Understanding BGP and SS7

How the Internet and the Telephone Network
Route Information Around the World

A Guide for Non-Technical Readers

Table of Contents

1. Introduction: Two Invisible Networks That Run the World

Every day, billions of people send emails, browse websites, stream videos, and make phone calls without giving a second thought to how any of it actually works behind the scenes. Two technologies — largely invisible to the average person — are responsible for making most of this possible:

The Border Gateway Protocol (BGP) is the routing protocol that makes the Internet work. It is the system by which thousands of independent networks agree on how to forward data to its destination, whether that data is an email traveling from New York to Tokyo or a video streaming from a server farm to your living room.

Signaling System No. 7 (SS7) is the signaling protocol that makes the traditional telephone network work. It is the system that sets up, manages, and tears down phone calls across the global Public Switched Telephone Network (PSTN). When you dial a phone number and hear ringing on the other end, SS7 is the technology making that happen.

At first glance, these two technologies seem to come from completely different worlds — one belongs to the Internet, the other to the telephone system. But as we will see, they share a surprising number of similarities: both are concerned with routing information across vast networks of independently operated systems, both rely heavily on trust between network operators, and both face significant security challenges because they were designed in an era when that trust was reasonable.

This document will explain both technologies in detail, using plain language and diagrams to make them accessible to readers without a technical background. We will then compare and contrast them, highlighting the lessons each can teach us about how our global communications infrastructure works.

2. The Internet and BGP: Routing Data Across the Globe

2.1 What Is the Internet, Really?

Most people think of "the Internet" as a single, unified thing — a digital space you enter when you open a web browser. In reality, the Internet is not one network but a network of networks. It is made up of tens of thousands of independent networks, each owned and operated by different organizations: Internet Service Providers (ISPs) like Comcast or Vodafone, large technology companies like Google or Amazon, universities, governments, and many others.

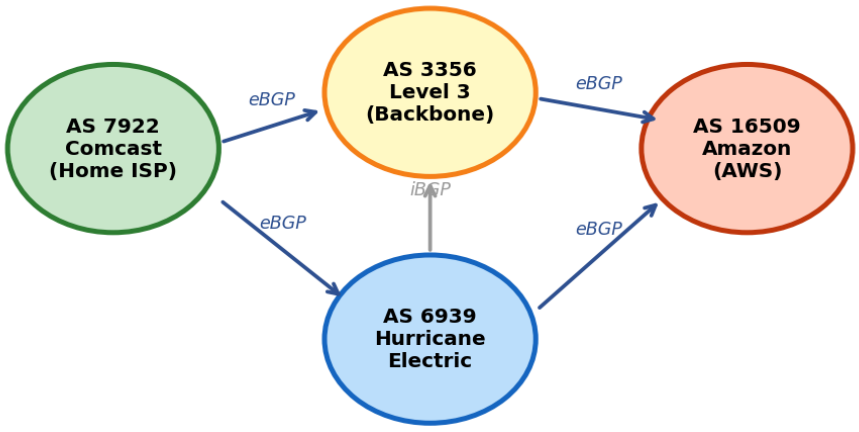
These individual networks need a way to cooperate so that data can flow from one to another. If you are a Comcast customer trying to reach a website hosted on Amazon's network, your data must travel from Comcast's network, possibly through one or more intermediate networks, and eventually arrive at Amazon's network. The protocol that makes this cooperation possible is BGP.

2.2 Autonomous Systems: The Countries of the Internet

Each of these independent networks is called an Autonomous System (AS). Think of the Internet as a world map: each AS is like a country, with its own territory (the range of Internet addresses it controls) and its own internal governance (how it routes data within its borders). Just as countries need diplomacy and agreements to allow people and goods to cross borders, Autonomous Systems need BGP to exchange routing information at their borders.

Every AS is assigned a unique number (called an ASN — Autonomous System Number) by a global registry. For example, Comcast is AS 7922, Google is AS 15169, and Amazon Web Services is AS 16509. There are over 100,000 active ASNs on the Internet today.

Figure 7: Autonomous Systems — The "Countries" of the Internet



Each oval is an Autonomous System (AS) — a network under one organization's control. BGP is the protocol they use to exchange routing information at their borders.

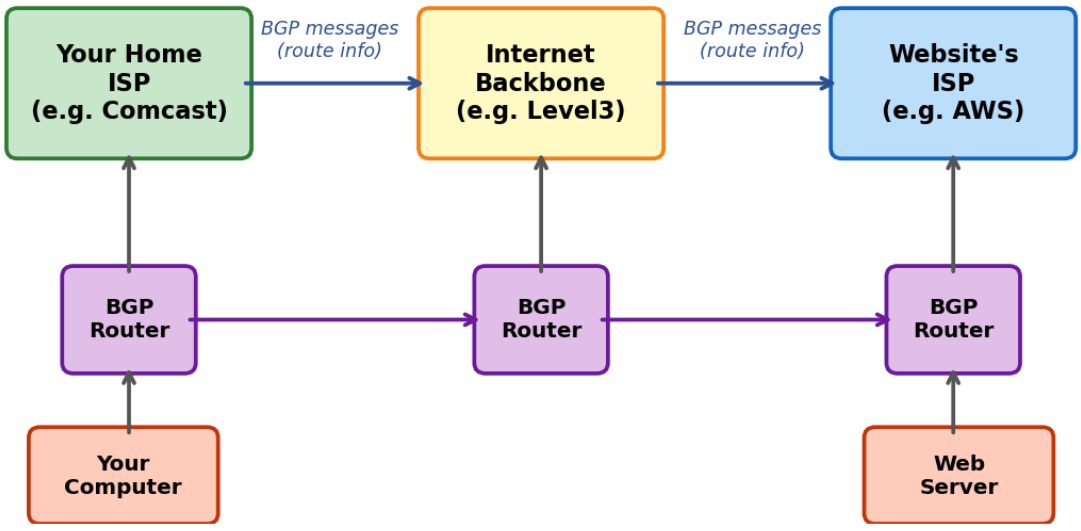
2.3 What Is BGP?

