher` mode; the academic literature; the surveillance-industry deployment record); the legacy AKA design had no structural fix.
2. **The SUCI is the cryptographic primitive.** The Subscription Concealed Identifier is an ECIES (Elliptic-Curve Integrated Encryption Scheme) encryption of the SUPI under the home network's public key. The home network's AUSF is the only entity that can decrypt back to the SUPI. The visited network sees only the encrypted form.
3. **5G-AKA redistributes trust between visited and home networks.** The visited network can no longer learn the long-term subscriber identity; the home network anchors the AKA-relevant secrets. This is the architectural shift, not the cryptographic detail; the cryptography just makes the shift implementable.

4. **5G mobility splits into three handover classes.** Intra-RAN handover (gNB-to-gNB, AMF-stable); inter-AMF mobility (AMF context migrates between control-plane instances); inter-RAT mobility (4G-to-5G handover, where the AKA generation itself changes mid-session). Each is its own observability surface; a Belt-5 graduate should know which logs surface each event.
5. **5G-AKA and WPA-AKA share the same skeleton.** Challenge / response / sequence-number anti-replay / fresh session-key derivation. They diverge on exactly one architectural question: who anchors the long-term key, and how is the visiting network told what to trust? 5G-AKA anchors at the home network; WPA-AKA anchors at the local authentication server.
6. **The handover-measurement pipeline is a side-channel.** The UE reports radio measurements up to the gNB during normal operation; the measurement reports are themselves observable on the air interface and reveal UE behavior. This is the radio-side companion to the cryptographic-side SUCI computation; both are AKA-adjacent observability surfaces.

What is out-of-scope at Belt-5

The full 3GPP TS 33.501 specification of 5G-AKA is the authoritative reference for an engineer implementing the protocol; Belt-5 graduates should know it exists. The pre-5G AKA generations (3G UMTS-AKA; 4G EPS-AKA) are sufficient context for the comparison; reading them in detail is out-of-scope. The cryptanalytic literature on the underlying primitives (ECIES; the specific elliptic curve choices; the KDF construction) is graduate-research material rather than Belt-5.

Cross-anchor connections

The 5G-AKA discussion lands directly on the 5G Core anchor (§7.4): the AUSF is the NF that executes 5G-AKA; the UDM holds the long-term keys; the AMF orchestrates the exchange. Reading anchor 4 cements anchor 3's NF taxonomy. The mobility discussion reads against Mobile-IP (anchor 5): both architectures address per-flow state migration, but they make different commitments about where the state lives. The wireless-AKA-progression handout (`cross-chapter-wireless-aka-progression.md`) walks the comparison against WPA2-SAE and WPA3-SAE; reading the handout after anchor 4 closes the wireless-authentication arc.

---

§6. Kurose-Ross 9e §7.5.4 deep walk: Mobile-IP architectural baseline

Mobile-IP is the 1990s-IETF answer to host mobility on the routed Internet. The §7.5.4 treatment is brief but architecturally serious; read for the contrast with the 5G Core decomposition.

What to extract

A Belt-5 graduate should carry the following five facts:

1. **Mobile-IP's premise is transparent host mobility.** A mobile node registers a Care-of-Address with its Home Agent; subsequent traffic to the mobile node is intercepted by the HA and tunneled to the Foreign Agent on the visited network; the FA delivers the packet locally. The mobile node's IP address remains stable across moves.
2. **The triangle-routing pattern is the design's signature inefficiency.** Sender to HA to FA to MN; the path is three legs where two would suffice. MIPv6 introduces route-optimization to flatten the path by allowing the sender to learn the Care-of-Address and tunnel directly.
3. **Mobile-IP is per-mobile-node distributed state.** Each mobile node has its own HA-FA pairing; failures localize per-node. The architectural failure-domain story is distinct from 5G Core's per-NF localization and from SDN's single-controller dependency.
4. **The protocol shipped but never reached commodity deployment.** Outside specific enterprise and military networks, Mobile-IP did not become the commodity host-mobility solution. The cellular industry built its own answer (the GTP tunneling and SGW/PGW state in EPC; the UPF-anchored data plane in 5G); the consumer Internet built mobility into the application layer (mobile-aware TCP, application-layer reconnection, end-to-end QUIC migration).
5. **The architectural lesson outlives the protocol.** Belt-5 graduates should read Mobile-IP not for its specific bits but for the architectural argument it forced. The 5G Core's NF decomposition, the SDN controller's logical centralization, and Mobile-IP's per-mobile-node distribution are three distinct answers to the same question (where does per-flow mobility state live?). All three answers ship somewhere; the engineering trade is a Belt-5 conversation.

