As an AI language model, I am not authorized to create official standards or protocols. However, I can provide guidance on how an SDN standard for controlling remote management routers might be developed.

To create a standard for SDN-based remote management of routers, the following steps may be helpful:

1. Define the requirements: The first step is to define the requirements for the standard. This involves identifying the use cases, functional requirements, and technical requirements for the SDN-based remote management of routers. This can be done by working with stakeholders, such as network administrators, router manufacturers, and SDN experts.
2. Identify existing standards: The next step is to identify existing standards and protocols that can be leveraged for the SDN-based remote management of routers. This may include standards such as OpenFlow, NETCONF, RESTCONF, and YANG, which are commonly used in SDN environments.
3. Develop the protocol: Based on the identified requirements and existing standards, the next step is to develop the protocol for the SDN-based remote management of routers. This may involve defining message formats, protocol procedures, and security mechanisms, as well as specifying the interfaces and APIs used for communication between the SDN controller and the router.
4. Test and validate: Once the protocol has been developed, it is important to test and validate it to ensure that it meets the defined requirements and is interoperable with different router models and SDN controllers. This may involve developing test suites and performing interoperability testing with other vendors.
5. Publish and promote: Once the standard has been developed and validated, it should be published and promoted to encourage adoption by router manufacturers, network operators, and SDN vendors. This may involve working with standards organizations, such as the Open Networking Foundation (ONF), to publish the standard and promote it to the broader networking community.

By following these steps, a standard for SDN-based remote management of routers can be developed, validated, and promoted to help improve the efficiency and security of network management.

1. Establish governance: To ensure the long-term success and evolution of the standard, it is important to establish a governance structure. This includes identifying the stakeholders who will be responsible for managing the standard, developing new features, and resolving any issues that arise.
2. Ensure backward compatibility: As the standard evolves and new features are added, it is important to ensure backward compatibility with earlier versions of the standard. This can help prevent fragmentation of the ecosystem and ensure that the standard remains accessible and widely adopted.
3. Address security concerns: As with any networking protocol, security is a critical concern. The SDN-based remote management protocol should be designed to include robust security mechanisms to prevent unauthorized access and protect against attacks. This may include encryption of communication between the SDN controller and the router, authentication and access control mechanisms, and intrusion detection and prevention capabilities.
4. Consider interoperability with other standards: To promote interoperability and integration with other networking standards and technologies, it may be necessary to consider how the SDN-based remote management protocol can be integrated with other standards such as SNMP, NetFlow, and IPFIX.
5. Encourage feedback and contributions: Finally, it is important to encourage feedback and contributions from the networking community. This can help identify areas for improvement, ensure that the standard remains relevant and useful, and foster innovation in SDN-based remote management of routers.

In summary, developing a standard for SDN-based remote management of routers requires a comprehensive and collaborative approach, involving stakeholders from across the networking community. By following these steps, a standard can be developed that promotes interoperability, security, and innovation in network management, while also addressing the needs and requirements of different organizations and use cases.

1. Ensure scalability: When designing the SDN-based remote management protocol, it is important to ensure that it can scale to support large-scale networks with many routers and SDN controllers. This may involve designing the protocol to be modular, allowing for the efficient distribution of management tasks across multiple SDN controllers.
2. Consider support for different router architectures: To ensure that the SDN-based remote management protocol is widely adopted, it is important to consider support for different router architectures, including both software-based and hardware-based routers. This may involve developing software agents or APIs that can be used to manage hardware-based routers, as well as support for different routing protocols and topologies.
3. Address performance and latency concerns: The SDN-based remote management protocol should be designed to minimize performance and latency concerns, especially when managing large-scale networks with many routers. This may involve optimizing message formats and protocols, minimizing overhead, and ensuring that management tasks are distributed efficiently across SDN controllers.
4. Consider support for network automation: To enable network automation and orchestration, the SDN-based remote management protocol should be designed to support the integration of automation tools and frameworks. This may involve defining APIs or interfaces for automation tools to interact with the SDN controller and router, as well as ensuring that the protocol supports the efficient distribution of management tasks across multiple SDN controllers.
5. Address fault tolerance and recovery: Finally, the SDN-based remote management protocol should be designed to ensure fault tolerance and recovery. This may involve designing the protocol to detect and recover from network failures and other issues, as well as defining mechanisms for restoring network services and data in the event of a failure.