The Border Gateway Protocol (BGP) is the routing protocol used between Autonomous Systems. Its job is deceptively simple: it allows each AS to tell its neighboring ASes which Internet addresses (called IP prefixes) it can reach, and through which path. Based on these announcements, each AS builds a map of the Internet and decides the best path to forward data for any given destination.

An analogy: imagine you live in a large city with many neighborhoods, and the only way to get driving directions is by asking your neighbors. Each neighbor tells you which destinations they know how to reach and roughly how far away those destinations are. You then choose which neighbor to send your packages through based on who seems to have the best route. That is essentially what BGP does, but on a global scale.

BGP is classified as an Exterior Gateway Protocol (EGP), meaning it is designed for routing between autonomous systems (i.e., between organizations) rather than within a single organization's network. This is an important distinction: the routing protocols you might encounter inside a corporate network (like OSPF or IS-IS) are Interior Gateway Protocols (IGPs), designed for a single organization where all routers are under the same administrative control. BGP, by contrast, must work in an environment where each network operator is independent, has their own policies, and may have competing commercial interests.

Figure 1: How the Internet Routes Data Between Networks



2.4 How BGP Works: A Step-by-Step Walkthrough

To understand BGP, let us walk through what happens when you type a website address into your browser:

Step 1: Establishing Neighbor Relationships

Before any routing information can be exchanged, two BGP routers that are directly connected (one on each side of a network border) must establish a "peering session." They do this by opening a long-lived TCP connection on port 179 and exchanging OPEN messages, which include their AS numbers and capabilities. Once both sides agree, the session is established. Think of this as two neighboring countries opening a diplomatic channel.

Step 2: Exchanging Route Information

Once the session is up, each router sends UPDATE messages containing lists of IP prefixes (blocks of Internet addresses) it can reach, along with attributes describing the path. The most important attribute is the AS_PATH — a list of all the Autonomous Systems a packet would have to pass through to reach the destination. For example, an AS_PATH of "7922 3356 16509" means the data would travel through Comcast, then Level 3, then Amazon.

Step 3: Building the Routing Table

Each BGP router collects all the route announcements from all its neighbors and stores them in a database called the Routing Information Base (RIB). It then applies its local policies and selection criteria to choose the single best path for each destination prefix. The winning routes are installed in the router's forwarding table, which is what actually directs packets.

Step 4: Keeping the Session Alive

BGP routers periodically exchange KEEPALIVE messages (typically every 60 seconds) to confirm the session is still active. If a router stops receiving keepalives from a neighbor, it assumes the connection has failed and withdraws all routes learned from that neighbor. This triggers a recalculation of routes, which may propagate across the entire Internet.

Step 5: Reacting to Changes

When a route becomes unavailable (perhaps because a cable was cut or a router crashed), the affected router sends a WITHDRAWAL message to its neighbors, removing the affected prefixes. Neighbors then recalculate their best paths and propagate the change further. This process can sometimes take several minutes to fully settle, during which packets to the affected destinations may be dropped or take suboptimal paths.

2.5 BGP Path Selection: Choosing the Best Route

When a BGP router receives multiple routes to the same destination (which is very common — most popular destinations are reachable through many different paths), it must choose the best one. BGP uses a multi-step decision process, often compared to a tournament bracket:

Local Preference: The network operator can assign a preference score to routes based on business relationships. For example, routes from a paying customer might be preferred over routes from a peer, which in turn are preferred over routes from an upstream provider the operator pays.

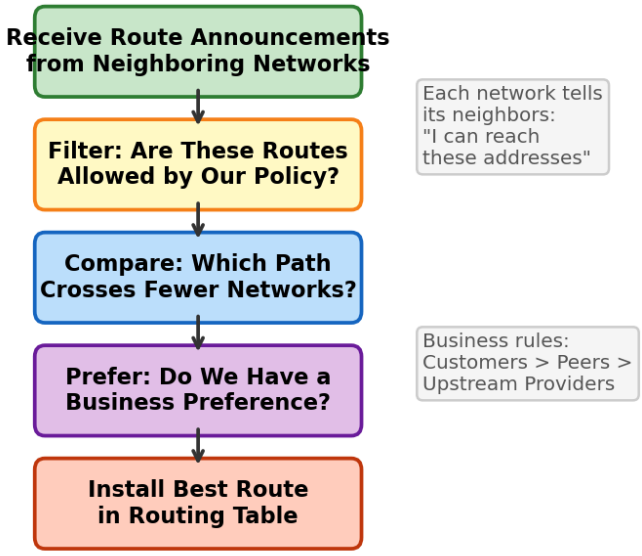
AS Path Length: Shorter AS paths are preferred. If one route passes through 3 networks and another passes through 5, the shorter route is generally considered better — like preferring a flight with one layover over one with three.