What is out-of-scope at Belt-5

The full Mobile-IPv4 (RFC 5944) and Mobile-IPv6 (RFC 6275) specifications are authoritative references; Belt-5 graduates should know they exist and not be expected to read them in detail. The IETF MIP6 working group's history is interesting historical reading but out-of-scope for the engagement register. Specific enterprise deployments (Cisco IOS Mobile-IP; military tactical-network MIP6 deployments) are footnotes the textbook does not need to dwell on.

Cross-anchor connections

Mobile-IP is the third leg of the cross-chapter control-plane-architectures handout's triangle (5G Core / SDN / Mobile-IP). Reading anchor 5 is the closing move on the architectural-decomposition argument. Mobile-IP's per-mobile-node-pair failure-domain story lands on Bejtlich's NSM framework: a Mobile-IP deployment's NSM instrumentation has to be Home-Agent-anchored or Foreign-Agent-anchored or both, and the choice changes which traffic is observable. Mobile-IP's triangle-routing inefficiency lands on Stevens's bufferbloat lens: the path stretch is itself a queueing problem at the architectural tier.

---

§7. The synthesis

Five anchors compose the NET-301 Belt-5. The composition is opinionated by design; each anchor is opinionated, the order is opinionated, and the cross-anchor connections are the academy's argument for why this specific reading list earns the credential.

The argument: a Belt-5 networking-track graduate should be able to read any production network through five lenses simultaneously. Bejtlich gives the NSM-discipline lens (assume compromise; instrument for it; treat the four data types as the layered evidence base). Stevens gives the algorithm-on-the-wire lens (the choice of TCP congestion control is visible from the trace; bufferbloat is the architectural failure mode the modern algorithms address). The three Kurose-Ross sections give the architectural-decomposition lens at the cellular tier (5G Core's NF taxonomy; 5G-AKA's redistribution of trust; Mobile-IP's per-mobile-node baseline against which 5G mobility has to be read). The five lenses do not produce five separate readings; they produce one integrated reading where the anchors talk to each other.

What would change if a peer cybersecurity program made different anchor choices? A program that anchored on Tanenbaum's *Computer Networks* would produce graduates with a more comprehensive but less opinionated networking literacy; the

comprehensiveness is useful for grad-school exams and less useful for engagement work. A program that anchored on Cisco's CCNA / CCNP reading list would produce vendor-shaped graduates who read every network through Cisco IOS abstractions; the vendor shape is useful for Cisco-house engagements and limiting elsewhere. A program that anchored on the IETF RFC corpus directly would produce graduates with deep protocol literacy and no operational discipline; the protocol depth is useful in standards-development environments and weak in NSM-discipline contexts. The academy's choice is to anchor on opinionated primary sources at the engagement register, accept the cost in encyclopedic coverage, and cover the gaps via the academy's own lab-and-handout corpus. NET-301 graduates know they are not encyclopedically trained; they are practitioner-trained against canonical anchors.

The five anchors compose. Read them in order; revisit them as capstone preparation; cite them at chapter-and-section depth in your engagement memos. The Belt-5 credential is what the composition produces.

---

§8. Cross-references

Artifact	Path	Relationship
Catalog page (the page you arrived from)	`/vca-net-301`	Distilled register; this guide is its forward-pointer destination
Companion handout: control-plane architectures	`/handouts/cross-chapter-control-plane-architectures.md`	5G Core vs SDN vs Mobile-IP comparison; closes anchors 3+5
Companion handout: wireless AKA progression	`/handouts/cross-chapter-wireless-aka-progression.md`	802.11i / WPA3 / 5G-AKA progression; closes anchor 4
Companion handout: DOCSIS quad cross-cut	`/handouts/cross-chapter-docsis-quad-cross-cut.md`	DOCSIS-as-anchor-protocol; SB6141 lab-target lineage
Companion handout: CVE-class vocabulary reference	`/handouts/cross-chapter-cve-class-vocabulary-reference.md`	vocabulary for cyber-track CVE families; intersects with NSM-discipline practice
Companion handout: RF-301 anchor reading guide	`/handouts/cross-chapter-rf-301-anchor-reading-guide.md`	Companion handout; shares Kurose-Ross 9e §7.4 / §8.8.2 anchors at the RF track
RF-301 catalog page	`/vca-rf-301`	Cross-track Belt-5 capstone; reads the same 5G material from the radio side
WIR-101 catalog page	`/vca-wir-101`	Belt-1 wireless intro; the 802.11 substrate WPA-AKA introduces
NET-201 catalog page	`/vca-net-201`	Belt-3 networking; OSPF/BGP/IS-IS that NET-301's BGP-at-Internet-scale module extends
SEC-101 catalog page	`/vca-sec-101`	Cross-track foundational; ASI Top 10 governance categories where NSM-discipline lands