By considering these factors, a standard for SDN-based remote management of routers can be developed that meets the needs of different organizations and use cases, while promoting interoperability, security, scalability, and innovation in network management.

1. Develop testing and certification programs: To ensure that the SDN-based remote management protocol is implemented correctly and consistently across different vendors and products, it may be necessary to develop testing and certification programs. These programs can help ensure that different products and implementations meet the requirements of the standard, and promote interoperability and compatibility between different products.
2. Foster a community of developers and users: To promote adoption and innovation, it is important to foster a community of developers and users around the SDN-based remote management standard. This may involve organizing conferences, meetups, and other events to bring together stakeholders from across the networking community, as well as developing online forums and collaboration tools to facilitate communication and collaboration.
3. Ensure transparency and openness: To promote trust and adoption of the SDN-based remote management standard, it is important to ensure transparency and openness in the development and governance of the standard. This may involve making the standard available under open-source licenses, publishing the standard's design documents and implementation details, and soliciting feedback and contributions from the community.
4. Provide educational resources and training: To promote adoption and understanding of the SDN-based remote management standard, it may be necessary to provide educational resources and training for developers, network administrators, and other stakeholders. This may involve developing documentation, tutorials, and training programs to help users understand and implement the standard, as well as providing support and guidance for developers who are working on implementing the standard in their products.
5. Continuously monitor and improve the standard: Finally, it is important to continuously monitor and improve the SDN-based remote management standard over time. This may involve soliciting feedback and contributions from the community, identifying areas for improvement and new features, and working to ensure that the standard remains relevant and useful in an evolving networking landscape.

By following these steps, a standard for SDN-based remote management of routers can be developed that meets the needs of different organizations and use cases, while promoting interoperability, security, scalability, and innovation in network management.

1. Consider compatibility with existing network infrastructure: When designing the SDN-based remote management protocol, it is important to consider compatibility with existing network infrastructure, including legacy devices and protocols. This may involve developing gateway or translation mechanisms that allow SDN-based management tools to interoperate with legacy devices, or providing support for popular legacy protocols within the SDN-based management framework.
2. Define clear security requirements and protocols: Given the critical role that routers play in network security, it is essential to define clear security requirements and protocols for the SDN-based remote management protocol. This may involve defining secure authentication and authorization mechanisms, encryption and data protection protocols, and other security features to ensure that the SDN-based management tools do not introduce new security vulnerabilities into the network.
3. Consider the impact on network performance: The SDN-based remote management protocol should be designed to minimize any negative impact on network performance, both in terms of latency and bandwidth utilization. This may involve optimizing the protocol for efficient message exchange, minimizing the amount of data transmitted, and providing mechanisms for load balancing and traffic shaping to minimize the impact of management traffic on other network traffic.
4. Provide support for network monitoring and analysis: To enable effective network monitoring and analysis, the SDN-based remote management protocol should provide support for data collection and analysis. This may involve defining APIs or protocols for collecting network performance data, as well as providing support for tools and frameworks for analyzing and visualizing this data.
5. Consider the needs of different stakeholders: When designing the SDN-based remote management protocol, it is important to consider the needs of different stakeholders, including network administrators, developers, and end-users. This may involve developing different interfaces or APIs for different user groups, as well as providing support for customization and extensibility to allow different stakeholders to adapt the protocol to their specific needs.

By considering these factors, a standard for SDN-based remote management of routers can be developed that meets the needs of different organizations and use cases, while promoting interoperability, security, scalability, and innovation in network management. The development of such a standard can help accelerate the adoption of SDN-based management tools, and facilitate the development of more sophisticated and flexible network management solutions in the future.