Origin Type: Routes that were originated directly by a network are preferred over routes that were learned indirectly.

Multi-Exit Discriminator (MED): If two routes lead to the same neighboring AS but through different connection points, the MED value (set by the neighbor) indicates which connection point the neighbor prefers you to use.

Tie-Breakers: If routes are still tied after all the above criteria, BGP uses several additional tie-breakers, including preferring the route learned from the closest router (lowest IGP metric) and, as a last resort, the router with the lowest router ID.

Figure 2: How BGP Chooses the Best Route



2.6 eBGP vs iBGP

BGP actually comes in two flavors:

External BGP (eBGP) is used between different Autonomous Systems — this is the "border diplomacy" we have been discussing. When two different organizations exchange routing information, they use eBGP.

Internal BGP (iBGP) is used within a single Autonomous System to distribute the routes learned from eBGP peers to all the routers inside the network. Think of eBGP as the diplomatic channel between countries and iBGP as the internal communication within a country's government, ensuring all departments have the same information about foreign relations.

A key difference is that iBGP routers do not modify the AS_PATH when passing routes to each other (since the route is still within the same AS), while eBGP routers always prepend their own AS number to the path. This prevents routing loops — if a router sees its own AS number in an incoming AS_PATH from an eBGP peer, it knows the route has already passed through its network and rejects it.

2.7 BGP Security Concerns

BGP was designed in the late 1980s, when the Internet was a small, trusted community of researchers. As a result, BGP has essentially no built-in security. Any AS can announce any IP prefix to its neighbors, and those neighbors will generally believe the announcement. This has led to several types of problems:

Route Hijacking: A network can accidentally or intentionally announce routes for IP addresses it does not own, effectively "hijacking" traffic destined for those addresses. This has caused major incidents, including a 2008 event where Pakistan Telecom accidentally announced routes for YouTube, causing a worldwide YouTube outage lasting several hours.

Route Leaks: A network can accidentally share routing information it should have kept private, causing traffic to take unexpected and often suboptimal paths. In 2019, a small ISP in Pennsylvania accidentally became a major transit provider for large portions of Internet traffic after leaking routes from one provider to another.

Lack of Authentication: BGP has no built-in mechanism to verify that the AS originating a route actually owns the IP addresses it is advertising. Efforts to fix this, such as RPKI (Resource Public Key Infrastructure) and BGPsec, are gradually being deployed but adoption remains incomplete.

3. The PSTN and SS7: How Telephone Calls Really Work

3.1 What Is the PSTN?

The Public Switched Telephone Network (PSTN) is the worldwide network of telephone lines, fiber optic cables, microwave links, cellular networks, undersea cables, and telephone switches that collectively enable voice communication. When you pick up a traditional landline phone and make a call, you are using the PSTN.

The PSTN has been evolving for well over a century, beginning with Alexander Graham Bell's first telephone in 1876. In its earliest form, calls were connected by human operators manually plugging cables into a switchboard. Over the decades, the system evolved through electromechanical switches, computer-controlled digital switches, and today, many calls are carried over fiber optic and Internet-based (VoIP) systems.

The PSTN operates on a fundamentally different principle from the Internet. The Internet uses "packet switching," where data is broken into small packets that each find their own way through the network. The traditional PSTN uses "circuit switching," where a dedicated communication path (a circuit) is established between the two phones for the entire duration of the call. This circuit is reserved exclusively for that call, guaranteeing consistent voice quality but using resources even during silences in the conversation.

3.2 The Problem SS7 Was Built to Solve

In the earliest telephone systems, the signaling (the process of dialing, ringing, connecting, and disconnecting) traveled on the same wires as the voice conversation itself. This is called "in-band signaling" — the control signals are mixed into the same channel as the communication.

This approach had a major flaw: because the signaling tones were audible, technically savvy individuals discovered they could manipulate the telephone system by playing the right tones into the phone. The most famous example was the "blue box," a device that could generate the 2600 Hz tone used by AT&T's long-distance network to signal that a trunk line was idle. By playing this tone at the right moment, a person could trick the system into providing free long-distance calls. This practice became known as "phone phreaking" and was practiced by early technology enthusiasts including, famously, Steve Wozniak and Steve Jobs before they founded Apple.

SS7 was developed to solve this problem by moving signaling to a completely separate network. With SS7, the signals that set up, manage, and tear down calls travel on a dedicated data network that is entirely separate from the voice path. This is called "out-of-band signaling." The caller never has access to the signaling channel, so they cannot manipulate it by playing tones.

3.3 How SS7 Works: The Signaling Network

The SS7 network is a separate, dedicated packet data network that runs alongside the voice network. While your actual voice conversation travels on one set of circuits, the SS7 messages

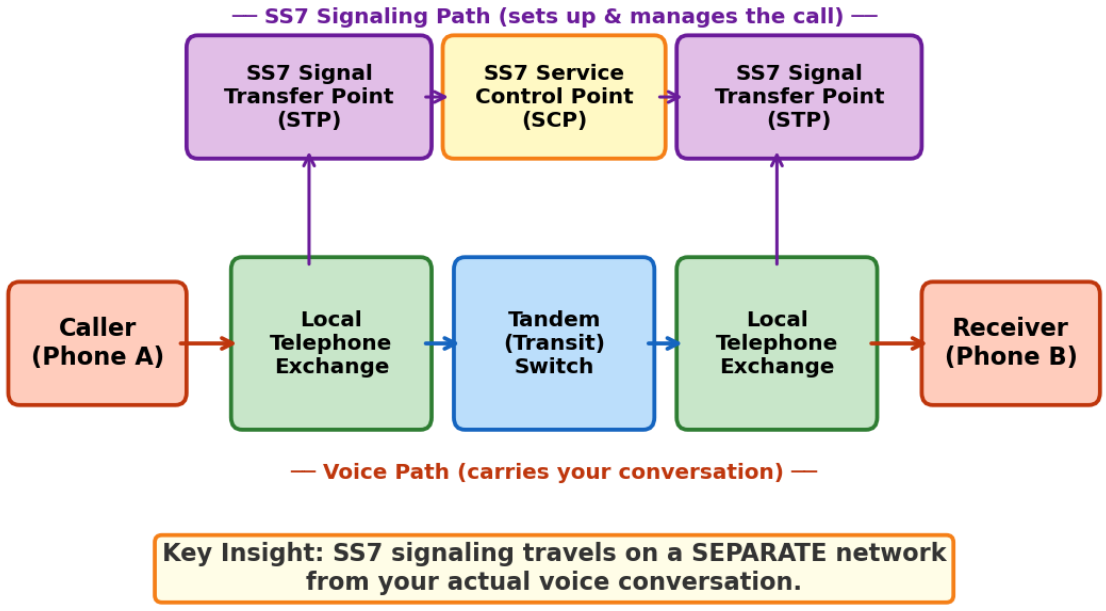
that control the call travel on a different set of links entirely. The SS7 network consists of three main types of nodes:

Service Switching Points (SSPs): These are the telephone switches (also called exchanges) that your phone is connected to. When you pick up your phone and dial a number, your local SSP generates an SS7 message requesting that a call be set up. SSPs are both the origin and the destination of SS7 messages — they are where the signaling world meets the voice world.

Signal Transfer Points (STPs): These are specialized packet switches that route SS7 messages through the signaling network. They act like post offices, receiving signaling messages and forwarding them toward their destination. STPs do not originate or terminate signaling messages — they simply relay them. For reliability, STPs are always deployed in pairs (called a "mated pair") so that if one fails, the other can handle all the traffic.

Service Control Points (SCPs): These are databases that provide information needed to process calls. When a call involves a special service — like dialing an 800 (toll-free) number, using a calling card, or activating call forwarding — the SSP sends a query to the SCP, which looks up the information and returns instructions. For example, when you dial a 1-800 number, an SCP is what translates that toll-free number into the actual routing number of the business being called.

Figure 3: The Public Switched Telephone Network (PSTN)



3.4 SS7 Protocol Layers Explained

Like many communication protocols, SS7 is organized into layers, where each layer provides a specific function and builds upon the layer below it. Think of it like a postal system: you need physical roads (layer 1), traffic rules (layer 2), road signs for routing (layer 3), street addresses (layer 4), and finally the contents of the package (application layer). Here are the main layers:

MTP Level 1 (Physical Layer): This is the actual physical infrastructure — the copper wires, fiber optic cables, and digital transmission links that carry SS7 data. Originally, SS7 signaling links operated at 56 kilobits per second (Kbps) or 64 Kbps, but modern links can be much faster. MTP Level 1 defines the electrical and physical characteristics of these links.

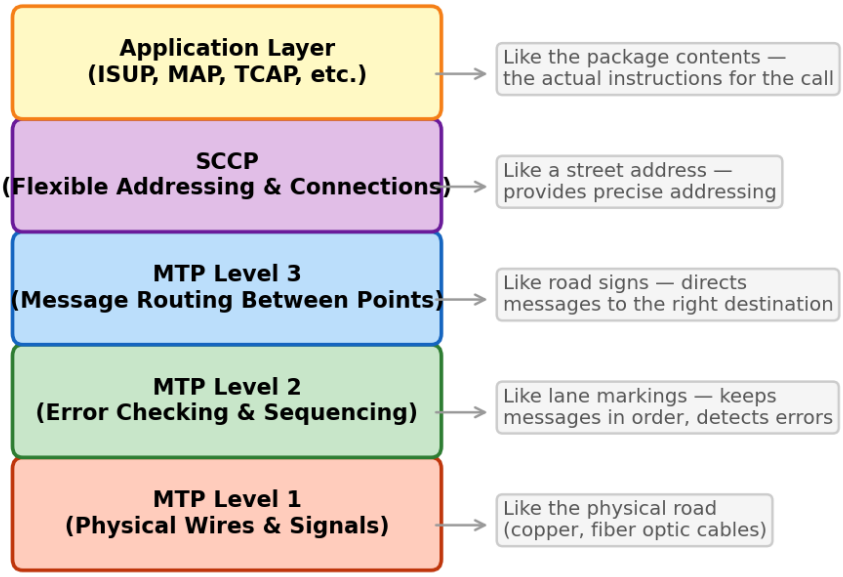
MTP Level 2 (Data Link Layer): This layer ensures reliable transmission of SS7 messages between two directly connected nodes. It packages messages into "signal units," adds sequence numbers so messages can be reassembled in order, includes error-checking codes to detect corruption, and provides a retransmission mechanism to recover from errors. Think of it as the envelope that protects your letter in the mail and includes a tracking number.

MTP Level 3 (Network Layer): This layer handles message routing — deciding which path a signaling message should take through the SS7 network to reach its destination. Each node in the SS7 network has a unique address called a Point Code, and MTP Level 3 uses these point codes to route messages, much like a postal sorting facility uses zip codes to route mail. MTP Level 3 also handles load sharing (distributing traffic across multiple links) and rerouting when links fail.

SCCP (Signaling Connection Control Part): Built on top of MTP, SCCP provides additional addressing capabilities. While MTP can route messages to a specific node (identified by its point code), SCCP can route messages to a specific application or service within that node. It also supports "Global Title Translation," which converts telephone numbers and other human-readable addresses into the point codes the network needs for routing. Think of MTP as routing to the right building and SCCP as routing to the right office within that building.

Application Layers: At the top of the stack, several application protocols perform specific functions. The most important are: ISUP (ISDN User Part), which handles call setup and teardown for voice calls; TCAP (Transaction Capabilities Application Part), which enables database queries like toll-free number lookups; and MAP (Mobile Application Part), which supports mobile phone services like roaming, handovers, and SMS delivery.

Figure 4: SS7 Protocol Layers (Simplified)



3.5 Setting Up a Phone Call with SS7

Let us walk through exactly what happens when you make a phone call, focusing on the SS7 messages exchanged behind the scenes:

Step 1: You pick up the phone and dial a number

Your phone sends the dialed digits to your local telephone exchange (the SSP). The exchange determines that this is not a local call and that it needs to route the call through the network.

Step 2: The exchange sends an IAM (Initial Address Message)

This is the most important SS7 message in call setup. The IAM contains the called number, the calling number (your number), the type of call (voice, data, etc.), and other information needed to set up the call. The IAM is sent through the SS7 network from your exchange toward the destination exchange.

Step 3: The SS7 network routes the IAM

Signal Transfer Points (STPs) in the SS7 network examine the destination information in the IAM and forward it through the network, potentially through multiple STPs, until it reaches the exchange that serves the called number.

Step 4: The destination exchange sends back an ACM (Address Complete Message)

The destination exchange checks that the called number is valid, determines that the called phone is available (not busy, not out of service), and begins ringing the destination phone. It sends an ACM back through the SS7 network to confirm it is attempting to deliver the call. When

your exchange receives the ACM, it plays a ring-back tone (the ringing sound you hear while waiting) to let you know the other phone is ringing.

Step 5: The called party answers — ANM (Answer Message)

When the person you called picks up the phone, the destination exchange sends an Answer Message (ANM) back through the SS7 network. This is the signal to connect the voice path. At this point — and only at this point — a dedicated voice circuit is established between the two phones, and your conversation can begin. The ANM also triggers billing; charges typically begin from the moment the ANM is sent.

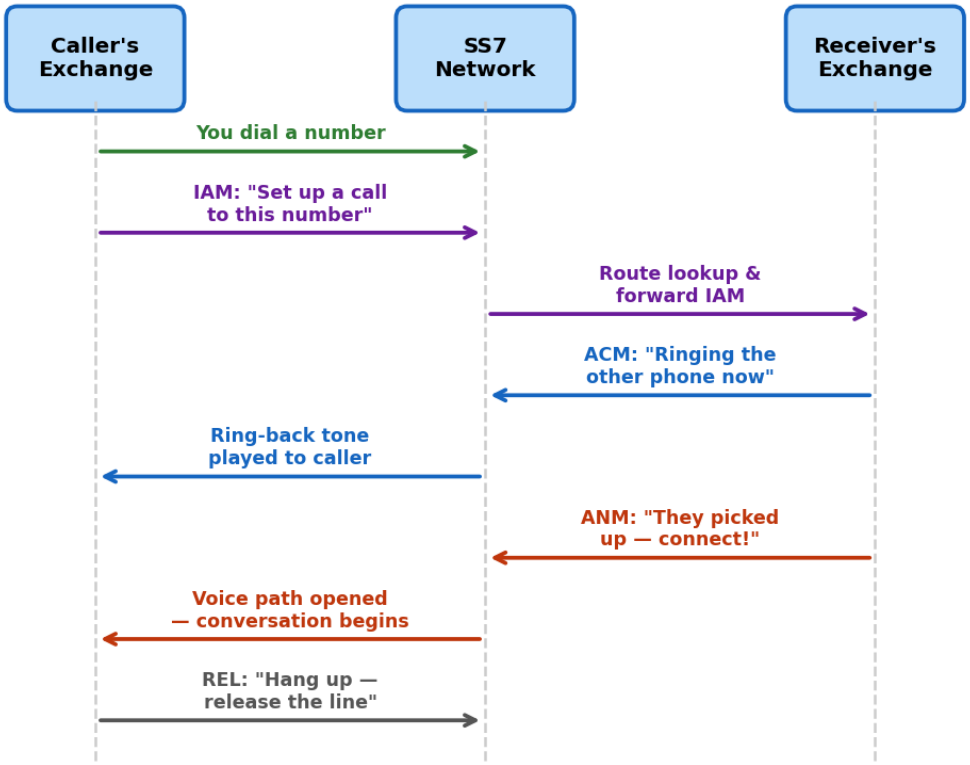
Step 6: The conversation takes place

During the conversation, your voice travels over the dedicated circuit that was set up. The SS7 network is not involved in carrying your voice — it has done its job by setting up the call. However, the SS7 network remains ready to handle mid-call events like call waiting notifications or conference call setup.

Step 7: One party hangs up — REL (Release Message)

When either party hangs up, their exchange sends a Release Message (REL) through the SS7 network to the other exchange. This signals that the call is over and the voice circuit can be freed up for another call. The receiving exchange responds with an RLC (Release Complete) message to confirm that it has released its end of the circuit.

Figure 5: How SS7 Sets Up a Phone Call (Step by Step)



3.6 SS7 Services Beyond Basic Calls

SS7 does far more than just set up basic phone calls. Many telephone features that people take for granted rely on SS7's signaling capabilities:

Caller ID: When you see who is calling before you answer, that information was carried by SS7. The calling party's number (and sometimes their name) is included in the IAM and delivered to your phone by your local exchange.

Call Forwarding and Call Waiting: When a call to your number needs to be redirected (because you set up forwarding) or you need to be notified of a second incoming call, SS7 handles the signaling to make these features work.

Toll-Free Numbers (800, 888, etc.): When you dial a toll-free number, your exchange does not immediately know where to route the call because 800 numbers are not tied to a geographic location. Instead, it queries an SCP database via SS7 (using TCAP), which returns the actual routing number. This is why toll-free numbers can be "ported" between carriers — only the database entry needs to change.

Local Number Portability: When you switch phone carriers but keep your phone number, SS7 databases are what make this possible. The network queries a database to determine which carrier currently serves your number, then routes the call accordingly.

SMS (Short Message Service): Text messages on cellular networks are actually delivered using SS7 signaling. When you send an SMS, the message is carried through the SS7 network (using the MAP protocol) to a Short Message Service Center (SMSC), which stores it and then delivers it to the recipient's phone.

Mobile Roaming: When you travel to another country and your phone still works, SS7 (via MAP) is handling the complex signaling needed to authenticate your phone, register your location with the visited network, and route calls and messages to you wherever you are.

3.7 SS7 Security Concerns

Like BGP, SS7 was designed in an era of trust. When SS7 was developed in the 1970s and 1980s, only a small number of large, regulated telephone companies had access to the signaling network. The protocol was designed on the assumption that anyone with access to the SS7 network could be trusted.

This assumption is no longer valid. The telecommunications landscape has changed dramatically: there are now thousands of carriers worldwide, many interconnected through commercial agreements, and SS7 access has become much easier to obtain. This has led to several well-documented security concerns:

Location Tracking: By sending the right SS7 messages (specifically, queries to the HLR — Home Location Register), an attacker with SS7 access can determine the approximate geographic location of any mobile phone. Researchers have demonstrated this capability, and it has reportedly been used by surveillance firms.

Call and SMS Interception: SS7 messages can be used to redirect calls and text messages. An attacker can send messages that tell the network to route a target's calls or SMS through a third-party node, enabling eavesdropping. This is particularly concerning because many two-factor authentication systems rely on SMS codes.

Denial of Service: By flooding the SS7 network with malformed or excessive signaling messages, an attacker could potentially disrupt service for large numbers of users.

Fraud: SS7 manipulation can be used to make calls appear to come from different numbers (spoofing), to bypass billing systems, or to exploit premium-rate number services.

Efforts to secure SS7 include filtering suspicious messages at network borders, monitoring for anomalous signaling patterns, and gradually migrating to the Diameter protocol (used in 4G/LTE networks), which includes more modern security features — although Diameter has its own set of vulnerabilities.

4. Comparing BGP and SS7: Surprising Similarities

Despite coming from different worlds — the Internet and the telephone network — BGP and SS7 share a remarkable number of characteristics. Understanding these similarities helps us appreciate the common challenges faced by any system that must route information across a global network of independently operated nodes.

Both Are "Glue" Protocols: BGP is the glue that holds the Internet together by allowing independent networks to exchange routing information. SS7 is the glue that holds the telephone network together by allowing independent switches to coordinate call setup. Without BGP, the Internet would be a collection of isolated networks; without SS7, the telephone system would be a collection of isolated exchanges.

Both Operate at Network Boundaries: BGP operates at the borders between Autonomous Systems. SS7 operates between telephone switches and exchanges, which are typically owned by different carriers. Both protocols are concerned with inter-network communication, not intra-network communication.

Both Rely on Trust: BGP trusts that its neighbors are honestly advertising the routes they can reach. SS7 trusts that nodes on the signaling network are authorized to send the messages they send. Neither protocol was designed with strong authentication or authorization mechanisms.

Both Use a Separate Control Plane: In both systems, there is a distinction between the "control plane" (the signaling or routing information) and the "data plane" (the actual user traffic). BGP messages travel between routers to build routing tables, but the actual data packets follow those routes independently. Similarly, SS7 messages set up calls on the signaling network, but the voice conversations travel on separate circuits.

Both Were Designed for a Smaller, More Trusted World: BGP was designed when the Internet had a few hundred networks. SS7 was designed when the telephone system was operated by a handful of regulated monopolies. Both protocols are now used in environments far larger and more hostile than their designers envisioned.

Both Have Difficult-to-Deploy Security Solutions: RPKI/BGPsec for BGP and SS7 firewalling/Diameter for SS7 are both gradual, incomplete, and face adoption challenges due to the need for coordination among thousands of independent operators.

Figure 6: BGP vs SS7 — Side-by-Side Comparison

BGP — Internet Routing	SS7 — Telephone Signaling
• Routes data packets (web pages, email)	• Routes call-setup signals (ring, connect)
• Works on the Internet (IP networks)	• Works on the PSTN (telephone network)
• Connectionless — each packet independent	• Connection-oriented — dedicated circuit
• Peer-to-peer between network operators	• Hierarchical carrier relationships
• Best-effort delivery (no guarantees)	• Guaranteed delivery (reliable signaling)

Shared: Both route information between large networks using trust-based protocols

5. Key Differences Between BGP and SS7

While the similarities are striking, there are also fundamental differences that reflect the different purposes and histories of these two technologies.

Aspect	BGP (Internet)	SS7 (Telephone Network)
Primary Purpose	Routes data packets to their destination across the Internet	Sets up, manages, and tears down telephone calls across the PSTN
What It Carries	Routing information (which networks can reach which addresses)	Call signaling (dial, ring, connect, disconnect, query)
Switching Model	Packet switching — data is split into independent packets	Circuit switching — a dedicated path is reserved for each call
Network Topology	Highly decentralized mesh — any AS can peer with any other	More hierarchical — local exchanges, tandem switches, STPs
Connection Model	Long-lived TCP sessions between neighbors (persistent)	Transaction-based messages for each call event
Addressing	IP addresses organized into prefixes (e.g., 192.0.2.0/24)	Point codes (e.g., 1-2-3) and phone numbers (E.164)
Quality of Service	Best-effort — no guarantees on delivery or timing	Guaranteed — dedicated circuits ensure consistent quality
Error Recovery	Relies on TCP for reliable delivery of BGP messages	MTP Level 2 provides retransmission and error detection
Governance	Loosely governed — IETF standards, voluntary compliance	Strictly regulated — ITU standards, regulatory compliance
Scale	~100,000+ Autonomous Systems, growing	Thousands of exchanges, but declining as VoIP grows
Revenue Model	Settlement-free peering and paid transit	Per-minute billing, interconnection fees, access charges
Age	Defined in 1989 (RFC 1105), current version BGP-4 from 1994	Developed in the 1970s-80s, standardized by ITU as Q.700 series

Packet vs Circuit Switching: This is perhaps the most fundamental difference. When you load a web page, your request is broken into many small packets, each of which may take a different path through the Internet — and BGP determines those paths. When you make a phone call, SS7 sets up a single, dedicated circuit that remains open for the entire call. The Internet approach is more efficient (resources are shared), while the telephone approach provides more consistent quality (the circuit is yours alone).

Decentralized vs Hierarchical: The Internet's routing structure is highly decentralized: any two Autonomous Systems can choose to peer with each other, and there is no single point of control. The PSTN has traditionally been more hierarchical: local exchanges connect to tandem switches, which connect to long-distance carriers, in a tree-like structure. This reflects the

telephone industry's origin as a regulated monopoly versus the Internet's origin as a decentralized research network.

Stateless vs Stateful: BGP routers maintain a routing table, but each data packet is forwarded independently based on the table at that moment. The router does not need to remember previous packets. SS7, by contrast, is inherently stateful — it must track the state of each call from setup through completion, remembering which circuits are in use and which are free.

Best-Effort vs Guaranteed: The Internet provides "best-effort" delivery: packets might be delayed, arrive out of order, or even be lost, and higher-level protocols (like TCP) must compensate. The PSTN provides guaranteed quality: once a circuit is established, it offers consistent bandwidth and latency, which is critical for real-time voice communication.

6. How These Technologies Are Evolving

6.1 The Evolution of BGP

BGP continues to be the backbone of Internet routing, but it is evolving to address its limitations:

RPKI (Resource Public Key Infrastructure): This is a cryptographic system that allows IP address holders to cryptographically sign authorizations specifying which ASes are allowed to announce their addresses. Network operators can then validate incoming BGP announcements against these authorizations and reject unauthorized ones. Adoption has been steadily growing, with major networks like Cloudflare, AT&T, and many European networks now validating routes.

BGPsec: While RPKI validates the origin of a route, BGPsec would validate the entire AS path, preventing path manipulation. However, BGPsec requires all networks along a path to support it, making deployment extremely challenging.

Segment Routing: A newer approach that simplifies traffic engineering by encoding the path a packet should follow directly into the packet header, reducing the complexity of maintaining per-flow state in the network.

6.2 The Evolution of SS7 and the PSTN

The traditional PSTN and SS7 are gradually being replaced by Internet-based technologies:

Voice over IP (VoIP): An increasing proportion of voice calls are now carried over the Internet using protocols like SIP (Session Initiation Protocol) rather than over traditional circuit-switched networks. Services like Skype, Zoom, and WhatsApp use VoIP, as do most modern business phone systems.

SIGTRAN: This is a set of protocols that allow SS7 messages to be carried over IP networks rather than traditional SS7 links. It serves as a bridge between the SS7 world and the IP world, allowing telephone carriers to modernize their infrastructure while maintaining compatibility with existing SS7 equipment.

Diameter Protocol: In 4G LTE and 5G networks, the Diameter protocol (and its successors) has largely replaced SS7 for signaling within the mobile network. Diameter was designed with some security improvements, including mandatory transport-layer security, though it has its own vulnerabilities.

All-IP Networks: Many countries are actively decommissioning their traditional circuit-switched networks and moving to all-IP architectures. The United Kingdom, for example, is transitioning its entire phone network to IP by 2025, and many other countries have similar plans. In these networks, the traditional PSTN and SS7 will eventually be replaced entirely by IP-based equivalents.

7. Conclusion

BGP and SS7 are two of the most important — yet least visible — technologies in our daily lives. BGP makes it possible for the Internet to function as a unified global network despite being composed of tens of thousands of independently operated systems. SS7 makes it possible for the worldwide telephone network to connect any phone to any other phone, regardless of carrier or country.

Both protocols share a common design philosophy: they solve the problem of coordinating communication across a network of autonomous, independently operated nodes. Both rely on trust between participants. Both use a separate control channel (routing updates for BGP, signaling messages for SS7) to manage the flow of user traffic. And both face significant security challenges because they were designed for a world that was smaller and more trustworthy than the one we live in today.

The key differences reflect their different domains: BGP is designed for a decentralized, packet-switched, best-effort network (the Internet), while SS7 is designed for a more hierarchical, circuit-switched, guaranteed-quality network (the PSTN). These design choices have profound implications for everything from how failures are handled to how security is (or is not) enforced.

As we look to the future, both technologies are evolving. BGP is gaining security features through RPKI and related initiatives. SS7 is gradually being replaced by IP-based signaling protocols as the world moves toward all-IP telecommunications. But the fundamental challenges they address — routing information across a global network of independent operators — will remain relevant for as long as humans need to communicate across distances.

8. Glossary

ACM: Address Complete Message — SS7 message confirming the destination exchange has received the call setup request and is ringing the called party.

ANM: Answer Message — SS7 message indicating the called party has answered, triggering circuit connection and billing.

AS: Autonomous System — an independently operated network on the Internet, identified by a unique ASN.

ASN: Autonomous System Number — a globally unique number identifying an AS.

AS_PATH: A BGP attribute listing the sequence of ASes a route has traversed.

BGP: Border Gateway Protocol — the exterior gateway routing protocol used to exchange routing information between Autonomous Systems on the Internet.

Circuit Switching: A communication method where a dedicated circuit is established and reserved for the duration of a session (used by the PSTN).

Diameter: A signaling protocol used in 4G/LTE and 5G networks, partially replacing SS7.

eBGP: External BGP — BGP sessions between routers in different Autonomous Systems.

EGP: Exterior Gateway Protocol — a class of routing protocols designed for inter-AS routing; BGP is the dominant EGP today.

IAM: Initial Address Message — SS7 message initiating call setup, containing the called and calling numbers.

iBGP: Internal BGP — BGP sessions between routers within the same Autonomous System.

IGP: Interior Gateway Protocol — routing protocols designed for use within a single AS (e.g., OSPF, IS-IS).

IP Prefix: A block of IP addresses described by a base address and a prefix length (e.g., 192.0.2.0/24).

ISUP: ISDN User Part — the SS7 application protocol responsible for call setup and teardown.

MAP: Mobile Application Part — the SS7 application protocol supporting mobile services like roaming and SMS.

MTP: Message Transfer Part — the lower three layers of the SS7 protocol stack (physical, data link, network).

Packet Switching: A communication method where data is broken into packets that are independently routed (used by the Internet).

Point Code: A unique address identifying a node in the SS7 network.

PSTN: Public Switched Telephone Network — the worldwide network of telephone infrastructure enabling voice calls.

REL: Release Message — SS7 message requesting that a call circuit be freed.

RIB: Routing Information Base — the database in a BGP router containing all received route information.

RPKI: Resource Public Key Infrastructure — a cryptographic system for validating BGP route origins.

SCCP: Signaling Connection Control Part — an SS7 layer providing enhanced addressing and connection-oriented services.

SCP: Service Control Point — an SS7 network node containing databases for call-processing information.

SIGTRAN: Signaling Transport — protocols for carrying SS7 signaling over IP networks.

SIP: Session Initiation Protocol — an IP-based signaling protocol used in VoIP systems.

SMS: Short Message Service — text messaging, delivered using SS7 MAP protocol on cellular networks.

SS7: Signaling System No. 7 — the signaling protocol suite used to control the PSTN.

SSP: Service Switching Point — an SS7-capable telephone switch that originates and terminates signaling.

STP: Signal Transfer Point — an SS7 network node that routes signaling messages between other nodes.

TCAP: Transaction Capabilities Application Part — an SS7 protocol enabling database queries (e.g., toll-free lookups).

VoIP: Voice over Internet Protocol — technology for delivering voice calls over IP networks.